CONTRATO: CAS-21-2025-AMARCO

CONTRATO **CERRADO** RELATIVO AL "**SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP**", QUE CELEBRAN, POR UNA PARTE, EL COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA, REPRESENTADO POR LA MTRA. KARINA SALAZAR HERNÁNDEZ, EN SU CARÁCTER DE DIRECTORA DE INFRAESTRUCTURA Y ADQUISICIONES, EN ADELANTE "**EL CONALEP**", Y POR LA OTRA, **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.** EN LO SUCESIVO **"EL PRESTADOR DE SERVICIOS"**, REPRESENTADO POR EL C. RUBÉN PLAZA AGUILAR, EN SU CARÁCTER DE APODERADO LEGAL A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ "**LAS PARTES**", AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

DECLARACIONES

1. **"EL CONALEP"** declara que:

I.1 Es un organismo público descentralizado del Estado, con personalidad jurídica y patrimonio propios, creado por decreto presidencial del 27 de diciembre de 1978, publicado en el Diario Oficial de la Federación el 29 del mismo mes y año, cuyo objeto es la impartición de educación profesional técnica, con la finalidad de satisfacer la demanda de personal técnico calificado para el sistema productivo del país, así como educación de bachillerato dentro del tipo medio superior, de conformidad con los diversos que reforman dicho decreto que creó a "**EL CONALEP**" de fecha 22 de noviembre de 1993, publicado en el Diario Oficial de la Federación el 08 de diciembre de 1993, y de fecha 29 de julio de 2011, publicado en el Diario Oficial de la Federación, el 04 de agosto de 2011.

I.2 Conforme a lo dispuesto por el artículo 39 fracción XII del Estatuto Orgánico del Colegio Nacional de Educación Profesional Técnica, en el que se regulan las atribuciones de la **MTRA. KARINA SALAZAR HERNÁNDEZ**, en su carácter de Directora de Infraestructura Y Adquisiciones, con R.F.C. SAHK810729TH1, designada a través de la Junta Directiva del Colegio Nacional de Educación Profesional Técnica en Primera Sesión Extraordinaria de fecha 28 de enero del 2025; nombramiento protocolizado de fecha 1 de febrero del 2025, signado por el **MTRO. RODRIGO ALEJANDRO ROJAS NAVARRETE, DIRECTOR GENERAL** de **"EL CONALEP"**, y de conformidad con lo establecido en el numeral 1.8.1., función 13, del Acuerdo DG-DCAJ05/2021, por el que se actualiza el Manual General de Organización del Colegio Nacional de Educación Profesional Técnica.

I.3 De conformidad con lo dispuesto en el numeral 1.2 del Manual General de Organización del Colegio Nacional de Educación Profesional Técnica, numeral 13 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Colegio Nacional de Educación Profesional Técnica suscribe el presente instrumento el **MTRO. JULIÁN JAVIER ROBLES RIVAS**, en su carácter de **DIRECTOR CORPORATIVO DE TECNOLOGÍAS APLICADAS**, con **R.F.C. RORJ7312163W3**, responsable para administrar y verificar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, en adelante "**ADMINISTRADOR DEL CONTRATO**" quien podrá ser sustituido en cualquier momento en su cargo o funciones, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, dirigido al representante de "**EL PRESTADOR DE SERVICIOS**" para los efectos del presente contrato, encargado del cumplimiento de las obligaciones contraídas en el presente instrumento jurídico.

I.4 La adjudicación del presente contrato se realizó mediante el procedimiento **de Invitación a Cuando Menos Tres Personas** de carácter Nacional y medio electrónico No. IA-11-L5X-011L5X001-N-44-2025, al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 35 fracción II y VI, 36, 39 fracción I, 55, y 56 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, "LAASSP", 14 y 51 de su Reglamento.

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

I.5 Cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, como se desprende de la suficiencia presupuestal número 08058 con folio 00000240, autorizada por la Coordinación de Presupuestos y Finanzas de la Dirección de Administración Financiera bajo la partida presupuestal 31901, de fecha 14 de julio de 2025.

I.6 Se encuentra inscrito en el Registro Federal de Contribuyentes con el alfanumérico **CNE781229BK4**.

I.7 Tiene establecido su domicilio en calle 16 de septiembre No. 147 norte, Col. Lázaro Cárdenas, Metepec, Estado de México, Código Postal 52148 mismo que señala para los fines y efectos legales del presente contrato.

II. "EL PRESTADOR DE SERVICIOS", por conducto de su representante declara que:

II.1 Es una persona moral legalmente constituida bajo las leyes mexicanas, mediante Escritura Pública número 125,134 de fecha 14 de marzo de 2007, otorgada ante la fe del Notario Público Número 129 del Distrito Federal hoy día Ciudad de México, Lic. Ignacio Soto Borja y Anda, e inscrita en el Registro Público de la Propiedad y de Comercio de la Ciudad de México, la Dirección General del Registro Público de Comercio del Distrito Federal hoy Ciudad de México, con folio mercantil 364029, con fecha 09 de mayo de 2007, así como las modificaciones al Acta Constitutiva realizadas a través del instrumento Notarial número 94,522 de fecha 2 de octubre de 2015, otorgada ante la fe del Notario Público Número 19 de la Ciudad de México, Lic. Miguel Alessio Robles, a través de la cual se protocolizo el Acta de la Asamblea General Ordinaria de Accionistas de IP PRODUCTOS Y SERVICIOS S.A. DE C.V. , celebrada el 01 de octubre de 2015, inscrita en el Registro Público de la Propiedad y de Comercio de la Ciudad de México, con folio mercantil 364029, con fecha 14 de octubre de 2015.

II.2 El C. Rubén Plaza Aguilar, en su carácter de Apoderado Legal de " **EL PRESTADOR DE SERVICIOS** " cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada en los términos, lo cual acredita mediante Escritura Pública número 122,872 de fecha 17 de febrero de 2021, otorgada ante la fe del Notario Público Número 56, de la Ciudad de México, Lic. Eduardo A. Martínez Urquidi, mismo que bajo protesta de decir verdad manifiesta que no le han sido limitado ni revocado en forma alguna.

II.3 El C. Rubén Plaza Aguilar, se identifica con Credencial para Votar vigente, expedida por el Instituto Nacional Electoral.

II.4 Conforme a su objeto social se dedica, entre otros a la planeación, al diseño, fabricación, compra, venta, importación, exportación, instalación, distribución, representación, peritaje, asesoría, mantenimiento y comercio en general de equipos eléctricos, electrónicos, mecánicos, de telecomunicaciones, de cómputo y los anexos y conexos a los mismos.

II.5 Reúne las condiciones técnicas, jurídicas y económicas, y cuenta con la organización y elementos necesarios para su cumplimiento.

II.6 Su representada poderdante se encuentra inscrita en el Registro Federal de Contribuyentes expedido por la Secretaria de Hacienda y Crédito Público con el alfanumérico **IPS0703142W1.**

II.7 Tiene capacidad jurídica para contratar y reúne las condiciones legales, técnicas y económicas necesarias para obligarse a la entrega de los servicios, objeto de este contrato.

II.8 Acredita el cumplimiento de sus obligaciones fiscales en términos de lo dispuesto en el artículo 32-D del Código Fiscal de la Federación vigente, incluyendo las de Aportaciones Patronales y Entero de Descuentos,

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y las de Seguridad Social ante el Instituto Mexicano del Seguro Social, conforme a las Opiniones de Cumplimiento de Obligaciones Fiscales emitidas por el SAT, INFONAVIT e IMSS, respectivamente.

II.9 Para los efectos derivados de este instrumento señala como su domicilio legal y fiscal el ubicado en calle **MONTECITO, NÚMERO 38, PISO 6 OFICINA 16, COLONIA NÁPOLES, BENITO JUÁREZ, CIUDAD DE MÉXICO, C.P. 03810** mismo que señala para los fines y efectos legales del presente contrato..

II.10 Bajo protesta de decir verdad, manifiesta que a la fecha no se encuentra inhabilitado por autoridad, dependencia o entidad alguna para formular propuestas o para la celebración del presente instrumento, en virtud de no encontrarse en los supuestos previstos en el artículo 71 y 90 de la "LAASSP".

II.11 Conoce el contenido de la **"LAASSP"** y su Reglamento, la publicación y alcance de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Colegio Nacional de Educación Profesional Técnica; y reconoce la facultad de la Dirección de Infraestructura y Adquisiciones para la aplicación de penas convencionales

III. De "LAS PARTES":

III.1 Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, por lo que de común acuerdo se obligan de conformidad con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

"EL PRESTADOR DE SERVICIOS" acepta y se obliga a proporcionar a **"EL CONALEP"** la prestación **del SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP**, en los términos y condiciones establecidos en la **INVITACIÓN**, el presente contrato y sus anexos **(ANEXO A Y ANEXO B)** que forman parte integrante del mismo.

SEGUNDA. MONTO DEL CONTRATO

"EL CONALEP" pagará a **"EL PRESTADOR DE SERVICIOS"** como contraprestación por los servicios objeto de este contrato, la cantidad **de $864,740.86 (OCHOCIENTOS SESENTA Y CUATRO MIL SETECIENTOS CUARENTA PESOS 86/100 M.N.),** sin incluir IVA.

El precio unitario es considerado fijo y en moneda nacional PESO MEXICANO hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en la prestación del servicio, por lo que "**EL PRESTADOR DE SERVICIOS**", no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

TERCERA. ANTICIPO.

Para el presente contrato **"EL CONALEP"** no otorgará anticipo a **"EL PRESTADOR DE SERVICIOS"**

CUARTA. FORMA Y LUGAR DE PAGO.

El pago se realizará en moneda nacional (pesos mexicanos), a mes vencido por partida completa, una vez entregado a entera satisfacción de "**EL CONALEP",** previa revisión y validación del cumplimiento por parte del Titular de la Dirección Corporativa de Tecnologías Aplicadas, quien es el Administrador del Contrato, en un plazo

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

no mayor a 17 días hábiles posteriores a la presentación del CFDI "Comprobante Fiscal Digital a través de Internet correspondiente, la cual deberá contener todos los requisitos fiscales vigentes, de conformidad con lo establecido en el Artículo 73 de la LAASSP, siempre y cuando reúna todos los requisitos establecidos por el Código Fiscal de la Federación y esté debidamente requisitada.

En caso de que la prestación del arrendamiento no sea por el mes completo que se trate, únicamente se pagará los días que efectivamente se recibió el arrendamiento a satisfacción de **"EL CONALEP"**, para estos casos los meses se entenderán siempre de 30 días.

Lo anterior, quedará condicionado proporcionalmente al pago que **"EL PRESTADOR DE SERVICIOS"** deba efectuar por concepto de penas convencionales o deducciones con motivo del incumplimiento parcial o total al mes correspondiente, en que pudiera incurrir respecto a la prestación del servicio.

Para el presente queda especificado que el pago por la prestación del servicio comenzará a correr a partir del siguiente día hábil de que el servicio quede debidamente configurado y en operación, a entera satisfacción "**EL CONALEP**", previa revisión y validación del Titular de la Unidad Administrativa requirente del servicio.

En caso de que la prestación del servicio no sea por el mes completo que se trate, únicamente se pagará los días que efectivamente se recibió el servicio a satisfacción, para estos casos los meses se entenderán siempre de 30 días. Lo anterior, quedará condicionado proporcionalmente al pago que el licitante adjudicado deba efectuar por concepto de penas convencionales o deducciones con motivo del incumplimiento parcial o total al mes correspondiente, en que pudiera incurrir respecto a la prestación del servicio.

De acuerdo con las disposiciones fiscales, el **"EL PRESTADOR DE SERVICIOS"** deberá enviar el archivo PDF y .XML de cada CFDI, dentro de los primeros 5 días hábiles posteriores al mes en el que se proporcionó el servicio, al correo electrónico javier.robles@conalep.edu.mx; y mamarquez@conalep.edu.mx.

El CFDI deberá expedirse a nombre del CONALEP con R.F.C. CNE-781229-BK4, domicilio fiscal, Calle 16 de septiembre No. 147 Norte, Colonia Lázaro Cárdenas, Metepec, Estado de México, C.P. 52148.

El cómputo del plazo para realizar el pago se contabilizará a partir del día hábil siguiente de la aceptación del CFDI o factura electrónica, y ésta reúna los requisitos fiscales que establece la legislación en la materia, el desglose de los servicios prestados, los precios unitarios, se verifique su autenticidad, no existan aclaraciones al importe y vaya acompañada con la documentación soporte de la prestación de los servicios facturados.

De conformidad con el artículo 90, del Reglamento de la **"LAASSP"**, en caso de que el CFDI o factura electrónica entregado presente errores, el Administrador del presente contrato o a quien éste designe por escrito, dentro de los 3 (tres) días hábiles siguientes de su recepción, indicará a **"EL PRESTADOR DE SERVICIOS"** las deficiencias que deberá corregir; por lo que, el procedimiento de pago reiniciará en el momento en que **"EL PRESTADOR DE SERVICIOS"** presente el CFDI y/o documentos soporte corregidos y sean aceptados.

El tiempo que **"EL PRESTADOR DE SERVICIOS"** utilice para la corrección del CFDI y/o d"ocumentación soporte entregada, no se computará para efectos de pago, de acuerdo con lo establecido en el artículo 73 de la **"LAASSP"**.

El CFDI o factura electrónica se deberá presentar desglosando el impuesto cuando aplique.

"EL PRESTADOR DE SERVICIOS" manifiesta su conformidad que, hasta en tanto no se cumpla con la verificación, supervisión y aceptación de la prestación de los servicios, no se tendrán como recibidos o aceptados por el Administrador del presente contrato.

Para efectos de trámite de pago, **"EL PRESTADOR DE SERVICIOS"** deberá ser titular de una cuenta bancaria, en la que se efectuará la transferencia electrónica de pago, respecto de la cual deberá proporcionar toda la información y documentación que le sea requerida por **"EL CONALEP"**, para efectos del pago.

"EL PRESTADOR DE SERVICIOS" deberá presentar la información y documentación que **"EL CONALEP"** le solicite para el trámite de pago, atendiendo a las disposiciones legales e internas de **"EL CONALEP"**.

El pago de la prestación de los servicios recibidos, quedará condicionado al pago que **"EL PRESTADOR DE SERVICIOS"** deba efectuar por concepto de penas convencionales y, en su caso, deductivas.

Para el caso de que se presenten pagos en exceso "**EL PRESTADOR DE SERVICIOS**" deberá reintegrar las cantidades pagadas en exceso, más los intereses correspondientes, conforme lo señalado en el segundo párrafo del artículo 73 de la "LAASSP", a más tardar dentro de los treinta días naturales siguientes a que le sea requerido el pago.

Los intereses se calcularán sobre las cantidades pagadas en exceso en cada caso y se computarán por días naturales desde la fecha del pago, hasta la fecha en que se pongan efectivamente las cantidades a disposición de la dependencia o entidad (artículo 73, párrafo tercero, de la "LAASSP").

QUINTA. LUGAR, PLAZOS Y CONDICIONES DE LA PRESTACIÓN DE LOS SERVICIOS.

Lugar: **"EL PRESTADOR DE SERVICIOS"** deberá prestar el "SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP", con base a lo establecido en el Anexo A.

Tiempo: Del 30 de agosto 2025 hasta el 31 de diciembre de 2025.

SEXTA. VIGENCIA

"LAS PARTES" convienen en que la vigencia del presente contrato será del 30 de agosto al 31 de diciembre de 2025

SÉPTIMA. MODIFICACIONES DEL CONTRATO.

"LAS PARTES" están de acuerdo que **"EL CONALEP"** por razones fundadas y explícitas podrá ampliar el monto o la cantidad de los servicios, de conformidad con el artículo 74 de la "LAASSP", siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) de los establecidos originalmente, el precio unitario sea igual al originalmente pactado y el contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

"EL CONALEP", podrá ampliar la vigencia del presente instrumento, siempre y cuando, no implique incremento del monto contratado o de la cantidad de los servicios solicitados, siendo necesario que se obtenga el previo consentimiento de **"EL PRESTADOR DE SERVICIOS"**.

De presentarse caso fortuito o fuerza mayor, o por causas atribuibles a **"EL CONALEP"**, se podrá modificar el plazo del presente instrumento jurídico, debiendo acreditar dichos supuestos con las constancias respectivas. La modificación del plazo por caso fortuito o fuerza mayor podrá ser solicitada por cualquiera de **"LAS PARTES".**

En los supuestos previstos en el párrafo anterior, no procederá la aplicación de penas convencionales por atraso.

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

Cualquier modificación al presente contrato deberá formalizarse a través de la Plataforma, por el servidor público de **"EL CONALEP"** que lo haya hecho, o quien lo sustituya o esté facultado para ello, para lo cual **"EL PRESTADOR DE SERVICIOS"** realizará el ajuste respectivo de la garantía de cumplimiento, en términos del artículo 91, último párrafo del Reglamento de la **"LAASSP"**, salvo que por disposición legal se encuentre exceptuado de presentar garantía de cumplimiento.

"EL CONALEP" se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos, especificaciones y, en general, cualquier cambio que implique otorgar condiciones más ventajosas a un proveedor comparadas con las establecidas originalmente.

OCTAVA. GARANTÍA DE LOS SERVICIOS

"**EL PRESTADOR DE SERVICIOS**", se obliga con "**EL CONALEP**" a entregar al inicio de la prestación del servicio, una garantía por la calidad de estos, durante la vigencia del presente contrato más un periodo de **90 DÍAS NATURALES**, la cual se constituirá mediante carta de vicios ocultos en hoja membretada suscrito por "**EL PRESTADOR DE SERVICIOS**".

NOVENA. GARANTÍA(S)

A) CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 69, fracción II, 70, fracción I (dependencias) o II (entidades), de la "LAASSP"; 85, fracción III, y 103 de su Reglamento "**EL PRESTADOR DE SERVICIOS**" se obliga a constituir una garantía **indivisible** por el
cumplimiento fiel y exacto de todas las obligaciones derivadas de este contrato, mediante fianza expedida por compañía afianzadora mexicana autorizada por la Comisión Nacional de Seguros y de Fianzas, a favor del COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA por un importe equivalente al 10% del monto del contrato, sin incluir el IVA.

Dicha fianza deberá ser entregada a **"EL CONALEP"**, a más tardar dentro de los 10 días naturales posteriores a la firma del presente contrato.

Si las disposiciones jurídicas aplicables lo permiten, la entrega de la garantía de cumplimiento se podrá realizar de manera electrónica.

En caso de que **"EL PRESTADOR DE SERVICIOS"** incumpla con la entrega de la garantía en el plazo establecido, **"EL CONALEP"** podrá rescindir el contrato y dará vista al Órgano Interno de Control para que proceda en el ámbito de sus facultades.

La garantía de cumplimiento no será considerada como una limitante de responsabilidad de **"EL PRESTADOR DE SERVICIOS"**, derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y no impedirá que **"EL CONALEP"** reclame la indemnización por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, **"EL PRESTADOR DE SERVICIOS"** se obliga a entregar a **"EL CONALEP",** dentro de los 10 (diez días) naturales siguientes a la formalización del mismo, de conformidad con el último párrafo del artículo 91, del Reglamento de la **"LAASSP"**, los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

Cuando la contratación abarque más de un ejercicio fiscal, la garantía de cumplimiento del contrato, podrá ser por el porcentaje que corresponda del monto total por erogar en el ejercicio fiscal de que se trate, y deberá ser renovada por **"EL PRESTADOR DE SERVICIOS"** cada ejercicio fiscal por el monto que se ejercerá en el mismo, la cual deberá presentarse a **"EL CONALEP"** a más tardar dentro de los primeros diez días naturales del ejercicio fiscal que corresponda.
Una vez cumplidas las obligaciones a satisfacción, el Administrador del contrato, procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales y dará inicio a los trámites para la cancelación de la garantía cumplimiento del contrato, lo que comunicará a **"EL PRESTADOR DE SERVICIOS".**

B) GARANTÍA PARA RESPONDER POR VICIOS OCULTOS.

"EL PRESTADOR DE SERVICIOS" deberá responder por los defectos, vicios ocultos y por la calidad de los servicios prestados, así como de cualquier otra responsabilidad en que hubiere incurrido, en los términos señalados en este contrato, convenios modificatorios respectivos y en la legislación aplicable, de conformidad con los artículos 75, párrafo segundo de la **"LAASSP"** y 96, párrafo segundo de su Reglamento.

"EL PRESTADOR DE SERVICIOS", quedará liberado de su obligación, una vez transcurridos la vigencia del presente contrato más un periodo de 90 DÍAS NATURALES, contados a partir de la fecha en que conste por escrito la recepción física de los servicios prestados, siempre y cuando **"EL CONALEP"** no haya identificado defectos o vicios ocultos en la calidad de los servicios prestados, así como cualquier otra responsabilidad en los términos de este contrato y convenios modificatorios respectivos.

DÉCIMA. OBLIGACIONES DE "EL PRESTADOR DE SERVICIOS".

"EL PRESTADOR DE SERVICIOS", se obliga a:

- **a)** Prestar los servicios en las fechas o plazos y lugares establecidos conforme a lo pactado en el presente contrato y anexos respectivos.
- **b)** Cumplir con las especificaciones técnicas, de calidad y demás condiciones establecidas en el presente contrato y sus respectivos anexos.
- **c)** Asumir la responsabilidad de cualquier daño que llegue a ocasionar a **"EL CONALEP"** o a terceros con motivo de la ejecución y cumplimiento del presente contrato.
- **d)** Proporcionar la información que le sea requerida por la Secretaría Anticorrupción y Buen Gobierno y el Órgano Interno de Control, de conformidad con el artículo 107 del Reglamento de la **"LAASSP"**.
- **e)** Mantener al corriente sus obligaciones fiscales durante la vigencia del presente contrato
- **f)** Entregar bimestralmente, las constancias de cumplimiento de la inscripción y pago de cuotas al Instituto Mexicano del Seguro Social del personal que utilice para la prestación de los servicios, únicamente será obligatorio para efectos del artículo 80, párrafo cuarto de del RLAASSP, en el caso de prestación de servicios que requieran del uso intensivo de mano de obra, y ésta aplique un costo superior al treinta por ciento del monto total del contrato.
- **g)** Notificar por escrito a "**EL CONALEP**" el cambio de domicilio legal, convencional y/o fiscal durante la vigencia del contrato y hasta por un año posterior al vencimiento del mismo.
- **h)** Reponer y realizar los servicios que no cumplan con las especificaciones establecidas en el contrato y en sus Anexos, bajo su responsabilidad y sin costo adicional para "EL CONALEP".

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

DÉCIMA PRIMERA. OBLIGACIONES DE "EL CONALEP"

"EL CONALEP", se obliga a:

a) Otorgar las facilidades necesarias, a efecto de que **"EL PRESTADOR DE SERVICIOS"** lleve a cabo en los términos convenidos la prestación de los servicios objeto del contrato.

b) Realizar el pago correspondiente en tiempo y forma.

c) Extender a **"EL PRESTADOR DE SERVICIOS",** por conducto del servidor público facultado, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

DÉCIMA SEGUNDA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DE LOS SERVICIOS

El Administrador del presente contrato el **MTRO. JULIÁN JAVIER ROBLES RIVAS**, en su carácter de **DIRECTOR CORPORATIVO DE TECNOLOGÍAS APLICADAS**, con R.F.C. **RORJ7312163W3**, es el responsable de administrar y verificar que el servicio cumpla con las especificaciones solicitadas en el Anexo A y demás condiciones establecidas en el contrato, siendo el único facultado para solicitar a la Titular de la Dirección de Infraestructura y Adquisiciones las penalizaciones, deductivas y liberaciones de pago que correspondan, auxiliado por el personal que designe por escrito para vigilar, supervisar, controlar e informar que los servicios se ejecuten.

Los servicios se tendrán por recibidos previa revisión del Administrador del presente contrato, la cual consistirá en la verificación del cumplimiento de las especificaciones establecidas y en su caso en los anexos respectivos, así como las contenidas en la propuesta técnica.

"EL CONALEP", a través del Administrador del contrato, rechazará los servicios, que no cumplan las especificaciones establecidas en este contrato y en sus Anexos, obligándose **"EL PRESTADOR DE SERVICIOS"** en este supuesto a realizarlos nuevamente bajo su responsabilidad y sin costo adicional para **"EL CONALEP",** sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondiente.

"EL CONALEP", a través del Administrador del contrato, podrá aceptar los servicios que incumplan de manera parcial o deficiente las especificaciones establecidas en este contrato y en los anexos respectivos, sin perjuicio de la aplicación de las deducciones al pago que procedan, y reposición del servicio, cuando la naturaleza propia de éstos lo permita.

DÉCIMA TERCERA. DEDUCCIONES

De conformidad con el artículo 76 de la LAASSP y 97 de su Reglamento, "**EL CONALEP**" aplicará por incumplimiento parcial o deficiente en la prestación de los servicios, conforme a lo siguiente:

- Se aplicará una deductiva al oferente por el cumplimiento parcial o deficiente en el arrendamiento. Dicha deductiva será del 2% sobre el monto de la facturación del mes inmediato anterior correspondiente al equipo que no sea sustituido o reparado en los términos y plazos establecidos en el presente anexo por cada día natural de atraso.

- Igual porcentaje, se aplicará como deductiva en los casos que el oferente suspenda el arrendamiento por cualquier causa injustificada, esto es fuera de los casos de fuerza mayor o caso fortuito debidamente acreditado y documentado, por cada día natural que suspenda el arrendamiento, independientemente de

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

que no se pagaría arrendamiento por el tiempo que dure la suspensión.

- Adicional a lo anterior, se aplicarán deductivas por cada día natural de incumplimiento en los tiempos de atención y solución de fallas o la petición de la reasignación o reubicación de equipos, así como en los niveles de atención señalados en el apartado "Niveles de atención" del Anexo A.

En caso de que los conceptos en los que subsistan el cumplimiento parcial o la deficiencia sean equivalentes al importe de la garantía otorgada por el prestador del servicio adjudicado, el Administrador del Contrato podrá optar por cancelar total o parcialmente el servicio aplicando la pena convencional máxima al licitante, lo anterior, en términos del artículo 100 del Reglamento de la Ley antes citada, o bien, optar por rescindir el contrato en término de la Ley.

Para efectos de lo establecido en el párrafo anterior, el prestador del servicio adjudicado deberá entregar las notas de crédito que correspondan debidamente requisitadas.

En caso de reincidencia en alguna de estas deducciones y/o penalizaciones, se podrá iniciar el procedimiento de rescisión administrativa, de conformidad con lo establecido en el Artículo 77 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el Artículo 98 de su Reglamento.

Se aplicarán por los daños y perjuicios generados a EL CONALEP y a sus servidores públicos por el prestador del servicio adjudicado, causados por negligencia y/u omisión en el cumplimiento de las obligaciones establecidas en el Contrato y sus Anexos, por lo que se aplicará una pena equivalente a los daños y perjuicios generados por las omisiones o actos negligentes de el prestador del servicio adjudicado.

Las penas convencionales, deducciones y penas contractuales, serán calculadas y comunicadas por la titularidad de la Dirección de Infraestructura y Adquisiciones del CONALEP.

La suma de todas las penas y deductivas aplicadas no deberá exceder del monto de la garantía de cumplimiento del Contrato y se determinará en función de los Servicios no proporcionados o la calidad de éstos.

En el supuesto que el incumplimiento de el prestador del servicio adjudicado rebase la fecha límite máxima para que proporcione los servicios, por haber agotado el monto de la Garantía de Cumplimiento del Contrato, "EL CONALEP" podrá iniciar el procedimiento de rescisión administrativa, de conformidad con lo previsto en el artículo 77 de la LAASSP y 98 de su Reglamento, lo cual no limita que el procedimiento de rescisión se pueda iniciar en cualquier momento.

De no existir pagos pendientes, se requerirá a **"EL PRESTADOR DE SERVICIOS"** que realice el pago de la deductiva a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor del Colegio Nacional de Educación Profesional Técnica. En caso de negativa se procederá a hacer efectiva la garantía de cumplimiento del contrato.

Las deducciones económicas se aplicarán sobre la cantidad indicada sin incluir impuestos.

DÉCIMA CUARTA. PENAS CONVENCIONALES

De conformidad con el Artículo 75 de la LAASSP y 96 de su Reglamento, "**EL CONALEP**" aplicará con motivo de incumplimiento en la entrega del servicio, las penas convencionales de acuerdo con lo siguiente:

En el arrendamiento:

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

- "**EL PRESTADOR DE SERVICIOS**" se obliga a pagar a "**EL CONALEP**" una pena convencional del 2% sobre el monto mensual del pago previsto para los equipos no entregados, instalados, configurados y puestos en marcha, en un plazo no mayor a 90 días naturales a partir del día hábil siguiente a la fecha de adjudicación del contrato, entregado a través de acta administrativa levantada para ello, suscrita por el Titular de la Dirección Corporativa de Tecnologías Aplicadas, quien funge como Administrador del Contrato, debidamente firmada por el oferente adjudicado y los testigos respectivos, por cada día natural de atraso.

- La misma pena se aplicará por cada día natural de atraso, en el caso de que el oferente adjudicado no proporcione la mesa de ayuda dentro del plazo establecido de 5 días hábiles anteriores a la fecha del inicio del Arrendamiento, verificando que la mesa permita la solicitud de soporte y asistencia técnica para la atención, diagnóstico y solución de fallas y orientación de uso de los equipos de Telefonía IP, para lo cual el oferente deberá proporcionar números convencionales y celulares, además de correos electrónicos del representante por el designado.

El total de la pena convencional no podrá exceder el monto de la garantía de cumplimiento sin considerar el impuesto al valor agregado (I.V.A.).

En los entregables:

- El licitante adjudicado se obliga a pagar al CONALEP una pena convencional por no presentar los entregables mensuales en los plazos establecidos en el apartado "Entregables" del Anexo A. "Descripción Técnica del Arrendamiento". Dicha pena será del 2% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso.

El importe de las penas convencionales, no podrán exceder del monto de la garantía de cumplimiento del contrato, en el caso de exceptuarse la presentación de la garantía, el monto máximo de las penas convencionales y/o deductivas por atraso será del veinte por ciento del monto de los bienes, arrendamientos o servicios entregados o prestados fuera del plazo convenido, lo anterior en términos del artículo 75 de la LAASSP y 96 del reglamento.

En caso de que subsista el incumplimiento, ya sea parcial o total, y/o rebase la fecha límite máxima para la prestación del servicio, por haber agotado el monto de la Garantía de Cumplimiento del Contrato, el administrador del contrato podrá optar por cancelar total o parcialmente el servicio aplicando la pena convencional máxima al "**EL PRESTADOR DE SERVICIOS**", lo anterior, en términos del artículo 100 del Reglamento de la LAASSP, o bien, podrá iniciar el procedimiento de rescisión administrativa, de conformidad con lo previsto en el artículo 77 de la LAASSP, lo cual no limita que el procedimiento de rescisión se pueda iniciar en cualquier momento.

Las penas convencionales por atraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio o cumplimiento de obligaciones, que se aplicarán a el prestador del servicio adjudicado, serán de acuerdo con lo establecido en el artículo 75 de la "LAASSP" y 96 de su Reglamento

El pago de los servicios quedará condicionado, proporcionalmente, al pago que **"EL PRESTADOR DE SERVICIOS"** deba efectuar por concepto de penas convencionales por atraso; en el supuesto que el contrato sea rescindido en términos de lo previsto en la **CLÁUSULA VIGÉSIMA CUARTA DE RESCISIÓN**, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

El pago de la pena podrá efectuarse a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor del Colegio Nacional de Educación Profesional Técnica; o bien, a través de un

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

comprobante de egreso (CFDI de Egreso) conocido comúnmente como Nota de Crédito, en el momento en el que emita el comprobante de Ingreso (Factura o CFDI de Ingreso) por concepto de los servicios, en términos de las disposiciones jurídicas aplicables.

DÉCIMA QUINTA. LICENCIAS, AUTORIZACIONES Y PERMISOS

"EL PRESTADOR DE SERVICIOS" se obliga a observar y mantener vigentes las licencias, autorizaciones, permisos o registros requeridos para el cumplimiento de sus obligaciones.

DÉCIMA SEXTA. PÓLIZA DE RESPONSABILIDAD CIVIL

Para la prestación de los servicios materia del presente contrato, no se requiere que **"EL PRESTADOR DE SERVICIOS"** contrate una póliza de seguro por responsabilidad civil.

DÉCIMA SÉPTIMA. TRANSPORTE

"EL PRESTADOR DE SERVICIOS" se obliga bajo su costa y riesgo, a trasportar los bienes e insumos necesarios para la prestación del servicio objeto de este contrato, desde su lugar de origen, hasta las instalaciones señaladas en el **(ANEXO A)** del presente contrato.

DÉCIMA OCTAVA. IMPUESTOS Y DERECHOS

"EL CONALEP" y "EL PRESTADOR DE SERVICIOS", serán responsables individualmente del cumplimiento de sus respectivas obligaciones fiscales, así como del entero y pago de los impuestos y demás contribuciones causadas en virtud del contrato que se formalice, en los términos de las leyes aplicables, por lo que, ni **"EL CONALEP"** y **"EL PRESTADOR DE SERVICIOS"**, serán considerados como obligados solidarios en lo que se refiere a dichas obligaciones de carácter fiscal.

Es obligación de "**EL PRESTADOR DE SERVICIOS**", pagar y enterar por concepto de contribuciones en materia del Impuesto Sobre Nómina (ISN) o Impuesto Sobre Erogaciones por Remuneraciones al Trabajo Personal (ISERTP) del personal que preste sus servicios en la entidad correspondiente, de acuerdo con la normatividad vigente, lo cual deberá acreditar a "**EL CONALEP**" cuando así lo requiera.

"**EL CONALEP**" se reserva el derecho de enterar a la Hacienda del Estado cuando la autoridad lo solicite.

"EL CONALEP", únicamente pagará el Impuesto al Valor Agregado de conformidad con las disposiciones fiscales vigentes, por lo que todos los demás impuestos, derechos y gastos que se generen correrán por cuenta de "**EL PRESTADOR DE SERVICIOS**", asimismo, para el pago de dicho impuesto se aplicará lo correspondiente a la normatividad vigente de la Ley del Impuesto al Valor Agregado.

DÉCIMA NOVENA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES

"EL PRESTADOR DE SERVICIOS" no podrá ceder total o parcialmente los derechos y obligaciones derivados del presente contrato, a favor de cualquier otra persona física o moral, con excepción de los derechos de cobro, en cuyo caso se deberá contar con la conformidad previa y por escrito de **"EL CONALEP"**.

Se exceptúa de lo anterior en el caso de fusión, escisión, o transformación de sociedades, siempre que la nueva sociedad que resulte cuente con la solvencia técnica, jurídica y económica exigidas al adjudicarse el contrato,

cumpla con lo dispuesto en el Reglamento de la **"LAASSP"** y no se encuentre en los supuestos de impedimento previstos en la **"LAASSP"**.

VIGÉSIMA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS

"EL PRESTADOR DE SERVICIOS" será responsable en caso de infringir patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional e internacional, con motivo del cumplimiento de las obligaciones del presente contrato, por lo que se obliga a responder personal e ilimitadamente de los daños y perjuicios que pudiera causar a **"EL CONALEP"** o a terceros.

De presentarse alguna reclamación en contra de **"EL CONALEP"**, por cualquiera de las causas antes mencionadas, **"EL PRESTADOR DE SERVICIOS"**, se obliga a salvaguardar los derechos e intereses de **"EL CONALEP"** de cualquier controversia, liberándola de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole, sacándola en paz y a salvo.

En caso de que **"EL CONALEP"** tuviese que erogar recursos por cualquiera de estos conceptos, **"EL PRESTADOR DE SERVICIOS"** se obliga a reembolsar de manera inmediata los recursos erogados por aquella.

VIGÉSIMA PRIMERA. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES.

"LAS PARTES" acuerdan que la información que se intercambie de conformidad con las disposiciones del presente instrumento, se tratará de manera confidencial, siendo de uso exclusivo para la consecución del objeto del presente contrato y no podrá difundirse a terceros de conformidad con lo establecido en la Ley General de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en posesión de Sujetos Obligados, y demás legislación aplicable.

Para el tratamiento de los datos personales que **"LAS PARTES"** recaben con motivo de la celebración del presente contrato, deberá de realizarse con base en lo previsto en los Avisos de Privacidad respectivos.

Por tal motivo, **"EL PRESTADOR DE SERVICIOS"** asume cualquier responsabilidad que se derive del incumplimiento de su parte, o de sus empleados, a las obligaciones de confidencialidad descritas en el presente contrato.

Asimismo **"EL PRESTADOR DE SERVICIOS"** deberá observar lo establecido en el Anexo aplicable a la Confidencialidad de la información del presente contrato.

VIGÉSIMA SEGUNDA. SUSPENSIÓN TEMPORAL DE LA PRESTACIÓN DE LOS SERVICIOS.

Con fundamento en el artículo 80 de la **"LAASSP"** y 102, fracción II, de su Reglamento, **"EL CONALEP"** en el supuesto de caso fortuito o de fuerza mayor o por causas que le resulten imputables, podrá suspender la prestación de los servicios, de manera temporal, quedando obligado a pagar a **"EL PRESTADOR DE SERVICIOS"**, aquellos servicios que hubiesen sido efectivamente prestados, y en su caso, se reintegrarán los anticipos no amortizados, así como, al pago de gastos no recuperables previa solicitud y acreditamiento.

Una vez que hayan desaparecido las causas que motivaron la suspensión, el contrato podrá continuar produciendo todos sus efectos legales, si **"EL CONALEP"** así lo determina; y en caso que subsistan los supuestos que dieron origen a la suspensión, se podrá iniciar la terminación anticipada del contrato, conforme lo dispuesto en la cláusula siguiente.

VIGÉSIMA TERCERA. TERMINACIÓN ANTICIPADA DEL CONTRATO

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

"EL CONALEP" cuando concurran razones de interés general, de común acuerdo o bien, cuando por causas justificadas se extinga la necesidad de requerir los servicios originalmente contratados y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a **"EL CONALEP"**, o se determine la nulidad de los actos que dieron origen al presente contrato, con motivo de la resolución de una inconformidad o intervención de oficio, emitida por la Secretaría Anticorrupción y Buen Gobierno, podrá dar por terminado anticipadamente el presente contrato sin responsabilidad alguna para **"EL CONALEP"**, ello con independencia de lo establecido en la cláusula que antecede.

Cuando **"EL CONALEP"** determine dar por terminado anticipadamente el contrato, lo notificará a **"EL PRESTADOR DE SERVICIOS"** hasta con 30 (treinta) días naturales anteriores al hecho, debiendo sustentarlo en un dictamen que precise las razones o las causas justificadas que le dieron origen a la misma, una vez notificada la terminación anticipada, se extinguirá el contrato, lo que dará lugar a formalizar el finiquito entre las partes.

En el finiquito se harán constar los pagos que, en su caso, deba efectuar "**EL CONALEP**" por concepto de los servicios prestados hasta el momento de la terminación anticipada, además, en su caso, pactará en el mismo el reembolso a "**EL PRESTADOR DE SERVICIOS"** de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato.

VIGÉSIMA CUARTA. RESCISIÓN

"EL CONALEP" podrá iniciar en cualquier momento el procedimiento de rescisión, cuando **"EL PRESTADOR DE SERVICIOS"** incurra en alguna de las siguientes causales:

a) Contravenir los términos pactados para la prestación de los servicios, establecidos en el presente contrato;
b) Transferir en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;
c) Ceder los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de **"EL CONALEP"**;
d) Suspender total o parcialmente y sin causa justificada la prestación de los servicios del presente contrato;
e) No realizar la prestación de los servicios en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos;
f) No proporcionar a los Órganos de Fiscalización, la información que le sea requerida con motivo de las auditorías, visitas e inspecciones que realicen;
g) Ser declarado en concurso mercantil, o por cualquier otra causa distinta o análoga que afecte su patrimonio;
h) En caso de que compruebe la falsedad de alguna manifestación, información o documentación proporcionada para efecto del presente contrato;
i) No entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;
j) Cuando la suma de las penas convencionales exceda el monto total de la garantía de cumplimiento del contrato;
k) Cuando la suma de las deducciones al pago, excedan el límite máximo establecido para las deducciones;
l) Divulgar, transferir o utilizar la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de **"EL CONALEP"** en los términos de lo dispuesto en la **CLÁUSULA VIGÉSIMA PRIMERA DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES** del presente instrumento jurídico;
m) Impedir el desempeño normal de labores de **"EL CONALEP";**
n) Cambiar su nacionalidad por otra e invocar la protección de su gobierno contra reclamaciones y órdenes de **"EL CONALEP"**, cuando sea extranjero, y

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

o) No presentar la opinión favorable de sus obligaciones fiscales, con una vigencia no mayor a 30 días a la firma del contrato, y
p) Incumplir cualquier obligación distinta de las anteriores y derivadas del presente contrato.
q) Cuando no notifique por escrito a "EL CONALEP" el cambio de domicilio legal, convencional y/o fiscal durante la vigencia del contrato y hasta por un año posterior al vencimiento del mismo.
r) No reponer los servicios que no cumplan con las especificaciones establecidas en el contrato y en sus Anexos, bajo su responsabilidad y sin costo adicional para "EL CONALEP".

"**EL CONALEP"** de conformidad con lo dispuesto en los artículos 77 de la "LAASSP" y 98 segundo párrafo del Reglamento podrá rescindir administrativamente sin declaración judicial.

Para el caso de optar por la rescisión del contrato, **"EL CONALEP"** comunicará por escrito a **"EL PRESTADOR DE SERVICIOS"** el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles contados a partir del día siguiente de la notificación, exponga lo que a su derecho convenga y aporte en su caso las pruebas que estime pertinentes.

Transcurrido dicho término **"EL CONALEP"**, en un plazo de 10 (diez) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho valer **"EL PRESTADOR DE SERVICIOS"**, determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará a **"EL PRESTADOR DE SERVICIOS"** dicha determinación dentro del citado plazo.

Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"EL CONALEP"** por concepto del contrato hasta el momento de rescisión, o los que resulten a cargo de **"EL PRESTADOR DE SERVICIOS".**

Iniciado un procedimiento de conciliación **"EL CONALEP"** podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato se realiza la prestación de los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de **"EL CONALEP"** de que continúa vigente la necesidad de la prestación de los servicios, aplicando, en su caso, las penas convencionales correspondientes.

"EL CONALEP" podrá determinar no dar por rescindido el contrato, cuando durante el procedimiento advierta que la rescisión del mismo pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, **"EL CONALEP"** elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no rescindirse el contrato, **"EL CONALEP"** establecerá con **"EL PRESTADOR DE SERVICIOS"**, otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento, aplicando las sanciones correspondientes. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 74 de la **"LAASSP"**.

No obstante, de que se hubiere firmado el convenio modificatorio a que se refiere el párrafo anterior, si se presenta de nueva cuenta el incumplimiento, **"EL CONALEP"** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, o rescindirlo, aplicando las sanciones que procedan.

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

Si se llevara a cabo la rescisión del contrato, y en el caso de que a **"EL PRESTADOR DE SERVICIOS"** se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el artículo 73, párrafo cuarto, de la **"LAASSP"**.

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"EL CONALEP"**.

VIGÉSIMA QUINTA. RELACIÓN Y EXCLUSIÓN LABORAL

"EL PRESTADOR DE SERVICIOS" reconoce y acepta ser el único patrón de todos y cada uno de los trabajadores que intervienen en la prestación del servicio, deslindando de toda responsabilidad a **"EL CONALEP"** respecto de cualquier reclamo que en su caso puedan efectuar sus trabajadores, sea de índole laboral, fiscal o de seguridad social y en ningún caso se le podrá considerar patrón sustituto, patrón solidario, beneficiario o intermediario.

"EL PRESTADOR DE SERVICIOS" asume en forma total y exclusiva las obligaciones propias de patrón respecto de cualquier relación laboral, que el mismo contraiga con el personal que labore bajo sus órdenes o intervenga o contrate para la atención de los asuntos encomendados por **"EL CONALEP"**, así como en la ejecución de los servicios.

Para cualquier caso no previsto, **"EL PRESTADOR DE SERVICIOS"** exime expresamente a **"EL CONALEP"** de cualquier responsabilidad laboral, civil o penal o de cualquier otra especie que en su caso pudiera llegar a generarse, relacionado con el presente contrato.

Para el caso que, con posterioridad a la conclusión del presente contrato, **"EL CONALEP"** reciba una demanda laboral por parte de trabajadores de **"EL PRESTADOR DE SERVICIOS"**, en la que se demande la solidaridad y/o sustitución patronal a **"EL CONALEP"**, **"EL PRESTADOR DE SERVICIOS"** queda obligado a dar cumplimiento a lo establecido en la presente cláusula.

VIGÉSIMA SEXTA. DISCREPANCIAS

"LAS PARTES" convienen que, las estipulaciones que se establezcan en este contrato no deberán modificar las condiciones previstas en la convocatoria a la invitación, y sus juntas de aclaraciones; en caso de discrepancia, prevalecerá lo estipulado en estas, conforme a lo previsto en el artículo 66, párrafo segundo de la **"LAASSP"** y artículo 81, fracción IV del Reglamento.

VIGÉSIMA SÉPTIMA. CONCILIACIÓN.

"LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato podrán someterse al procedimiento de conciliación establecido en los artículos 109, 111 y 112 de la **"LAASSP"**, y 126 al 136 de su Reglamento.

VIGÉSIMA OCTAVA. DOMICILIOS

"LAS PARTES" señalan como sus domicilios legales para todos los efectos a que haya lugar y que se relacionan en el presente contrato, los que se indican en el apartado de Declaraciones, por lo que cualquier notificación judicial o extrajudicial, emplazamiento, requerimiento o diligencia que en dichos domicilios se practique, será enteramente válida, al tenor de lo dispuesto en el Título Tercero del Código Civil Federal.

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

CONTRATO: CAS-21-2025-AMARCO

VIGÉSIMA NOVENA. LEGISLACIÓN APLICABLE

"LAS PARTES" se obligan a sujetarse estrictamente para la prestación de los servicios objeto del presente contrato a todas y cada una de sus cláusulas, sus anexos que forman parte integral del mismo, a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento; Código Civil Federal; Ley Federal de Procedimiento Administrativo, Código Federal de Procedimientos Civiles; Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento.

TRIGÉSIMA. JURISDICCIÓN

"LAS PARTES" convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales con sede en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

"LAS PARTES" manifiestan estar conformes y enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman en las fechas especificadas.

POR:
"EL CONALEP"

NOMBRE	CARGO	R.F.C.
KARINA SALAZAR HERNÁNDEZ **REPRESENTANTE DE "EL CONALEP"**	**DIRECTORA DE INFRAESTRUCTURA Y ADQUISICIONES**	SAHK810729TH1
JULIÁN JAVIER ROBLES RIVAS **ADMINISTRADOR DEL CONTRATO**	**DIRECTOR CORPORATIVO DE TECNOLOGÍAS APLICADAS**	RORJ7312163W3

POR:
"EL PRESTADOR DE SERVICIOS"

NOMBRE	R.F.C.
RUBÉN PLAZA AGUILAR **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.**	IPS0703142W1

Calle 16 de septiembre No. 147 Norte, Col. Lázaro Cárdenas, CP. 52148, Metepec, Estado de México.
Tel. 722 271 0800 www.conalep.edu.mx

Cadena original:

cf10d3eb4b80f1fdd74306ab6e6152f1822b19451b959eba448ba2d0b2beb22b

Firmante: KARINA SALAZAR HERNANDEZ
RFC: SAHK810729TH1

Número de Serie: 00001000000701530711
Fecha de Firma: 22/09/2025 18:59

Certificado:

MIIGRzCCBC+gAwIBAgIUMDAwMDEwMDAwMDA3MDE1MzA3MTEwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29iLm14MSYwJAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTIzMDgwNzE5MDIxNFoXDTI3MDgwNzE5MDIxNFowgdIxITAfBgNVBAMTGEtBUklOQSBTQUxBWkFSIEhFUk5BTkRFWjEhMB8GA1UEKRMYS0FSSU5BIFNBTEFaQVIgSEVSTkFOREVaMSEwHwYDVQQKExhLQVJJTkEgU0FMQVpBUiBIRVJOQU5ERVoxCzAJBgNVBAYTAk1YMSUwIwYJKoZIhvcNAQkBFhZrYXJpbmFzYWxoQGhvdG1haWwuY29tMRYwFAYDVQQtEw1TQUhLODEwNzI5VEgxMRswGQYDVQQFExJTQUhLODEwNzI5TVRTTFJSMDIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQD6ElFFwLB6UBdBc6r/wF9GhbyXfBeGrOFk/RFJD/0CbnloaOpYKb0cpeFVm87wkSOQrI+hsI1JxN6mYjn0cC7GP8RToW6X1ZA78fw/qbTAnAYojnlvP/k3ZgArfTwjDdDUEm97Fp6mKEAgcUBwAUVPa0Uw8IwFMHJ+zxadW9Xrtx5A3nUBZY94gKyzic5TPx5Wo3AYES985mAtz0cyFWrKo/my1vTNTj8FPYCwqHT3SeyMDCHlxpnuyYf0HOrSXnffmdFfO/mT24EPPL0oAGFdxn9+kA+JazWuROnEqvIoAfFZXq81xtpL617DYJgsP+8OQmN79SLWvn2pH5ukZwWNAgMBAAGjTzBNMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgPYMBEGCWCGSAGG+EIBAQQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDBAYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggIBAJ3qHqrGdtpQz39LlmRVGhVRntFJAEsT5l5u8zW9nF8c8tL9D2F+cPyipuPctbKlLCJkYiYFCZ45H53PkGGuuG0JRNDpSmF4rqa0AgkdEHivsJ/4eJNMJKS+fefSrET0fVrKlsm5UJLjGYyENyvX8EhPyDD4Gdd5VpblcOnS/a7Sx+5ckzMiFRk0L9oHHcaHVT7bOfk8h06wk8Q7Q/kx6moHihZcJPYWJf7eIEc4TrLDnP2hLKIzv5GJY5FuVZdQwHBACqp1qZzQYiIPxxXiNYmXlZjVeyftywymxkgY1dzFBd/LlV8ihJ6NTsYtoU+/4uvBa5Szr2ql2Rt413cNTivzAeFGBs4pSXiV6++e6EuGumYaw4jhpjQTOtGlKfZI7pJw6ClO85av61FJQo++v6MKpVfjW62KSsE/ySGFYE3nh2SmZE1lxOdmGSe7uobeK7D/DpDRZcQUccNgkwrEWfLTCIv5Avjtsb5l66exRPkQ1Fl0A9MaMrAA3MY2pALYRPzR139xmjn5cS1qGbqbTAwvz1bZ7fX2gfcGXpaDM6liXMjH0s3r8C8OtZQM7mApTuIeDS7eNoHpmSHuBYJRGrYuAoa6sKltyEJHIuPt8nKTNN+ZQnlwfJu6zb/B+wjoZw7Jx7S8bmzUuW4NGETBj1o0hy/p1iIvDN+8thMbYiJ3

Firma:

YCwEolw1fUrmU228Ug4TxuPunWBdso2BlcX4rfjibE19ZCqiNxDfs9bdpxxio/Zl8aoEGZ3oDnQ8qV17CdAywtyi4BwPeajeGWH9pyH3tG4/WyjBXlJMpijp9aclq68EYywBZUUZGYCFMAoqY/tWtRjII1L9TzG0ZufAkLEV5fnNIwcTnUvtBUoTxUmhWsrxTeCq9XWp3OfUypB7MnaTArGQ4sXQU6CLoNyl7g2rr8NGiEwsW10dpb+WAlQDYgm6X5Rj2YZPjfPvuyiuEJHMs8Es9oFMIECxXg4tTvdW8KntnGSOtEOTPz7cJD4524zs6dv6bb8hgQ9skK6mf8x5bw==

Firmante: JULIAN JAVIER ROBLES RIVAS
RFC: RORJ7312163W3

Número de Serie: 00001000000519109829
Fecha de Firma: 22/09/2025 19:03

Certificado:

MIIGPjCCBCagAwIBAgIUMDAwMDEwMDAwMDA1MTkxMDk4MjkwDQYJKoZIhvcNAQELBQAwggGEMSAwHgYDVQQDDBdBVVRPUklEQUQgQ0VSVElGSUNBRE9SQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWG2NvbnRhY3RvLnRlY25pY29Ac2F0LmdvYi5teDEmMCQGA1UECQwdQVYuIEhJREFMR08gNzcsIENPTC4gR1VFUlJFUk8xDjAMBgNVBBEMBTA2MzAwMQswCQYDVQQGEwJNWDEZMBcGA1UECAwQQ0lVREFEIERFIE1FWElDTzETMBEGA1UEBwwKQ1VBVUhURU1PQzEVMBMGA1UELRMMU0FUOTcwNzAxTk4zMVwwWgYJKoZIhvcNAQkCE01yZXNwb25zYWJsZTogQURNSU5JU1RSQUNJT04gQ0VOVFJBTCBERSBTRVJWSUNJT1MgVFJJQlVUQVJJT1MgQUwgQ09OVFJJQlVZRU5URTAeFw0yMzA0MTMxOTIzMDlaFw0yNzA0MTMxOTIzNDlaMIHaMSMwIQYDVQQDExpKVUxJQU4gSkFWSUVSIFJPQkxFUyBSSVZBUzEjMCEGA1UEKRMaSlVMSUFOIEpBVklFUiBST0JMRVMgUklWQVMxIzAhBgNVBAoTGkpVTElBTiBKQVZJRVIgUk9CTEVTIFJJVkFTMQswCQYDVQQGEwJNWDEnMCUGCSqGSIb3DQEJARYYamphdmllcnJvYmxlc3JAZ21haWwuY29tMRYwFAYDVQQtEw1ST1JKNzMxMjE2M1czMRswGQYDVQQFExJST1JKNzMxMjE2SERGQlZMMTgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCoE3gltp+KMFew20oLCRGmMqs+nByJO8XIROql7IZ3y4lJphLr7a784DWcr3f0BbNETW2OUgEm/hNCr4N8rKJd9kIIQRRzNUUMuPXz5ZGuj4PC2ZCdCNWKo3fxq/ZPuiamPyhxbSgCyNee2Cgjd1t09EbgnamEvcaCx8ViFlZDVEft3oQjwh36k3DsWlQgNB+k/bFOa/QlNyeMlWErF11gVe4PHvs+QEyvyt9y1QaYTqAREY8V4kmUwWUjFuON6BukYPOLWf/02cQAfBzw7KUyOJvmH9Ap22C35k4KDTlqjgA7JFWN6ntFUYvcROWRJzeGIDfTvDlHnvXhPn4oLsfzAgMBAAGjTzBNMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgPYMBEGCWCGSAGG+EIBAQQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDBAYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggIBAF+Vzdi/cmcTQ1Uae/8Z9W9mJd1YL1EbV/FXYzpIyWpIPdvjmo6NNBhLWQ/W+P/WUWGxUJCd1u30rRbYs4iU4oaR91FI9eI1geB3vLjSLQNgU/J0bkOUnTKLeQ7rNl78aPRX1Z9QCBqEfeOpE3PRspr3cUuiAnyku8cl7hfNUE2rXRRr7qzasyKp1WcoOm5U2MD6my+Ok23tBEOhPLn4XQ9s9O58y0X/0PXxduO8iD+gugshYMmRTVBb0SA66QRgiwRQwBoMKck4k6DtCXjmNxAC+pgY2keszVEz9zBRnzfCVSp9OFdehcFM61SGy8hBD1+4DkwDSVaNdqjCKc55LOoBd5uUWq6rewvArtG5iiyqVKuxBXnywKY2TaTPhaEZBCH2KzwiZe3EGMvRpvjp3jGoAkqwlgHOLif9gAf/EAgqOgyW0B2/biWjA2cEexTAQEx/LwP8FMnTeNvwiVvNY7b4+IKUYTRz5SX5aJCaZ8V4QqUda4iMg6BlR+C78pRzlo98+9QSudlJQvd003cYzyvYOnsKinvGzx15Pg1PgpU0Uz+lNgqiyiZfSMvGrGzLdEG7jKIHjaKqVJISiwmcJkqEiD2zGpM4nbY7vLo2suf9glRXKaZMeOu5Doiiuzhs4UKI9zpKv4DJCSsXk+K2Eqh0mVTLS0EjfmfAPHLXuNu2

Firma:

Fn4XaPe/L8JeCYFIq9o0eycSLSfHB+XtIVrN59VFGqgVknT8iSlOHdlmTTunTqIZdHLcPKXyJZc0ATl5oytCILO6+8s0BCDZEr5WNOQZh6NGs7lKnAzr3MhwfUL/QjwwUlX5zOMuQTGU/NOiiPHYLtDZOtew8OdR8AllhxNUl4NIgbQXoXd/Mw1x63z8LT9ePHGM7JilfWlW6SJaZI+TTmFXRuV1ojQCMXjnj90w06HgM0dV1SJy7KoM1hK4i9l1nXqGOjAmon7akWc7gVQdLA2I9k1KzTqnGQcDT2DOBmgJ/3c0tlCsETVj9Z0XszsYbFniVXACADEOuDB2EJDR4g==

Firmante: IP PRODUCTOS Y SERVICIOS SA DE CV
RFC: IPS0703142W1

Número de Serie: 00001000000706634103
Fecha de Firma: 22/09/2025 21:13

Certificado:

MIIGcjCCBFqgAwIBAgIUMDAwMDEwMDAwMDA3MDY2MzQxMDMwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29iLm14MSYwJAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTI0MDQxOTIwNTMyM1oXDTI4MDQxOTIwNTQwM1owgf0xKjAoBgNVBAMTIUlQIFBST0RVQ1RPUyBZIFNFUlZJQ0lPUyBTQSBERSBDVjEqMCgGA1UEKRMhSVAgUFJPRFVDVE9TIFkgU0VSVklDSU9TIFNBIERFIENWMSowKAYDVQQKEyFJUCBQUk9EVUNUT1MgWSBTRVJWSUNJT1MgU0EgREUgQ1YxCzAJBgNVBAYTAk1YMSMwIQYJKoZIhvcNAQkBFhRhZ2FyY2lhQHNhdnNlLmNvbS5teDElMCMGA1UELRMcSVBTMDcwMzE0MlcxIC8gUEFBUjY5MDcwNzlUMjEeMBwGA1UEBRMVIC8gUEFBUjY5MDcwN0hNQ0xHQjA3MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAh/JVjsAvVNXvggOmXpGbegYopb629MkZRsCTPbJQ0jAnKg00CgO6Hj4LF1WC2UlrwttrW3sssebQmuO53A7RnLUwYrvJp/XJmYVAwLbqbMg3dSFhpVH+crPWDl9ua8NAmiPo7xKxt/O+qzNhL7nsYwaPbJM5JFC+eRAILf7Y6l5jANRi/oe3LmNXwvzLbD4sx0UCQcVdFYc8Qpfb20xFRe+1Qim6hfYrla5yR2z5cTOq/G7PWdqs5pMsqbblV2XutN1a3shMjR89m6nW5ZdCWYPtYqzfUafZqWMbMkwEFJXif9jyCAm6Vu2M+novDBosjdoB6ebgRQYxU4oqxCeEiwIDAQABo08wTTAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwID2DARBglghkgBhvhCAQEEBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4ICAQBiHuId8DsqyMrFkmZfPjgSmNHuSkUCiWvIiWdUyaBUBkWD40ru5BF+Vbp36ZSKnlA7H8rcJzCamXO7LwQbXKl/MtwE5SyCsrFMx7wYAxvJvS4xVNEudPlF+RDd8J4DQUNWuBMLWke9Js/SCuBB4wH74UhCX3eoN7js2c6hruMIxf0zikWgcktLEYSM67o7WUj7Y5qgbsrtAYAKagrn8/SZGC6lt4FXpyeJuFyjeSoMNnMSEoqFTQQfsMcFFjRlFhl9XNthtt26/kYUyNAZ3WvsfVmmWRcTksgynkJeXWB2THfMVL1IIDDXEOU6WxdAoGtXs0FzVP9vPq6xMC1RHwodwT48E1qz0dXultV/mT3ooth4v2K9DK9del10JXgMH52wTnWfix3Qp9BcKgH+//Erk4TZ8PG7Ld1stFrEoiE8n2KlcN9UNezsyGBSr1mQIh2gL/ETq4fKcHLALjuum6sEwF/Pjr2yrC5BqYhV/4rSAjfQrUMYx1LHLyM/uhVtoXKN53aDrDZ7rAikRMT65qlO+ziw0norh2mFz7KaAW+s5pNWp6KYRPV8a7bJwbStKy8bj6F/kDqmXU/5K9UuiyBT+A7mt6kBqBV4pgX95wmT+0Jks1rONmM1waLOu3A9f8xecoiTbf4u+AhopKRSMChkT8sFJDPJ/AfLiBeSmfA6nQ==

Firma:

WISmz1ptIChISe8UeC3Wi2ZsJC7ASf5Jkl4sbOzuh7lpQp/PSTJ0WOyfNCzjMIJr6v2jMSaIxvqeVzmPY5QHKF10UrqZF3nkBBZdSeMk93jwZZsIqMLj+rKgBz6/YhKtE6GumgbO5FMHX8UrYLkvXW8t5W5A0Gbz
fRc/eCTd8vZsmz+aA7ScDhbHi7afaLV9OZFfApBKQ8S3OKBRQGgvKszF9th/SQDpwuUEmkd0z8Prw9iEQYBWYeRC3NMXoAzCD2gxkQEEh1OySJ7xf+B77ppB3f6PfqkZa8rsHZuD0YmKNWqT+VuxCAPpBRybKu7k
OTDhWLkZXpzfSUUIfs5F1g==

TRANSFORMACIONES TECNOLÓGICAS

IP Productos y Servicios S.A. de C.V.

RFC: IPS0703142W1

PROPUESTA TÉCNICA
CUMPLIMIENTO A LO SOLICITADO EN LA FRACCIÓN IV,
PUNTO 4.1, INCISO A), Punto 1 DE LA CONVOCATORIA

Estado de México a 22 de agosto de 2025.

COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA

P r e s e n t e

De conformidad con lo establecido en la Convocatoria de Invitación a Cuando Menos Tres Personas de Carácter Nacional Electrónica **No. IA-11-L5X-011L5X001-N-44-2025**, relativa a la contratación del **"SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP"**, manifiesto bajo protesta de decir verdad:

El que suscribe Ruben Plaza Aguilar en mi carácter de representante legal de IP Productos y Servicios, S.A. de C.V. en cumplimiento a lo solicitado en la FRACCIÓN IV.- REQUISITOS QUE LOS LICITANTES DEBEN CUMPLIR EN SUS PROPOSICIONES, Punto 4.1 Documentación que deberán presentar los licitantes participantes, inciso a) Contenido de la propuesta técnica, Punto 1 Oferta Técnica, al respecto y cumpliendo con la totalidad de las especificaciones técnicas señaladas en el "Anexo Técnico" publicado a continuación presento a su consideración la Propuesta Técnica de mi representada:

A T E N T A M E N T E

Rubén Plaza Aguilar
Representante Legal
IP Productos y Servicios S.A. de C.V.

PROPUESTA TÉCNICA EN CUMPLIMIENTO AL ANEXO NO. 1
"Descripción Técnica del Servicio"

Convocatoria de Invitación a Cuando Menos Tres Personas de Carácter Nacional Electrónica No. IA-11-L5X-011L5X001-N-44-2025, para la contratación del **"SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP", que corresponde al proyecto "Operación de las comunicaciones y conectividad institucional", en adhesión al contrato marco para el "Arrendamiento de Equipo para Telefonía IP y videoconferencia para las Dependencias y Entidades de la Administración Pública Federal".**

Con fundamento en los artículos 24, 35 Fracción II y IV y 56 de la LAASSP, y artículo 51 de su reglamento.

ANEXO 1
DESCRIPCIÓN TÉCNICA DEL SERVICIO

PARTIDA 1. ESPECIFICACIONES TÉCNICAS DEL SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP

IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado proveerá el servicio telefónico, así como la instalación de equipos, puesta en operación a punto y soporta técnico especializado para proporcionar los servicios de voz y datos, mediante la integración de un servicio On Premise Centralizado de Telefonía IP para Colegio Nacional de Educación Profesional Técnica, CONALEP, en apego al Contrato Marco denominado "Arrendamiento de equipo para telefonía IP y videoconferencia para las Dependencias y Entidades de la Administración Pública Federal".

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que la vigencia será a partir de un día posterior a la notificación de fallo y hasta el 31 de diciembre de 2025.

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado será el responsable del correcto funcionamiento de los aparatos telefónicos.

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que la contratación del servicio es en apego al contrato marco, de acuerdo al periodo de transición establecido en dicho contrato.

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que la vigencia de la garantía será la misma del periodo de la vigencia del contrato.

IP Productos y Servicios, S.A. de C.V. considera en su propuesta los accesorios necesarios de hardware y/o software para la correcta operación y funcionamiento del servicio.

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que todos los equipos suministrados, incluidos los de reemplazo, serán nuevos.

IP Productos y Servicios, S.A. de C.V. considera en su propuesta la presentación bimestralmente, las constancias de la inscripción y pago de cuotas al Instituto Mexicano Del Seguro Social del personal que utilice para la prestación de los servicios, únicamente será obligatorio para efectos del artículo 80, párrafo cuarto del RLAASSP, en el caso de prestación de servicios que requieran del uso intensivo de mano de obra, y ésta implique un costo superior al treinta por ciento del monto total del contrato.

Descripción de los equipos

El Colegio Nacional de Educación Profesional Técnica (CONALEP) requiere la contratación del "Servicio de Arrendamiento de equipo para telefonía IP", conforme a:

Partida	Cantidad	Descripción	Periodo
Única	1 Servicio de Arrendamiento	"**Servicio de arrendamiento de equipo telefónico IP**", que corresponde al proyecto "Operación de las comunicaciones y conectividad institucional", en adhesión al contrato marco para el "Arrendamiento de Equipo para Telefonía IP y videoconferencia para las Dependencias y Entidades de la Administración Pública Federal".	Periodo comprendido un día posterior a la notificación del fallo al 31 de diciembre de 2025.

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que los equipos para telefonía IP se suministrarán de acuerdo con lo especificado en las características técnicas e incluye como mínimo los elementos de hardware, software y funcionalidades requeridas en el presente anexo técnico, en apego a lo establecido en el contrato marco al cual se adhiere, denominado "Arrendamiento de equipo para telefonía IP y videoconferencia para las Dependencias y Entidades de la Administración Pública Federal".

La finalidad de la contratación es proporcionar al CONALEP las herramientas tecnológicas en materia de telefonía IP, que permiten la interconexión para los servicios de voz y datos, bajo el protocolo IP, a fin de proporcionar los servicios y, de esta manera, alcanzar sus metas.

Cuadro 1. Equipos en arrendamiento requeridos para telefonía IP

Partida contrato marco	Tipo	Componente	Unidad de medida	Cantidad Solicitada
1	**Equipo Telefonía IP**	**Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition para 1000 ext.**	Equipo	**1**
3		**Gateway para troncales marca Avaya, marca Avaya modelo IP Office 500 v2**	Equipo	**3**
12		**Servicio de Tarificación Telefónica marca Intersel, modelo Intertel Suite (Hasta 1000 extensiones a tarificar)**	Equipo o licencia	**1**

Componente	Cantidad	Número de líneas SIP	Extensiones	Ubicación Física
Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition para 1000 ext.	1	108	780	Calle 16 de Septiembre #147 Norte, Colonia Lázaro Cárdenas, Metepec Estado de México, C.P. 52148
Call Center	1			
Servicio de Tarificación Telefónica marca Intersel, modelo Intertel Suite (Hasta 1000 extensiones a tarificar)	1			

IP Productos y Servicios S.A. de C.V.

RFC: IPS0703142W1

Componente	Cantidad	Número de líneas SIP	Extensiones	Ubicación Física
Gateway para troncales marca Avaya, modelo IP Office 500 v2	1	8	20	Santiago Graff No. 105, Col. Parque Industrial, C.P. 50200, Toluca, Edo. Méx. (Pasando el PRI tomar carretera. Toluca - Atlacomulco km. 3, o dar vuelta pasando la gasolinera a la segunda calle a la derecha al fondo está la Bodega Central)
	1	16	50	Av. Conalep No. 137 y av. Símbolos patrios, Col. la experimental, San Antonio de la Cal, C.P. 71236, Oaxaca, Oaxaca.
	1	230	150	Av. Azcapotzalco No. 158 (entre Golfo de Tehuantepec y Mar Mediterráneo), Col. Tacuba, Delegación Miguel Hidalgo, C.P. 11410, CDMX

- El tarificador propuesto tiene la capacidad de tarificar el total de las extensiones de todos los sitios. (Metepec, Toluca, Oaxaca y CDMX).
- Los aparatos telefónicos son propiedad de CONALEP marca Grandstream, por lo cual IP Productos y Servicios, S.A. de C.V. incluye en su propuesta el licenciamiento necesario y garantizar la integración de estos con la solución ofertada.
- IP Productos y Servicios, S.A. de C.V. incluye en su propuesta la cantidad de 3 agentes con las funcionalidades propias del Call Center.

Método de evaluación

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que el método de evaluación de las propuestas será binario.

Forma de adjudicación

Dado que el CONALEP requiere en arrendamiento las partidas 1, 3 y 12 del contrato marco, que corresponden a los equipos agrupados por el tipo de telefonía IP definidos en el Cuadro 1. Equipos en arrendamiento requeridos para telefonía IP, estos tendrán que ser propuestos y adjudicados a un mismo licitante, que reúna en su conjunto las mejores condiciones en cuanto a precio.

El CONALEP no requiere el arrendamiento de ninguno de los equipos agrupados por el tipo de videoconferencia definidos en las partidas del Cuadro 1. Equipos en arrendamiento requeridos para telefonía IP, por lo que IP Productos y Servicios, S.A. de C.V. no considera estas partidas en su propuesta técnico-económica.

Criterios aplicables para el arrendamiento de equipo para telefonía IP

IP Productos y Servicios, S.A. de C.V. considera en su propuesta lo siguiente:

- Que las especificaciones plasmadas en el presente anexo técnico son los requerimientos mínimos para la contratación.
- Todos los equipos suministrados, incluidos los de reemplazo, son nuevos.
- Se realizará la instalación, configuración y puesta a punto de los equipos propuestos en las instalaciones que el

CONALEP le indiquen, además de garantizar la integración y compatibilidad de los componentes de Hardware descritos en el presente anexo técnico, así como los elementos necesarios para la integración y funcionalidad total requerida.

- IP Productos y Servicios, S.A. de C.V. considera en su propuesta todas las actualizaciones del software necesario para el correcto funcionamiento de los equipos descritos en el presente anexo técnico durante la vigencia de la garantía.
- Dado que el CONALEP requiere el arrendamiento de tres de los equipos agrupados por el tipo de telefonía IP definidos en las partidas del Cuadro 1. Equipos en arrendamiento requeridos para telefonía IP, estos tendrán que ser propuestos y adjudicados a un mismo licitante que reúna en su conjunto las mejores condiciones en cuanto a precio.
- IP Productos y Servicios, S.A. de C.V. entregará dentro de los primeros 15 días hábiles posteriores a la fecha de adjudicación del contrato, un plan de trabajo donde se describan las actividades que se tienen que realizar para la correcta entrega, instalación, configuración y puesta a punto de los equipos requeridos por el CONALEP, con aprobación de esta.
- IP Productos y Servicios, S.A. de C.V. como posible proveedor de los equipos para telefonía IP incluye en su propuesta, el suministro de todos los accesorios necesarios, para la correcta instalación, integración, operación y funcionalidad de los equipos.
- El tiempo de entrega, instalación, configuración y puesta a punto de los equipos propuestos en las instalaciones que el CONALEP le indiquen, se realizará dentro de un plazo no mayor a 90 días naturales a partir del día hábil siguiente a la fecha de la adjudicación del contrato.
- IP Productos y Servicios, S.A. de C.V. realizará la entrega de los equipos para telefonía IP requeridos por el CONALEP en los domicilios indicados.
- Para el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition, Gateway con capacidad de supervivencia marca Avaya, modelo IP Office 500 v2, Gateway para troncales marca Avaya, modelo IP Office 500 v2 y el Equipo Multipunto de videoconferencia (MCU) (partidas 1, 2, 3 y 13), el tiempo de atención vía telefónica 24x7x365 será en un tiempo no mayor a 15 minutos, y se brindará durante 24 horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio, ésta se otorgará dentro de las 6 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique reemplazo de partes, el tiempo de solución máximo será de 24 horas naturales para la UODCDMX y sus 27 planteles y para la RCEO y sus 6 planteles, a partir del levantamiento del reporte.
- Para las partidas 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15 y 16, el tiempo de atención vía telefónica será en un tiempo no mayor a 15 minutos, y se brindará durante 24 horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio, ésta deberá otorgarse dentro de las 24 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique reemplazo de partes, el tiempo de solución máximo será de 48 horas naturales para la UODCDMX y sus 27 planteles y para la RCEO y sus 6 planteles, a partir del levantamiento del reporte.
- IP Productos y Servicios, S.A. de C.V. cuenta con medios de comunicación para reportar fallas de equipo (mesa de ayuda). Los medios para reportar fallas al menos son un número convencional, un celular y un correo electrónico.
- IP Productos y Servicios, S.A. de C.V. será responsable en el caso de que se violen derechos de propiedad industrial, patentes o derechos de autor, respecto al software y/o hardware utilizados en los equipos, dejando en todo momento a salvo al CONALEP.
- IP Productos y Servicios, S.A. de C.V. considera en su propuesta que proveerá los recursos humanos necesarios para cumplir las tareas de:
    - Maniobra, carga, descarga, desembalaje, ensamblado, retiro de empaques y entrega de los equipos.
    - Instalación, configuración y puesta a punto de los equipos, de acuerdo con las recomendaciones y mejores prácticas del fabricante.

- IP Productos y Servicios, S.A. de C.V. será responsable de que la totalidad de componentes que conformen los equipos sean compatibles.

Características técnicas de los equipos para telefonía IP incluidas en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition

Los equipos para equipo de telefonía IP cuenta con lo siguiente:

- Sistema de Procesamiento de Llamadas IP
- Mecanismos de cifrado para voz incluidos en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition
- Mecanismos de Supervivencia
- Servicios Troncales Digitales
- Servicio de Directorio Telefónico
- Servicios de Terminales Telefónicas
- Servicio de teléfono basado en software marca Avaya, modelo IX Workplace
- Correo de Voz con Servicio de Mensajería
- Servicio de Distribución Automática de Llamadas marca Avaya, modelo Avaya Contact Center Select
- Servicio de Operadora Automática incluida en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition
- Servicio de Operadora Manual
- Implementación de la Solución y Migración de Servicios
- Conectividad con Redes de Voz entre Entidades
- Servicio de tarificación y reporte de llamadas

Los equipos para Telefonía IP se apegan a las características técnicas que se describen a continuación:

Partida 1 del contrato marco: Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition

IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado incluye en su propuesta para arrendamiento de equipo de telefonía IP con Sistemas de Procesamientos de Llamadas IP cumplen con las condiciones de operación y/o características técnicas siguientes:

- IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado proveerá en configuración redundante y de alta disponibilidad el Sistema de Procesamiento de Llamadas IP, de tal manera que ante la falla del procesador de llamadas principal, se tenga el soporta de otro procesador de llamadas que tome el control de todos los dispositivos asociados al procesador de llamadas principal, esto es, se mantendrá el procesamiento de las llamadas de las extensiones IP aún y cuando estén basadas en SIP (Session Initiation Protocol), así como de las extensiones analógicas, con todas sus funcionalidades asociadas, sin afectación de las llamadas establecidas al momento de la falla.
- IP Productos y Servicios, S.A. de C.V. incluye en la solución ofertada todo el hardware, software y licenciamiento necesario, para garantizar la redundancia geográfica del Sistema de Procesamientos de Llamadas IP, de tal forma que ante la eventual falla del Procesador de Llamadas principal y de su redundancia, de manera automática entre en operación la redundancia geográfica (siempre y cuando no se pierda la comunicación vía la red privada virtual entre ambos inmuebles), tomando el control de todos los dispositivos asociados, conservando el Plan de Marcación, sin pérdida de las llamadas establecidas y de ninguna de las Funcionalidades básicas incluidas en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition solicitadas. El Sistema de

Procesamiento de Llamadas IP, cuando esté operando la redundancia geográfica, garantiza que no se presentará ninguna degradación en el Servicio integral de telefonía y telecomunicaciones.

- El Sistema de Procesamiento de Llamadas IP, cuenta con la capacidad de maneja el Protocolo SIP para permitir el registro de cualquier dispositivo que cumpla con este protocolo.
- El Sistema de Procesamiento de Llamadas IP, soporta por sí mismo o con los elementos necesarios, las siguientes troncales: IP, SIP, E1 R2 Modificado, E1 PRI ISDN, E1 con soporta de Q. Sig., Troncales analógicas y Troncales ISDN BRI.
- El Sistema de Procesamiento de Llamadas IP permite la configuración y/o programación de troncales SIP.
- IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado realizará las configuraciones necesarias a fin de que se respeten los planes de marcación que tienen establecidos el CONALEP, siendo estos de 4 o 5 dígitos al menos.
- El equipo de voz IP, soporta la configuración y operación del Plan Técnico Fundamental de Numeración de marcación a 10 dígitos ordenado por Instituto Federal de Telecomunicaciones (IFETEL), debiendo discriminar si el servicio es llamada local, nacional, o celular, a fin de poder realizar la configuración correspondiente de acuerdo con el perfil de privilegios otorgados a cada uno de los usuarios finales.
- El Sistema de Procesamiento de Llamadas IP, maneja al menos los siguientes tipos de extensiones:
    - SIP con mecanismos de cifrado basados en al menos AES-128 y los protocolos SRTP y TLS al menos versión 2, para cualquier localidad.
- Adicionalmente, el Sistema de Procesamiento de Llamadas IP, cuenta con la capacidad de:
    - Restringir a un número determinado de llamadas máximas permitidas de manera concurrente entre inmuebles.
    - Registrar y controlar terminales telefónicas y de video.
    - Registrar y controlar tanto terminales basadas en hardware como en software para estaciones de trabajo Windows, teléfonos inteligentes (Smartphone) y tabletas con Sistemas Operativos iOS (Apple) o Android.

Funcionalidades básicas incluidas en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition

IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado incluye en su propuesta técnica, que todas las facilidades básicas descritas anteriormente, se incluyen como facilidades estándar asociadas a los "Servicios de Voz IP" con Teléfono IP, con excepción de aquellas para las cuales el administrador del contrato establezca alguna restricción, de la cual informará a IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado al inicio de la vigencia del contrato.

IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado incluye en su propuesta técnica, que el Sistema de Procesamiento de Llamadas IP que se utilice para proporcionar el Servicio de Voz IP objeto de estas especificaciones técnicas, cuenta con los elementos necesarios para garantizar como mínimo, el cumplimiento de las siguientes Funcionalidades básicas incluidas en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition:

Establecimiento de llamadas.	Capacidad de realizar llamadas internas dentro de un inmueble o hacia otro inmueble y desde y hacia la Red Pública de Telefonía.
Estado de la llamada por línea.	Facilidad que permite visualizar en el display del Teléfono IP, el estado de las llamadas establecidas (recibidas o generadas), en el que se muestre como mínimo el número y la duración

Marcación Entrante Directa (DID).	Reconocimiento de los 4 dígitos de la funcionalidad de Marcación Directa Entrante (DID o Direct lnward Dialing).
Identificación de la línea de llamada (CUD)/nombre del llamante (CNID).	Funcionalidades que permiten que un teléfono que recibe una llamada, además de timbrar, también reciba la información del número telefónico de la línea que lo llama (CLID o Calling Une Identification) y en su caso, el nombre asociado a dicha línea telefónica (CNJD o Calling Number Identification).
D Soporta de XML	A través de lo cual los teléfonos IP son capaces de acceder a un servidor que les permita desplegar la información que obtengan del mismo en sus pantallas.
Señalización de Mensajes de Voz.	Indicador visual y/o audible en el teléfono de que se está recibiendo un mensaje de .voz y/o indicador visual y/o audible en el teléfono de que se recibió un mensaje de voz.
Indicador de llamada en espera.	Indicador audible mediante un tono que se escuchará cuando se tenga una llamada en espera, además de un indicador visual en el display del Teléfono IP, que deberá activarse cuando se pone en espera una llamada.
Configuración de varias líneas.	Facilidad que permite configurar en un Teléfono IP, varias líneas o accesos asociados a un número de extensión.
Configuración de varios números.	Facilidad que permite configurar varios números de extensión diferentes en un mismo Teléfono IP, en función de la cantidad de teclas disponibles.
Multi representación de número.	Facilidad que permite que se anuncien las llamadas de un mismo número de extensión. en diferentes teléfonos IP, inclusive en inmuebles diferentes.
Marcación rápida.	El Sistema permite a través del Teléfono IP, la programación de marcaciones rápidas mediante teclas, dependiendo de la capacidad de teclas programables.
Marcación abreviada.	La marcación abreviada permite a los usuarios, marcar números de teléfono predefinidos con solo uno o dos dígitos.
Control de volumen.	El Sistema permite fijar el volumen mínimo de audio y tono de timbre de los teléfonos.
Intercomunicador silencioso.	Capacidad para que una llamada entrante timbre únicamente en el teléfono de la asistente, al tiempo que en el teléfono del superior aparece el número telefónico de la persona que llama y, en caso de ser interna, también el nombre.
Transferencia de llamadas con *y* sin consulta.	Esta facilidad permite transferir una llamada establecida (interna o externa) a otra extensión o a cualquier otro número telefónico externo. consultando previamente si se desea recibir la llamada o directamente sin realizar esta consulta.
Desvío automático de llamadas (Externas/Internas).	Facilidad que permite que todas las llamadas dirigidas a una extensión puedan enrutarse hacia otra extensión, una operadora, un número externo o un equipo de correo de voz automáticamente.

Desvío de llamadas en ocupado.	En una llamada establecida, se deberá recibir una alerta en la pantalla del teléfono, indicando que hay una llamada entrante y cuentase con la opción de desviarla al correo de voz del usuario o un número predeterminado.
Desvío de llamadas no atendidas.	Facilidad que redirige todas las llamadas entrantes de una extensión, en el caso de que no se contesten, a un número telefónico predefinido o al correo de voz del usuario, después de un determinado número de timbrados.
Conferencia Múltiple.	Capacidad de establecer conferencias de un mínimo de 6 participantes. Se deberán visualizar el nombre y/o número de línea de los participantes.
Remarcación.	Facilidad que permite remarcar el último número marcado, con una tecla específica o digitando algún prefijo.
Re Llamada.	Al marcar a una extensión de la Red, si no se contesta o está ocupada, se cuenta con la opción de programar una re-llamada, que deberá activarse cuando el usuario al que se llamó esté disponible. La llamada podrá ser automática o a elección del usuario, cancelarla o realizarla.
Acceso Remoto.	Funcionalidad que permite el acceso externo vía PSTN al "Sistema de Procesamiento de Llamadas IP", marcando un número predeterminado. Una vez establecida la llamada el usuario deberá autenticarse con un código de acceso (NIP), para permitirle realizar llamadas conforme a los privilegios que tenga autorizados
Identificación de número entrante / saliente.	En la pantalla del teléfono deberá aparecer el número al que se llama o del que se recibe la llamada. También aplica si el teléfono está habilitado con varias líneas. Identificación del nombre en llamadas internas entrantes / salientes. En llamadas internas entrantes o salientes, la pantalla del Teléfono IP deberá indicar el nombre asociado al número telefónico marcado o desde el que se recibe la llamada.
Restricción de identificación del usuario que llama.	Facilidad que permite realizar llamadas a números internos, sin que se anuncie el nombre y número de extensión.
Función de No Molestar.	Facilidad que permite a los usuarios que no quieren ser molestados por llamadas entrantes, pulsar una tecla o un prefijo para que no timbre el teléfono.
Arreglo Jefe / Secretaria.	Configuración de esquemas Jefe-Secretaria con consulta y transferencia de llamada, además de Cuenta con identificación visual del estado de la línea del Jefe (colgado-descolgado al menos).
Aparcamiento de llamada.	Esta función permite poner una llamada en espera (estacionarla) pulsando una tecla o prefijo y recuperarla desde otro teléfono.
Captura de llamadas por grupo.	Configuración de un grupo de teléfonos que permite, que de cualquiera de ellos, se pueda responder las llamadas del resto.
Retención/Recuperación de llamada.	Esta facilidad permite a un usuario atender una llamada, no obstante, tenga una llamada establecida. El usuario puede elegir atender la nueva llamada poniendo a la primera en espera o alternarlas.

Códigos de Seguridad.	El Sistema cuenta con la funcionalidad de marcación a números restringidos (larga distancia, llamadas a celular y números de entretenimiento como mínimo), a través de un Código de Seguridad personalizado de al menos 5 dígitos, que podrá utilizar el usuario en cualquier teléfono físico basado en hardware de la Red.
Marcaciones rápidas con códigos de seguridad.	El Sistema cuenta con fa funcionalidad de configurar marcaciones rápidas, que incluyan los códigos de seguridad requeridos para realizar las llamadas, en su caso.
Categorías de marcación.	El Sistema permite establecer categorías de marcación por teléfono, permitiendo o negando el acceso a ciertos números, tanto internos como de la telefonía pública fija o móvil.
Música en espera.	Facilidad que permite oír música o mensajes de audio de fondo, cuando se pone una llamada en espera. El Sistema incluye la música, por lo que respecta a los mensajes de audio, podrán ser predefinidos por LA ENTIDAD.
Historial de llamadas.	En los teléfonos IP, se deberá observar el registro de las llamadas recibidas, realizadas y perdidas, con información de fa llamada como; día, hora y duración, como mínimo.
Timbres distintivos del teléfono.	Facilidad que permite personalizar el tono del timbre del Teléfono IP.
Personalización de la pantalla del Teléfono IP.	Personalización de la imagen de fondo de la pantalla.
Bloqueo de llamadas salientes/entrantes.	El Sistema cuenta con la capacidad para filtrar y bloquear, llamadas salientes y/o entrantes a números específicos o patrón de números.
Timbrado distintivo para llamadas internas y externas.	Capacidad que permite configurar timbres distintivos, para diferenciar las llamadas internas de las externas.
Generación de tonos (DTMF).	Envío de tonos desde Teléfonos IP hacia la Red Pública, con el fin de interactuar con sistemas de audio respuesta.
Acceso al correo de voz.	Facilidad que permite acceder al correo de voz mediante una tecla predefinida en el Teléfono IP. Para escuchar los mensajes de voz, se deberá requerir de una contraseña.
Configuración de Redes Privadas.	El Sistema cuenta con la capacidad de configurar redes privadas, con esquemas de marcación cerrada. El Sistema de Procesamiento de Llamadas IP, permite inclusive la programación de un número de Red Privada en un Teléfono IP de cualquiera de las categorías solicitadas (con excepción de las analógicas), sin que se pierda el esquema de marcación cerrada.
Acceso a Directorio Telefónico	Capacidad del Sistema de acceder al Directorio Telefónico a través de los teléfonos I P. que IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado considere el acceso a LDAP.

Mecanismos de cifrado para voz incluidos en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition

Para asegurar la confidencialidad e integridad de la información de voz, así como del modelo propuesto para la solución de Telefonía IP, IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado considera en su propuesta técnica, que el Sistema de Procesamiento de Llamadas IP, que el hardware, software y licenciamiento necesarios que

se utilicen para proporcionar el servicio de Voz IP y funcionalidades solicitadas, cuentan con los elementos necesarios para garantizar, el cumplimiento de los siguientes mecanismos de seguridad:

- La solución propuesta por IP Productos y Servicios, S.A. de C.V. garantiza la encriptación de la llamada de punto a punto y en conferencia al menos AES-128 y los protocolos SRTP (Secure Real-time Transport Protocol) y TLS (Transport Layer Security), definidos en los RFC 3711 y RFC 2246 respectivamente. Esta condición aplicará solamente entre teléfonos IP y equipos y dispositivos que formen parte de la solución de Telefonía IP y para las llamadas establecidas entre ellas.
- Los teléfonos IP y las extensiones configuradas a través de software, manejan mecanismos de encriptación basados en al menos en AES-128, con la utilización del protocolo SRTP para el transporte de la voz y por medio de al menos en AES-128 y TLS para la señalización de la misma llamada.
- La solución garantiza que la modalidad de encriptación solicitada anteriormente se mantendrá en comunicaciones establecidas con el correo de voz desde la red instalada en el CONALEP.
- El modelo de encriptación solicitado se mantendrá con cualquier Gateway de Voz IP que esté en operación en la solución de Comunicaciones IP propuesta por IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado, bajo los estándares solicitados.
- IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado garantiza en su propuesta, que durante la vigencia del Contrato la infraestructura para proporcionar el servicio de Voz IP puede operar en su conjunto con una técnica de encriptación superior a AES-128, que será implementada sin ningún costo adicional para el CONALEP. IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado realizará una evaluación previa, para determinar el impacto del cambio, de los cuales informará al CONALEP para la toma de decisiones conjuntas.
- El Sistema de Procesamiento de Llamadas IP propuesto, cuenta con la capacidad de maneja Códigos de Seguridad personales de 5 dígitos como mínimo, para hacer uso de facilidades telefónicas como llamada a celular y/o larga distancia, en cualquier teléfono físico basado en hardware de la Red.
- El modelo de Comunicaciones IP propuesto incluye mecanismos de autenticación a nivel digital, que permiten a los teléfonos IP autenticarse con el Sistema de Procesamiento de Llamadas IP, por medio de certificados digitales para garantizar que son dispositivos validos en la Red con la categoría establecida.
- El Sistema de Procesamiento de Llamadas IP, así como los Gateway de voz propuestos en la solución, incluyen y soportan, mecanismos internos de seguridad como; accesos a la administración vía HTTPS (Hyper Text Transfer Protocol Secure) y/o CLI por medio de TELNET y SSH.

Partida 3 del contrato marco: Gateway para troncales marca Avaya, modelo IP Office 500 v2

IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica todos los elementos de hardware, software y licenciamiento necesarios para operar las troncales que CONALEP tiene definidos actualmente. Adicionalmente, la solución que ofrezca para el manejo de las troncales digitales cumple con las condiciones de operación y/o características técnicas siguientes:

- La solución soporta los siguientes tipos de troncales; IP, SIP, E1 PRI ISDN, E1 con soporta de Q.SIG, troncales analógicas (FXO) y Troncales ISDN BRI y está preparada con el hardware, software y licenciamiento necesario para operar las troncales digitales E1 R2 Modificado.
- La solución para el manejo de troncales digitales, garantiza que, ante la caída o saturación del grupo de troncales asociadas a un determinado sitio, se podrá realizar de manera automática, la toma de troncal de otro sitio que cuente con este servicio.
- La comunicación entre el Gateway de voz que se proponga para el manejo de las troncales digitales y el Sistema de Procesamiento de Llamadas IP y Teléfonos IP del CONALEP, se cifra con al menos AES-128 y utilizar el estándar SRTP.

- La solución para el manejo de las troncales digitales E1, cuenta con la función de cancelación de eco por hardware, conforme ITU-T G.168, además de maneja los tipos de señalizaciones Q.SIG, R2 Modificado, con funciones completas, sin restricción mediante licenciamiento.
- La solución incluye los acopladores de impedancia (Balum) necesarios para la correcta operación de la solución.

Los Gateway que se utilizarán para el servicio de Troncales Digitales y Mecanismos de Supervivencia, cumplen con las siguientes características y funcionalidades:

- Cuenta con la última versión liberada del Sistema Operativo con que cuente el fabricante al momento de instalar el equipo. La documentación comprobatoria de este requerimiento se integra en la propuesta de IP Productos y Servicios, S.A. de C.V.
- Maneja las siguientes interfaces físicas: Fast Ethernet o Gigabit Ethernet.
- Maneja las siguientes interfaces físicas: BRI, E1 G.703, troncales E1 para conexión de la PSTN (con manejo de R2 modificado, Q.SIG).
- Maneja Voz sobre IP (VoIP), además de soportar interfaces de voz digital (E1s) con interfaces de voz analógicas de los tipos FXS y FXO.
- Incluye los módulos de digitalización de voz DSP (Digital Signal Processor), necesarios para la correcta operación de la totalidad de los puertos de voz.
- Maneja mecanismos de control de llamadas, para garantizar el ancho de banda necesario para gestionar un número configurable de llamadas máximas simultáneas entre sitios.
- Cuenta con la capacidad de manejo de los protocolos HTTP, HTTPS, SMTP, SIP, TLS, IPv4 IPv6.
- Soporta de configuración de hora vía NTP.
- Soportar los códec G.711a, G.711u, G.722, G.729a y G.729ab e iLBC.
- Cuenta con la capacidad de maneja las llamadas simultáneas de voz necesarias, para atender los requerimientos de los usuarios en los sitios donde se instalarán.
- Maneja el modo de operación de conmutador IP de contingencia, soportando el Servicio de Supervivencia para la totalidad de terminales IP y analógicas de los sitios donde se instalarán.
- Cuenta con la capacidad y recursos para maneja al menos cinco conferencias simultáneas de voz de seis participantes.
- Maneja los estándares IEEE 802.1q, SNMP y SIP.
- La administración del equipo está basada en control de acceso por roles y se podrá realizar vía puerto de consola.

Partida 3 del contrato marco: Servicio de Tarificación Telefónica marca Intersel, modelo Intertel Suite

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que para la operación de tarificación se requiere un sistema de procesamiento del registro detallado de llamadas, CDR (Call Detail Recording por sus siglas en inglés), esta facilidad proporciona el detalle de las operaciones que realiza el sistema de telefonía.

- Número de llamadas por categorías:
  - Móvil
  - Fijo
  - Local
  - Nacional
  - Internacional
- Fecha, hora y duración de llamadas.
- Origen y destino.
- Costos de llamada por licitante adjudicado y tipo de llamada.

- Identificar códigos de autorización por usuario.

Los resultados generados por el reporte avanzado serán impresos, exportados en diferentes formatos o visualizados en pantalla.

Obtención de reportes de Directorio Telefónico de extensiones, ordenar por número de extensión, alfabético por nombre o por departamento.

Distribución Automática de Llamadas marca Avaya, modelo Avaya Contact Center Select

IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado considera propuesta técnica, el hardware, software y licenciamiento necesario para Distribución Automática de Llamadas marca Avaya, modelo Avaya Contact Center Select (Automatic Call Distribution o ACD por sus siglas en ingles), que se implementará a través del Sistema de Procesamiento de Llamadas IP y cuenta con las funcionalidades siguientes:

- Selección de línea secuencial.
- Bajo este esquema el sistema deberá enrutar la llamada hacia los agentes disponibles basándose en el orden de ingreso de estos al sistema. Esto es, que las llamadas serán preferentemente enrutadas hacia aquellos agentes disponibles que hayan ingresado con mayor anticipación al sistema.
- Redireccionamiento a servicio nocturno.
- Bajo este esquema las llamadas son redireccionadas hacia un servicio nocturno en el caso de que todos los agentes se encuentren ocupados, o bien hayan salido del sistema.
- Encolamiento de llamadas cuando todos los agentes se encuentren ocupados.
- El sistema es capaz de mantener encoladas todas las nuevas llamadas hasta que un agente que estaba ocupado se libere y conteste la llamada.
- Encolamiento de llamadas con redireccionamiento posterior hacia un usuario virtual (opcional)
- Ajuste de Prioridad de Encolamiento.
- El sistema es capaz de permitir ajustar la secuencia en la cual las llamadas son contestadas basándose en la prioridad de estas. De esta manera, al recibir una llamada con alta prioridad hacia una determinada cola de atención y todos los agentes pertenecientes a la misma se encuentren ocupados, el agente es capaz de poner esta llamada en primer lugar de la cola pudiendo contestar la llamada de alta prioridad inmediatamente después de haber concluido su llamada actual dejando así las llamadas menos importantes en la cola.
- Cuenta con la capacidad de asignar diferentes Perfiles a los agentes y configurar diferentes Perfiles por grupo de agentes.
- Si la solución está basada en Sistema Operativo Windows, IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado proporcionará el software de antivirus necesario. El software de antivirus se mantendrá actualizado durante la vigencia de la garantía.
- Soporta la capacidad de grabación de llamadas de manera automática.
- Identificación visual desde el teléfono de si hay una o más llamadas en espera, para agilizar la llamada que se tiene en el momento.
- Contestación automática al momento de asignar al agente, es decir, el agente no deberá presionar ningún botón para que la llamada sea considerada como atendida.
- Configuración de los mensajes que escuchará el usuario cuando; todos los operadores estén ocupados, la llamada se reciba fuera de los horarios de servicio, así como de los mensajes que se requieran por parte del CONALEP.
- Capacidad de generar reportes de distribución de llamadas, llamadas abandonadas, nivel de servicio, llamadas por agente entre otros.

IP Productos y Servicios S.A. de C.V.

Servicio de Operadora Automática incluida en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition

Se entiende como Servicios de Operadora Automática, la funcionalidad asociada a un Sistema de Procesamiento de Llamadas IP, para que las llamadas de usuarios externos o internos, dirigidas a un número de grupo de troncales del CONALEP, las distribuya el sistema de procesamiento a la operadora automática, misma que le ofrecerá al usuario de forma automática la opción de consulta y/o solicitud de información o enviarlo a una determinada extensión (con o sin DID asociado).

Por lo anterior IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado considera en su propuesta técnica el Servicio de Operadora Automática incluida en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition cumpliendo con lo siguiente:

- El Servicio de Operadora Automática incluida en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition provee un menú de opciones de navegación, para dividir fácilmente el tráfico en áreas de atención y, en caso de solicitarlo el CONALEP, en requerimientos de información más especializados, para canalizar las llamadas a su destino correspondiente. El administrador del contrato, en conjunto con IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado que resulte adjudicado, establecerán en la fase de planeación los menús de navegación y la política para el desborde de las llamadas, así mismo, la solución cuenta con la posibilidad de ofrecer dos menús, uno para el día (horario hábil de atención), y uno para la noche (informativo), de acuerdo con las solicitudes del CONALEP.
- Cuando se seleccione una opción inválida en el menú, se transferirá la llamada al inicio de este. Si no se selecciona ninguna opción del menú, la llamada se transferirá automáticamente al Servicio de Operadora Manual después de un tiempo programable.
- La Operadora Automática cuenta con la facilidad de enrutar la llamada hacia algún número de extensión del CONALEP con o sin DID asociado, siempre y cuando la persona que llama lo conozca y lo digite. El Sistema de Procesamiento de Llamadas IP, puede supervisar la transferencia de la llamada, si el usuario se encuentra en estado libre o desviado a otra extensión, la llamada se transferirá, si el usuario está ocupado, la persona que llama será dirigida al buzón de voz de este, en caso de Cuenta con este servicio.
- El Servicio de Operadora Automática incluida en el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition opera de forma centralizada en los sitios donde lo solicite el CONALEP, atendiendo cada uno, las llamadas entrantes de los números de grupo de las troncales del sitio asociado.
- Cada solución de Operadora Automática que solicite el CONALEP maneja los puertos de acceso serán definidos por el CONALEP, para las peticiones y/consultas que realicen los usuarios externos e internos.
- La solución de Operadora Automática cuenta con la capacidad de maneja una determinada cantidad de sesiones concurrentes hacia cada uno de los sitios de la Red del CONALEP, conforme a los requerimientos de éstas y con base a la capacidad de puertos solicitados para cada Operadora Automática. En su caso, la asignación de sesiones concurrentes se determinará de común acuerdo entre el administrador del contrato del CONALEP y IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado que resulte adjudicado.
- El Sistema de Procesamiento de Llamadas IP cuenta con la capacidad de desbordar a las Operadoras Automáticas, las llamadas externas que ingresen por los Números de Grupo de las troncales de los sitios, donde se cuente con este tipo de servicios, conforme a los requerimientos que establezca el administrador del contrato del CONALEP.

Manuales para equipos de telefonía IP

IP Productos y Servicios, S.A. de C.V. considera en su propuesta entregar manual del equipo para su instalación, configuración y operación en idioma español, además proporcionará la liga del sitio Web en el cual se puede descargar.

Medios para Reportar Fallas para Equipos de Telefonía IP

- IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado entregará el procedimiento de recepción de reportes y atención de fallas de los equipos, dentro de los cinco (5) días hábiles anteriores a la fecha del inicio del Arrendamiento.
- Se indicará una línea telefónica del fabricante o centro de atención telefónica certificado o aprobado por el fabricante sin costo de llamada para el usuario y un correo electrónico del fabricante, como canales para hacer efectiva la garantía de los equipos.

Requerimientos para equipos de telefonía IP

Los equipos ofertados por IP Productos y Servicios, S.A. de C.V., por partida son nuevos de una misma marca y modelo y cumplen con las características técnicas, solicitadas en el presente anexo técnico.
IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica la entrega de la siguiente documentación:

- Carta original, en papel membretado y vigente, firmada por el fabricante de los equipos a ofertar detallando marca y modelo de los equipos propuestos y que certifique la configuración de los equipos propuestos para cada una de las partidas descritas en el presente anexo técnico.
- Carta original, en papel membretado y vigente, firmada por el fabricante de los equipos a ofertar en donde designe al licitante como distribuidor autorizado y certificado de los equipos propuestos.
- Carta original, en papel membretado y vigente, firmada por el fabricante de los equipos a ofertar en donde manifieste que IP Productos y Servicios, S.A. de C.V. cuenta con personal certificado por el fabricante para la instalación, configuración y puesta a punto de los equipos propuestos.
- Carta original, en papel membretado y firmada por el fabricante en la que se relacionen sus centros de servicio autorizados.
- Carta original del fabricante en la que se manifiesta que cuentan con la infraestructura técnica y de servicio y que garantiza la existencia de refacciones para el mantenimiento de los bienes objeto del arrendamiento, durante la vigencia del contrato de arrendamiento.
- Carta original del fabricante en la que se manifiesta que los equipos objeto del arrendamiento, no tendrán un anuncio de fin de vida ni anuncio de fin de mantenimiento durante la vigencia del contrato de arrendamiento.
- IP Productos y Servicios, S.A. de C.V. presenta dentro de su propuesta técnica los documentos impresos con los que se acredite el cumplimiento de las normas y certificaciones (Carta del Fabricante) requeridas en el presente anexo técnico, en la ficha técnica deberá identificar cada una de las características técnicas solicitadas para los equipos descritos en las diferentes partidas. Los catálogos o folletos están impresos en idioma español; de no ser así, se acompañan a estos con una traducción al español. En caso de que alguna referencia solicitada no se refleje en la ficha técnica del equipo, pero si este soportado por el fabricante, el CONALEP aceptará una carta de fabricante mencionando el soporta de la funcionalidad solicitada.
- Carta original, en papel membretado y firmada por IP Productos y Servicios, S.A. de C.V. en el que manifiesta que los equipos que ofertará y suministrará son nuevos, no armados, no remanufacturados y de fabricación reciente (máximo dos años).

Capacitación

- IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado incluye en su propuesta curso de capacitación del equipo para Red telefonía IP impartido en un centro de capacitación autorizado y avalado por el fabricante, para al menos dos personas, con una duración mínima de 40 horas.

- En caso de que el CONALEP lo requiera, IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado incluye en su propuesta curso de capacitación del equipo para videoconferencia impartido en un centro de capacitación autorizado y avalado por el fabricante, para al menos dos personas, con una duración mínima de 40 horas.
- Los cursos de capacitación incluyen la operación, administración y configuración de los bienes propuestos.
- La fecha en que se realizará la capacitación será definida entre IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado y el CONALEP.

Instalación

La instalación, configuración y puesta a punto de los bienes ofertados será realizada por parte de IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado y de común acuerdo con el CONALEP.

- Para la instalación, configuración y puesta a punto de los bienes ofertados, IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado entregará un plan de trabajo al Administrador del Contrato del CONALEP, quien aprobará dicho plan.
- El CONALEP determinará la ubicación física en donde se requiera instalar los equipos.

Entregables para equipos de telefonía IP

Los entregables se definen como IP Productos y Servicios, S.A. de C.V. considera en su propuesta que la entrega de los equipos, documentación inicial, final y reportes mensuales inherentes al presente anexo técnico, los cuales se derivan de la contratación específica que se celebre al amparo del contrato marco, es responsabilidad de IP Productos y Servicios, S.A. de C.V. entregarlos al Administrador del Contrato del CONALEP.

El Administrador del Contrato y el representante designado por IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado serán responsables de dar seguimiento y cumplimiento a lo establecido en el presente anexo técnico.

IP Productos y Servicios, S.A. de C.V. entregará de forma electrónica, archivos con la relación en la que se indique marca, modelo y número de serie, así como las remisiones de entrega firmadas por el responsable de las áreas que designe el Administrador del Contrato del CONALEP para IP Productos y Servicios, S.A. de C.V. considera en su propuesta que la entrega de los equipos.

Dentro de los primeros quince (15) días hábiles posteriores a la adjudicación del contrato, IP Productos y Servicios, S.A. de C.V. entregará lo siguiente:

- Cronograma de actividades.
- El plan de trabajo detallado para la instalación, configuración y puesta a punto de los bienes ofertados para el CONALEP, con su debida aprobación. El plan de trabajo incluye la definición, desarrollo y mantenimiento de un plan de pruebas para validar la correcta instalación, configuración y puesta a punto.
- IP Productos y Servicios, S.A. de C.V. entregará una matriz de escalamiento que permite al CONALEP contactar al personal designado por IP Productos y Servicios, S.A. de C.V. para asegurar el cumplimiento conforme al presente anexo técnico. De igual manera, IP Productos y Servicios, S.A. de C.V. proporcionará un documento donde se plasme el procedimiento que seguirá para resolución de incidentes.

IP Productos y Servicios, S.A. de C.V. entregará el procedimiento de recepción de reportes para la atención y resolución de fallas de los equipos dentro de los cinco (5) días hábiles posteriores a la adjudicación del Contrato.

IP Productos y Servicios, S.A. de C.V. entregará la memoria técnica dentro de los primeros diez (10) días hábiles posteriores a la puesta en operación de los equipos para de telefonía IP y videoconferencia conteniendo lo siguiente:

- Relación de equipos utilizados para la implementación de la solución.
- Diagramas de conectividad. Los diagramas se incluyen dentro de la memoria técnica en formato electrónico (Microsoft Office Visio).
- Registro de las pruebas de conectividad realizadas.
- IP Productos y Servicios, S.A. de C.V. incluye una copia del respaldo de los equipos de la solución implementada en medio magnético.
- En caso de sustitución de equipos o cambio de configuración en los mismos, la memoria técnica deberá ser actualizada por IP Productos y Servicios, S.A. de C.V.

Entregables mensuales

Entrega dentro de los primeros 10 días hábiles siguientes a la conclusión del mes que se pretende facturar, de los siguientes documentos:

- Relación total de los equipos entregados en arrendamiento por parte de IP Productos y Servicios, S.A. de C.V. a entera satisfacción del CONALEP.
- Reporte de incidencias.

Mesa de ayuda para equipos de telefonía IP

IP Productos y Servicios, S.A. de C.V. pondrá a disposición del CONALEP una mesa de ayuda dentro de los cinco (5) días hábiles anteriores a la fecha del inicio del Arrendamiento para que el CONALEP, mediante la presentación de reportes, pueda solicitar soporta y asistencia técnica para la atención, diagnóstico y solución de fallas y orientación de uso de los equipos de Telefonía IP, para lo cual IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado proporcionará números convencionales y celulares, además de correos electrónicos del representante designado por IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado.

Niveles de atención para equipos de telefonía IP

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que los tiempos de atención y solución de fallas requeridos son:

- La garantía en sitio de los bienes se cubrirá en las instalaciones del CONALEP en donde se encuentre instalado el equipo.
- Para el Equipo de procesamiento de llamadas IP marca Avaya, modelo IP Office Server Edition, Gateway con capacidad supervivencia, Gateway para troncales marca Avaya, modelo IP Office 500 v2 y el Equipo Multipunto de videoconferencia (MCU) (partidas 1, 2, 3 y 13), el tiempo de atención vía telefónica será en un tiempo no mayor a 15 minutos, y se brindará durante 24 horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio, ésta deberá otorgarse dentro de las 6 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique reemplazo de partes, el tiempo de solución máximo será de 24 horas naturales para la Ciudad de México, Área Metropolitana y zonas foráneas, a partir del levantamiento del reporte.
- Para las partidas 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15 y 16, el tiempo de atención vía telefónica será en un tiempo no mayor a 15 minutos, y se brindará durante 24 horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio, ésta deberá otorgarse dentro de las 24 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique reemplazo de partes, el tiempo de

solución máximo será de 48 horas naturales para la Ciudad de México, Área Metropolitana y para las zonas foráneas, a partir del levantamiento del reporte.

De implicarse la reparación de los equipos señalados en las dos viñetas anteriores, se atenderá lo siguiente:

- Si el tiempo de reparación excede el tiempo establecido en los puntos antes mencionados, al día siguiente hábil, IP Productos y Servicios, S.A. de C.V. entregará un equipo de respaldo equivalente mientras se soluciona el problema.
- Si la reparación excede los 30 días naturales a partir de la fecha del reporte, al día siguiente hábil, IP Productos y Servicios, S.A. de C.V. entregará a cambio, instalar, configurar y poner a punto un equipo nuevo con las características iguales o superiores al arrendado.
- Si el equipo presenta más de cinco fallas dentro de un periodo de 30 días naturales, IP Productos y Servicios, S.A. de C.V. lo sustituirá por uno de características iguales o superiores, en un plazo no mayor a un día hábil a partir del quinto reporte de falla en el mes para la UODCDMX y sus planteles y dos días hábiles a partir del quinto reporte de falla en el mes para la RCEO y sus planteles, incluyendo el tiempo de atención.

En caso de reasignación o reubicación, se atenderá lo siguiente:

- Dicha solicitud deberá atenderse a partir del levantamiento del reporte por parte del Administrador del Contrato, en un plazo no mayor a dos (2) días hábiles cuando la reasignación o reubicación se realice dentro del mismo inmueble, y dentro del plazo de tres (3) días hábiles cuando la reasignación o reubicación de los equipos deba efectuarse en inmuebles diferentes del CONALEP, siempre que éstos se localicen en la UODCDMX y sus planteles. Los plazos antes mencionados podrán ampliarse hasta por cinco (5) días hábiles cuando las reasignaciones o reubicaciones se realicen en la RCEO y sus planteles. En todos los casos, se considerarán días laborables y en un horario de 9:00 a 19:00 horas. Dichos periodos incluyen el tiempo de atención.

Otros supuestos:

- En caso de robo o daño de los equipos destinados al arrendamiento por causas atribuibles al licitante durante los procesos de entrega, o durante su instalación y/o configuración, IP Productos y Servicios, S.A. de C.V. los sustituirá por equipos con características iguales o superiores, dentro del plazo señalado en el apartado "Plazo de entrega de los equipos", sin otorgarse plazos adicionales para tal efecto y sin costo adicional para el CONALEP.
- IP Productos y Servicios, S.A. de C.V. proporcionará durante la vigencia de la garantía los niveles de atención descritos en la siguiente tabla:

Actividad	Descripción	Alcance	Nivel de servicio
Entregables	IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado entregará los equipos arrendados. IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado entregará de forma electrónica, archivos con la relación en el que se indique marca, modelo y número de serie, así como las remisiones de entrega firmadas	Arrendamiento de equipo para telefonía IP	Dentro de los 90 días naturales a partir del día hábil siguiente a la fecha de adjudicación del contrato.

Actividad	Descripción	Alcance	Nivel de servicio
	por el responsable de las áreas que designe el Administrador del Contrato para IP Productos y Servicios, S.A. de C.V. considera en su propuesta que la entrega de los equipos.		
Entregables	IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado deberá de entregar: Cronograma de actividades. El plan de trabajo detallado para la instalación, configuración y puesta a punto de los bienes ofertados para el CONALEP, con su debida aprobación. El plan de trabajo incluye la definición, desarrollo y mantenimiento de un plan de pruebas para validar la correcta instalación, configuración y puesta a punto. IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado entregará una matriz de escalamiento que permite al CONALEP contactar al personal designado por IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado para asegurar el cumplimiento conforme al presente anexo técnico. De igual manera, IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado proporcionará un documento donde se plasme el procedimiento que seguirá para resolución de incidentes.	Arrendamiento de equipo para telefonía IP	Dentro de los primeros quince (15) días hábiles posteriores a la adjudicación del contrato.
Entregables	IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado entregará el procedimiento de recepción de reportes y atención de fallas de los equipos, dentro de los cinco (5) días hábiles posteriores a la adjudicación del contrato.	Arrendamiento de equipo para telefonía IP	dentro de los cinco (5) días hábiles posteriores a la adjudicación del contrato.
Entregables	Memoria técnica conteniendo: Relación de equipos utilizados para la implementación de la solución. Diagramas de conectividad. Los diagramas se incluyen dentro de la memoria técnica en formato electrónico (Microsoft Office Visio).	Arrendamiento de equipo para telefonía IP	Dentro de los primeros diez (10) días hábiles posteriores a la puesta en operación de los equipos para de telefonía IP.

Actividad	Descripción	Alcance	Nivel de servicio
	Registro de las pruebas de conectividad realizadas. IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado incluye una copia del respaldo de los equipos de la solución implementada en medio magnético. En caso de sustitución de equipos o cambio de configuración en los mismos, la memoria técnica deberá ser actualizada por IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado.		
Entregables mensuales	IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado entregará: Relación total de los equipos entregados en arrendamiento por parte de IP Productos y Servicios, S.A. de C.V. a entera satisfacción del CONALEP. Reporte de incidencias.	Arrendamiento de equipo para telefonía IP	Dentro de los primeros diez (10) días hábiles siguientes a la conclusión del mes que se pretende facturar.
Mesa de Ayuda	Poner a disposición del CONALEP una Mesa de Ayuda para el levantamiento de reportes de fallas de los equipos.	Arrendamiento de equipo para telefonía IP	Dentro de los cinco (5) días hábiles anteriores a la fecha del inicio del Arrendamiento.
Atención de fallas	Atención y reparación de fallas y problemas relacionadas con los equipos puestos en marcha en el CONALEP como parte del arrendamiento.	Arrendamiento de equipo para telefonía IP.	• Para el equipo de procesamiento de llama-das IP, Gateway con capacidad supervivencia, Gateway para troncales marca Avaya, modelo IP Office 500 v2 y el Equipo Multipunto de videoconferencia (MCU) (partidas 1, 2, 3 y 13), el tiempo de atención vía telefónica será en un tiempo no mayor a 15 minutos, y se brindará durante 24 horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio, ésta deberá otorgarse dentro de las 6 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique reemplazo de partes, el tiempo de solución máximo será de 24 horas naturales para la Ciudad de México, Área Metropolitana y zonas foráneas, a partir del levantamiento del reporte. • Para las partidas 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15 y 16, el tiempo de atención vía telefónica será en un tiempo no mayor a 15 minutos, y se brindará durante 24

Actividad	Descripción	Alcance	Nivel de servicio
			horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio, ésta deberá otorgarse dentro de las 24 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique reemplazo de partes, el tiempo de solución máximo será de 48 horas naturales para la Ciudad de México, Área Metropolitana y para las zonas foráneas, a partir del levantamiento del reporte. De implicarse la reparación de los equipos señalados en las dos viñetas anteriores, se atenderá lo siguiente: - Si el tiempo de reparación excede el tiempo establecido en los puntos antes mencionados, al día siguiente hábil, IP Productos y Servicios, S.A. de C.V. entregará un equipo de respaldo equivalente mientras se soluciona el problema. - Si la reparación excede los 30 días naturales a partir de la fecha del reporte, al día siguiente hábil, IP Productos y Servicios, S.A. de C.V. entregará a cambio, instalar, configurar y poner a punto un equipo nuevo con las características iguales o superiores al arrendado - Si el equipo presenta más de cinco fallas dentro de un periodo de 30 días naturales, IP Productos y Servicios, S.A. de C.V. lo sustituirá por uno de características iguales o superiores, en un plazo no mayor a un día hábil a partir del quinto reporte de falla en el mes para la Ciudad de México y Área Metropolitana y dos días hábiles a partir del quinto reporte de falla en el mes para las zonas foráneas incluyendo el tiempo de atención.
Reasignación o reubicación de los equipos otorgados en arrendamiento por IP Productos y Servicios, S.A. de C.V. en la Ciudad de México, zona	Atención para la reasignación o reubicación de los equipos en las instalaciones o sedes del CONALEP.	Todos los equipos y servicios objeto del arrendamiento que se detallan en el presente Anexo Técnico e instalados en la Ciudad de México, zona	En caso de reasignación o reubicación, se atenderá lo siguiente: Dicha solicitud deberá atenderse a partir del levantamiento del reporte por parte del Administrador del Contrato, en un plazo no mayor a dos (2) días hábiles cuando la reasignación o reubicación se realice dentro del mismo inmueble y en un plazo de tres

Actividad	Descripción	Alcance	Nivel de servicio
Metropolitana y zonas foráneas		Metropolitana y zonas foráneas.	(3) días hábiles cuando la reasignación o reubicación de los equipos deba efectuarse en inmuebles diferentes del CONALEP, siempre que éstos se localicen en la Ciudad de México y Área Metropolitana. Los plazos antes mencionados podrán ampliarse a cinco (5) días hábiles cuando las reasignaciones o reubicaciones se realicen en las zonas foráneas. En todos los casos se considerarán días laborables y en un horario de 9:00 a 19:00 horas. Dichos periodos incluyen el tiempo de atención.

De tenerse incumplimientos por parte de IP Productos y Servicios, S.A. de C.V., IP Productos y Servicios, S.A. de C.V. considera en su propuesta que los tiempos de atención y solución de fallas o la petición de la reasignación o reubicación de los equipos, así como en los niveles de atención señalados anteriormente, se aplicarán las deductivas a que haya lugar, de conformidad con el apartado "Penas convencionales y Deductivas".

Vigencia de la contratación

El "Servicio de Arrendamiento de Equipo Telefónico IP", que corresponde al proyecto "Operación de las comunicaciones y conectividad institucional", en adhesión al contrato marco para el "Arrendamiento de Equipo para Telefonía IP y videoconferencia para las Dependencias y Entidades de la Administración Pública Federal" deberá contratarse con una vigencia por el periodo comprendido un día posterior a la notificación del fallo al 31 de diciembre de 2025.

Plazo de entrega de los equipos

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que la entrega de los equipos, su instalación, configuración y puesta a punto se realizará en un plazo no mayor a noventa (90) días naturales a partir del día hábil siguiente a la fecha de adjudicación del contrato.

Se hará constar la entrega en mención, a través de acta administrativa levantada para ello, suscrita por el Administrador del Contrato, IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado y de los testigos respectivos.

De tenerse incumplimientos por parte de IP Productos y Servicios, S.A. de C.V. en los tiempos señalados para la realización de las entregas iniciales o posteriores, se aplicarán las penas convencionales a que haya lugar, de conformidad con el apartado "Penas Convencionales y Deductivas".

Penas convencionales y deductivas

De conformidad con el artículo 53 y 53 BIS de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), 95, 96 y 97 de su Reglamento el "CONALEP" aplicará con motivo de incumplimiento en la entrega del servicio, las penas convencionales de acuerdo con lo siguiente:

En el arrendamiento:

IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado se obliga a pagar al CONALEP una pena convencional del 2% sobre el monto mensual del pago previsto para los equipos no entregados, instalados, configurados y puestos en marcha, en un plazo no mayor a 90 días naturales a partir del día hábil siguiente a la fecha de adjudicación del contrato, entregado a través de acta administrativa levantada para ello, suscrita por el Titular de la Dirección de Tecnologías de la Información y la Comunicación, quien funge como Administrador del Contrato, debidamente firmada por el oferente adjudicado y los testigos respectivos, por cada día natural de atraso.

La misma pena se aplicará por cada día natural de atraso, en el caso de que el oferente adjudicado no proporcione la mesa de ayuda dentro del plazo establecido de 5 días hábiles anteriores a la fecha del inicio del Arrendamiento, verificando que la mesa permita la solicitud de soporta y asistencia técnica para la atención, diagnóstico y solución de fallas y orientación de uso de los equipos de Telefonía IP, para lo cual el oferente proporcionará números convencionales y celulares, además de correos electrónicos del representante por el designado.

IP Productos y Servicios, S.A. de C.V. considera en su propuesta que el total de la pena convencional no podrá exceder el monto de la garantía de cumplimiento sin considerar el impuesto al valor agregado (I.V.A), de conformidad con lo establecido en el artículo 53 de la LAASSP.

En los entregables:

IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado se obliga a pagar al CONALEP una pena convencional por no presentar los entregables mensuales en los plazos establecidos en el apartado "Entregables" del Anexo 1. "Descripción Técnica del Arrendamiento". Dicha pena será del 2% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso.
El total de la pena convencional no podrá exceder el monto de la garantía de cumplimiento sin considerar el impuesto del valor agregado (I.V.A), de conformidad con lo establecido en el artículo 53 de la LAASSP.

Deductivas:

Se aplicará una deductiva al oferente por el cumplimiento parcial o deficiente en el arrendamiento. Dicha deductiva será del 2% sobre el monto de la facturación del mes inmediato anterior correspondiente al equipo que no sea sustituido o reparado en los términos y plazos establecidos en el presente anexo por cada día natural de atraso, lo anterior, de conformidad en lo establecido en el artículo 53 bis de la LAASSP.

Igual porcentaje, se aplicará como deductiva en los casos que el oferente suspenda el arrendamiento por cualquier causa injustificada, esto es fuera de los casos de fuerza mayor o caso fortuito debidamente acreditado y documentado, por cada día natural que suspenda el arrendamiento, independientemente de que no se pagaría arrendamiento por el tiempo que dure la suspensión.

Adicional a lo anterior, se aplicarán deductivas por cada día natural de incumplimiento en IP Productos y Servicios, S.A. de C.V. considera en su propuesta que los tiempos de atención y solución de fallas o la petición de la reasignación o reubicación de equipos, así como en los niveles de atención señalados en el apartado "Niveles de atención".

En caso de que los conceptos en los que subsistan el cumplimiento parcial o la deficiencia sean equivalentes al importe de la garantía otorgada por IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado, el Administrador del Contrato podrá optar por cancelar total o parcialmente el arrendamiento aplicando la pena convencional máxima al licitante, lo anterior, en términos del artículo 100 del Reglamento de la Ley antes citada, o bien, optar por rescindir el contrato en término de la Ley.

Garantía de cumplimiento

1.- Las obligaciones derivadas de la suscripción del contrato respectivo serán garantizadas por IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado mediante la entrega de una póliza de fianza expedida por una institución autorizada en los términos de las disposiciones aplicables, a favor del "Colegio Nacional de Educación Profesional Técnica"; dicha garantía deberá constituirse por el 10% del monto total del contrato, de conformidad con los Artículos 81 fracción II y 85 fracción III del Reglamento de la LAASSP.

- La garantía será entregada dentro de los 10 días naturales siguientes a la fecha de firma del contrato respectivo. Para la expedición de la fianza se deberá observar el texto el que se entregará al ganador.
- La garantía de cumplimiento del contrato será indivisible.

2.- IP Productos y Servicios, S.A. de C.V. considera en su propuesta que a la entrega de los bienes, presentará el escrito al que alude la Regla 9 "FORMATO PARA DAR CUMPLIMIENTO A LA REGLA 9 DE LAS REGLAS PARA LA DETERMINACIÓN, ACREDITACIÓN Y VERIFICACIÓN DEL CONTENIDO NACIONAL DE LOS BIENES QUE SE OFERTAN Y ENTREGAN EN LOS PROCEDIMIENTOS DE CONTRATACIÓN, ASÍ COMO LA APLICACIÓN DEL REQUISITO DE CONTENIDO NACIONAL EN LA CONTRATACIÓN DE OBRAS PÚBLICA", a fin de ratificar la manifestación que presenten en su propuesta referente a la Regla No. 8 del grado de contenido nacional de los bienes ofertados, por lo que el área encargada de recibir los bienes deberá conservar los documentos originales y proporcionará copia al área contratante a efecto de que exista evidencia en el expediente de contratación.

3.- IP Productos y Servicios, S.A. de C.V. presenta carta en papel membretado con firma autógrafa (no rúbrica), en el formato que le proporcione el CONALEP, en la que se compromete a cumplir satisfactoriamente con las especificaciones requeridas en el texto de la convocatoria y sus anexos están libres de defectos y vicios ocultos, y en caso de ser adjudicado, el servicio cumplirá con las mismas características a las ofertadas.

Administrador del contrato

El Titular de la Dirección de Tecnologías de la Información y la Comunicación, quien es administrador del contrato, será el responsable de calcular y notificar a IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado, las penas convencionales y las deductivas que se hubieran determinado en el periodo de evaluación. Para la recepción del servicio de arrendamiento, el Administrador del Contrato verificará el cumplimiento de las condiciones establecidas para el otorgamiento de la adquisición, de conformidad con lo establecido en el penúltimo párrafo del artículo 84 del reglamento de la LAASSP.

Confidencialidad

IP Productos y Servicios, S.A. de C.V. presenta en su propuesta técnica carta en papel membretado firmada por el representante
legal, donde se compromete a mantener absoluta confidencialidad de la información a la cual tenga acceso de forma directa o a través del personal que otorgue el arrendamiento, siendo responsable de cada uno de los integrantes del personal asignado para el desarrollo y operación del proyecto, respetando el manejo correcto de la información.

Toda la información a la que tenga acceso el personal que el oferente designe para el cumplimiento del contrato, es considerada de carácter confidencial conforme a lo establecido en la Ley General de Transparencia y Acceso a Información Pública.

IP Productos y Servicios S.A. de C.V.

Responsabilidad laboral

IP Productos y Servicios, S.A. de C.V. en caso de resultar adjudicado se constituye como único patrón del personal que ocupe para llevar a cabo la prestación del arrendamiento y será el único responsable de las obligaciones que en virtud de disposiciones legales y demás ordenamientos en materia de trabajo y Seguridad Social, les deriven frente a dicho personal, liberando al CONALEP de cualquier responsabilidad laboral al respecto.

Cotización

IP Productos y Servicios, S.A. de C.V. cotiza por precios unitarios sin incluye el I.V.A y en moneda nacional (pesos mexicanos), conforme al presente anexo técnico y a los formatos que se acompañan. Las cotizaciones se presentan por precios unitarios, considerando el periodo comprendido un día posterior a la notificación del fallo al 31 de diciembre de 2025.

Protesto lo necesario
A T E N T A M E N T E

Rubén Plaza Aguilar
Representante Legal
IP Productos y Servicios S.A. de C.V.

IP Productos y Servicios S.A. de C.V.

RFC: IPS0703142W1

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA DETALLANDO MARCA Y MODELO

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Por medio de la presente hago de su conocimiento, que la empresa **Avaya Communication de México, S.A. de C.V.**, certifica la configuración y el diseño de los equipos propuestos para cada una de las partidas descritas en el presente anexo técnico ofertado por **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.**, de los productos marca Avaya para el proceso en referencia.

Referencia	Descripción del producto	Marca	Modelo
5.1	Equipo de Procesamiento de llamadas IP	AVAYA	Avaya Aura Comminication Manager / Avaya Aura Session Manager / Avaya Aura System Manager, Avaya IP Office Server/Select
5.2	Gateway con capacidad de supervivencia	AVAYA	G450 Media Gateway / G430 Media Gateway, Avaya IP500 v2
5.5	Gateway para troncales	AVAYA	G450 Media Gateway / G430 Media Gateway, Avaya IP500 v2
5.5	E1 R2 MODIFICADO	AVAYA	MM710B, Avaya IP Office IP500 Trunk Card
5.5	Troncales Analógicas (FXO)	AVAYA	MM711, Avaya IP Office IP500 Trunk Card
5.6.1	Terminal IP Básica	AVAYA	Avaya J159
5.6.2	Terminal IP Semi-ejecutiva	AVAYA	Avaya J189
5.6.3	Terminal IP Ejecutiva	AVAYA	Avaya Vantage K175
5.6.4	Teléfonos para sala de conferencia	AVAYA	Avaya J159
5.7	Adaptadores de teléfonos analógicos (ATA)	AVAYA	Avaya IP500 v2
5.9	Servicio de teléfono basado en software	AVAYA	Avaya IX Workplace
5.10	Correo de voz con servicios de mensajería	AVAYA	Avaya IX Messaging, Avaya Voicemail Pro
5.13	Servicios de movilidad	AVAYA	Avaya IX Workplace/ Avaya Session Border Controller for Enterprise
5.14	Controlador de borde de sesión (Session Border Controller)	AVAYA	Avaya Session Border Controller for Enterprise
6.1	Equipo Terminal para sala de videoconferencia	AVAYA	Avaya IX Room System XT 5000
6.2	Equipo Multipunto de Videoconferencia (MCU)	AVAYA	Avaya Equinox Media Server
6.3	Plataforma de Administración de la Solución de Videoconferencia	AVAYA	Avaya Equinox Management
6.4	Plataforma de Grabación de la Solución de Videoconferencia	AVAYA	Avaya Equinox Streaming and Recording
6.5	Equipo de Registro Gatekeeper/Sip Server	AVAYA	Avaya Equinox Management / Avaya Session Border Controller for Enterprise

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

IP Productos y Servicios S.A. de C.V.

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA DISTRIBUIDOR AUTORIZADO

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Presente,

Por medio de la presente, hago de su conocimiento, que la empresa **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.,** es distribuidor autorizado de **Avaya Communication de México, S.A. de C.V.**, y certificado de los equipos propuestos de la marca Avaya en el presente anexo técnico.

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto que crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA PERSONAL CERTIFICADO

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Presente.

Hago de su conocimiento, que la empresa **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.,** cuenta con personal certificado para la instalación, configuración y puesta a punto de los equipos propuestos de la marca Avaya en el presente **proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.**

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto que crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA CENTROS DE SERVICIO

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Por medio de la presente hago de su conocimiento que Avaya cuenta con el centro de servicio autorizado para soporte y cobertura a Nivel Nacional en Av. Presidente Masaryk #111. Piso 6. Col Polanco V Sección en la CDMX.

- Línea Telefónica de atención de fabricante: Ciudad de México (55) 5278 78 78 o fuera de la Ciudad de México al 01 8000-00AVAYA.
- Correo Electrónico del fabricante para atención: calaccs@avaya.com o via: https://support.avaya.com/support/dashboard.action

Y además cuenta con los siguientes depósitos para garantizar la entrega de refaccionamiento a nivel nacional:

Site Name	City	Country	Address	Zip Code	3PL vendor
MX-MTY	Monterrey	MEXICO	Prolongación Pino Suárez # 3005	64410	DHL
MX-TIJ	Tijuana	MEXICO	Blvd Juan Alessio # 12440, Parque Industrial Pacifico II	22490	DHL
MX-GDL	Guadalajara	MEXICO	Parque Logístico Tlaquepark Periférico Sur Manuel Gómez Morin #5890 Col. Artesanos Tlaquepaque Jalisco	45590	DHL
MX-MEX	Ciudad de México	MEXICO	Calle Nicanor Arvide no. 425. Col. Arvide	1280	DHL
MX-QRO	Querétaro	MEXICO	Islas Baleares No. 19 Bosques del Acueducto Querétaro CP 76020	76020	DHL
MX-MZT	Mazatlán	MEXICO	Av. Ejército Nacional #3 Emiliano Zapata Col. Tierra Libertad	82150	DHL
MX-CUN	Cancún	MEXICO	Av. Francisco I Madero Derivación Esq. Calle 133 super manzana 101 Manzana 54 Lote 16, Zona Urbana	77520	DHL

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto que crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA REFACCIONES

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Presente,

Por este medio y a nombre de mi representada **AVAYA COMMUNICATION DE MEXICO S.A. DE C.V.,** manifiesto que contamos con infraestructura técnica y de servicio garantizando la existencia de refacciones para el mantenimiento de los equipos de la marca Avaya, ofertados por la empresa **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.,** no saldrán de soporte en México durante los próximos 5 años posteriores al fallo, por lo que se garantiza la disponibilidad de los equipos y su refaccionamiento durante dicho periodo.

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto que crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

IP Productos y Servicios S.A. de C.V.

RFC: IPS0703142W1

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA NO ANUNCIO FIN DE VIDA

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Presente,

Por medio de la presente y a nombre de mi representada AVAYA COMMUNICATION DE MEXICO S.A. DE C.V., manifiesto que los equipos objeto del presente contrato de arrendamiento, ofertados por la empresa **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.,** se encuentran vigentes y de línea, los cuales no tienen anuncio de fin de vida o venta, por lo que existirán refacciones y soporte técnico durante los 5 (cinco) posteriores al fallo, garantizando la disponibilidad de los equipos y su refaccionamiento durante la vigencia del contrato de arrendamiento.

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto que crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Soporte de Funcionalidades Soportadas.
Equipos de Telefonía IP.

Mi representada afirma cabal cumplimiento en el requerimiento descrito en todas y cada una de las funcionalidades descritas, sin embargo; lo resuelve a través de otros protocolos, características y funcionalidades más actuales o similares que reemplazan o sustituye a lo citado en el presente anexo técnico del **Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.".**

Las marca tecnológica que represento e incluyo a través de mi Distribuidor autorizado **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.,** en el presente " **Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.**", cumple cabalmente con el servicio que describe y los fines para los cuales se solicita esta solución, sin embargo se solicitan en la redacción del presente anexo varias especificaciones técnicas y protocolos, los cuales, las marca que represento los realizan de manera distinta con funcionalidades y protocolos más avanzados y de nueva generación.

- En documentación de mi representada no es demostrable la palabra "ITU-T G.168", sin embargo, dado que la recomendación mencionada hace referencia a Digital Network Echo Cancellers (compensadores de eco de redes digitales), mediante esta carta hago constar el soporte de este requerimiento (ITU-T G.168) con capacidades de hardware provistas por la tarjetería de troncales digitales E1 (tarjeta modelo MM71OB) la cual soporta cancelación de eco en cualquier dirección.

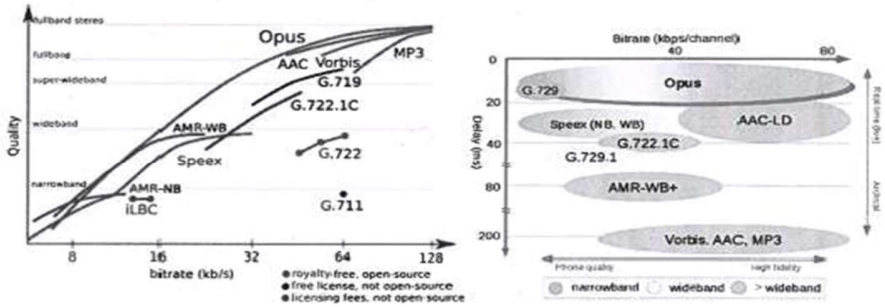
Hacemos referencia a la siguiente liga:
https://compranetinfo.hacienda.gob.mx/descargas/consolidadas/20191114_Respuestas consolidado.pdf

- Mi representada garantiza el cumplimiento al 100% de las funcionalidades solicitadas sin degradación de las mismas al integrar elementos periféricos de terceros como son: Balums, ATAs, Tarificador, Pantallas para la Solución de videoconferencia y Diademas Inalámbricas, por lo que hago constar y avalo la integración nativamente con los equipos propuestos por **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.,** sin que esto represente ni un riesgo en la operación, funcionalidades ni servicios, garantizando en todo momento el cumplimiento de lo solicitado en cada uno de estos puntos.
- En la documentación de mi representada no son demostrables los códecs: iLBC, G.722.1, G.722.2 ni AAC-LD, sin embargo, por medio de la presente garantizo el cumplimiento de las características técnicas solicitadas mediante el soporte de Opus, el cual es un codec muy versátil y abierto, mismo que ha demostrado tener una mejor calidad que todos los demás códecs de audio, ya que el mismo cubre y supera las especificaciones de los códecs antes mencionados (mayor espectro de frecuencia, más amplio rango de bitrate, mejor tolerancia a latencia, etc), cubriendo desde calidad telefónica hasta audio de alta fidelidad como se indica en la tabla que se presenta a continuación:

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

	Sample Rate	Bit Rate	Latency	Constant bitrate (CBR)	Variable bitrate (VBR)	Stereo	Multichannel
OPUS	8-48 Khz	6-510 kbit/s	5-66.5 ms	Si	Si	Si	Si hasta 255 canales
G.722.1	16 Khz	24, 32 kbit/s	40 ms	Si	no	no	no
G.722.2	16 Khz	6.60, 8.85, 12.65, 14.25, 15.85, 18.25, 19.85, 23.05, 23.85 kbit/s	25 ms	si	si	si:solo en mpeg-4	no
ILBC	8 Khz	13.33, 15.20 kbit/s	25, 40 ms	Si	no	no	no
AAC-LD	22.05-48 Khz	112-320 kbit/s	20 ms		Si	si	si



Fuente: opus-codec.org/comparison/

- En la documentación de mi representada no es demostrable la característica de 800x480 pixeles, sin embargo, se está incluyendo una Terminal IP con pantalla táctil capacitiva de 5" con capacidades de color de alta resolución grafico mismas que superan y solventan las funcionalidades, servicios y operación requerida para la Terminal IP Semi Ejecutiva.

Hacemos referencia a la siguiente liga:
https://compranetinfo.hacienda.gob.mx/descargas/consolidadas/20191114_Respuestas consolidado.pdf

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto que crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

IP Productos y Servicios S.A. de C.V.

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA CUMPLIMIENTO DE NORMAS HOJA 1 DE 2

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Presente,

Por medio de la presente hago de su conocimiento que los equipos marca AVAYA:

Referencia	Descripción del producto	Marca	Modelo
5.1	Equipo de Procesamiento de llamadas IP	AVAYA	Avaya Aura Comminication Manager / Avaya Aura Session Manager / Avaya Aura System Manager, Avaya IP Office Server/Select
5.2	Gateway con capacidad de supervivencia	AVAYA	G450 Media Gateway / G430 Media Gateway, Avaya IP500 v2
5.5	Gateway para troncales	AVAYA	G450 Media Gateway / G430 Media Gateway, Avaya IP500 v2
5.5	E1 R2 MODIFICADO	AVAYA	MM710B, Avaya IP Office IP500 Trunk Card
5.5	Troncales Analógicas (FXO)	AVAYA	MM711, Avaya IP Office IP500 Trunk Card
5.6.1	Terminal IP Básica	AVAYA	Avaya J159
5.6.2	Terminal IP Semi-ejecutiva	AVAYA	Avaya J189
5.6.3	Terminal IP Ejecutiva	AVAYA	Avaya Vantage K175
5.6.4	Teléfonos para sala de conferencia	AVAYA	Avaya J159
5.7	Adaptadores de teléfonos analógicos (ATA)	AVAYA	Avaya IP500 v2
5.9	Servicio de teléfono basado en software	AVAYA	Avaya IX Workplace
5.10	Correo de voz con servicios de mensajería	AVAYA	Avaya IX Messaging, Avaya Voicemail Pro
5.13	Servicios de movilidad	AVAYA	Avaya IX Workplace/ Avaya Session Border Controller for Enterprise
5.14	Controlador de borde de sesión (Session Border Controller)	AVAYA	Avaya Session Border Controller for Enterprise
6.1	Equipo Terminal para sala de videoconferencia	AVAYA	Avaya IX Room System XT 5000
6.2	Equipo Multipunto de Videoconferencia (MCU)	AVAYA	Avaya Equinox Media Server
6.3	Plataforma de Administración de la Solución de Videoconferencia	AVAYA	Avaya Equinox Management
6.4	Plataforma de Grabación de la Solución de Videoconferencia	AVAYA	Avaya Equinox Streaming and Recording

IP Productos y Servicios S.A. de C.V.

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA CUMPLIMIENTO DE NORMAS HOJA 2 DE 2

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

6.5	Equipo de Registro Gatekeeper/Sip Server	AVAYA	Avaya Equinox Management / Avaya Session Border Controller for Enterprise

Cumplen con las siguientes normas nacionales o internacionales:

- NOM-019-SCFI-1998 "Seguridad de equipo de procesamiento de datos".
- Energy Star

AVAYA tiene el compromiso y responsabilidad para el cuidado y protección del medio ambiente y cuenta con Normas y Políticas a nivel Global.
https://www.avaya.com/en/about-avaya/corporate-responsibility

AVAYA

Corporate Responsibility Policy

AVAYA

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto que crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

IP Productos y Servicios S.A. de C.V.

CARTA CONTRATO MARCO DEL FABRICANTE AVAYA CAPACITACIÓN

AVAYA

Avaya Communication de México, S.A. de C.V.
Avenida Presidente Masaryk No. 111 – piso 6
Colonia Chapultepec Morales, C.P. 11570
Delegación Miguel Hidalgo, México D.F.
Tel: 5278 7800
www.avaya.com.mx

Ciudad de México a 12 marzo de 2021

SECRETARIA DE HACIENDA Y CREDITO PUBLICO.
COORDINACION DE ESTRATEGIA DIGITAL NACIONAL (CEDN)
Proceso para la celebración del Contrato Marco para el Arrendamiento de Equipo para Telefonía IP y Videoconferencia para las Dependencias y Entidades de la Administración Pública Federal.

Presente.

Por medio de la presente, hago de su conocimiento, que la empresa **IP PRODUCTOS Y SERVICIOS S.A. DE C.V.,** incluye en su propuesta los cursos validados y certificados de los productos de la marca **Avaya**, cumpliendo con la capacitación solicitada en el procedimiento en referencia, los cuales son cursos de capacitación para la operación, administración y configuración de la solución de Servicio de Telefonía IP y Videoconferencia.

La presente carta únicamente se extiende con fines informativos y no constituye ni podrá interpretarse bajo ningún concepto que crea obligaciones o responsabilidades a nombre de **Avaya Communication de México, S.A. de C.V.**

Atentamente,

Arturo Vargas Sadala
Representante Legal
Avaya Communication de México, S.A. de C.V.

TRANSFORMACIONES TECNOLÓGICAS

IP Productos y Servicios S.A. de C.V.

RFC: IPS0703142W1

MANIFESTACIÓN DE QUE LOS EQUIPOS QUE OFERTA Y SUMINISTRARÁ SON NUEVOS, NO ARMADOS, NO REMANUFACTURADOS Y DE FABRICACIÓN RECIENTE

Estado de México a 22 de agosto de 2025.

Colegio Nacional de Educación Profesional Técnica
P R E S E N T E.

De conformidad con lo establecido en la Convocatoria de Invitación a Cuando Menos Tres Personas de Carácter Nacional Electrónica **No. IA-11-L5X-011L5X001-N-44-2025**, relativa a la contratación del **"SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP"**, manifiesto bajo protesta de decir verdad:

El que suscribe Ruben Plaza Aguilar en mi carácter de representante legal de IP Productos y Servicios, S.A. de C.V. en cumplimiento a lo solicitado en el Anexo Técnico.- Requerimientos para equipos de telefonía IP octava viñeta, manifiesta que los equipos que oferta y suministrará son nuevos, no armados, no remanufacturados y de fabricación reciente (máximo dos años).

Protesto lo necesario
A T E N T A M E N T E

Rubén Plaza Aguilar
Representante Legal
IP Productos y Servicios S.A. de C.V.

TRANSFORMACIONES TECNOLÓGICAS

IP Productos y Servicios S.A. de C.V.

RFC: IPS0703142W1

FORMATO M
MANIFESTACIÓN PARA DAR CUMPLIMIENTO A LO DISPUESTO EN EL GRADO DE CONTENIDO NACIONAL (REGLA 8)

Estado de México a 22 de agosto de 2025.

Colegio Nacional de Educación Profesional Técnica
IP Productos y Servicios, S.A. de C.V.
P R E S E N T E.

Me refiero al procedimiento de Invitación a Cuando Menos Tres Personas de Carácter Nacional Electrónica Número IA-11-L5X-011L5X001-N-44-2025 en el que mi representada, la empresa IP Productos y Servicios, S.A. de C.V. participa a través de la proposición que se contiene en el presente sobre, y de conformidad con lo previsto en los artículos 28 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 35 de su Reglamento, manifiesto bajo protesta de decir verdad que es de nacionalidad mexicana y que la totalidad de los bienes que oferta mi representada en dicha proposición, bajo la partida No. UNICA serán producidos en los Estados Unidos de America y contarán con un grado de contenido nacional de cuando menos el 35% como caso de excepción reconocido en la Regla 11.

De igual forma manifiesto bajo protesta de decir verdad, que tengo conocimiento de lo previsto en el artículo 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; en este sentido, me comprometo, en caso de ser requerido, a aceptar una verificación del cumplimiento de los requisitos sobre el contenido nacional de los bienes aquí ofertados, a través de la exhibición de la información documental correspondiente y/o a través de una inspección física de la planta industrial en la que se producen los bienes, conservando dicha información por tres años a partir de la entrega de los bienes a la convocante.

En cumplimiento a lo solicitado en el Anexo Técnico (GARANTÍA DE CUMPLIMIENTO) Punto 2 donde solicita la Convocante presentar escrito a fin de ratificar la manifestación que presenta mi representada referente a la Regla No. 8 del grado de contenido nacional de los bienes ofertados.

Protesto lo necesario
A T E N T A M E N T E

Rubén Plaza Aguilar
Representante Legal
IP Productos y Servicios S.A. de C.V.

TRANSFORMACIONES TECNOLÓGICAS

IP Productos y Servicios S.A. de C.V.

RFC: IPS0703142W1

MANIFESTACIÓN DEL COMPROMISO DE CUMPLIR SATISFACTPRIAMENTE CON LAS ESPECIFICACIONES REQUERIDAS EN EL TEXTO DE LA CONVOCATORIA, SUS ANEXOS Y DE QUE ESTÁN LIBRES DE DEFECTOS Y VICIOS OCULTOS

Estado de México a 22 de agosto de 2025.

Colegio Nacional de Educación Profesional Técnica
P R E S E N T E.

De conformidad con lo establecido en la Convocatoria de Invitación a Cuando Menos Tres Personas de Carácter Nacional Electrónica **No. IA-11-L5X-011L5X001-N-44-2025**, relativa a la contratación del **"SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP"**, manifiesto bajo protesta de decir verdad:

El que suscribe Ruben Plaza Aguilar en mi carácter de representante legal de IP Productos y Servicios, S.A. de C.V. en cumplimiento a lo solicitado en el Anexo Técnico.- Garantía de cumplimiento, Punto 3, se compromete a cumplir satisfactoriamente con las especificaciones requeridas en el texto de la convocatoria y sus anexos están libres de defectos y vicios ocultos, y en caso de ser adjudicado, el servicio cumplirá con las mismas características a las ofertadas.

Protesto lo necesario
A T E N T A M E N T E

Rubén Plaza Aguilar
Representante Legal
IP Productos y Servicios S.A. de C.V.

TRANSFORMACIONES TECNOLÓGICAS

IP Productos y Servicios S.A. de C.V.

RFC: IPS0703142W1

EN CUMPLIMIENTO A LO SOLICITADO EN EL ANEXO TÉCNICO
CONFIDENCIALIDAD

Estado de México a 22 de agosto de 2025.

Colegio Nacional de Educación Profesional Técnica
P R E S E N T E.

De conformidad con lo establecido en la Convocatoria de Invitación a Cuando Menos Tres Personas de Carácter Nacional Electrónica **No. IA-11-L5X-011L5X001-N-44-2025**, relativa a la contratación del **"SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP"**, manifiesto bajo protesta de decir verdad:

El que suscribe Ruben Plaza Aguilar en mi carácter de representante legal de IP Productos y Servicios, S.A. de C.V. en cumplimiento a lo solicitado en el Anexo Técnico.- Confidencialidad, se compromete a mantener absoluta confidencialidad de la información a la cual tenga acceso de forma directa o a través del personal que otorgue el arrendamiento, siendo responsable de cada uno de los integrantes del personal asignado para el desarrollo y operación del proyecto, respetando el manejo correcto de la información.

Toda la información a la que tenga acceso el personal que IP Productos y Servicios, S.A. de C.V. designe para el cumplimiento del contrato es considerada de carácter confidencial conforme a lo establecido en la Ley General de Transparencia y Acceso a Información Pública.

Protesto lo necesario
A T E N T A M E N T E

Rubén Plaza Aguilar
Representante Legal
IP Productos y Servicios S.A. de C.V.

TABLA DE REFERENCIAS

MODELO DE EQUIPO IP OFFICE SERVER EDITION

EQUIPO DE PROCESAMIENTO DE LLAMADAS

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL	URL
El proveedor en su propuesta para adquisición de equipo de telefonía IP con Sistemas de Procesamientos de Llamadas IP deberá cumplir con las condiciones de operación y/o características técnicas siguientes:	PROPUESTA TÉCNICA	PROPUESTA TÉCNICA	IP Productos y Servicios, S.A. de C.V. en su propuesta para adquisición de equipo de telefonía IP con Sistemas de Procesamientos de Llamadas IP considera que cumplir con las condiciones de operación y/o características técnicas siguientes:	IP Productos y Servicios, S.A. de C.V. en su propuesta para adquisición de equipo de telefonía IP con Sistemas de Procesamientos de Llamadas IP considera que cumplir con las condiciones de operación y/o características técnicas siguientes:	PROPUESTA TÉCNICA
Proveer en configuración redundante y de alta disponibilidad el Sistema de Procesamiento de Llamadas IP, de tal manera que ante la falla del procesador de llamadas principal, se tenga el soporte de otro procesador de llamadas que tome el control de todos los dispositivos asociados al procesador de llamadas principal, esto es, se debe mantener el procesamiento de las llamadas de las extensiones IP aún y cuando estén basadas en SIP (Session Initiation Protocol), así como de las extensiones analógicas, con todas sus funcionalidades asociadas, sin afectación de las llamadas establecidas al momento de la falla.	70 PROPUESTA TÉCNICA	IP Office Server Edition IP Office Server Edition provides IP Office telephony capabilities, unified communications, mobility, and collaboration. It also provides high availability, ease of use, and low total cost of ownership (TCO). Targeted at the midsize enterprise, IP Office Server Edition supports up to 150 sites, 3000 users, and comprehensive resilience. IP Office Server Edition Solution provides the following: • A single Server Edition Primary server provides IP Office, Voicemail Pro, and Avaya one-X® Portal for IP Office. • A Server Edition Secondary server increases the capacity and provide resilience. La solución de Supervivencia opera para los teléfonos IP basados en el protocolo SIP, para lo cual IP Productos y Servicios, S.A. de C.V. incluye todo el hardware, software y licenciamiento necesario.	IP Office Server Edition IP Office Server Edition proporciona capacidades de telefonía IP Office, comunicaciones unificadas, movilidad y colaboración. También proporciona alta disponibilidad, facilidad de uso y bajo costo total de propiedad (TCO). Dirigido a la mediana empresa, IP Office Server Edition admite hasta 150 sitios, 3000 usuarios y resiliencia integral. La solución IP Office Server Edition proporciona lo siguiente: • Un único servidor primario de Server Edition proporciona IP Office, Voicemail Pro y Avaya one-X® Portal for IP Office. • Un servidor secundario de Server Edition aumenta la capacidad y proporciona resistencia. La solución de Supervivencia opera para los teléfonos IP basada en el protocolo SIP, para lo cual IP Productos y Servicios, S.A. de C.V. incluye todo el hardware, software y licenciamiento necesario.	IP Office Server Edition IP Office Server Edition proporciona capacidades de telefonía IP Office, comunicaciones unificadas, movilidad y colaboración. También proporciona alta disponibilidad, facilidad de uso y bajo costo total de propiedad (TCO). Dirigido a la mediana empresa, IP Office Server Edition admite hasta 150 sitios, 3000 usuarios y resiliencia integral. La solución IP Office Server Edition proporciona lo siguiente: • Un único servidor primario de Server Edition proporciona IP Office, Voicemail Pro y Avaya one-X® Portal for IP Office. • Un servidor secundario de Server Edition aumenta la capacidad y proporciona resistencia. La solución de Supervivencia opera para los teléfonos IP basada en el protocolo SIP, para lo cual IP Productos y Servicios, S.A. de C.V. incluye todo el hardware, software y licenciamiento necesario.	https://downloads.avaya.com/css/P8/documents/101049385 PROPUESTA TÉCNICA

Incluir en la solución ofertada todo el hardware, software y licenciamiento necesario, para garantizar la redundancia geográfica del Sistema de Procesamientos de Llamadas IP, de tal forma que ante la eventual falla del Procesador de Llamadas principal y de su redundancia, de manera automática entre en operación la redundancia geográfica (siempre y cuando no se pierda la comunicación vía la RPV entre ambos inmuebles), tomando el control de todos los dispositivos asociados, conservando el Plan de Marcación, sin pérdida de las llamadas establecidas y de ninguna de las funcionalidades básicas solicitadas. El Sistema de Procesamiento de Llamadas IP, cuando esté operando la redundancia geográfica, debe garantizar que no se presentará ninguna degradación en el Servicio integral de telefonía y telecomunicaciones.	70 PROPUESTA TÉCNICA	IP Office Server Edition IP Office Server Edition provides IP Office telephony capabilities, unified communications, mobility, and collaboration. It also provides high availability, ease of use, and low total cost of ownership (TCO). Targeted at the midsize enterprise, IP Office Server Edition supports up to 150 sites, 3000 users, and comprehensive resilience. IP Office Server Edition Solution provides the following: • A single Server Edition Primary server provides IP Office, Voicemail Pro, and Avaya one-X® Portal for IP Office. • A Server Edition Secondary server increases the capacity and provide resilience. La solución de Supervivencia opera para los teléfonos IP basados en el protocolo SIP, para lo cual IP Productos y Servicios, S.A. de C.V. incluye todo el hardware, software y licenciamiento necesario.	IP Office Server Edition IP Office Server Edition proporciona capacidades de telefonía IP Office, comunicaciones unificadas, movilidad y colaboración. También proporciona alta disponibilidad, facilidad de uso y bajo costo total de propiedad (TCO). Dirigido a la mediana empresa, IP Office Server Edition admite hasta 150 sitios, 3000 usuarios y resiliencia integral. La solución IP Office Server Edition proporciona lo siguiente: • Un único servidor primario de Server Edition proporciona IP Office, Voicemail Pro y Avaya one-X® Portal for IP Office. • Un servidor secundario de Server Edition aumenta la capacidad y proporciona resistencia. La solución de Supervivencia opera para los teléfonos IP basada en el protocolo SIP, para lo cual IP Productos y Servicios, S.A. de C.V. incluye todo el hardware, software y licenciamiento necesario.	IP Office Server Edition IP Office Server Edition proporciona capacidades de telefonía IP Office, comunicaciones unificadas, movilidad y colaboración. También proporciona alta disponibilidad, facilidad de uso y bajo costo total de propiedad (TCO). Dirigido a la mediana empresa, IP Office Server Edition admite hasta 150 sitios, 3000 usuarios y resiliencia integral. La solución IP Office Server Edition proporciona lo siguiente: • Un único servidor primario de Server Edition proporciona IP Office, Voicemail Pro y Avaya one-X® Portal for IP Office. • Un servidor secundario de Server Edition aumenta la capacidad y proporciona resistencia. La solución de Supervivencia opera para los teléfonos IP basada en el protocolo SIP, para lo cual IP Productos y Servicios, S.A. de C.V. incluye todo el hardware, software y licenciamiento necesario.	https://downloads.avaya.com/css/P8/documents/101049385 PROPUESTA TÉCNICA
El Sistema de Procesamiento de Llamadas IP, deberá contar con la capacidad de manejar el Protocolo SIP para permitir el registro de cualquier dispositivo que cumpla con este protocolo.	Avaya IP Office ™ Platform Solution Description	19, 20	IP Office supports PSTN, SIP, POTs, digital time division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist	IP Office admite PSTN, SIP, POT, teléfonos digitales multiplexados por división de tiempo y teléfonos IP digitales, todos en el mismo sistema. IP Office permite todas las tecnologías para convivir	https://downloads.avaya.com/css/P8/documents/101049368
El Sistema de Procesamiento de Llamadas IP, deberá soportar por sí mismo o con los elementos necesarios, las siguientes troncales: IP, SIP, E1 R2 Modificado, E1 PRI ISDN, E1 con soporte de Q.Sig,	Avaya IP Office ™ Platform Solution Description	19, 20	IP Office supports PSTN, SIP, POTs, digital time division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist	IP Office admite PSTN, SIP, POT, teléfonos digitales multiplexados por división de tiempo y teléfonos IP digitales, todos en el mismo sistema. IP Office permite todas las tecnologías para convivir	https://downloads.avaya.com/css/P8/documents/101049368

Troncales analógicas y Troncales ISDN BRI.					
El Sistema de Procesamiento de Llamadas IP deberá permitir la configuración y/o programación de troncales SIP.	Avaya IP Office ™ Platform Solution Description	19, 20	IP Office supports PSTN, SIP, POTs, digital time division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist	IP Office admite PSTN, SIP, POT, teléfonos digitales multiplexados por división de tiempo y teléfonos IP digitales, todos en el mismo sistema. IP Office permite todas las tecnologías para convivir	https://downloads.avaya.com/css/P8/documents/101049368
El proveedor deberá de realizar las configuraciones necesarias a fin de que se respeten los planes de marcación que tienen establecidos las Dependencias o Entidades, siendo estos de 4 o 5 dígitos al menos.	Avaya IP Office™ Platform Feature Description	25	Plan de marcación IP Office tiene un programa de numeración muy flexible para comandos de extensiones, grupos de búsqueda y funciones. Si bien el sistema tiene una numeración predeterminada para los códigos de función y las extensiones, se pueden redefinir. Las extensiones y los grupos de búsqueda predeterminados tienen números de 3 dígitos que comienzan en el 200, pero se pueden cambiar a entre 2 y 9 dígitos con IP Office Manager.	Plan de marcación IP Office tiene un programa de numeración muy flexible para comandos de extensiones, grupos de búsqueda y funciones. Si bien el sistema tiene una numeración predeterminada para los códigos de función y las extensiones, se pueden redefinir. Las extensiones y los grupos de búsqueda predeterminados tienen números de 3 dígitos que comienzan en el 200, pero se pueden cambiar a entre 2 y 9 dígitos con IP Office Manager.	https://downloads.avaya.com/css/P8/documents/101049385
El equipo de voz IP, deberá de soportar la configuración y operación del Plan Técnico Fundamental de Numeración de marcación a 10 dígitos ordenado por Instituto Federal de Telecomunicaciones (IFETEL), debiendo discriminar si el servicio es llamada local, nacional, o celular, a fin de poder realizar la configuración correspondiente de acuerdo al perfil de privilegios otorgados a cada uno de los usuarios finales.	Avaya IP Office™ Platform Feature Description	29	Las rutas de menor costo pueden traducir automáticamente el número interno a una llamada de marcación directa en la red pública mientras otros usuarios están en espera.	Las rutas de menor costo pueden traducir automáticamente el número interno a una llamada de marcación directa en la red pública mientras otros usuarios están en espera.	https://downloads.avaya.com/css/P8/documents/101049385
El Sistema de Procesamiento de Llamadas IP, deberá manejar al menos los siguientes tipos de extensiones:	n/a	n/a	n/a	n/a	n/a
SIP con mecanismos de cifrado basados en al menos AES-128 y los protocolos SRTP y TLS al menos versión 2, para cualquier localidad.	IP Office Platform Security Guidelines	12, 71	· TLS/SRTP encryption · RTP encryption/authentications setting should be AES-128/CTR plus SHA-1/80.	· TLS/SRTP encryption · RTP encryption/authentications setting should be AES-128/CTR plus SHA-1/80.	https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/manuals/mgr/ipo_security_guidelines.pdf
Adicionalmente, el Sistema de Procesamiento de Llamadas IP, deberá contar con la capacidad de:	n/a	n/a	n/a	n/a	n/a
Restringir a un número determinado de llamadas máximas permitidas de	Avaya IP Office™ Platform	58	En los sistemas IP500 V2, la red multisitio (con SCN) requiere una o más licencias	En los sistemas IP500 V2, la red multisitio (con SCN) requiere una o más licencias adicionales. Los sistemas de	https://downloads.avaya.com/css/P8/documents/101049385

manera concurrente entre inmuebles.	Feature Description		adicionales. Los sistemas de expansión Server Edition (V2) no requieren licencias de red de voz. Las capacidades Q.SIG, H.323 y SCN no están activadas de forma predeterminada en IP500 V2. Se requiere una licencia adicional para activar esta funcionalidad con 4 canales de red simultáneos (no hay límite de canal para Q.SIG). Es posible obtener licencias para canales adicionales en incrementos de 4.	expansión Server Edition (V2) no requieren licencias de red de voz. Las capacidades Q.SIG, H.323 y SCN no están activadas de forma predeterminada en IP500 V2. Se requiere una licencia adicional para activar esta funcionalidad con 4 canales de red simultáneos (no hay límite de canal para Q.SIG). Es posible obtener licencias para canales adicionales en incrementos de 4.	
Registrar y controlar terminales telefónicas y de video.	Avaya IP Office™ Platform Feature Description	83	IP Office Manager Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.	IP Office Manager Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.	https://downloads.avaya.com/css/P8/documents/101049385
Registrar y controlar tanto terminales basadas en hardware como en software para estaciones de trabajo Windows, teléfonos inteligentes (Smartphone) y tabletas con Sistemas Operativos iOS (Apple) o Android.	Avaya IP Office™ Platform Feature Description	83	IP Office Manager Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.	IP Office Manager Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.	https://downloads.avaya.com/css/P8/documents/101049385

FUNCIONALIDADES BÁSICAS

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL	URL
El proveedor deberá incluir en su propuesta técnica que todas las facilidades básicas descritas anteriormente, y se incluirán como facilidades estándar asociadas a los "Servicios de Voz IP" con Teléfono IP, con excepción de aquellas para las cuales el administrador del contrato establezca alguna	N/A	N/A	N/A	N/A	

restricción, de la cual informará al licitante que resulte adjudicado al inicio de la vigencia del contrato.					
El Proveedor debe incluir en su propuesta técnica, que el Sistema de Procesamiento de Llamadas IP que se utilice para proporcionar el Servicio de Voz IP objeto de estas especificaciones técnicas, deberá contar con los elementos necesarios para garantizar como mínimo, el cumplimiento de las siguientes funcionalidades básicas:	N/A	N/A	N/A	N/A	
● Establecimiento de llamadas. Capacidad de realizar llamadas internas dentro de un inmueble o hacia otro inmueble y desde y hacia la Red Pública de Telefonía.	Avaya IP Office ™ Platform Solution Description	20, 21, 83	In order to make use of VoIP, IP Office uses signaling protocols called H.323 and Session Initiation Protocol (SIP), to establish end-to-end connections for the voice path through an IP network. This connection ensures that each end is able to transmit and receive voice and provides the network addressing for end-to-end packet transmission. IP Office Manager Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.	Para hacer uso de VoIP, IP Office usa protocolos de señalización llamados H.323 e Inicio de sesión Protocolo (SIP), para establecer conexiones de extremo a extremo para la ruta de voz a través de una red IP. Esta conexión asegura que cada extremo pueda transmitir y recibir voz y proporciona la red direccionamiento para la transmisión de paquetes de extremo a extremo. IP Office Manager Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.	https://downloads.avaya.com/css/P8/documents/101049368 https://downloads.avaya.com/css/P8/documents/101049385
● Estado de la llamada por línea. Facilidad que permite visualizar en el display del	Avaya IP Office ™ Platform	90	Detalles de la llamada Información acerca de llamadas entrantes y salientes; incluye	Detalles de la llamada Información acerca de llamadas entrantes y salientes; incluye	https://downloads.avaya.com/css/P8/documents/101049385

Teléfono IP, el estado de las llamadas establecidas (recibidas o generadas), en el que se muestre como mínimo el número y la duración.	Feature Description		información de duración, identificador de llamada y enrutamiento	información de duración, identificador de llamada y enrutamiento	
• Marcación Entrante Directa (DID). Reconocimiento de los 4 dígitos de la funcionalidad de Marcación Directa Entrante (DID o Direct Inward Dialing).	Avaya IP Office ™ Platform Feature Description	26	Marcación directa interna (DID/DDI) se basa en el intercambio de teléfono local para transmitir todo o parte del número marcado a IP Office	Marcación directa interna (DID/DDI) se basa en el intercambio de teléfono local para transmitir todo o parte del número marcado a IP Office	https://downloads.avaya.com/css/P8/documents/101049385
• Identificación de la línea de llamada (CLID) /nombre del llamante (CNID). Funcionalidades que permiten que un teléfono que recibe una llamada, además de timbrar, también reciba la información del número telefónico de la línea que lo llama (CLID o Calling Line Identification) y en su caso, el nombre asociado a dicha línea telefónica (CNID o Calling Number Identification).	Avaya IP Office ™ Platform Feature Description	35	Pantalla para nombre de directorio de llamada entrante Los administradores pueden seleccionar el CLID o el nombre de directorio como pantalla predeterminada para las llamadas entradas.	Pantalla para nombre de directorio de llamada entrante Los administradores pueden seleccionar el CLID o el nombre de directorio como pantalla predeterminada para las llamadas entradas.	https://downloads.avaya.com/css/P8/documents/101049385
• Soporte de XML a través de lo cual los teléfonos IP deberán ser capaces de acceder a un servidor que les permita desplegar la información que obtengan del mismo en sus pantallas.	Avaya IP Office ™ Platform Solution Description	29	Open APIs/SDKs With Release 10.1, IP Office supports a new Management API/SDK to address the needs of "Easy Button" setups. • Request and response are in XML and JSON format	API / SDK abiertos Con la versión 10.1, IP Office admite una nueva API / SDK de administración para abordar las necesidades de las configuraciones de "Botón fácil". • La solicitud y la respuesta están en formato XML y JSON	https://downloads.avaya.com/css/P8/documents/101049368
• Señalización de Mensajes de Voz. Indicador visual y/o audible en el teléfono de que se está recibiendo un mensaje de voz y/o indicador visual y/o audible en el teléfono de que se recibió un mensaje de voz.	Avaya IP Office™ Platform Feature Description	65	IP Officeutiliza la indicación de mensaje en espera (MWI) para establecer una luz u otra indicación en los teléfonos cuando se dejó un nuevo mensaje para el usuario, ya sea en un buzón de correo de voz personal o en un buzón de correo de voz de grupo o un mensaje de devolución de llamada.	IP Officeutiliza la indicación de mensaje en espera (MWI) para establecer una luz u otra indicación en los teléfonos cuando se dejó un nuevo mensaje para el usuario, ya sea en un buzón de correo de voz personal o en un buzón de correo de voz de grupo o un mensaje de devolución de llamada.	https://downloads.avaya.com/css/P8/documents/101049385

• Indicador de llamada en espera. Indicador audible mediante un tono que deberá escucharse cuando se tenga una llamada en espera, además de un indicador visual en el display del Teléfono IP, que debe activarse cuando se pone en espera una llamada.	Avaya IP Office™ Platform Feature Description	20	Llamada en espera El usuario puede no querer que las llamadas reciban el tono de ocupado si están atendiendo otra llamada. En lugar del tono de ocupado, la llamada recibe un tono de timbre normal. EL usuario oye una alerta de que hay una llamada en espera.	Llamada en espera El usuario puede no querer que las llamadas reciban el tono de ocupado si están atendiendo otra llamada. En lugar del tono de ocupado, la llamada recibe un tono de timbre normal. EL usuario oye una alerta de que hay una llamada en espera.	https://downloads.avaya.com/css/P8/documents/101049385
• Configuración de varias líneas. Facilidad que permite configurar en un Teléfono IP, varias líneas o accesos asociados a un número de extensión.	Avaya IP Office™ Platform Feature Description	63	Botones de apariencia en puente Los botones de apariencia en puente le permiten al usuario tener un botón de apariencia que corresponda con el botón de apariencia de llamada de otro usuario.	Botones de apariencia en puente Los botones de apariencia en puente le permiten al usuario tener un botón de apariencia que corresponda con el botón de apariencia de llamada de otro usuario.	https://downloads.avaya.com/css/P8/documents/101049385
• Configuración de varios números. Facilidad que permite configurar varios números de extensión diferentes en un mismo Teléfono IP, en función de la cantidad de teclas disponibles.	Avaya IP Office™ Platform Feature Description	62	Botones de apariencia de llamada El número de botones de apariencia de llamada configurados para un usuario determina el número de llamadas simultáneas que puede realizar o responder. Si se utilizan todos los botones de apariencia de llamada, se recomienda un mínimo de tres botones de apariencia de llamada cuando sea posible	Botones de apariencia de llamada El número de botones de apariencia de llamada configurados para un usuario determina el número de llamadas simultáneas que puede realizar o responder. Si se utilizan todos los botones de apariencia de llamada, se recomienda un mínimo de tres botones de apariencia de llamada cuando sea posible	https://downloads.avaya.com/css/P8/documents/101049385
• Multirepresentación de número. Facilidad que permite que se anuncien las llamadas de un mismo número de extensión, en diferentes teléfonos IP, inclusive en inmuebles diferentes.	Avaya IP Office™ Platform Feature Description	62	Botones de apariencia Muchos teléfonos IP y digitales de Avaya cuentan con botones programables. Es posible asignar funciones de apariencia a estos botones que permiten la administración de llamadas	Botones de apariencia Muchos teléfonos IP y digitales de Avaya cuentan con botones programables. Es posible asignar funciones de apariencia a estos botones que permiten la administración de llamadas	https://downloads.avaya.com/css/P8/documents/101049385
• Marcación rápida. El Sistema deberá permitir a través del Teléfono IP, la programación de marcaciones rápidas mediante teclas,	Avaya IP Office™ Platform Feature Description	41	• Funciones locales del teléfono: remarcado, silenciar, selección de audio (altavoz/auricular), Registro de llamadas, Control de volumen,	• Funciones locales del teléfono: remarcado, silenciar, selección de audio (altavoz/auricular), Registro de llamadas, Control de volumen, contactos locales,	https://downloads.avaya.com/css/P8/documents/101049385

dependiendo de la capacidad de teclas programables.			contactos locales, marcaciones rápidas, marcaciones automáticas	marcaciones rápidas, marcaciones automáticas	
• Marcación abreviada. La marcación abreviada deberá permitir a los usuarios, marcar números de teléfono pre-definidos con solo uno o dos dígitos.	Avaya IP Office™ Platform Feature Description	41	• Funciones locales del teléfono: remarcado, silenciar, selección de audio (altavoz/auricular), Registro de llamadas, Control de volumen, contactos locales, marcaciones rápidas, marcaciones automáticas	• Funciones locales del teléfono: remarcado, silenciar, selección de audio (altavoz/auricular), Registro de llamadas, Control de volumen, contactos locales, marcaciones rápidas, marcaciones automáticas	https://downloads.avaya.com/css/P8/documents/101049385
• Control de volumen. El Sistema deberá permitir fijar el volumen mínimo de audio y tono de timbre de los teléfonos.	Avaya IP Office™ Platform Feature Description	41	• Funciones locales del teléfono: remarcado, silenciar, selección de audio (altavoz/auricular), Registro de llamadas, Control de volumen, contactos locales, marcaciones rápidas, marcaciones automáticas	• Funciones locales del teléfono: remarcado, silenciar, selección de audio (altavoz/auricular), Registro de llamadas, Control de volumen, contactos locales, marcaciones rápidas, marcaciones automáticas	https://downloads.avaya.com/css/P8/documents/101049385
• Intercomunicador silencioso. Capacidad para que una llamada entrante timbre únicamente en el teléfono de la asistente, al tiempo que en el teléfono del superior aparece el número telefónico de la persona que llama y, en caso de ser interna, también el nombre.	Avaya IP Office™ Platform Feature Description	20	la Intrusión silenciosa o el Anuncio discreto pueden resultar efectivos en una situación en la que un usuario hace una intrusión en una llamada para anunciar en forma discreta que un cliente muy importante está en espera. El jefe escucha a su secretaria mientras habla con la persona que realiza la llamada, pero este no podrá escuchar a la secretaria.	la Intrusión silenciosa o el Anuncio discreto pueden resultar efectivos en una situación en la que un usuario hace una intrusión en una llamada para anunciar en forma discreta que un cliente muy importante está en espera. El jefe escucha a su secretaria mientras habla con la persona que realiza la llamada, pero este no podrá escuchar a la secretaria.	https://downloads.avaya.com/css/P8/documents/101049385
• Transferencia de llamadas con y sin consulta. Esta facilidad deberá permitir transferir una llamada establecida (interna o externa) a otra extensión o a cualquier otro número telefónico externo, consultando previamente si se desea recibir la llamada o directamente sin realizar esta consulta.	Avaya IP Office™ Platform Feature Description	18	Transferencia El usuario puede transferir una llamada en curso a una extensión interna o a un número público externo. El sistema coloca la llamada en espeta mientras realiza la transferencia.	Transferencia El usuario puede transferir una llamada en curso a una extensión interna o a un número público externo. El sistema coloca la llamada en espeta mientras realiza la transferencia.	https://downloads.avaya.com/css/P8/documents/101049385

• Desvío automático de llamadas (Externas/Internas). Facilidad que permite que todas las llamadas dirigidas a una extensión puedan enrutarse hacia otra extensión, una operadora, un número externo o un equipo de correo de voz automáticamente.	Avaya IP Office™ Platform Feature Description	17	Reenvío incondicional El sistema reenvía todas las llamadas del usuario a un número, pero si la llamada no tiene respuesta dentro del período configurado, el sistema la envía al correo de voz, siempre que esta función esté activada.	Reenvío incondicional El sistema reenvía todas las llamadas del usuario a un número, pero si la llamada no tiene respuesta dentro del período configurado, el sistema la envía al correo de voz, siempre que esta función esté activada.	https://downloads.avaya.com/css/P8/documents/101049385
• Desvío de llamadas en ocupado. En una llamada establecida, se debe recibir una alerta en la pantalla del teléfono, indicando que hay una llamada entrante y deberá contarse con la opción de desviarla al correo de voz del usuario o un número predeterminado.	Avaya IP Office™ Platform Feature Description	16	Reenviar si da ocupado Si está habilitado, este reenvío se activará cuando el usuario esté ocupado y reciba otra llamada desviada, pero no incluye las llamadas para un grupo de búsqueda al que pertenezca.	Reenviar si da ocupado Si está habilitado, este reenvío se activará cuando el usuario esté ocupado y reciba otra llamada desviada, pero no incluye las llamadas para un grupo de búsqueda al que pertenezca.	https://downloads.avaya.com/css/P8/documents/101049385
• Desvío de llamadas no atendidas. Facilidad que redirige todas las llamadas entrantes de una extensión, en el caso de que no se contesten, a un número telefónico predefinido o al correo de voz del usuario, después de un determinado número de timbrados.	Avaya IP Office™ Platform Feature Description	15	Reenvío El usuario puede reenviar llamadas a otra extensión o a un número externo, incluso a dispositivos móviles.	Reenvío El usuario puede reenviar llamadas a otra extensión o a un número externo, incluso a dispositivos móviles.	https://downloads.avaya.com/css/P8/documents/101049385
• Conferencia Múltiple. Capacidad de establecer conferencias de un mínimo de 6 participantes. Se deberán visualizar el nombre y/o número de línea de los participantes.	Avaya IP Office™ Platform Feature Description	79	Conferencia Los usuarios pueden colocar las llamadas en espera y crear una conferencia con el teléfono o aplicaciones del escritorio. Se pueden agregar miembros adicionales a la conferencia; no obstante, una sola conferencia no puede tener más de 64 miembros (con IP500 V2 solamente y más con Server Edition). El sistema admite 128 canales de conferencia	Conferencia Los usuarios pueden colocar las llamadas en espera y crear una conferencia con el teléfono o aplicaciones del escritorio. Se pueden agregar miembros adicionales a la conferencia; no obstante, una sola conferencia no puede tener más de 64 miembros (con IP500 V2 solamente y más con Server Edition). El sistema admite 128 canales de conferencia en e IP500 V2, lo que permite realizar varias	https://downloads.avaya.com/css/P8/documents/101049385

			en e IP500 V2, lo que permite realizar varias conferencias de cualquier tamaño de entre 3 y 64 participantes	conferencias de cualquier tamaño de entre 3 y 64 participantes	
• Remarcación. Facilidad que permite remarcar el último número marcado, con una tecla específica o digitando algún prefijo	Avaya IP Office™ Platform Feature Description	41	Funciones locales del teléfono: remarcado	Funciones locales del teléfono: remarcado	https://downloads.avaya.com/css/P8/documents/101049385
• Re Llamada. Al marcar a una extensión de la Red, si no se contesta o está ocupada, se deberá contar con la opción de programar una Re-llamada, que debe activarse cuando el usuario al que se llamó esté disponible. La llamada podrá ser automática o a elección del usuario, cancelarla o realizarla.	Avaya IP Office™ Platform Feature Description	60	IP Office puede volver a llamar a un usuario en forma automática.	IP Office puede volver a llamar a un usuario en forma automática.	https://downloads.avaya.com/css/P8/documents/101049385
• Acceso Remoto. Funcionalidad que permite el acceso externo vía PSTN al "Sistema de Procesamiento de Llamadas IP", marcando un número predeterminado. Una vez establecida la llamada el usuario debe autenticarse con un código de acceso (NIP), para permitirle realizar llamadas conforme a los privilegios que tenga autorizados.	Avaya IP Office™ Platform Feature Description	47	Funciones de acceso remoto El firewall integral de IP Office, las cuotas de servicio y las bandas de tiempo se aplican a las llamadas de acceso remoto. Es posible complementar la seguridad del acceso remoto mediante el uso de CHAP (contraseñas cifradas) para verificar los usuarios finales o PAP que no admiten el cifrado. Las bandas de tiempo pueden controlar las horas en las que el servicio de acceso remoto está disponible.	Funciones de acceso remoto El firewall integral de IP Office, las cuotas de servicio y las bandas de tiempo se aplican a las llamadas de acceso remoto. Es posible complementar la seguridad del acceso remoto mediante el uso de CHAP (contraseñas cifradas) para verificar los usuarios finales o PAP que no admiten el cifrado. Las bandas de tiempo pueden controlar las horas en las que el servicio de acceso remoto está disponible.	https://downloads.avaya.com/css/P8/documents/101049385
• Identificación de número entrante / saliente. En la pantalla del teléfono deberá aparecer el número al que se llama o del que se recibe la llamada. También aplica si el teléfono está habilitado con varias líneas. Identificación del nombre	Avaya IP Office™ Platform Feature Description	66	Identificador de llamada Si el proveedor de servicios brinda un identificador de llamada, IP Office envía la llamada a la aplicación o teléfono que conteste y la ingresa en el registro o historial de llamadas	Identificador de llamada Si el proveedor de servicios brinda un identificador de llamada, IP Office envía la llamada a la aplicación o teléfono que conteste y la ingresa en el registro o historial de llamadas admitido. Si el identificador de llamada reconoce el	https://downloads.avaya.com/css/P8/documents/101049385

en llamadas internas entrantes / salientes. En llamadas internas entrantes o salientes, la pantalla del Teléfono IP deberá indicar el nombre asociado al número telefónico marcado o desde el que se recibe la llamada			admitido. Si el identificador de llamada reconoce el número porque está en el directorio, IP Office muestra el nombre del directorio que corresponda.	número porque está en el directorio, IP Office muestra el nombre del directorio que corresponda.	
• Restricción de identificación del usuario que llama. Facilidad que permite realizar llamadas a números internos, sin que se anuncie el nombre y número de extensión.	Avaya IP Office™ Platform Feature Description	24	Privacidad del usuario Es necesario asegurar a ciertos usuarios la confidencialidad de la comunicación. Se debe proteger a estos usuarios de manera que los demás usuarios no puedan ver quién los está llamando y de que puedan impedir que otros contesten sus llamadas.	Privacidad del usuario Es necesario asegurar a ciertos usuarios la confidencialidad de la comunicación. Se debe proteger a estos usuarios de manera que los demás usuarios no puedan ver quién los está llamando y de que puedan impedir que otros contesten sus llamadas.	https://downloads.avaya.com/css/P8/documents/101049385
• Función de No Molestar. Facilidad que permite a los usuarios que no quieren ser molestados por llamadas entrantes, pulsar una tecla o un prefijo para que no timbre el teléfono.	Avaya IP Office™ Platform Feature Description	22	No molestar El usuario puede suspender temporariamente las llamadas que suenan en sus teléfonos.	No molestar El usuario puede suspender temporariamente las llamadas que suenan en sus teléfonos.	https://downloads.avaya.com/css/P8/documents/101049385
• Arreglo Jefe / Secretaria. Configuración de esquemas Jefe- Secretaria con consulta y transferencia de llamada, además de contar con identificación visual del estado de la línea del Jefe (colgado-descolgado al menos).	Avaya IP Office™ Platform Feature Description	63	Los botones de apariencia en puente permiten el funcionamiento emparejado estilo "jefe/secretario" entre dos usuarios y solo se admite para los usuarios que tienen botones de línea de llamada.	Los botones de apariencia en puente permiten el funcionamiento emparejado estilo "jefe/secretario" entre dos usuarios y solo se admite para los usuarios que tienen botones de línea de llamada.	https://downloads.avaya.com/css/P8/documents/101049385
• Aparcamiento de llamada. Esta función permite poner una llamada en espera (estacionarla) pulsando una tecla o prefijo y recuperarla desde otro teléfono	Avaya IP Office™ Platform Feature Description	17	Estacionar Como alternativa para poner una llamada en espera, una llamada se puede estacionar en el sistema y ser atendida por otro usuario.	Estacionar Como alternativa para poner una llamada en espera, una llamada se puede estacionar en el sistema y ser atendida por otro usuario.	https://downloads.avaya.com/css/P8/documents/101049385
• Captura de llamadas por grupo. Configuración de un grupo de teléfonos que permite, que de cualquiera de ellos, se pueda responder las llamadas del resto.	Avaya IP Office™ Platform Feature Description	23	Captura El usuario puede responder una llamada presentada a otra extensión. La capturar de llamadas incluyen: • Capturar cualquier	Captura El usuario puede responder una llamada presentada a otra extensión. La capturar de llamadas incluyen: • Capturar cualquier	https://downloads.avaya.com/css/P8/documents/101049385

			llamada timbrando en otra extensión.	llamada timbrando en otra extensión.	
● Retención/Recuperación de llamada. Esta facilidad permite a un usuario atender una llamada, no obstante, tenga una llamada establecida. El usuario puede elegir atender la nueva llamada poniendo a la primera en espera o alternarlas.	Avaya IP Office™ Platform Feature Description	17	En espera El usuario puede colocar llamadas en espera y activar la música de llamada en especial, si así lo desea. Una llamada en espera regresa a la extensión luego de un período de espera, configurado por el administrador del sistema, para que las llamadas en espera no sean olvidadas.	En espera El usuario puede colocar llamadas en espera y activar la música de llamada en especial, si así lo desea. Una llamada en espera regresa a la extensión luego de un período de espera, configurado por el administrador del sistema, para que las llamadas en espera no sean olvidadas.	https://downloads.avaya.com/css/P8/documents/101049385
● Códigos de Seguridad. El Sistema deberá contar con la funcionalidad de marcación a números restringidos (larga distancia, llamadas a celular y números de entretenimiento como mínimo), a través de un Código de Seguridad personalizado de al menos 5 dígitos, que podrá utilizar el usuario en cualquier teléfono físico basado en hardware de la Red.	Avaya IP Office™ Platform Feature Description	29	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	https://downloads.avaya.com/css/P8/documents/101049385
● Marcaciones rápidas con códigos de seguridad. El Sistema deberá contar con la funcionalidad de configurar marcaciones rápidas, que incluyan los códigos de seguridad requeridos para realizar las llamadas, en su caso.	Avaya IP Office™ Platform Feature Description	66	El directorio también aporta una lista de los números marcados con más frecuencia en todo el sistema para agregarlos a la marcación rápida	El directorio también aporta una lista de los números marcados con más frecuencia en todo el sistema para agregarlos a la marcación rápida	https://downloads.avaya.com/css/P8/documents/101049385
● Categorías de marcación El Sistema deberá permitir establecer categorías de marcación por teléfono, permitiendo o negando el	Avaya IP Office™ Platform Feature Description	29	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus	https://downloads.avaya.com/css/P8/documents/101049385

acceso a ciertos números, tanto internos como de la telefonía pública fija o móvil.			sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	
• Música en espera. Facilidad que permite oír música o mensajes de audio de fondo, cuando se pone una llamada en espera. El Sistema deberá incluir la música, por lo que respecta a los mensajes de audio, podrán ser predefinidos por LA ENTIDAD.	Avaya IP Office™ Platform Feature Description	28	Música de espera Los administradores pueden acceder a hasta 32 fuentes de música de espera. En los sistemas Linux, se admiten hasta cuatro fuentes USB	Música de espera Los administradores pueden acceder a hasta 32 fuentes de música de espera. En los sistemas Linux, se admiten hasta cuatro fuentes USB	https://downloads.avaya.com/css/P8/documents/101049385
• Historial de llamadas En los teléfonos IP, se deberá observar el registro de las llamadas recibidas, realizadas y perdidas, con información de la llamada como; día, hora y duración, como mínimo.	Avaya IP Office™ Platform Feature Description	65	Historial de llamadas IP Office guarda un registro de las llamadas realizadas y recibidas, incluidas aquellas que no fueron respondidas. Se guardan los detalles de ambos usuarios (30 entradas como máximo) y de los grupos de búsqueda (10 entradas como máximo).	Historial de llamadas IP Office guarda un registro de las llamadas realizadas y recibidas, incluidas aquellas que no fueron respondidas. Se guardan los detalles de ambos usuarios (30 entradas como máximo) y de los grupos de búsqueda (10 entradas como máximo).	https://downloads.avaya.com/css/P8/documents/101049385
• Timbres distintivos del teléfono. Facilidad que permite personalizar el tono del timbre del Teléfono IP	Avaya IP Office™ Platform Feature Description	15	Timbre característico El sistema utiliza diferentes secuencias de timbre para indicar tipos de llamada. Por ejemplo, las llamadas internas y externas pueden tener diferentes timbres; esta función se llama timbre característico.	Timbre característico El sistema utiliza diferentes secuencias de timbre para indicar tipos de llamada. Por ejemplo, las llamadas internas y externas pueden tener diferentes timbres; esta función se llama timbre característico.	https://downloads.avaya.com/css/P8/documents/101049385

• Personalización de la pantalla del Teléfono IP. Personalización de la imagen de fondo de la pantalla.	Using Avaya 9621G/9641G/9641GS IP Deskphones H.323	23	• My Pictures: Using this feature you can use pictures from a USB device as the phone screensaver.Note: This feature is applicable only to the 9641G and 9641GS deskphones.	• Mis imágenes: con esta función puede usar imágenes de un dispositivo USB como protector de pantalla del teléfono. Nota: esta función se aplica únicamente a los teléfonos de escritorio 9641G y 9641GS.	https://downloads.avaya.com/css/P8/documents/101024380
• Bloqueo de llamadas salientes/entrantes. El Sistema debe contar con la capacidad para filtrar y bloquear, llamadas salientes y/o entrantes a números específicos o patrón de números.	Avaya IP Office™ Platform Feature Description	29	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	https://downloads.avaya.com/css/P8/documents/101049385
• Timbrado distintivo para llamadas internas y externas. Capacidad que permite configurar timbres distintivos, para diferenciar las llamadas internas de las externas.	Avaya IP Office™ Platform Feature Description	15	Timbre característico El sistema utiliza diferentes secuencias de timbre para indicar tipos de llamada. Por ejemplo, las llamadas internas y externas pueden tener diferentes timbres; esta función se llama timbre característico.	Timbre característico El sistema utiliza diferentes secuencias de timbre para indicar tipos de llamada. Por ejemplo, las llamadas internas y externas pueden tener diferentes timbres; esta función se llama timbre característico.	https://downloads.avaya.com/css/P8/documents/101049385
• Generación de tonos (DTMF). Envío de tonos desde Teléfonos IP hacia la Red Pública, con el fin de interactuar con sistemas de audio respuesta	Avaya IP Office™ Platform Feature Description	35	DTMF fuera de banda Los ingenieros de implementación pueden configurar una multifrecuencia de doble tono (DTMF) fuera de banda en una extensión IP para que se envíe una señal al otro extremo de la conexión con los dígitos que un generador local	DTMF fuera de banda Los ingenieros de implementación pueden configurar una multifrecuencia de doble tono (DTMF) fuera de banda en una extensión IP para que se envíe una señal al otro extremo de la conexión con los dígitos que un generador local DTMF tiene que volver a	https://downloads.avaya.com/css/P8/documents/101049385

			DTMF tiene que volver a generar en nombre de la extensión IP que envía la señal. Esto es útil cuando se navega por sistemas de correo de voz externos y de operadores automáticos.	generar en nombre de la extensión IP que envía la señal. Esto es útil cuando se navega por sistemas de correo de voz externos y de operadores automáticos.	
● Acceso al correo de voz. Facilidad que permite acceder al correo de voz mediante una tecla predefinida en el Teléfono IP. Para escuchar los mensajes de voz, se deberá requerir de una contraseña.	IP Office™ Platform 11.0	44	· Embedded Voicemail Embedded Voicemail supports basic voicemail mailbox operation, simple auto-attendants and hunt group announcements.	· Buzón de voz integrado El correo de voz integrado admite la operación básica del buzón de correo de voz, asistentes automáticos simples y grupo de búsqueda anuncios.	https://downloads.avaya.com/css/P8/documents/101047526
● Configuración de Redes Privadas. El Sistema deberá contar con la capacidad de configurar redes privadas, con esquemas de marcación cerrada El Sistema de Procesamiento de Llamadas IP, deberá permitir inclusive la programación de un número de Red Privada en un Teléfono IP de cualquiera de las categorías solicitadas (con excepción de las analógicas), sin que se pierda el esquema de marcación cerrada.	Avaya IP Office™ Platform Feature Description	83	IP Office Manager Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.	IP Office Manager Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.	https://downloads.avaya.com/css/P8/documents/101049385
● Acceso a Directorio Telefónico Capacidad del Sistema de acceder al Directorio Telefónico a través de los teléfonos IP, que EL PROVEEDOR considere el acceso a LDAP.	Avaya IP Office™ Platform Feature Description	30	Invalidar restricción permite marcar números desde el directorio, con remarcar, registro de llamadas, programación de botón, códigos abreviados y números ingresados de forma manual hacia números externos presentes en el directorio público (Directorio de sistema, LDAP, HTTP)	Invalidar restricción permite marcar números desde el directorio, con remarcar, registro de llamadas, programación de botón, códigos abreviados y números ingresados de forma manual hacia números externos presentes en el directorio público (Directorio de sistema, LDAP, HTTP)	https://downloads.avaya.com/css/P8/documents/101049385

MECANISMO DE CIFRADO DE VOZ

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL	URL
Para asegurar la confidencialidad e integridad de la información de voz, así como del modelo propuesto para la solución de Telefonía IP, el proveedor deberá considerar en su propuesta técnica, que el Sistema de Procesamiento de Llamadas IP, que el hardware, software y licenciamiento necesarios que se utilicen para proporcionar el servicio de Voz IP y funcionalidades solicitadas, deberán contar con los elementos necesarios para garantizar como mínimo, el cumplimiento de los siguientes mecanismos de seguridad:	N/A	N/A	N/A	N/A	N/A
• La solución propuesta deberá garantizar la encriptación de la llamada de punto a punto y en conferencia al menos AES-128 y los protocolos SRTP (Secure Real-time Transport Protocol) y TLS (Transport Layer Security), definidos en los RFC 3711 y RFC 2246 respectivamente. Esta condición aplicará solamente entre teléfonos IP y equipos y dispositivos que formen parte de la solución de Telefonía IP de las Dependencias o Entidades y para las llamadas establecidas entre ellas.	IP Office Platform Security Guidelines	12, 71	· TLS/SRTP encryption · RTP encryption/authentications setting should be AES-128/CTR plus SHA-1/80.	· TLS/SRTP encryption · RTP encryption/authentications setting should be AES-128/CTR plus SHA-1/80.	https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/manuals/mgr/ipo_security_guidelines.pdf
• Los teléfonos IP y las extensiones configuradas a través de software, deberán manejar mecanismos de encriptación basados en al menos en AES-128, con la utilización del protocolo SRTP para el transporte de	IP Office Platform Security Guidelines	71	· All SIP extensions where possible should be configured for best effort (capability negotiation or 'cap-neg'); this allows the IP Office settings to dictate SRTP behaviour.	· Todas las extensiones SIP, cuando sea posible, deben configurarse para el mejor esfuerzo (negociación de capacidad o 'cap-neg'); esto permite que la configuración de IP Office dicte el comportamiento de SRTP.	https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/manuals/mgr/ipo_security_guidelines.pdf

la voz y por medio de al menos en AES-128 y TLS para la señalización de la misma llamada.			· Ensure consistency between the system and per-extension SRTP settings for SIP soft clients that connect to IP Office in simultaneous-registration mode (Avaya Communicator and one-X Portal for IP Office Mobile).	· Garantice la coherencia entre el sistema y la configuración SRTP por extensión para los clientes de software SIP que se conectan a IP Office en modo de registro simultáneo (Avaya Communicator y one-X Portal para IP Office Mobile).	
● La solución deberá garantizar que la modalidad de encriptación solicitada anteriormente, se mantendrá en comunicaciones establecidas con el Correo de Voz desde la red instalada en las Dependencias o Entidades.	IP Office Platform Security Guidelines	71	Ensure consistency between the system and per-extension SRTP settings for SIP soft clients that connect to ·IP Office in simultaneous-registration mode (Avaya Communicator and one-X Portal for IP Office Mobile).	Garantice la coherencia entre el sistema y la configuración SRTP por extensión para los clientes de software SIP que se conectan a · IP Office en modo de registro simultáneo (Avaya Communicator y one-X Portal para IP Office Mobile).	https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/manuals/mgr/ipo_security_guidelines.pdf
● El modelo de encriptación solicitado se deberá mantener con cualquier Gateway de Voz IP que esté en operación en la solución de Comunicaciones IP propuesta por EL PROVEEDOR, bajo los estándares solicitados.	Avaya IP Office ™ Platform Solution Description	102	Configurable security settings include the following features: • Encryption and message authentication • Configuring integrated firewall settings • Digital certificates • Prevention of tool fraud by restricting user privileges and using security policy configuration to manage account credentials and access control	Los ajustes de seguridad configurables incluyen las siguientes características: • Cifrado y autenticación de mensajes • Configurar la configuración del firewall integrado • Certificados digitales • Prevención del fraude de herramientas al restringir los privilegios del usuario y utilizar la configuración de la política de seguridad para administrar las credenciales de la cuenta y el control de acceso	https://downloads.avaya.com/css/P8/documents/101049385
● EL PROVEEDOR deberá garantizar en su propuesta, que durante la vigencia del Contrato la infraestructura para proporcionar el Servicios de Voz IP puede operar en su conjunto con una técnica de encriptación superior a la definida por en al menos en AES-128, será implementada sin ningún costo adicional para las Dependencias o Entidades. El proveedor deberá realizar una evaluación previa, para determinar el impacto del	PROPUESTA TÉCNICA	PROPUESTA TÉCNICA	● IP Productos y Serviicos, S.A. de C.V. garantiza en su propuesta ofertada, que durante la vigencia del Contrato la infraestructura para proporcionar el Servicios de Voz IP puede operar en su conjunto con una técnica de encriptación superior a la definida por en al menos en AES-128, será implementada sin ningún costo adicional para las Dependencias o	● IP Productos y Serviicos, S.A. de C.V. garantiza en su propuesta ofertada, que durante la vigencia del Contrato la infraestructura para proporcionar el Servicios de Voz IP puede operar en su conjunto con una técnica de encriptación superior a la definida por en al menos en AES-128, será implementada sin ningún costo adicional para las Dependencias o Entidades. IP Productos y Serviicos, S.A. de C.V. realizará una evaluación previa, para	PROPUESTA TÉCNICA

cambio, de los cuales deberá informar a las Dependencias o Entidades para la toma de decisiones conjuntas.			Entidades. IP Productos y Serviicos, S.A. de C.V. realizará una evaluación previa, para determinar el impacto del cambio, de los cuales deberá informar a las Dependencias o Entidades para la toma de decisiones conjuntas.	determinar el impacto del cambio, de los cuales deberá informar a las Dependencias o Entidades para la toma de decisiones conjuntas.	
• El Sistema de Procesamiento de Llamadas IP propuesto, deberá contar con la capacidad de manejar Códigos de Seguridad personales de 5 dígitos como mínimo, para hacer uso de facilidades telefónicas como llamada a celular y/o larga distancia, en cualquier teléfono físico basado en hardware de la Red.	Avaya IP Office™ Platform Feature Description	29	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	https://downloads.avaya.com/css/P8/documents/101049385
• El modelo de Comunicaciones IP propuesto, deberá incluir mecanismos de autenticación a nivel digital, que permitan a los teléfonos IP autenticarse con el Sistema de Procesamiento de Llamadas IP, por medio de certificados digitales para garantizar que son dispositivos validos en la Red con la categoría establecida.	Avaya IP Office ™ Platform Solution Description	102	Configurable security settings include the following features: • Encryption and message authentication • Configuring integrated firewall settings • Digital certificates • Prevention of tool fraud by restricting user privileges and using security policy configuration to manage account credentials and access control	Los ajustes de seguridad configurables incluyen las siguientes características: • Cifrado y autenticación de mensajes • Configurar la configuración del firewall integrado • Certificados digitales • Prevención del fraude de herramientas al restringir los privilegios del usuario y utilizar la configuración de la política de seguridad para administrar las credenciales de la cuenta y el control de acceso	https://downloads.avaya.com/css/P8/documents/101049385
• El Sistema de Procesamiento de Llamadas IP, así como los	Avaya IP Office ™	70	The other option is to allow users to access the client over a secure	La otra opción es permitir que los usuarios accedan al cliente a través de un	https://downloads.avaya.com/css/P8/documents/101049385

Gateway de voz propuestos en la solución, deben incluir y soportar, mecanismos internos de seguridad como; accesos a la administración vía HTTPS (Hyper Text Transfer Protocol Secure) y/o CLI por medio de TELNET y SSH.	Platform Feature Description		and unsecure protocol (HTTP/HTTPS).	protocolo seguro y no seguro (HTTP / HTTPS).	

MODELO DE EQUIPO IP OFFICE 500 V2

GATEWAY CON CAPACIDAD DE SUPERVIVENCIA

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL	URL
El Proveedor deberá considerar en su propuesta técnica todo el hardware, software, y licenciamiento necesario para proporcionar la solución de supervivencia o contingencia, que cumpla con las condiciones de operación y/o características técnicas siguientes:	PROPUESTA TÉCNICA	PROPUESTA TÉCNICA	IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica el suministro de todo el hardware, software, y licenciamiento necesario para proporcionar la solución de supervivencia o contingencia, que cumple con las condiciones de operación y/o características técnicas siguientes:	IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica el suministro de todo el hardware, software, y licenciamiento necesario para proporcionar la solución de supervivencia o contingencia, que cumple con las condiciones de operación y/o características técnicas siguientes:	PROPUESTA TÉCNICA
• La solución de Supervivencia deberá estar habilitada y operar en caso necesario en los sitios solicitados por la Dependencia o Entidad, con excepción de los sitios donde se instale un Sistema de Procesamiento de llamadas IP.	Avaya IP Office ™ Platform Solution Description	70	IP Office Server Edition IP Office Server Edition provides IP Office telephony capabilities, unified communications, mobility, and collaboration. It also provides high availability, ease of use, and low total cost of ownership (TCO). Targeted at the midsize enterprise, IP Office Server Edition supports up to 150 sites, 3000 users, and comprehensive resilience. IP Office Server Edition Solution provides the following: • A single Server Edition Primary server provides	IP Office Server Edition IP Office Server Edition proporciona capacidades de telefonía IP Office, comunicaciones unificadas, movilidad y colaboración. También proporciona alta disponibilidad, facilidad de uso y bajo costo total de propiedad (TCO). Dirigido a la mediana empresa, IP Office Server Edition admite hasta 150 sitios, 3000 usuarios y resiliencia integral. La solución IP Office Server Edition proporciona lo siguiente: • Un único servidor primario de Server Edition proporciona IP Office, Voicemail Pro y Avaya one-	https://downloads.avaya.com/css/P8/documents/101049385

			IP Office, Voicemail Pro, and Avaya one-X® Portal for IP Office. • A Server Edition Secondary server increases the capacity and provide resilience.	X® Portal for IP Office. • Un servidor secundario de Server Edition aumenta la capacidad y proporciona resistencia.	
• La solución de Supervivencia deberá operar para los teléfonos IP basados en el protocolo SIP, para lo cual se debe incluir todo el hardware, software y licenciamiento necesario.	Avaya IP Office ™ Platform Solution Description	70 PROPUESTA TÉCNICA	IP Office Server Edition IP Office Server Edition provides IP Office telephony capabilities, unified communications, mobility, and collaboration. It also provides high availability, ease of use, and low total cost of ownership (TCO). Targeted at the midsize enterprise, IP Office Server Edition supports up to 150 sites, 3000 users, and comprehensive resilience. IP Office Server Edition Solution provides the following: • A single Server Edition Primary server provides IP Office, Voicemail Pro, and Avaya one-X® Portal for IP Office. • A Server Edition Secondary server increases the capacity and provide resilience. La solución de Supervivencia opera para los teléfonos IP basados en el protocolo SIP, para lo cual IP Productos y Servicios, S.A. de C.V. incluye todo el hardware, software y licenciamiento necesario.	IP Office Server Edition IP Office Server Edition proporciona capacidades de telefonía IP Office, comunicaciones unificadas, movilidad y colaboración. También proporciona alta disponibilidad, facilidad de uso y bajo costo total de propiedad (TCO). Dirigido a la mediana empresa, IP Office Server Edition admite hasta 150 sitios, 3000 usuarios y resiliencia integral. La solución IP Office Server Edition proporciona lo siguiente: • Un único servidor primario de Server Edition proporciona IP Office, Voicemail Pro y Avaya one-X® Portal for IP Office. • Un servidor secundario de Server Edition aumenta la capacidad y proporciona resistencia. La solución de Supervivencia opera para los teléfonos IP basada en el protocolo SIP, para lo cual IP Productos y Servicios, S.A. de C.V. incluye todo el hardware, software y licenciamiento necesario.	https://downloads.avaya.com/css/P8/documents/101049385 PROPUESTA TÉCNICA
• En los sitios donde se encuentre instalado un Gateway de sobrevivencia local, la solución de Supervivencia se deberá activar de manera automática, sin intervención del administrador de la Red, en el momento en que se	Administering Avaya IP Office™ Platform with Manager	3	Add a Server Edition Secondary to provide resilience at any level. The Server Edition Secondary Server provides resilience for the Server Edition Primary Server users, H.323 and SIP extensions, hunt	Agregue un servidor secundario de Server Edition para proporcionar resistencia en cualquier nivel. El servidor secundario de Server Edition proporciona resistencia para los usuarios del servidor primario de Server Edition,	https://documentation.avaya.com/bundle/AdministeringAvayaIPOfficePlatformManagerR11.0/page/Server_Edition_Resilience.html#

pierda la comunicación vía la RPV (Red Privada Virtual) de las Dependencias o Entidades hacia el sistema principal o ante la eventual caída total del mismo.			groups, and voicemail without any administration. A Server Edition Expansion System can be backed up to either the Server Edition Primary, Server Edition Secondary, or another Server Edition Expansion System.	extensiones H.323 y SIP, grupos de búsqueda y correo de voz sin ninguna administración. Se puede realizar una copia de seguridad de un sistema de expansión Server Edition en el sistema de expansión Server Edition primario, Server Edition secundario u otro sistema de expansión Server Edition.	
• La operación en modo de Supervivencia, deberá garantizar que todos los servicios de telefonía del inmueble donde se active, continúen operando de manera local de la misma forma que en modo normal, conservando las funcionalidades básicas siguientes:	Administering Avaya IP Office™ Platform with Manager	3	Add a Server Edition Secondary to provide resilience at any level. The Server Edition Secondary Server provides resilience for the Server Edition Primary Server users, H.323 and SIP extensions, hunt groups, and voicemail without any administration. A Server Edition Expansion System can be backed up to either the Server Edition Primary, Server Edition Secondary, or another Server Edition Expansion System.	Agregue un servidor secundario de Server Edition para proporcionar resistencia en cualquier nivel. El servidor secundario de Server Edition proporciona resistencia para los usuarios del servidor primario de Server Edition, extensiones H.323 y SIP, grupos de búsqueda y correo de voz sin ninguna administración. Se puede realizar una copia de seguridad de un sistema de expansión Server Edition en el sistema de expansión Server Edition primario, Server Edition secundario u otro sistema de expansión Server Edition.	https://documentation.avaya.com/bundle/AdministeringAvayaIPOfficePlatformManagerR11.0/page/Server_Edition_Resilience.html#
o Transferencia de llamada con y sin consulta.	Avaya IP Office™ Platform Feature Description	18	Transferencia El usuario puede transferir una llamada en curso a una extensión interna o a un número público externo. El sistema coloca la llamada en espeta mientras realiza la transferencia.	Transferencia El usuario puede transferir una llamada en curso a una extensión interna o a un número público externo. El sistema coloca la llamada en espeta mientras realiza la transferencia.	https://downloads.avaya.com/css/P8/documents/101049385
o Desvío automático de llamadas (externas/internas).	Avaya IP Office™ Platform Feature Description	17	Reenvío incondicional El sistema reenvía todas las llamadas del usuario a un número, pero si la llamada no tiene respuesta dentro del período configurado, el sistema la envía al correo de voz, siempre que esta función esté activada.	Reenvío incondicional El sistema reenvía todas las llamadas del usuario a un número, pero si la llamada no tiene respuesta dentro del período configurado, el sistema la envía al correo de voz, siempre que esta función esté activada.	https://downloads.avaya.com/css/P8/documents/101049385

o Llamada en espera.	Avaya IP Office™ Platform Feature Description	20	Llamada en espera El usuario puede no querer que las llamadas reciban el tono de ocupado si están atendiendo otra llamada. En lugar del tono de ocupado, la llamada recibe un tono de timbre normal. EL usuario oye una alerta de que hay una llamada en espera.	Llamada en espera El usuario puede no querer que las llamadas reciban el tono de ocupado si están atendiendo otra llamada. En lugar del tono de ocupado, la llamada recibe un tono de timbre normal. EL usuario oye una alerta de que hay una llamada en espera.	https://downloads.avaya.com/css/P8/documents/101049385
o Llamadas entre teléfonos del mismo sitio.	Avaya IP Office™ Platform Feature Description	25	Plan de marcación IP Office tiene un programa de numeración muy flexible para comandos de extensiones, grupos de búsqueda y funciones. Si bien el sistema tiene una numeración predeterminada para los códigos de función y las extensiones, se pueden redefinir. Las extensiones y los grupos de búsqueda predeterminados tienen números de 3 dígitos que comienzan en el 200, pero se pueden cambiar a entre 2 y 9 dígitos con IP Office Manager.	Plan de marcación IP Office tiene un programa de numeración muy flexible para comandos de extensiones, grupos de búsqueda y funciones. Si bien el sistema tiene una numeración predeterminada para los códigos de función y las extensiones, se pueden redefinir. Las extensiones y los grupos de búsqueda predeterminados tienen números de 3 dígitos que comienzan en el 200, pero se pueden cambiar a entre 2 y 9 dígitos con IP Office Manager.	https://downloads.avaya.com/css/P8/documents/101049385
o Llamadas hacia la PSTN en los inmuebles que cuenten con troncales.	Avaya IP Office ™ Platform Solution Description	19, 20	IP Office supports PSTN, SIP, POTs, digital time division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist	IP Office admite PSTN, SIP, POT, teléfonos digitales multiplexados por división de tiempo y teléfonos IP digitales, todos en el mismo sistema. IP Office permite todas las tecnologías para convivir	https://downloads.avaya.com/css/P8/documents/101049368
o Configuración de varias líneas (múltiples llamadas por línea telefónica).	Avaya IP Office™ Platform Feature Description	63	Botones de apariencia en puente Los botones de apariencia en puente le permiten al usuario tener un botón de apariencia que corresponda con el botón de apariencia de llamada de otro usuario.	Botones de apariencia en puente Los botones de apariencia en puente le permiten al usuario tener un botón de apariencia que corresponda con el botón de apariencia de llamada de otro usuario.	https://downloads.avaya.com/css/P8/documents/101049385

o Configuración de varios números (múltiples líneas por Teléfono IP).	Avaya IP Office™ Platform Feature Description	62	Botones de apariencia de llamada El número de botones de apariencia de llamada configurados para un usuario determina el número de llamadas simultáneas que puede realizar o responder. Si se utilizan todos los botones de apariencia de llamada, se recomienda un mínimo de tres botones de apariencia de llamada cuando sea posible	Botones de apariencia de llamada El número de botones de apariencia de llamada configurados para un usuario determina el número de llamadas simultáneas que puede realizar o responder. Si se utilizan todos los botones de apariencia de llamada, se recomienda un mínimo de tres botones de apariencia de llamada cuando sea posible	https://downloads.avaya.com/css/P8/documents/101049385
o Marcación rápida.	Avaya IP Office™ Platform Feature Description	66	El directorio también aporta una lista de los números marcados con más frecuencia en todo el sistema para agregarlos a la marcación rápida	El directorio también aporta una lista de los números marcados con más frecuencia en todo el sistema para agregarlos a la marcación rápida	https://downloads.avaya.com/css/P8/documents/101049385
o Códigos de Seguridad para llamadas de larga distancia y celular.	Avaya IP Office™ Platform Feature Description	29	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	Códigos de autorización Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan. Restricción de llamadas Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema	https://downloads.avaya.com/css/P8/documents/101049385
o Identificador de llamada con nombre y número telefónico de quien llama.	Avaya IP Office ™ Platform Feature Description	35	Pantalla para nombre de directorio de llamada entrante Los administradores pueden seleccionar el CLID o el nombre de directorio como	Pantalla para nombre de directorio de llamada entrante Los administradores pueden seleccionar el CLID o el nombre de directorio como pantalla	https://downloads.avaya.com/css/P8/documents/101049385

			pantalla predeterminada para las llamadas entradas.	predeterminada para las llamadas entradas.	
o Música en espera.	Avaya IP Office™ Platform Feature Description	28	Música de espera Los administradores pueden acceder a hasta 32 fuentes de música de espera. En los sistemas Linux, se admiten hasta cuatro fuentes USB	Música de espera Los administradores pueden acceder a hasta 32 fuentes de música de espera. En los sistemas Linux, se admiten hasta cuatro fuentes USB	https://downloads.avaya.com/css/P8/documents/101049385
o Tono de llamada en espera.	Avaya IP Office™ Platform Feature Description	20	Llamada en espera El usuario puede no querer que las llamadas reciban el tono de ocupado si están atendiendo otra llamada. En lugar del tono de ocupado, la llamada recibe un tono de timbre normal. EL usuario oye una alerta de que hay una llamada en espera.	Llamada en espera El usuario puede no querer que las llamadas reciban el tono de ocupado si están atendiendo otra llamada. En lugar del tono de ocupado, la llamada recibe un tono de timbre normal. EL usuario oye una alerta de que hay una llamada en espera.	https://downloads.avaya.com/css/P8/documents/101049385
o Conferencias de 6 participantes.	Avaya IP Office™ Platform Feature Description	79	Conferencia Los usuarios pueden colocar las llamadas en espera y crear una conferencia con el teléfono o aplicaciones del escritorio. Se pueden agregar miembros adicionales a la conferencia; no obstante, una sola conferencia no puede tener más de 64 miembros (con IP500 V2 solamente y más con Server Edition). El sistema admite 128 canales de conferencia en e IP500 V2, lo que permite realizar varias conferencias de cualquier tamaño de entre 3 y 64 participantes	Conferencia Los usuarios pueden colocar las llamadas en espera y crear una conferencia con el teléfono o aplicaciones del escritorio. Se pueden agregar miembros adicionales a la conferencia; no obstante, una sola conferencia no puede tener más de 64 miembros (con IP500 V2 solamente y más con Server Edition). El sistema admite 128 canales de conferencia en e IP500 V2, lo que permite realizar varias conferencias de cualquier tamaño de entre 3 y 64 participantes	https://downloads.avaya.com/css/P8/documents/101049385
o Marcación Directa Entrante (DID).	Avaya IP Office ™ Platform Feature Description	35	Pantalla para nombre de directorio de llamada entrante Los administradores pueden seleccionar el CLID o el nombre de directorio como pantalla predeterminada para las llamadas entradas.	Pantalla para nombre de directorio de llamada entrante Los administradores pueden seleccionar el CLID o el nombre de directorio como pantalla predeterminada para las llamadas entradas.	https://downloads.avaya.com/css/P8/documents/101049385

o Deberá soportar troncales analógicas	Avaya IP Office ™ Platform Solution Description	19, 20	IP Office supports PSTN, SIP, POTs, digital time division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist	IP Office admite PSTN, SIP, POT, teléfonos digitales multiplexados por división de tiempo y teléfonos IP digitales, todos en el mismo sistema. IP Office permite todas las tecnologías para convivir	https://downloads.avaya.com/css/P8/documents/101049368
o Manejo de señalización R2 modificado en troncales E1.	Avaya IP Office ™ Platform Solution Description	19, 20	IP Office supports PSTN, SIP, POTs, digital time division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist	IP Office admite PSTN, SIP, POT, teléfonos digitales multiplexados por división de tiempo y teléfonos IP digitales, todos en el mismo sistema. IP Office permite todas las tecnologías para convivir	https://downloads.avaya.com/css/P8/documents/101049368
o Manejo de SIP.	Avaya IP Office ™ Platform Solution Description	19, 20	IP Office supports PSTN, SIP, POTs, digital time division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist	IP Office admite PSTN, SIP, POT, teléfonos digitales multiplexados por división de tiempo y teléfonos IP digitales, todos en el mismo sistema. IP Office permite todas las tecnologías para convivir	https://downloads.avaya.com/css/P8/documents/101049368
o Acceso a correo de voz	Administering Avaya IP Office™ Platform with Manager	3	• Voicemail Pro server	• Voicemail Pro server	https://documentation.avaya.com/bundle/AdministeringAvayaIPOfficePlatformManagerR11.0/page/Server_Edition_Resilience.html#
o Traducción de dígitos marcados.	Avaya IP Office™ Platform Feature Description	29	Las rutas de menor costo pueden traducir automáticamente el número interno a una llamada de marcación directa en la red pública mientras otros usuarios están en espera.	Las rutas de menor costo pueden traducir automáticamente el número interno a una llamada de marcación directa en la red pública mientras otros usuarios están en espera.	https://downloads.avaya.com/css/P8/documents/101049385
o Conservación de llamada ante la recuperación de la conexión al Sistema de Procesamiento.	Administering Avaya IP Office™ Platform with Manager	3	Calls anchored on the home system lose all voice paths during failover. Direct media calls in a stable state might maintain voice paths until the next call event, but this is not guaranteed.	Las llamadas ancladas en el sistema doméstico pierden todas las rutas de voz durante la conmutación por error. Las llamadas de medios directas en un estado estable pueden mantener rutas de voz hasta el próximo evento de llamada, pero esto no está garantizado.	https://documentation.avaya.com/bundle/AdministeringAvayaIPOfficePlatformManagerR11.0/page/ResiliencyPhones.html#

MODELO DE EQUIPO IP OFFICE 500 V2

GATEWAY PARA TRONCALES

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL	URL
El proveedor deberá considerar en su propuesta técnica todos los elementos de hardware, software y licenciamiento necesarios, para operar las troncales que las Dependencias o Entidades tiene contratadas actualmente. Adicionalmente, la solución que ofrezca para el manejo de las troncales digitales, deberá cumplir con las condiciones de operación y/o características técnicas siguientes:	PROPUESTA TÉCNICA	PROPUESTA TÉCNICA	IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro de todos los elementos de hardware, software y licenciamiento necesarios, para operar las troncales que las Dependencias o Entidades tiene contratadas actualmente. Adicionalmente, la solución que se oferta para el manejo de las troncales digitales cumple con las condiciones de operación y/o características técnicas siguientes:	IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro de todos los elementos de hardware, software y licenciamiento necesarios, para operar las troncales que las Dependencias o Entidades tiene contratadas actualmente. Adicionalmente, la solución que se oferta para el manejo de las troncales digitales cumple con las condiciones de operación y/o características técnicas siguientes:	PROPUESTA TÉCNICA
• La solución deberá soportar los siguientes tipos de troncales; IP, SIP, E1 PRI ISDN, E1 con soporte de Q.Sig, troncales analógicas (FXO) y Troncales ISDN BRI y deberá estar preparada con el hardware, software y licenciamiento necesario para operar las troncales digitales E1 R2 Modificado.	Deploying Avaya IP Office™ Platform IP500 V2	42, 27, 314, 240	El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios. La tarjeta puede configurarse para troncales E1 PRI, T1 de hurto de bits, T1 PRI o E1R2 PRI. Conexión ISDN PRI (NET) Conexión ISDN BRI (NET) Troncal analógica de 16 líneas El módulo de Troncales analógicas IP500 se utiliza asimismo para agregar 16 troncales análogas adicionales a un sistema IP Office.	El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios. La tarjeta puede configurarse para troncales E1 PRI, T1 de hurto de bits, T1 PRI o E1R2 PRI. Conexión ISDN PRI (NET) Conexión ISDN BRI (NET) Troncal analógica de 16 líneas El módulo de Troncales analógicas IP500 se utiliza asimismo para agregar 16 troncales análogas adicionales a un sistema IP Office. IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el	

			IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro de el hardware, software y licenciamiento necesario para operar las troncales digitales E1 R2 Modificado.	suministro de el hardware, software y licenciamiento necesario para operar las troncales digitales E1 R2 Modificado.	
• La solución para el manejo de troncales digitales, deberá garantizar que, ante la caída o saturación del grupo de troncales asociadas a un determinado sitio, se podrá realizar de manera automática, la toma de troncal de otro sitio que cuente con este servicio.	Deploying Avaya IP Office™ Platform IP500 V2	107	4.Otra troncal puede configurarse como Reserva en caso de perder la conexión de troncal con la Red. De ser posible, ésta debería ser una troncal de un proveedor distinto, ya que esto disminuye las probabilidades de que ambas fuentes fallen al mismo tiempo.	4.Otra troncal puede configurarse como Reserva en caso de perder la conexión de troncal con la Red. De ser posible, ésta debería ser una troncal de un proveedor distinto, ya que esto disminuye las probabilidades de que ambas fuentes fallen al mismo tiempo.	
• La comunicación entre el Gateway de Voz que se proponga para el manejo de las troncales digitales y el Sistema de Procesamiento de Llamadas IP y Teléfonos IP de las Dependencias o Entidades, se deberá cifrar con al menos AES-128 y utilizar el estándar SRTP.	IP Office Platform Security Guidelines	12, 71	· TLS/SRTP encryption · RTP encryption/authentications setting should be AES-128/CTR plus SHA-1/80.	· TLS/SRTP encryption · RTP encryption/authentications setting should be AES-128/CTR plus SHA-1/80.	https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/manuals/mgr/ipo_security_guidelines.pdf
• La solución para el manejo de las troncales digitales E1, debe contar con la función de cancelación de eco por hardware, conforme ITU-T G.168, además de manejar los tipos de señalizaciones Q.SIG, R2 Modificado, con funciones completas, sin restricción mediante licenciamiento.	Deploying Avaya IP Office™ Platform IP500 V2	229, 231	Códecs G.711, G.729a y G.723 con cancelación de eco de 64ms. · El sistema IP Office admite 8 canales B sin licencia en cada puerto PRI-U IP500 instalado.	Códecs G.711, G.729a y G.723 con cancelación de eco de 64ms. · El sistema IP Office admite 8 canales B sin licencia en cada puerto PRI-U IP500 instalado.	
• La solución deberá incluir los acopladores de impedancia (Balum) necesarios para la correcta operación de la solución.	PROPUESTA TÉCNICA	PROPUESTA TÉCNICA	IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro de los acopladores de impedancia (Balum) necesarios para la correcta operación de la solución.	IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro de los acopladores de impedancia (Balum) necesarios para la correcta operación de la solución.	PROPUESTA TÉCNICA
Los Gateway que se utilicen en la solución para el servicio de Troncales Digitales y Mecanismos de Supervivencia, deberán	n/a	n/a	n/a	n/a	n/a

cumplir con las siguientes características y funcionalidades:					
• Contar con la última versión liberada del Sistema Operativo con que cuente el fabricante al momento de instalar el equipo. La documentación comprobatoria de este requerimiento se deberá integrar en la propuesta del proveedor.	PROPUESTA TÉCNICA	PROPUESTA TÉCNICA	IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica la instalación de la última versión liberada del Sistema Operativo con que cuente el fabricante al momento de instalar el equipo. La documentación comprobatoria de este requerimiento se incluye en la propuesta ofertada.	IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica la instalación de la última versión liberada del Sistema Operativo con que cuente el fabricante al momento de instalar el equipo. La documentación comprobatoria de este requerimiento se incluye en la propuesta ofertada.	PROPUESTA TÉCNICA
• Manejar las siguientes interfaces físicas: Fast Ethernet o Gigabit Ethernet.	Avaya IP Office™ Platform Feature Description	59, 60	Conmutador integral de Ethernet de nivel 3 y 10/100 Mbit La conmutación de capa 3 es de particular utilidad en situaciones donde se desea una red "confiable" e "insegura", donde la red "insegura" no está controlada y lleva el tráfico público. Es posible configurar un firewall entre dos segmentos LAN mediante el conmutador de capa 3 de IP Office. IP500 V2 admite un conmutador Ethernet de capa 3 y dos puertos con el firewall entre ellos. Ambos puertos conmutados tienen sus propias direcciones IP (LAN1 y LAN2)	Conmutador integral de Ethernet de nivel 3 y 10/100 Mbit La conmutación de capa 3 es de particular utilidad en situaciones donde se desea una red "confiable" e "insegura", donde la red "insegura" no está controlada y lleva el tráfico público. Es posible configurar un firewall entre dos segmentos LAN mediante el conmutador de capa 3 de IP Office. IP500 V2 admite un conmutador Ethernet de capa 3 y dos puertos con el firewall entre ellos. Ambos puertos conmutados tienen sus propias direcciones IP (LAN1 y LAN2)	https://downloads.avaya.com/css/P8/documents/101049385
• Manejar las siguientes interfaces físicas: BRI, E1 G.703, troncales E1 para conexión de la PSTN (con manejo de R2 modificado, Q.SIG).	Deploying Avaya IP Office™ Platform IP500 V2	42, 27, 314, 240	El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios. La tarjeta puede configurarse para troncales E1 PRI, T1 de hurto de bits, T1 PRI o E1R2 PRI.	El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios. La tarjeta puede configurarse para troncales E1 PRI, T1 de hurto de bits, T1 PRI o E1R2 PRI.	

			Conexión ISDN PRI (NET) Conexión ISDN BRI (NET) Troncal analógica de 16 líneas El módulo de Troncales analógicas IP500 se utiliza asimismo para agregar 16 troncales análogas adicionales a un sistema IP Office. IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro de el hardware, software y licenciamiento necesario para operar las troncales digitales E1 R2 Modificado.	Conexión ISDN PRI (NET) Conexión ISDN BRI (NET) Troncal analógica de 16 líneas El módulo de Troncales analógicas IP500 se utiliza asimismo para agregar 16 troncales análogas adicionales a un sistema IP Office. IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro de el hardware, software y licenciamiento necesario para operar las troncales digitales E1 R2 Modificado.	
• Manejar Voz sobre IP (VoIP), además de soportar interfaces de voz digital (E1s) con interfaces de voz analógicas de los tipos FXS y FXO.	Deploying Avaya IP Office™ Platform IP500 V2	42, 27, 314, 240	El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios. La tarjeta puede configurarse para troncales E1 PRI, T1 de hurto de bits, T1 PRI o E1R2 PRI. Conexión ISDN PRI (NET) Conexión ISDN BRI (NET) Troncal analógica de 16 líneas El módulo de Troncales analógicas IP500 se utiliza asimismo para agregar 16 troncales análogas adicionales a un sistema IP Office. IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro del hardware, software y licenciamiento necesario para operar	El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios. La tarjeta puede configurarse para troncales E1 PRI, T1 de hurto de bits, T1 PRI o E1R2 PRI. Conexión ISDN PRI (NET) Conexión ISDN BRI (NET) Troncal analógica de 16 líneas El módulo de Troncales analógicas IP500 se utiliza asimismo para agregar 16 troncales análogas adicionales a un sistema IP Office. IP Productos y Servicios, S.A. de C.V. considerar en su propuesta técnica el suministro del hardware, software y licenciamiento necesario para operar las troncales digitales E1 R2 Modificado.	

			las troncales digitales E1 R2 Modificado.		
• Incluir los módulos de digitalización de voz DSP (Digital Signal Processor), necesarios para la correcta operación de la totalidad de los puertos de voz.	Deploying Avaya IP Office™ Platform IP500 V2	25	Esta tarjeta está disponible en variantes que soportan 32 o 64 canales de compresión de voz para el uso con llamadas VoIP.	Esta tarjeta está disponible en variantes que soportan 32 o 64 canales de compresión de voz para el uso con llamadas VoIP.	
• Manejar mecanismos de control de llamadas, para garantizar el ancho de banda necesario para gestionar un número configurable de llamadas máximas simultáneas entre sitios.	Avaya IP Office™ Platform Feature Description	105	Permite la realización de llamadas adicionales donde se requiere un ancho de banda superior a un solo canal. La cantidad máxima de canales disponibles para los datos se puede fijar según el servicio. Cuando el ancho de banda disponible alcanza un límite definido por el usuario, se pueden agregar automáticamente canales adicionales. De la misma forma, cuando el tráfico cae entonces la cantidad de canales en uso se puede reducir automáticamente. Si no hay tráfico de datos en ninguno de los canales en uso, entonces se pueden borrar todas las líneas. Como la mayoría de las transportadoras tienen un costo mínimo para las llamadas, se puede configurar el período en que un canal debe estar inactivo antes de borrarlo. Mediante estos mecanismos los costos de la llamada se pueden controlar eficazmente mientras se asegura que el ancho de banda esté disponible cuando sea necesario.	Permite la realización de llamadas adicionales donde se requiere un ancho de banda superior a un solo canal. La cantidad máxima de canales disponibles para los datos se puede fijar según el servicio. Cuando el ancho de banda disponible alcanza un límite definido por el usuario, se pueden agregar automáticamente canales adicionales. De la misma forma, cuando el tráfico cae entonces la cantidad de canales en uso se puede reducir automáticamente. Si no hay tráfico de datos en ninguno de los canales en uso, entonces se pueden borrar todas las líneas. Como la mayoría de las transportadoras tienen un costo mínimo para las llamadas, se puede configurar el período en que un canal debe estar inactivo antes de borrarlo. Mediante estos mecanismos los costos de la llamada se pueden controlar eficazmente mientras se asegura que el ancho de banda esté disponible cuando sea necesario.	https://downloads.avaya.com/css/P8/documents/101049385

• Contar con la capacidad de manejo de los protocolos HTTP, HTTPS, SMTP, SIP, TLS, IPv4 IPv6.	Deploying Avaya IP Office™ Platform IP500 V2 Application Notes for Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0.1 with AT&T IP Toll Free Service using IPv6 - Issue 1.0	46, 70, 69 9, 59	· Las alarmas que se pueden configurar para salir vía SNP pueden ser también enrutadas a correo electrónico SMTP y/o Syslog. El Protocolo predeterminado es UDP. La aplicación también admite conexiones TCP, HTTP y HTTPS. · Conexión segura Utiliza una conexión TLS cifrada al sistema. IP Office LAN1 interface connected to the CPE private network. (IPv4) The outside IPv6 Address of the Avaya SBCE on the B1 interface was selected from the drop-down menu.	· Las alarmas que se pueden configurar para salir vía SNP pueden ser también enrutadas a correo electrónico SMTP y/o Syslog. El Protocolo predeterminado es UDP. La aplicación también admite conexiones TCP, HTTP y HTTPS. · Conexión segura Utiliza una conexión TLS cifrada al sistema. IP Office LAN1 interface connected to the CPE private network. (IPv4) The outside IPv6 Address of the Avaya SBCE on the B1 interface was selected from the drop-down menu.	https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/appnotes/2020/TF-IPO11SBC8IP6.pdf
• Soporte de configuración de hora vía NTP	Date and Time Settings	1	•Enable Network Time Protocol When selected, the server obtains the current date and time from the NTP servers listed in the NTPServers list below. It then uses that date and time and makes regular NTP requests for updates.	• Habilitar el protocolo de tiempo de red Cuando se selecciona, el servidor obtiene la fecha y hora actuales de los servidores NTP que se enumeran en la lista NTPServers a continuación. Luego usa esa fecha y hora y realiza solicitudes periódicas de NTP para actualizaciones.	https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/appliance/_hm_print_window.htm?date_and_time_settings.htm
• Soportar los códec G.711a, G.711u, G.722, G.729a y G.729ab e iLBC.	Deploying Avaya IP Office™ Platform IP500 V2	43	Estos son compatibles con los códecs comunes de audio IP G.711, G.723 y G.729a. Las tarjetas combinadas VCM IP500 e IP500 también admiten G.722	Estos son compatibles con los códecs comunes de audio IP G.711, G.723 y G.729a.	
• Contar con la capacidad de manejar las llamadas simultáneas de voz necesarias, para atender los requerimientos de los usuarios en los sitios donde se instalarán.	Deploying Avaya IP Office™ Platform IP500 V2	25	Esta tarjeta está disponible en variantes que soportan 32 o 64 canales de compresión de voz para el uso con llamadas VoIP.	Esta tarjeta está disponible en variantes que soportan 32 o 64 canales de compresión de voz para el uso con llamadas VoIP.	
• Manejar el modo de operación de conmutador IP de contingencia,	Avaya IP Office™ Platform	40	Las siguientes funciones se encuentran disponibles	Las siguientes funciones se encuentran disponibles en los teléfonos SIP	https://downloads.avaya.com/css/P8/documents/101049385

soportando el Servicio de Supervivencia para la totalidad de terminales IP y analógicas de los sitios donde se instalarán.	Feature Description		en los teléfonos SIP centralizados de la serie 9600 cuando están registrados en IP Office con el modo Día lluvioso:	centralizados de la serie 9600 cuando están registrados en IP Office con el modo Día lluvioso:	
• Contar con la capacidad y recursos para manejar al menos, 5 conferencias simultáneas de voz de 6 participantes	Deploying Avaya IP Office™ Platform IP500 V2	209	128 como estándar, pero máximo 64 en cualquier conferencia individual. Se aplica la supresión de silencio a las conferencias con más de 10 participantes.	128 como estándar, pero máximo 64 en cualquier conferencia individual. Se aplica la supresión de silencio a las conferencias con más de 10 participantes.	
• Manejar los estándares IEEE 802.1q, SNMP y SIP.	Avaya IP Office™ Platform Feature Description	103, 197, 42	• 802.1Q La información disponible vía SNMP Como se describió anteriormente, la información SNMP puede ser encuestada por la aplicación SNMP o recibida como resultado de una trampa SNMP enviada por IP Office. El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios.	• 802.1Q La información disponible vía SNMP Como se describió anteriormente, la información SNMP puede ser encuestada por la aplicación SNMP o recibida como resultado de una trampa SNMP enviada por IP Office. El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios.	https://downloads.avaya.com/css/P8/documents/101049385
• La administración del equipo deberá estar basada en control de acceso por roles y deberá poder realizarse vía puerto de consola	Deploying Avaya IP Office™ Platform IP500 V2	62	· IP Office Manager Esta es una aplicación basada en Windows. IP Office Manager se usa para acceder todo de la configuración de IP Office. Pueden definirse distintos niveles de acceso para controlar cuáles partes de la configuración puede visualizar y modificar el usuario. También puede utilizar IP Office Manager para actualizar los archivos del software utilizado por el sistema IP Office.	· IP Office Manager Esta es una aplicación basada en Windows. IP Office Manager se usa para acceder todo de la configuración de IP Office. Pueden definirse distintos niveles de acceso para controlar cuáles partes de la configuración puede visualizar y modificar el usuario. También puede utilizar IP Office Manager para actualizar los archivos del software utilizado por el sistema IP Office.	

MODELO DE EQUIPO INTERTEL SUITE

SERVICIO DE TARIFICACIÓN TELEFÓNICA

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL
Para la operación de tarificación se requiere un sistema de procesamiento del registro detallado de llamadas, CDR (Call Detail Recording por sus siglas en inglés), esta facilidad proporciona el detalle de las operaciones que realiza el sistema de telefonía.	PROPUESTA TECNICA	PROPUESTA TECNICA	Para la operación de tarificación, IP Productos y Servicios, S.A. de C.V. hace el suministro de un sistema de procesamiento del registro detallado de llamadas, CDR (Call Detail Recording por sus siglas en inglés), esta facilidad proporciona el detalle de las operaciones que realiza el sistema de telefonía.	PROPUESTA TECNICA
● Número de llamadas por categorías:				
o Móvil	Características Intertel Codes	2	móviles	móviles
o Fijo	Características Intertel Codes	3	Local Celular local Larga distancia nacional Celular nacional Larga distancia Internacional Internas Red Servicios Números 800 Números 900	Local Celular local Larga distancia nacional Celular nacional Larga distancia Internacional Internas Red Servicios Números 800 Números 900
o Local	Características Intertel Codes	3	Local Celular local Larga distancia nacional Celular nacional Larga distancia Internacional Internas Red Servicios Números 800 Números 900	Local Celular local Larga distancia nacional Celular nacional Larga distancia Internacional Internas Red Servicios Números 800 Números 900
o Nacional	Características Intertel Codes	3	Local Celular local Larga distancia nacional Celular nacional Larga distancia Internacional Internas Red Servicios Números 800 Números 900	Local Celular local Larga distancia nacional Celular nacional Larga distancia Internacional Internas Red Servicios Números 800 Números 900
o Internacional	Características Intertel Codes	3	Local Celular local Larga distancia nacional Celular nacional Larga distancia Internacional Internas	Local Celular local Larga distancia nacional Celular nacional Larga distancia Internacional Internas

			Red Servicios Números 800 Números 900	Red Servicios Números 800 Números 900
• Fecha, hora y duración de llamadas	Portal de Reportes - Manual de Usuario	50	indica los totales por la hora en la que se realizaron las llamadas, por el día de la semana o por la fecha	indica los totales por la hora en la que se realizaron las llamadas, por el día de la semana o por la fecha
• Origen y destino	Portal de Reportes - Manual de Usuario	53	Llamadas finalizadas por origen o destino	Llamadas finalizadas por origen o destino
• Costos de llamada por proveedor y tipo de llamada.	Portal de Reportes - Manual de Usuario	59	Importe (costo de la llamada).	Importe (costo de la llamada).
• Identificar códigos de autorización por usuario.	Características Intertel Codes	3	usuarios en base a códigos	usuarios en base a códigos
Los resultados generados por el reporte avanzado deberán podér ser impresos, exportados en diferentes formatos o visualizados en pantalla.	Portal de Reportes - Manual de Usuario	23	Con Intertel, cada usuario podrá consultar el Dashboard O también pueden ser impresos o exportados en formato PDF, JPEG, PNG, SVG.	Con Intertel, cada usuario podrá consultar el Dashboard O también pueden ser impresos o exportados en formato PDF, JPEG, PNG, SVG.
Obtención de reportes reportes de Directorio Telefónico de extensiones, ordenar por número de extensión, alfabético por nombre o por departamento.	Portal de Reportes - Manual de Usuario	16	Directorio telefónico Desde el Portal de Reportes usted tendrá acceso al listado telefónico de su empresa	Directorio telefónico Desde el Portal de Reportes usted tendrá acceso al listado telefónico de su empresa

CORREO DE VOZ CON SERVICIO DE MENSAJERÍA

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL	URL
El proveedor deberá considerar en su propuesta técnica como parte de la solución para los Servicios de Voz, los Sistemas de Correo de Voz con Servicios de Mensajería, mismos que el administrador del contrato de "Las Requirentes", validará y/o ajustará en la fase de planeación para efectos de la implementación, sin embargo, durante la vigencia del contrato podrán ser modificados en cantidades de acuerdo	PROPUESTA TECNICA	PROPUESTA TECNICA	IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica como parte de la solución para los Servicios de Voz, los Sistemas de Correo de Voz con Servicios de Mensajería, mismos que el administrador del contrato de "Las Requirentes", validará y/o ajustará en la fase de planeación para efectos de la implementación, sin embargo, durante la vigencia del contrato	IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica como parte de la solución para los Servicios de Voz, los Sistemas de Correo de Voz con Servicios de Mensajería, mismos que el administrador del contrato de "Las Requirentes", validará y/o ajustará en la fase de planeación para efectos de la implementación, sin embargo, durante la vigencia del contrato podrán ser modificados en cantidades de acuerdo con	PROPUESTA TECNICA

con las solicitudes de "Las Requirentes", sin costo de implementación adicional para "Las Requirentes", lo anterior para ofrecer estas funcionalidades a los usuarios del Servicio integral de telefonía y telecomunicaciones, sin importar el sitio donde se encuentren.			podrán ser modificados en cantidades de acuerdo con las solicitudes de "Las Requirentes", sin costo de implementación adicional para "Las Requirentes", lo anterior para ofrecer estas funcionalidades a los usuarios del Servicio integral de telefonía y telecomunicaciones, sin importar el sitio donde se encuentren.	las solicitudes de "Las Requirentes", sin costo de implementación adicional para "Las Requirentes", lo anterior para ofrecer estas funcionalidades a los usuarios del Servicio integral de telefonía y telecomunicaciones, sin importar el sitio donde se encuentren.	
La solución de Correo de Voz con Servicios de Mensajería para el Servicio de telefonía IP, deberán cumplir con las características técnicas y/o funcionalidades siguientes:	PROPUESTA TECNICA	PROPUESTA TECNICA	La solución de Correo de Voz con Servicios de Mensajería para el Servicio de telefonía IP propuesta por IP Productos y Servicios, S.A. de C.V. ,cumple con las características técnicas y/o funcionalidades siguientes:	La solución de Correo de Voz con Servicios de Mensajería para el Servicio de telefonía IP propuesta por IP Productos y Servicios, S.A. de C.V. ,cumple con las características técnicas y/o funcionalidades siguientes:	PROPUESTA TECNICA
• Contar con la capacidad de habilitar el servicio de mensajería de voz por usuario, el cual podrá ser consultado mediante una tecla de acceso rápido en el teléfono, con el uso de una clave de usuario y contraseña como medida de seguridad.	Avaya 9641GS IP Deskphone Using Avaya 9621G/9641G/9641GS IP Deskphones SIP	3 15	Permanently-labeled feature buttons: speaker, mute, headset, contacts, home, history, message, phone, forwarding, volume (separate volume levels in handset, speaker, ringer, and headset) • Red LEDs for speaker, mute, headset, message and history Scrolling and navigation Use the up and down arrow buttons on the right side of the screen to scroll up or down the list. Es posible acceder a los mensajes de correo de voz de forma local o remota a través de cualquier teléfono (el sistema le solicitará a los usuarios ingresar un PIN si utilizan un teléfono diferent+D9e al de su extensión o	Botones de función etiquetados permanentemente: altavoz, silencio, auriculares, contactos, inicio, historial, mensaje, teléfono, reenvío, volumen (volumen separado niveles en el auricular, el altavoz, el timbre y los auriculares) • LED rojos para altavoz, silencio, auriculares, mensaje e historial Desplazamiento y navegación Use los botones de flecha hacia arriba y hacia abajo en el lado derecho de la pantalla para desplazarse hacia arriba o hacia abajo en la lista Es posible acceder a los mensajes de correo de voz de forma local o remota a través de cualquier teléfono (el sistema le solicitará a los usuarios ingresar un PIN si utilizan un teléfono diferent+D9e	https://downloads.avaya.com/css/P8/documents/101049385

			ubicación asignada, por ejemplo un teléfono celular).	al de su extensión o ubicación asignada, por ejemplo un teléfono celular).	
• Contar con la facilidad de acceso a los mensajes de voz, desde cualquier teléfono dentro o fuera de la Red de "Las Requirentes", marcando a un número directo donde deberá contestar una grabación que solicite el número de extensión y contraseña del buzón de voz y, en caso de ser válidos, indicará la cantidad de mensajes que se tienen pendientes de escuchar, permitiendo escucharlos, guardarlos o borrarlos.	Avaya IP Office™ Platform Feature Description	42	Es posible acceder a los mensajes de correo de voz de forma local o remota a través de cualquier teléfono (el sistema le solicitará a los usuarios ingresar un PIN si utilizan un teléfono diferent+D9e al de su extensión o ubicación asignada, por ejemplo un teléfono celular).	Es posible acceder a los mensajes de correo de voz de forma local o remota a través de cualquier teléfono (el sistema le solicitará a los usuarios ingresar un PIN si utilizan un teléfono diferent+D9e al de su extensión o ubicación asignada, por ejemplo un teléfono celular).	https://downloads.avaya.com/css/P8/documents/101049385
• Contar con la capacidad de personalizar un mínimo de 3 diferentes mensajes de bienvenida, configurables por el administrador del Sistema o por el usuario a través de su Teléfono IP, que se puedan activar o desactivar a consideración del usuario o administrador del sistema (opcional).	Avaya IP Office™ Platform Feature Description	44	Saludos personalizados Sí Saludos personales extendidos Sí	Saludos personalizados Sí Saludos personales extendidos Sí	https://downloads.avaya.com/css/P8/documents/101049385
• Contar con la funcionalidad de aviso de mensajes de voz normal y/o urgente	Avaya IP Office™ Platform Feature Description	41	Definir prioridad de mensajes Sí	Definir prioridad de mensajes Sí	https://downloads.avaya.com/css/P8/documents/101049385
• Contar con la funcionalidad de poder asociar extensiones alternas configurables por el administrador o por el usuario, asociadas a un mismo buzón de voz.	Avaya IP Office™ Platform Feature Description	47	El uso compartido de escritorio le permite a los usuarios el uso no exclusivo de una única extensión. El usuario inicia sesión con su propia identidad, de modo que puede recibir las llamadas y acceder a su propio correo de voz y a otros servicios.	El uso compartido de escritorio le permite a los usuarios el uso no exclusivo de una única extensión. El usuario inicia sesión con su propia identidad, de modo que puede recibir las llamadas y acceder a su propio correo de voz y a otros servicios.	https://downloads.avaya.com/css/P8/documents/101049385
• El Servicio de correo de voz debe soportar SMTP para enviar los mensajes de voz vía correo electrónico a los usuarios. La solución deberá permitir que, al abrir el	Avaya IP Office™ Platform Feature Description	42, 44	Funciones de mensajería El servicio de mensajería le permite a los usuarios administrar todos sus mensajes, es decir los	Funciones de mensajería El servicio de mensajería le permite a los usuarios administrar todos sus mensajes, es decir los mensajes de correo electrónico y de correo de	https://downloads.avaya.com/css/P8/documents/101049385

mensaje, este pueda ser escuchado y manejado por medio de controles que permitan avanzar, retroceder, detener, acelerar o ralentizar el mensaje para su mejor comprensión.			mensajes de correo electrónico y de correo de voz, en un solo lugar. Guardar mensaje Eliminar mensaje Reenviar mensaje a otro buzón Reenviar a varios buzones Reenviar con mensaje de enca bezado Repetir mensaje Retroceder mensaje Avanzar mensaje Saltar un mensaje	voz, en un solo lugar. Guardar mensaje Eliminar mensaje Reenviar mensaje a otro buzón Reenviar a varios buzones Reenviar con mensaje de enca bezado Repetir mensaje Retroceder mensaje Avanzar mensaje Saltar un mensaje	
• La solución de Mensajería deberá contar con capacidad de almacenaje para cada uno de los buzones de mensajes de voz de al menos 5 minutos y soportar protocolos SIP y SRTP. La cantidad de canales hacia la solución de correo de voz con mensajería requerida será determinada por cada una de "Las Requirentes", así como la cantidad de mensajes por buzón a almacenar.	Avaya IP Office™ Platform Feature Description	43, 74, 109	Tiempo de grabación Dependiente de la PC (requiere 1 MB por minuto) • Compatibilidad con TSL/SRTP RFC 3261 [8] SIP: protocolo de inicio de sesión La cantidad de canales hacia la solución de correo de voz con mensajería requerida será determinada por IP Productos y Servicios, S.A. de C.V., así como la cantidad de mensajes por buzón a almacenar.	Tiempo de grabación Dependiente de la PC (requiere 1 MB por minuto) • Compatibilidad con TSL/SRTP RFC 3261 [8] SIP: protocolo de inicio de sesión La cantidad de canales hacia la solución de correo de voz con mensajería requerida será determinada por IP Productos y Servicios, S.A. de C.V., así como la cantidad de mensajes por buzón a almacenar.	https://downloads.avaya.com/css/P8/documents/101049385

MODELO DE EQUIPO AVAYA CONTACT CENTER SELECT

DISTRIBUCIÓN AUTOMÁTICA DE LLAMADAS

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL	URL
El Proveedor deberá considerar en su propuesta técnica, el hardware, software y licenciamiento necesario para Distribución Automática de Llamadas (Automatic Call Distribution o ACD por sus siglas en ingles), que se implementará a través del Sistema de Procesamiento	PROPUESTA TECNICA	PROPUESTA TECNICA	IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica, el hardware, software y licenciamiento necesario para Distribución Automática de Llamadas (Automatic Call Distribution o ACD por sus siglas en ingles),	PROPUESTA TECNICA	El Proveedor deberá considerar en su propuesta técnica, el hardware, software y licenciamiento necesario para Distribución Automática de Llamadas (Automatic Call Distribution o ACD por sus siglas en ingles), que se implementará a través del Sistema de

de Llamadas IP y deberá contar con las funcionalidades siguientes:			que se implementará a través del Sistema de Procesamiento de Llamadas IP y que cuenta con las funcionalidades siguientes:		Procesamiento de Llamadas IP y deberá contar con las funcionalidades siguientes:
• Selección de línea secuencial	Administering Avaya IP Office™ Platform with Manager	697	Sequential Group (formerly Hunt or Linear Group)	Grupo secuencial (anteriormente Hunt o Grupo lineal)	• Selección de línea secuencial
• Bajo este esquema el sistema deberá enrutar la llamada hacia los agentes disponibles basándose en el orden de ingreso de estos al sistema. Esto es, que las llamadas deberán ser preferentemente enrutadas hacia aquellos agentes disponibles que hayan ingresado con mayor anticipación al sistema	Avaya Contact Center Select Solution Description	153	The Experience Portal applications then collect the customer's response and return it to Avaya Contact Center Select for further treatments, or routing to the next available and appropriate Agent.	Las aplicaciones de Experience Portal luego recopilan la respuesta del cliente y la devuelven a Avaya Contact Center Select para recibir más tratamientos, o enviarla al siguiente Agente disponible y apropiado.	• Bajo este esquema el sistema deberá enrutar la llamada hacia los agentes disponibles basándose en el orden de ingreso de estos al sistema. Esto es, que las llamadas deberán ser preferentemente enrutadas hacia aquellos agentes disponibles que hayan ingresado con mayor anticipación al sistema
• Re-direccionamiento a servicio nocturno	Avaya Contact Center Select Solution Description	124	Night Service Yes Avaya Contact Center Select	Servicio nocturno Sí Avaya Contact Center Select	• Re-direccionamiento a servicio nocturno
• Bajo este esquema las llamadas deberán ser redireccionadas hacia un servicio nocturno en el caso de que todos los agentes se encuentren ocupados, o bien hayan salido del sistema	Avaya Contact Center Select Solution Description	134, 47	Forward on Busy = Yes These treatments can tell callers the estimated amount of time before their call is answered or play music to callers while they wait in queue. Additionally, you can use time of day, day of week, or contact center activity to determine how a contact is handled.	Reenviar si ocupado = Sí Estos tratamientos pueden indicar a las personas que llaman la cantidad estimada de tiempo antes de que se responda su llamada, o reproducir música para las personas que llaman mientras esperan en la cola. Además, puede utilizar la hora del día, el día de la semana o la actividad del centro de contacto para determinar cómo se gestiona un contacto.	• Bajo este esquema las llamadas deberán ser re direccionadas hacia un servicio nocturno en el caso de que todos los agentes se encuentren ocupados, o bien hayan salido del sistema
• Encolamiento de llamadas cuando todos los agentes se encuentran ocupados	Avaya Contact Center Select Solution Description	136	Queuing = Yes Configure system to limit the number of calls that can be waiting to be serviced in a hunt group. For example, when all parties in the group are busy.	Cola = Sí Configure el sistema para limitar la cantidad de llamadas que pueden estar esperando ser atendidas en un grupo de búsqueda. Por ejemplo, cuando todas las partes del grupo están ocupadas.	• Encolamiento de llamadas cuando todos los agentes se encuentran ocupados

• El sistema deberá ser capaz de mantener encoladas todas las nuevas llamadas hasta que un agente que estaba ocupado se libere y conteste la llamada	Avaya Contact Center Select Solution Description	136	Queuing = Yes Configure system to limit the number of calls that can be waiting to be serviced in a hunt group. For example, when all parties in the group are busy. These treatments can tell callers the estimated amount of time before their call is answered or play music to callers while they wait in queue. Additionally, you can use time of day, day of week, or contact center activity to determine how contact is handled.	Cola = Sí Configure el sistema para limitar la cantidad de llamadas que pueden estar esperando ser atendidas en un grupo de búsqueda. Por ejemplo, cuando todas las partes del grupo están ocupadas. Estos tratamientos pueden indicar a las personas que llaman la cantidad estimada de tiempo antes de que se responda su llamada, o reproducir música para las personas que llaman mientras esperan en la cola. Además, puede utilizar la hora del día, el día de la semana o la actividad del centro de contacto para determinar cómo se gestiona un contacto.	• El sistema deberá ser capaz de mantener encoladas todas las nuevas llamadas hasta que un agente que estaba ocupado se libere y conteste la llamada
• Encolamiento de llamadas con re direccionamiento posterior hacia un usuario virtual (opcional)	Avaya Contact Center Select Solution Description	136, 47	Queuing = Yes Configure system to limit the number of calls that can be waiting to be serviced in a hunt group. For example, when all parties in the group are busy. These treatments can tell callers the estimated amount of time before their call is answered, or play music to callers while they wait in queue. Additionally, you can use time of day, day of week, or contact center activity to determine how a contact is handled.	Cola = Sí Configure el sistema para limitar la cantidad de llamadas que pueden estar esperando ser atendidas en un grupo de búsqueda. Por ejemplo, cuando todas las partes del grupo están ocupadas. Estos tratamientos pueden indicar a las personas que llaman la cantidad estimada de tiempo antes de que se responda su llamada, o reproducir música para las personas que llaman mientras esperan en la cola. Además, puede utilizar la hora del día, el día de la semana o la actividad del centro de contacto para determinar cómo se gestiona un contacto.	• Encolamiento de llamadas con redireccionamiento posterior hacia un usuario virtual (opcional)
• Ajuste de Prioridad de Encolamiento	Avaya Contact Center Select Solution Description	52	you can configure routing rules to use in rule groups. Use keyword groups and sender groups to decide how to route contacts. Configure which skillset and priority the email	puede configurar reglas de enrutamiento para usar en grupos de reglas. Utilice grupos de palabras clave y grupos de remitentes para decidir cómo enrutar los contactos. Configure el conjunto de habilidades y	• Ajuste de Prioridad de Encolamiento

			contact is assigned to, based on the input for routing contacts.	la prioridad a la que se asigna el contacto de correo electrónico, según la entrada para enrutar contactos.	
• El sistema deberá ser capaz de permitir ajustar la secuencia en la cual las llamadas son contestadas basándose en la prioridad de las mismas. De esta manera, al recibir una llamada con alta prioridad hacia una determinada cola de atención y todos los agentes pertenecientes a la misma se encuentren ocupados, el agente deberá ser capaz de poner esta llamada en primer lugar de la cola pudiendo contestar la llamada de alta prioridad inmediatamente después de haber concluido su llamada actual dejando así las llamadas menos importantes en la cola.	Avaya Contact Center Select Solution Description	52	you can configure routing rules to use in rule groups. Use keyword groups and sender groups to decide how to route contacts. Configure which skillset and priority the email contact is assigned to, based on the input for routing contacts.	puede configurar reglas de enrutamiento para usar en grupos de reglas. Utilice grupos de palabras clave y grupos de remitentes para decidir cómo enrutar los contactos. Configure el conjunto de habilidades y la prioridad a la que se asigna el contacto de correo electrónico, según la entrada para enrutar contactos.	• El sistema deberá ser capaz de permitir ajustar la secuencia en la cual las llamadas son contestadas basándose en la prioridad de las mismas. De esta manera, al recibir una llamada con alta prioridad hacia una determinada cola de atención y todos los agentes pertenecientes a la misma se encuentren ocupados, el agente deberá ser capaz de poner esta llamada en primer lugar de la cola pudiendo contestar la llamada de alta prioridad inmediatamente después de haber concluido su llamada actual dejando así las llamadas menos importantes en la cola.
• Deberá contar con la capacidad de asignar diferentes Perfiles a los agentes y configurar diferentes Perfiles por grupo de agentes.	Avaya Contact Center Select Solution Description	25	The skillset drop-down list is grouped by contact type and then sorted alphabetically within the contact type group.	La lista desplegable del conjunto de habilidades se agrupa por tipo de contacto y luego se ordena alfabéticamente dentro del grupo de tipo de contacto.	• Deberá contar con la capacidad de asignar diferentes Perfiles a los agentes y configurar diferentes Perfiles por grupo de agentes.
• Si la solución está basada en Sistema Operativo Windows, el Proveedor deberá proporcionar el software de antivirus necesario. El software de antivirus deberá mantenerse actualizado durante la vigencia de la garantía.	Avaya Contact Center Select Solution Description	15	Avaya Contact Center Select Release 7.0 is supported on the Microsoft Windows Server 2012 R2 operating system.	Avaya Contact Center Select versión 7.0 es compatible con el sistema operativo Microsoft Windows Server 2012 R2.	• Si la solución está basada en Sistema Operativo Windows, el Proveedor deberá proporcionar el software de antivirus necesario. El software de antivirus deberá mantenerse actualizado durante la vigencia de la garantía.
• Deberá soportar la capacidad de grabación de llamadas de manera automática	Avaya Contact Center Select Solution Description	52	Call Recording Avaya Contact Center Select supports IP Office Call Recording. IP Office Call Recording provides regulatory type recording, including the option to pause automatic recording for Payment	Grabación de llamada Avaya Contact Center Select es compatible con la grabación de llamadas de IP Office. La grabación de llamadas de IP Office proporciona una grabación de tipo reglamentario, incluida la opción de pausar la	• Deberá soportar la capacidad de grabación de llamadas de manera automática

			Card Industry (PCI) security compliance.	grabación automática para el cumplimiento de la seguridad de la industria de tarjetas de pago (PCI).	
• Identificación visual desde el teléfono de si hay una o más llamadas en espera, para agilizar la llamada que se tiene en el momento.	Avaya Contact Center Select Solution Description	59	Agent Desktop always uses 3–line appearance with reserve last call appearance, regardless of the IP Office settings on the agent's phone. When an agent logs on using Agent Desktop, the Agent Desktop phone configuration overrides the IP Office phone configuration.	Agent Desktop siempre usa una apariencia de 3 líneas con reserva de última llamada, independientemente de la configuración de IP Office en el teléfono del agente. Cuando un agente inicia sesión con Agent Desktop, la configuración del teléfono de Agent Desktop anula la configuración del teléfono de IP Office.	• Identificación visual desde el teléfono de si hay una o más llamadas en espera, para agilizar la llamada que se tiene en el momento.
• Contestación automática al momento de asignar al agente, es decir, el agente no debe presionar ningún botón para que la llamada sea considerada como atendida.	Avaya Contact Center Select Solution Description	60	After the answer feature is available any subsequent attempts to answer a call in Agent Desktop are successful.	Una vez que la función de respuesta está disponible, cualquier intento posterior de responder una llamada en Agent Desktop se realiza correctamente.	• Contestación automática al momento de asignar al agente, es decir, el agente no debe presionar ningún botón para que la llamada sea considerada como atendida.
• Configuración de los mensajes que escuchará el usuario cuando; todos los operadores estén ocupados, la llamada se reciba fuera de los horarios de servicio, así como de los mensajes que se requieran por parte de **LAS DEPENDENCIAS o ENTIDADES**.	Avaya Contact Center Select Solution Description	47	These treatments can tell callers the estimated amount of time before their call is answered or play music to callers while they wait in queue. Additionally, you can use time of day, day of week, or contact center activity to determine how a contact is handled.	Estos tratamientos pueden indicar a las personas que llaman la cantidad estimada de tiempo antes de que se responda su llamada, o reproducir música para las personas que llaman mientras esperan en la cola. Además, puede utilizar la hora del día, el día de la semana o la actividad del centro de contacto para determinar cómo se gestiona un contacto.	• Configuración de los mensajes que escuchará el usuario cuando; todos los operadores estén ocupados, la llamada se reciba fuera de los horarios de servicio, así como de los mensajes que se requieran por parte de **LAS DEPENDENCIAS o ENTIDADES**.
• Capacidad de generar reportes de distribución de llamadas, llamadas abandonadas, nivel de servicio, llamadas por agente entre otros.	Avaya Contact Center Select Solution Description	127	Historical Reports Scheduled Interval Daily Weekly Monthly Quarterly Skillset Trunk Agents Abandoned Contacts Overflow Contacts Threshold Exceeded Contact Classification Source Of Disconnect Agent Station Key Email Report Notifications System Status Reports	Informes históricos Programado Intervalo Diario Semanal Mensual Trimestral Conjunto de habilidades Maletero Agentes Contactos abandonados Contactos de desbordamiento Umbral excedido Clasificación de contactos Fuente de desconexión Clave de la estación del agente Informe de correo	• Capacidad de generar reportes de distribución de llamadas, llamadas abandonadas, nivel de servicio, llamadas por agente entre otros.

				electrónico Notificaciones Informes de estado del sistema	

SERVICIO DE OPERADORA AUTOMÁTICA

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	PÁGINA DEL DOCUMENTO DE REFERENCIA	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL
Se entenderá como Servicios de Operadora Automática, la funcionalidad asociada a un Sistema de Procesamiento de Llamadas IP, para que las llamadas de usuarios externos o internos, dirigidas a un número de grupo de troncales de las Dependencias o Entidades, las distribuya el sistema de procesamiento a la operadora automática, misma que le ofrecerá al usuario de forma automática la opción de consulta y/o solicitud de información o enviarlo a una determinada extensión (con o sin DID asociado).	Operadora Automática 1	1	Marcación por número Esta opción permite que quienes llaman con teléfonos DTMF maquen el número de extensión del usuario que requieren. No se establece ningún destino para esta opción. Se debe incluir el aviso para usar esta opción en el saludo con las opciones del menú dela operadora automática. Se requiere un número de extensión con una longitud uniforme para todos los usuarios y los miembros del grupo de búsqueda. La configuración Marcación directa por número de la operadora automática afecta el funcionamiento de esta opción. Transferencia Normal Se puede utilizar con o sin una configuración de Destino. Cuando no existe una configuración de Destino, esta acción se comporta como una acción de Marcación por número. Cuando hay una configuración de Destino, esta acción espera una conexión antes de transferir la llamada. El llamador puede escuchar una música en espera. No se escuchan anuncios.	Marcación por número Esta opción permite que quienes llaman con teléfonos DTMF maquen el número de extensión del usuario que requieren. No se establece ningún destino para esta opción. Se debe incluir el aviso para usar esta opción en el saludo con las opciones del menú dela operadora automática. Se requiere un número de extensión con una longitud uniforme para todos los usuarios y los miembros del grupo de búsqueda. La configuración Marcación directa por número de la operadora automática afecta el funcionamiento de esta opción. Transferencia Normal Se puede utilizar con o sin una configuración de Destino. Cuando no existe una configuración de Destino, esta acción se comporta como una acción de Marcación por número. Cuando hay una configuración de Destino, esta acción espera una conexión antes de transferir la llamada. El llamador puede escuchar una música en espera. No se escuchan anuncios.
Por lo anterior el Proveedor deberá considerar en su propuesta técnica el Servicio de Operadora Automática cumpliendo con lo siguiente:	PROPUESTA TÉCNICA	PROPUESTA TÉCNICA	Por lo anterior IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica el Servicio de Operadora Automática cumpliendo con lo siguiente:	Por lo anterior IP Productos y Servicios, S.A. de C.V. considera en su propuesta técnica el Servicio de Operadora Automática cumpliendo con lo siguiente:
• El Servicio de Operadora Automática	Operadora Automática 1	1, 2	Transferencia de Centrex Marcación por nombre	Transferencia de Centrex Marcación por nombre

deberá proveer un menú de opciones de navegación, para dividir fácilmente el tráfico en áreas de atención y, en caso de solicitarlo las Dependencias o Entidades, en requerimientos de información más especializados, para canalizar las llamadas a su destino correspondiente. El administrador del contrato de las Dependencias o Entidades, en conjunto con el proveedor que resulte adjudicado, establecerán en la fase de planeación los menús de navegación y la política para el desborde de las llamadas, así mismo, la solución deberá contar con la posibilidad de ofrecer dos menús, uno para el día (horario hábil de atención), y uno para la noche (informativo), de acuerdo a las solicitudes de las Dependencias o Entidades.			Marcación por número Transferencia normal Sin definir Estacionar y enviar anuncio Volver a reproducir saludo Transferencia Transferencia a una operadora Destino	Marcación por número Transferencia normal Sin definir Estacionar y enviar anuncio Volver a reproducir saludo Transferencia Transferencia a una operadora Destino
• Cuando se seleccione una opción inválida en el menú, se deberá transferir la llamada al inicio del mismo. Si no se selecciona ninguna opción del menú, la llamada deberá transferirse automáticamente al Servicio de Operadora Manual después de un tiempo programable.	Operadora Automática 1	2	Volver a reproducir saludo Reproducir nuevamente el saludo de la operadora automática. Transferencia Transfiere la llamada al destino seleccionado. Se trata de una transferencia no supervisada; si el usuario que llama no obtiene respuesta, la llamada se administra como si fuera una llamada directa a ese número. Transferencia a una operadora Esta acción se puede realizar para transferir llamadas a otra operadora automática existente.	Volver a reproducir saludo Reproducir nuevamente el saludo de la operadora automática. Transferencia Transfiere la llamada al destino seleccionado. Se trata de una transferencia no supervisada; si el usuario que llama no obtiene respuesta, la llamada se administra como si fuera una llamada directa a ese número. Transferencia a una operadora Esta acción se puede realizar para transferir llamadas a otra operadora automática existente.
• La Operadora Automática deberá contar con la facilidad de enrutar la llamada hacia algún número de extensión de las Dependencias o	Operadora Automática 1	1, 2	Marcación por número Esta opción permite que quienes llaman con teléfonos DTMF maquen el número de extensión del usuario que requieren. No se establece	Marcación por número Esta opción permite que quienes llaman con teléfonos DTMF maquen el número de extensión del usuario que requieren. No se establece ningún destino para esta opción. Se

Entidades con o sin DID asociado, siempre y cuando el llamante externo lo conozca y lo digite. El Sistema de Procesamiento de Llamadas IP, deberá poder supervisar la transferencia de la llamada, si el usuario se encuentra en estado libre o desviado a otra extensión, la llamada se transferirá, si el usuario está ocupado, el llamante será dirigido al buzón de voz del mismo, en caso de contar con este servicio.			ningún destino para esta opción. Se debe incluir el aviso para usar esta opción en el saludo con las opciones del menú dela operadora automática. Se requiere un número de extensión con una longitud uniforme para todos los usuarios y los miembros del grupo de búsqueda. La configuración Marcación directa por número de la operadora automática afecta el funcionamiento de esta opción. Transferencia Normal Se puede utilizar con o sin una configuración de Destino. Cuando no existe una configuración de Destino, esta acción se comporta como una acción de Marcación por número. Cuando hay una configuración de Destino, esta acción espera una conexión antes de transferir la llamada. El llamador puede escuchar una música en espera. No se escuchan anuncios. Transferencia, transfiere la llamada al destino seleccionado. Se trata de una transferencia no supervisada; si el usuario que llama no obtiene respuesta, la llamada se administra como si fuera una llamada directa a ese número.	debe incluir el aviso para usar esta opción en el saludo con las opciones del menú dela operadora automática. Se requiere un número de extensión con una longitud uniforme para todos los usuarios y los miembros del grupo de búsqueda. La configuración Marcación directa por número de la operadora automática afecta el funcionamiento de esta opción. Transferencia Normal Se puede utilizar con o sin una configuración de Destino. Cuando no existe una configuración de Destino, esta acción se comporta como una acción de Marcación por número. Cuando hay una configuración de Destino, esta acción espera una conexión antes de transferir la llamada. El llamador puede escuchar una música en espera. No se escuchan anuncios. Transferencia Transfiere la llamada al destino seleccionado. Se trata de una transferencia no supervisada; si el usuario que llama no obtiene respuesta, la llamada se administra como si fuera una llamada directa a ese número.
• El Servicio de Operadora Automática deberá operar de forma centralizada en los sitios donde lo soliciten las Dependencias o Entidades, atendiendo cada uno, las llamadas entrantes de los números de grupo de las troncales del sitio asociado.	Avaya IP Office ™ Platform Solution Description	101, 119	Centralized voicemail IP Office with a centralized Voicemail Pro system in the SCN network Server Edition licenses • Centralized Voicemail Pro • Automated attendant	Buzón de voz centralizado IP Office con un sistema Voicemail Pro centralizado en la red SCN Licencias de Server Edition • Correo de voz Pro centralizado • Asistente automatizado
• Cada solución de Operadora Automática que soliciten las Dependencias o Entidades, deberá manejar los	PROPUESTA TÉCNICA	PROPUESTA TÉCNICA	IP Productos y Servicios, S.A. de C.V. considera en su propuesta la cantidad de puertos suficientes para que cada solución de Operadora	IP Productos y Servicios, S.A. de C.V. considera en su propuesta la cantidad de puertos suficientes para que cada solución de Operadora Automática que soliciten las Dependencias o

puertos de acceso serán definidos por las Dependencias o Entidades, para las peticiones y/consultas que realicen los usuarios externos e internos.			Automática que soliciten las Dependencias o Entidades maneje los puertos de acceso, los cuales serán definidos por las Dependencias o Entidades, para las peticiones y/consultas que realicen los usuarios externos e internos.	Entidades maneje los puertos de acceso, los cuales serán definidos por las Dependencias o Entidades, para las peticiones y/consultas que realicen los usuarios externos e internos.
• La solución de Operadora Automática, deberá contar con la capacidad de manejar una determinada cantidad de sesiones concurrentes hacia cada uno de los sitios de la Red de las Dependencias o Entidades, conforme a los requerimientos de éstas y con base a la capacidad de puertos solicitados para cada Operadora Automática. En su caso, la asignación de sesiones concurrentes se determinará de común acuerdo entre el administrador del contrato de las Dependencias o Entidades y el Proveedor que resulte adjudicado.	PROPUESTA TÉCNICA Avaya IP Office ™ Platform Solution Description	PROPUESTA TÉCNICA 101, 119	IP Productos y Servicios, S.A. de C.V. considera en su propuesta la cantidad de puertos suficientes para que cada solución de Operadora Automática que soliciten las Dependencias o Entidades maneje los puertos de acceso, los cuales serán definidos por las Dependencias o Entidades, para las peticiones y/consultas que realicen los usuarios externos e internos. Centralized voicemail IP Office with a centralized Voicemail Pro system in the SCN network	IP Productos y Servicios, S.A. de C.V. considera en su propuesta la cantidad de puertos suficientes para que cada solución de Operadora Automática que soliciten las Dependencias o Entidades maneje los puertos de acceso, los cuales serán definidos por las Dependencias o Entidades, para las peticiones y/consultas que realicen los usuarios externos e internos. Buzón de voz centralizado IP Office con un sistema Voicemail Pro centralizado en la red SCN
• El Sistema de Procesamiento de Llamadas IP deberá contar con la capacidad de desbordar a las Operadoras Automáticas, las llamadas externas que ingresen por los Números de Grupo de las troncales de los sitios, donde se cuente con este tipo de servicios, conforme a los requerimientos que establezca el administrador del contrato de las Dependencias o Entidades.	Operadora Automática 1	2	Transferencia a una operadora Esta acción se puede realizar para transferir llamadas a otra operadora automática existente.	Transferencia a una operadora Esta acción se puede realizar para transferir llamadas a otra operadora automática existente.

Protesto lo necesario
A T E N T A M E N T E

Rubén Plaza Aguilar
Representante Legal
IP Productos y Servicios S.A. de C.V.

Traducido del inglés al español - www.onlinedoctranslator.com

AVAYA

Descripción de la solución Avaya Contact Center Select

Versión 7.0.3
Edición 02.05
julio 2018

©2016-2018, Avaya Inc. Todos
los derechos reservados.

Aviso

Si bien se han realizado esfuerzos razonables para garantizar que la información de este documento sea completa y precisa en el momento de la impresión, Avaya no asume ninguna responsabilidad por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información de este documento sin la obligación de notificar a ninguna persona u organización sobre dichos cambios.

Descargo de responsabilidad de la documentación

"Documentación" se refiere a la información publicada en diversos medios que pueden incluir información sobre el producto, instrucciones de funcionamiento y especificaciones de rendimiento que generalmente se ponen a disposición de los usuarios de los productos. La documentación no incluye materiales de marketing. Avaya no será responsable de ninguna modificación, adición o eliminación de la versión original publicada de la Documentación, a menos que dichas modificaciones, adiciones o eliminaciones hayan sido realizadas por Avaya o en su nombre expreso. El usuario final acepta indemnizar y eximir de responsabilidad a Avaya, a los agentes, servidores y empleados de Avaya frente a todos los reclamos, juicios, demandas y juicios que surjan de, o en relación con, modificaciones, adiciones o eliminaciones posteriores a esta documentación, en la medida en que lo haga End Usuario.

Descargo de responsabilidad del enlace

Avaya no es responsable del contenido o la confiabilidad de los sitios web vinculados a los que se hace referencia en este sitio o la documentación proporcionada por Avaya. Avaya no es responsable de la precisión de la información, declaración o contenido proporcionado en estos sitios y no respalda necesariamente los productos, servicios o información descritos u ofrecidos en ellos. Avaya no garantiza que estos enlaces funcionen todo el tiempo y no tiene control sobre la disponibilidad de las páginas enlazadas.

Garantía

Avaya proporciona una garantía limitada para el hardware y el software de Avaya. Consulte su contrato de venta para establecer los términos de la garantía limitada. Además, el lenguaje de la garantía estándar de Avaya, así como la información sobre el soporte para este producto mientras está bajo garantía, está disponible para los clientes de Avaya y otras partes a través del sitio web de Soporte de Avaya:https://support.avaya.com/ helpcenter/ getGenericDetails?detailId=C20091120112456651010 bajo el enlace "Garantía y ciclo de vida del producto" o el sitio sucesor designado por Avaya. Tenga en cuenta que si adquirió los productos de un socio de canal autorizado de Avaya fuera de los Estados Unidos y Canadá, dicho socio de canal de Avaya le proporciona la garantía y no Avaya.

"Servicio alojado" hace referencia a una suscripción de servicio alojado de Avaya que adquiere de Avaya o de un socio de canal autorizado de Avaya (según corresponda) y que se describe con más detalle en SAS alojado u otra documentación de descripción del servicio con respecto al servicio alojado correspondiente. Si compra una suscripción al Servicio alojado, es posible que la garantía limitada anterior no se aplique, pero puede tener derecho a servicios de soporte en relación con el Servicio alojado, como se describe más adelante en los documentos de descripción del servicio para el Servicio alojado correspondiente. Comuníquese con Avaya o con el socio de canal de Avaya (según corresponda) para obtener más información.

Servicio alojado

LO SIGUIENTE SE APLICA ÚNICAMENTE SI COMPRA UNA SUSCRIPCIÓN AL SERVICIO ALOJADO DE AVAYA DE AVAYA O DE UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA), LOS TÉRMINOS DE USO PARA LOS SERVICIOS ALOJADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA,HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO BAJO EL ENLACE "Términos de uso de Avaya para servicios alojados" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, Y SON APLICABLES A CUALQUIER PERSONA QUE ACCEDA O UTILICE EL SERVICIO ALOJADO. AL ACCEDER O UTILIZAR EL SERVICIO ALOJADO, O AL AUTORIZAR A OTROS A HACERLO, USTED, EN NOMBRE DE USTED Y DE LA ENTIDAD PARA LA QUE LO ESTÁ HACIENDO (EN ADELANTE DENOMINADO INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA LOS TÉRMINOS DE USO. SI USTED ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR DICHA ENTIDAD A ESTOS TÉRMINOS DE USO. SI USTED NO TIENE DICHA AUTORIDAD, O SI USTED NO DESEA ACEPTAR ESTOS TÉRMINOS DE USO, NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO.

Licencias

LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA,HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, BAJO EL ENLACE "TÉRMINOS DE LICENCIA DE SOFTWARE DE AVAYA (Productos de Avaya)" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, SON APLICABLES A CUALQUIER PERSONA QUE DESCARGUE, UTILICE Y/O INSTALE SOFTWARE DE AVAYA, COMPRADO DE AVAYA INC., CUALQUIER AFILIADO DE AVAYA O UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA) BAJO UN ACUERDO COMERCIAL CON AVAYA O UN SOCIO DE CANAL DE AVAYA. A MENOS QUE AVAYA ACORDE LO CONTRARIO POR ESCRITO, AVAYA NO EXTENDERÁ ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE CUALQUIER PERSONA QUE NO SEA AVAYA, UNA AFILIADA DE AVAYA O UN SOCIO DE CANAL DE AVAYA; AVAYA SE RESERVA EL DERECHO DE TOMAR ACCIONES LEGALES CONTRA USTED Y CUALQUIER OTRA PERSONA QUE UTILICE O VENDA EL SOFTWARE SIN LICENCIA. AL INSTALAR, DESCARGAR O UTILIZAR EL SOFTWARE, O AUTORIZAR A OTROS A HACERLO, USTED, EN SU NOMBRE Y EN EL DE LA ENTIDAD PARA LA QUE ESTÁ INSTALANDO, INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA ESTOS TÉRMINOS Y CONDICIONES Y CREA UN CONTRATO VINCULANTE ENTRE USTED Y AVAYA INC. O LA AFILIADA DE AVAYA CORRESPONDIENTE ("AVAYA").

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el cual el alcance de la licencia se detalla a continuación. Cuando la documentación del pedido no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de Sistema Designado como se establece a continuación en la sección Licencia de Sistema(s) Designado(s) (DS) según corresponda. El número aplicable de licencias y unidades de capacidad para las que se otorga la licencia será uno (1), a menos que se especifique un número diferente de licencias o unidades de capacidad en la documentación u otros materiales disponibles para Usted. "Software" hace referencia a los programas informáticos en código objeto, proporcionados por Avaya o un socio de canal de Avaya, ya sea como productos independientes, preinstalados en productos de hardware y cualquier mejora, actualización, parche, corrección de errores, o versiones modificadas de los mismos. "Procesador designado" significa un único dispositivo informático independiente. "Servidor" hace referencia a un conjunto de Procesadores designados que aloja (física o virtualmente) una aplicación de software a la que acceden varios usuarios. "Instancia" significa una única copia del Software que se ejecuta en un momento determinado: (i) en una máquina física; o (ii) en una máquina virtual de software implementada ("VM") o implementación similar.

Tipos de licencia

Licencia de Usuario Concurrente (CU). El Usuario final puede instalar y utilizar el Software en varios Procesadores designados o en uno o más Servidores, siempre que solo el número de Unidades con licencia acceda y utilice el Software en un momento dado. Una "Unidad" hace referencia a la unidad en la que Avaya, a su exclusivo criterio, basa el precio de sus licencias y puede ser, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o correo de voz a nombre de una persona. o función corporativa (por ejemplo, webmaster o servicio de asistencia), o una entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software. Las Unidades pueden vincularse a un Servidor específico e identificado oa una Instancia del Software.

Software de la herencia de Nortel

"Software Heritage Nortel" significa el software que fue adquirido por Avaya como parte de su compra de Nortel Enterprise Solutions Business en diciembre de 2009. El software Heritage Nortel es el software incluido en la lista de productos Heritage Nortel ubicada enhttps://support.avaya.com/LicenseInfo bajo el enlace "Productos de Heritage Nortel" o el sitio sucesor designado por Avaya. Para el software Heritage Nortel, Avaya le otorga al Cliente una licencia para usar el software Heritage Nortel proporcionado en virtud del presente únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la Documentación, y únicamente como integrado, para ejecución en, o para comunicación con equipos Avaya. Los cargos por el software Heritage Nortel pueden basarse en el grado de activación o uso autorizado según se especifica en un pedido o factura.

Derechos de autor

Salvo que se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, la documentación, el software, el servicio alojado o el hardware proporcionado por Avaya. Todo el contenido de este sitio, la documentación, el Servicio alojado y el producto proporcionado por Avaya, incluida la selección, disposición y diseño del contenido, es propiedad de Avaya o de sus otorgantes de licencias y está protegido por derechos de autor y otras leyes de propiedad intelectual, incluida la ley sui generis. derechos relativos a la protección de las bases de datos. No puede modificar, copiar, reproducir, volver a publicar, cargar, publicar, transmitir o distribuir de ninguna manera ningún contenido, en su totalidad o en parte, incluido cualquier código y software, a menos que Avaya lo autorice expresamente. La reproducción, transmisión, difusión, almacenamiento o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede ser un delito,

virtualización

Lo siguiente se aplica si el producto se implementa en una máquina virtual. Cada producto tiene su propio código de pedido y tipos de licencia. Tenga en cuenta, a menos que se indique lo contrario, que cada Instancia de un producto debe solicitarse y solicitarse por separado. Por ejemplo, si el cliente usuario final o el socio de canal de Avaya desea instalar dos instancias del mismo tipo de productos, entonces se deben pedir dos productos de ese tipo.

Componentes de terceros

"Componentes de terceros" significa que ciertos programas de software o partes de los mismos incluidos en el Software o el Servicio alojado pueden contener software (incluido el software de código abierto) distribuido bajo acuerdos de terceros ("Componentes de terceros"), que contienen términos relacionados con los derechos de uso de ciertos partes del Software ("Términos de terceros"). Según sea necesario, la información sobre el código fuente del sistema operativo Linux distribuido (para aquellos productos que tienen el código fuente del sistema operativo Linux distribuido) y la identificación de los titulares de derechos de autor de los componentes de terceros y los términos de terceros que se aplican está disponible en los productos, la documentación o en el sitio web de Avaya. a:https://support.avaya.com/Copyright o el sitio sucesor designado por Avaya. Los términos de la licencia de software de código abierto proporcionados como Términos de terceros son consistentes con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del software de código abierto. Los Términos de terceros prevalecerán sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables en la medida en que estos Términos de licencia de software le impongan mayores restricciones que los Términos de terceros aplicables.

Lo siguiente se aplica solo si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO TIENE LICENCIA BAJO LA LICENCIA DE CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS POR LOS QUE NO RECIBE REMUNERACIÓN PARA (i) CODIFICAR VÍDEO EN CUMPLIMIENTO CON EL ESTÁNDAR AVC (“AVC VIDEO”) Y/O (ii) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL DE MPEG LA, LLC VERHTTP://WWW.MPEGLA.COM .

Proveedor de servicio

LO SIGUIENTE SE APLICA AL ALOJAMIENTO DE PRODUCTOS O SERVICIOS DE AVAYA POR PARTE DEL SOCIOS DE CANAL DE AVAYA. EL PRODUCTO O EL SERVICIO ALOJADO PUEDE UTILIZAR COMPONENTES DE TERCEROS SUJETOS A TÉRMINOS DE TERCEROS Y REQUIERE QUE UN PROVEEDOR DE SERVICIOS TENGA UNA LICENCIA INDEPENDIENTE DIRECTAMENTE DEL PROVEEDOR DE TERCEROS. EL ALOJAMIENTO DE PRODUCTOS DE AVAYA POR PARTE DE UN SOCIO DE CANAL DE AVAYA DEBE SER AUTORIZADO POR ESCRITO POR AVAYA Y SI DICHOS PRODUCTOS ALOJADOS UTILIZAN O INTEGRAN DETERMINADO SOFTWARE DE TERCEROS, INCLUYENDO, ENTRE OTROS, SOFTWARE O CÓDECS DE MICROSOFT, EL SOCIO DE CANAL DE AVAYA DEBE
OBTENGA DE FORMA INDEPENDIENTE CUALQUIER ACUERDO DE LICENCIA CORRESPONDIENTE, POR CUENTA DEL SOCIO DE CANAL DE AVAYA, DIRECTAMENTE DEL PROVEEDOR TERCERO CORRESPONDIENTE.

CON RESPECTO A LOS CÓDECS, SI EL SOCIO DE CANAL DE AVAYA ALOJA CUALQUIER PRODUCTO QUE UTILICE O INTEGRA EL CÓDEC G.729, EL CÓDEC H.264 O EL CÓDEC H.265, EL SOCIO DE CANAL DE AVAYA RECONOCE Y ACEPTA QUE EL SOCIO DE CANAL DE AVAYA ES RESPONSABLE DE TODAS LAS TARIFAS Y/O REGALÍAS RELACIONADAS. EL CÓDEC G.729 TIENE LICENCIA DE SIPRO LAB TELECOM INC. VER WWW.SIPRO.COM/CONTACTO.HTML . EL CÓDEC H.264 (AVC) TIENE LICENCIA BAJO LA LICENCIA DE LA CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS EN LOS QUE NO RECIBE REMUNERACIÓN PARA: (I) CODIFICAR VÍDEO DE CONFORMIDAD CON EL ESTÁNDAR AVC (“AVC VIDEO ”) Y/O (II) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO CON LICENCIA PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL PARA LOS CÓDECS H.264 (AVC) Y H.265 (HEVC) DE MPEG LA, LLC VERHTTP:// WWW.MPEGLA.COM .

De acuerdo con las leyes

Usted reconoce y acepta que es su responsabilidad cumplir con las leyes y reglamentaciones aplicables, incluidas, entre otras, las leyes y reglamentaciones relacionadas con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude y los derechos de interpretación musical, en el país o territorio donde se utiliza el producto Avaya.

Prevención del fraude de llamadas

El "fraude interurbano" es el uso no autorizado de su sistema de telecomunicaciones por parte de una parte no autorizada (por ejemplo, una persona que no es un empleado corporativo, agente, subcontratista o que no trabaja en nombre de su empresa). Tenga en cuenta que puede haber un riesgo de fraude de llamadas asociado con su sistema y que, si ocurre, puede resultar en cargos adicionales sustanciales para sus servicios de telecomunicaciones.

Intervención de fraude de llamadas de Avaya

Si sospecha que está siendo víctima de fraude de llamadas y necesita asistencia o soporte técnico, llame a la línea directa de intervención de fraude de llamadas del Centro de Servicio Técnico al +1-800-643-2353 para los Estados Unidos y Canadá. Para obtener números de teléfono de soporte adicionales, consulte el sitio web de soporte de Avaya:https://soporte.avaya.como el sitio sucesor designado por Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de soporte de seguridad de Avaya en la sección Políticas de seguridad y soporte dehttps://support.avaya.com/security.

Las sospechas de vulnerabilidades de seguridad de productos de Avaya se manejan según el Flujo de soporte de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Descarga de documentación

Para obtener las versiones más recientes de la documentación, consulte el sitio web de soporte de Avaya:https://soporte.avaya.com, o el sitio sucesor designado por Avaya.

Comuníquese con el soporte de Avaya

Consulte el sitio web de soporte de Avaya:https://soporte.avaya.compara avisos y artículos sobre productos o Servicios alojados, o para informar un problema con su producto o Servicio alojado de Avaya. Para obtener una lista de números de teléfono y direcciones de contacto de soporte, vaya al sitio web de Soporte de Avaya:https://soporte.avaya.com(o el sitio sucesor designado por Avaya), desplácese hasta la parte inferior de la página y seleccione Contactar con el soporte de Avaya.

Marcas registradas

Las marcas comerciales, los logotipos y las marcas de servicio ("Marcas") que se muestran en este sitio, la Documentación, los Servicios alojados y los productos proporcionados por Avaya son Marcas registradas o no registradas de Avaya, sus afiliados, sus licenciantes, sus proveedores u otros terceros. Los usuarios no pueden usar dichas Marcas sin el consentimiento previo por escrito de Avaya o de un tercero que pueda ser propietario de la Marca. Nada de lo contenido en este sitio, la Documentación, los Servicios alojados y los productos debe interpretarse como una concesión, por implicación, impedimento legal o de otro modo, de cualquier licencia o derecho sobre las Marcas sin el permiso expreso por escrito de Avaya o el tercero aplicable.

Avaya es una marca registrada de Avaya Inc.

Avaya, el logotipo de Avaya, Avaya one-X®Portal, Avaya Aura®
Gerente de comunicación, Avaya Aura®Portal de experiencias, Avaya Aura®
Diseñador de orquestación, Avaya Aura®Gerente de sesión, Avaya Aura®
System Manager y Application Enablement Services son marcas
comerciales registradas o marcas comerciales de Avaya Inc. en los Estados
Unidos de América y/u otras jurisdicciones.

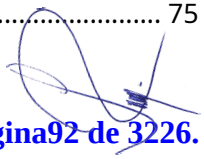
Todas las marcas comerciales que no son de Avaya son propiedad de sus
respectivos dueños. linux®es la marca registrada de Linus Torvalds en los EE. UU.
y otros países.

Contenido

Capítulo 1 Introducción..... 11
Objetivo..... 11
Público objetivo..... 11
Recursos Relacionados..... 11
Documentación de Avaya Contact Center Select 11
Visualización de videos de orientación de Avaya..... 14
Apoyo..... 14
Capítulo 2: Cambios en esta versión..... 15
Cambios de características en la compilación base de la versión 7.0..... 15
Inserción automática de un dígito inicial antes de marcar números usando Agent Desktop Directorio telefónico 15
Avaya Contact Center Select es compatible con Microsoft Windows Server 2012 R2 15
Cambios en Avaya Media Server..... 15
Aplicación Navegador de agentes de Contact Center..... dieciséis
Caducidad de la contraseña de administración de Contact Center Manager..... 17
Soporte de Contact Center Manager Administration para la base de datos de Caché 17
Servicios de Contact Center protegidos por defecto..... 17
Notificación de caducidad de licencia de emergencia 18
Forzar el cambio de contraseña cuando los usuarios inicien sesión en Contact Center Manager Administration para la primera vez..... 18
Nuevo dispositivo de hardware de Avaya Contact Center Select..... 18
Nuevas especificaciones mínimas de hardware de Avaya Contact Center Select..... 19
Nuevas especificaciones mínimas de máquina virtual de Avaya Contact Center Select..... 19
Caducidad de la contraseña en Contact Center Manager Administration 19
Asistente para la creación de informes 20
Mejoras en la capacidad de servicio en Contact Center 7.0..... 20
Compatibilidad con la adición de imágenes y logotipos de la empresa a las firmas..... 20
Soporte para copiar el CLID de un cliente usando Agent Desktop..... 20
Soporte para mostrar el historial de inicio de sesión en Contact Center Manager Administration, Agente Escritorio y Administrador de seguridad 21
Compatibilidad con códigos de motivo No listo forzados..... 21
Compatibilidad con secuencias de comandos mediante CLID y Wild CLID en entornos SIP..... 21
Bloqueo temporal de los usuarios de Contact Center Manager Administration..... 21
Cambios de características en la versión 7.0 Feature Pack 1..... 22
Agent Desktop utiliza un directorio de usuario como el directorio de exploración de archivos predeterminado 22
Actualización automática de conjuntos de habilidades sin personal para informes en tiempo real 22
Avaya Contact Center Select es compatible con la versión 10 de IP Office..... 22
Póngase en contacto con el SDK del servicio de control 23
Los navegadores web integrados en Agent Desktop utilizan la última versión de Internet Explorer instalado en el sistema del cliente 23

Restricciones de extensión de archivo para archivos adjuntos 23
Rendimiento operativo mejorado para la continuidad del negocio 23
La función de mensajería instantánea es compatible con Microsoft Skype for Business 2015 24
Nueva aplicación para instalar Feature Packs y Service Packs 24
Las contraseñas de las cuentas multimedia deben cumplir con los criterios mínimos de complejidad 24
Provisión de agregar un nombre descriptivo para un agente de chat en la web 24
Eliminación de la contraseña predeterminada del panel de Agent Desktop 25
Lista de conjuntos de aptitudes ordenada al crear una visualización de vallas publicitarias 25
Compatibilidad con la interfaz Open Queue Open 25
Compatibilidad con VMware 6.0 25
Entrenamiento de susurro 25
Cambios de características en la versión 7.0 Feature Pack 2 26
Inicio de sesión integrado de Agent Desktop 26
Medidas de seguridad de asignación de conjunto de habilidades del agente 26
Aumento de la relación de contacto con los clientes de CCMM 26
Tienda de seguridad fuera de línea 26
Compatibilidad con Servicios de Escritorio remoto para Agent Desktop 26
Eliminación de la configuración de seguridad predeterminada 27
Integración de API REST 27
Sincronización de cambios de usuario de accssync a IP Office 27
Compatibilidad con VMware 6.5 27
Cambios de funciones en la versión 7.0 Feature Pack 3 27
Capacidad para almacenar archivos adjuntos de correo electrónico en la base de datos 28
Cifrado de la base de datos del centro de contacto 28
Gestión de datos - privacidad del cliente 28
Mejoras de la API REST 28
Compatibilidad con Security Manager para certifcados encadenados 28
Soporte para aplicar un indicador de restricción a un cliente 28
Otros cambios en la versión 7.0 29
Agent Desktop ya no es compatible con la implementación como un cliente pesado 29
El archivo OVA de Avaya Contact Center Select ya no está disponible 29
Versiones compatibles con IP Office 29
Versiones compatibles con Microsoft Exchange Server 29
Las versiones de Microsoft Internet Explorer ya no son compatibles 29
Ya no se admiten las comunicaciones de capa de sockets seguros 30
Windows Server 2008 ya no es compatible 30
Otros cambios en la versión 7.0 Feature Pack 1 30
Mejoras en la seguridad del centro de contacto 30
Firma del bloque de mensajes del servidor habilitada en Windows Server 2012 30
Componentes de terceros actualizados 31
Otros cambios en la versión 7.0 Feature Pack 2 31
Los usuarios de CCMA deben iniciar sesión antes de cambiar la contraseña 31
Cuenta de instalación para la instalación de Contact Center 31

Componentes de terceros actualizados 31
Otros cambios en la versión 7.0 Feature Pack 3..... 32
Aura de Avaya®Actualización del servidor de medios 32
Compatibilidad con versiones anteriores de Contact Center con la versión anterior de Agent Desktop 32
Versiones compatibles con IP Office 32
Componentes de terceros actualizados 33
Capítulo 3: Descripción general de Avaya Contact Center Select..... 34
Licencia..... 36
Sincronización de datos de usuario 39
Topología..... 40
Versiones compatibles con IP Office 43
Descripción general de la configuración de la solución 44
Ejemplo de flujo de llamada de voz simple..... 46
Ejemplos de aplicaciones de flujo de voz de Orchestration Designer..... 47
Procesamiento de contactos multimedia..... 50
Flujo de mensajes de correo electrónico simple 51
Grabacion de llamada..... 52
Agentes remotos..... 53
Compatibilidad con dominios y grupos de trabajo de Avaya Contact Center Select..... 54
Avisos de seguridad de Avaya 56
Avaya Contact Center Select Business Continuity..... 56
Actualizaciones y migraciones 56
Fuente de información de la desconexión de la llamada 57
Reenviar automáticamente el correo de voz de IP Office a los agentes multimedia..... 58
Limitaciones..... 59
Capítulo 4: DVD de Avaya Contact Center Select..... 63
Especificación del servidor de la independencia del proveedor de la plataforma..... sesenta y cinco
Especificación del servidor de nivel de entrada..... sesenta y cinco
Especificación de servidor de rango medio 66
Especificación de servidor de gama alta 68
Tamaños de las particiones del disco duro de Contact Center..... 69
Rendimiento del servidor y configuración del firmware..... 70
Firmware del servidor 71
Interfase Extensible de Firmware Unificado..... 71
Administración de energía y rendimiento 72
Caché de disco y RAID 72
Memoria y arquitectura de memoria no uniforme..... 73
Hiperprocesamiento 73
Dispositivos de hardware no utilizados 73
Resumen..... 74
Especificaciones del software Avaya Contact Center Select DVD 74
Requisitos de nomenclatura del servidor..... 74
Revisiones de seguridad de Microsoft 75



Actualizaciones del sistema operativo 75
Requisitos de software de terceros 77
Directrices para el uso de software antivirus 78
Licencias de DVD de Avaya Contact Center Select 80
Capítulo 5: Dispositivo de software Avaya Contact Center Select 81
Máquina virtual Avaya Contact Center Select 83
Discos duros y particiones de máquinas virtuales de Contact Center 84
Requisitos de nomenclatura del servidor 85
Revisiones de seguridad de Microsoft 85
Actualizaciones del sistema operativo 85
Requisitos de software de terceros 87
Directrices para el uso de software antivirus 88
Aura de Avaya® Servidor multimedia OVA 90
Avaya WebLM OVA 91
Especificaciones y creación de perfiles del servidor host de VMware 92
Ejemplos de creación de perfiles de VMware 95
Consideraciones de virtualización 97
Funciones de VMware 98
Consideraciones sobre el host de VMware vSphere 99
Rendimiento del servidor y configuración del firmware 100
Prácticas recomendadas de redes de VMware 103
Consideraciones sobre las instantáneas de Avaya Contact Center Select VMware 104
Aura de Avaya® Consideraciones sobre la instantánea de VMware del servidor de medios 105
Orientación para los requisitos de almacenamiento 105
Supervisión y gestión del rendimiento 106
Solución de problemas de VMware 107
Licencias de dispositivos de software 108
Capítulo 6: Dispositivo de hardware Avaya Contact Center Select 109
Especificación del servidor del dispositivo de hardware 110
Especificaciones de software del dispositivo de hardware de Avaya Contact Center Select 112
Requisitos de nomenclatura del servidor 113
Revisiones de seguridad de Microsoft 113
Actualizaciones del sistema operativo 113
Requisitos de software de terceros 115
Directrices para el uso de software antivirus 116
Licencias de dispositivos de hardware 118
Capítulo 7: Límites de capacidad de la solución y funciones admitidas 120
Límites máximos de capacidad de Avaya Contact Center Select 120
Límites máximos de configuración de Avaya Contact Center Select 123
Funciones admitidas de Avaya Contact Center Select 123
Funciones de telefonía admitidas 129
Dispositivos de telefonía compatibles 138
Soporte de acceso remoto 140

Página93 de 3226.

Funcionalidad admitida por Communication Control Toolkit..... 140
Capítulo 8: Avaya Aura®Integración del portal de experiencias..... 145
Métodos de transferencia de datos 146
Aura de Avaya®Diseñador de la orquestación del portal de experiencias..... 146
XML de voz..... 147
XML de control de llamadas 147
Avaya Contact Center Select habilitado para SIP..... 147
P-Encabezado SIP intrínseco..... 148
Información de usuario a usuario 149
Identificador universal de llamadas 149
Interfaz Avaya Aura®Experience Portal y Contact Center habilitado para SIP..... 149
Ejemplo de flujo de llamadas para el front-end Avaya Aura®Portal de experiencia y contacto habilitado para SIP
Centro..... 151
Avaya Aura de back-end®Experience Portal y Contact Center habilitado para SIP..... 153
Ejemplo de flujo de llamadas usando el back-end Avaya Aura®Experience Portal y habilitado para SIP
Centro de contacto..... 154
Avaya Aura de back-end®Experience Portal utilizando la creación de contexto y el contacto habilitado para SIP
Centro..... 155
Ejemplo de flujo de llamadas usando el back-end Avaya Aura®Portal de experiencia con el contexto
Aplicación de ejemplo de creación 158
Avaya DevConnect..... 159
Capítulo 9: Requisitos del equipo cliente de administración.....160
Requisitos de hardware de la computadora del administrador 160
Requisitos del sistema operativo del cliente 161
Compatibilidad con el cliente de administración de Citrix 162
Requisitos de software de terceros 163
Capítulo 10: Requisitos de la computadora Agent Desktop.....164
Idiomas localizados de Agent Desktop..... 164
Requisitos de hardware de la computadora Agent Desktop..... 165
Requisitos del sistema operativo del cliente 166
Requisitos de software de terceros 167
Requisitos de infraestructura de red del cliente de Agent Desktop..... 167
Compatibilidad con servicios de escritorio remoto 174
Compatibilidad con el cliente Citrix 176
Puertos de red de Agent Desktop 176
Capítulo 11: Requisitos de la aplicación Contact Center Agent Browser..... 177
Requisitos del navegador web 178
Capítulo 12: Comunicaciones TLS seguras de Avaya Contact Center Select..... 180
Conceptos básicos de seguridad HTTPS 180
Almacén de seguridad de Avaya Contact Center Select..... 181
Administrador de seguridad de Avaya Contact Center Select..... 184
Seguridad TLS en un entorno de Continuidad de Negocio..... 186
Migración de sistemas seguros de Contact Center..... 187

Página94 de 3226.

Notificaciones de almacenamiento de Avaya Contact Center Select Security..... 187
Firma del bloque de mensajes del servidor 188
Capítulo 13: Matriz de puertos de Avaya Contact Center Select..... 189
Requisitos del puerto del Contact Center Manager Server..... 189
Requisitos del puerto de administración de Contact Center Manager..... 190
Requisitos de puerto de Communication Control Toolkit..... 191
Requisitos del puerto de Contact Center Multimedia..... 192
Aura de Avaya®Requisitos del puerto del servidor de medios..... 193

Capítulo 1 Introducción

Objetivo

Este documento describe una solución de Avaya desde una perspectiva holística que se centra en las vistas estratégica, empresarial y funcional de la arquitectura. Este documento también incluye una descripción de alto nivel de cada configuración de referencia verificada para la solución.

Público objetivo

Este documento está destinado al personal que desea comprender cómo la solución y las configuraciones de referencia verificadas relacionadas cumplen con los requisitos del cliente.

Recursos Relacionados

Documentación de Avaya Contact Center Select

La siguiente tabla enumera los documentos relacionados con Avaya Contact Center Select. Descargue los documentos del sitio web de soporte de Avaya enhttp://soporte.avaya.com .

Título	Utilice este documento para:	Audiencia
Visión general		
Descripción de la solución Avaya Contact Center Select	Este documento proporciona una descripción técnica de Avaya Contact Center Select. Describe las características del producto, especificaciones, licencias e interoperabilidad con otros productos compatibles.	clientes y ventas, servicios y apoyo personal
Catálogo de documentación de Avaya Contact Center Select	Este documento describe la documentación disponible de Avaya Contact Center Select	clientes y ventas, servicios y apoyo personal

La tabla continúa...

Título	Utilice este documento para:	Audiencia
	recursos e indica el tipo de información en cada documento.	
Diccionario de datos de gestión del rendimiento del centro de contacto	Este documento contiene tablas de referencia que describen las estadísticas y datos en los informes históricos y en tiempo real generados en Contact Center.	Sistema administradores y centro de contacto supervisores
Implementar		
DVD de implementación de Avaya Contact Center Select	Este documento contiene información sobre la instalación, la configuración inicial y la verificación del DVD de Avaya Contact Center Select. Este documento contiene información sobre el mantenimiento y la resolución de problemas del servidor Avaya Contact Center Select.	Implementación personal
Implementación del dispositivo de software Avaya Contact Center Select	Este documento contiene información sobre la preparación de Avaya Contact Center Select Software Appliance (VMware), implementación, configuración inicial y verificación. Este documento contiene información sobre el mantenimiento y la resolución de problemas del dispositivo de software.	Implementación personal
Implementación del dispositivo de hardware de Avaya Contact Center Select	Este documento contiene información sobre la instalación, la configuración inicial y la verificación de Avaya Contact Center Select Hardware Appliance (servidor físico). Este documento contiene información sobre el mantenimiento y la solución de problemas del dispositivo de hardware.	Implementación personal
Continuidad comercial de Avaya Contact Center Select	Este documento contiene información sobre la implementación de Avaya Contact Center Select Business Continuity.	Implementación personal
Actualización y parches de Avaya Contact Center Select	Este documento contiene información sobre la actualización y parches de Avaya Contact Center Select.	Implementación personal y sistema administradores
administrando		
Administración de Avaya Contact Center Select	Este documento contiene información y procedimientos para configurar los usuarios, perfiles y datos de configuración del centro de contacto. Este documento contiene información sobre cómo crear informes históricos y en tiempo real de Avaya Contact Center Select.	Sistema administradores y centro de contacto supervisores
Administración avanzada de Avaya Contact Center Select	Este documento contiene información sobre cómo administrar Avaya Contact Center Select	Sistema administradores

La tabla continúa...

Página97 de 3226.

Título	Utilice este documento para:	Audiencia
	servidor, licencias y configuración multimedia.	
Uso del Diseñador de orquestación del centro de contacto	Este documento contiene información y procedimientos para configurar aplicaciones de script y flujo en Contact Center Diseñador de orquestación.	Sistema administradores
mantenimiento		
Códigos de eventos del centro de contacto	Este documento contiene una lista de errores en la suite Contact Center y recomendaciones para resolverlos. Este documento es una hoja de cálculo de Microsoft Excel.	Sistema administradores y personal de apoyo
Usando		
Uso de Agent Desktop para Avaya Contact Center Select	Este documento brinda información y procedimientos para los agentes que usan la aplicación Agent Desktop para aceptar, administrar y cerrar contactos de todo tipo de medios en Contact Center.	Centro de contacto agentes y supervisores
Uso de la aplicación Navegador de agentes de Contact Center	Este documento brinda información y procedimientos para los agentes que usan la aplicación Agent Browser para iniciar sesión en Contact Center y realizar tareas básicas.	Centro de contacto agentes

Búsqueda de documentos en el sitio web de soporte de Avaya

Procedimiento

1. Navegue hastahttp://soporte.avaya.com/ .
2. En la parte superior de la pantalla, escriba su nombre de usuario y contraseña y haga clic en**Acceso**.
3. Haga clic en**Soporte por producto**>**Documentos**.
4. en**Ingrese su producto aquí**, escriba el nombre del producto y luego seleccione el producto de la lista.
5. En**Elija Liberar**, seleccione un número de versión apropiado.
6. En el**Tipo de contenido**filtro, haga clic en un tipo de documento o haga clic en**Seleccionar todo**para ver una lista de todos los documentos disponibles.

   Por ejemplo, para guías de usuario, haga clic en**Guías de usuario**en el**Tipo de contenido**filtrar. La lista muestra los documentos solo de la categoría seleccionada.
7. Haga clic en**Ingresar**.

Página98 de 3226.

Visualización de videos de mentores de Avaya

Los videos de orientación de Avaya brindan contenido técnico sobre cómo instalar, configurar y solucionar problemas de los productos de Avaya.

Acerca de esta tarea

Los videos están disponibles en el sitio web de soporte de Avaya, enumerados bajo el tipo de documento de video y en el canal administrado por Avaya en YouTube.

Procedimiento

- Para encontrar videos en el sitio web de soporte de Avaya, vaya ahttp://soporte.avaya.com y realice una de las siguientes acciones:
  - En**Búsqueda**, escribeVídeos de orientación de Avayapara ver una lista de los videos disponibles.
  - En**Búsqueda**, escriba el nombre del producto. En la página Resultados de la búsqueda, seleccione**Video**en el **Tipo de contenido**columna de la izquierda.
- Para encontrar los videos de Avaya Mentor en YouTube, vaya awww.youtube.com/AvayaMentor y realice una de las siguientes acciones:
  - Ingrese una palabra clave o palabras clave en el**Canal de búsqueda**para buscar un producto o tema específico.
  - Desplácese hacia abajo en Listas de reproducción y haga clic en el nombre de un tema para ver la lista disponible de videos publicados en el sitio web.

Nota:

Los videos no están disponibles para todos los productos.

Apoyo

Vaya al sitio web de soporte de Avaya enhttp://soporte.avaya.com para obtener la documentación, los avisos de productos y los artículos de conocimiento más actualizados. También puede buscar notas de la versión, descargas y resoluciones de problemas. Utilice el sistema de solicitud de servicio en línea para crear una solicitud de servicio. Chatea con agentes en vivo para obtener respuestas a tus preguntas o solicita a un agente que te conecte con un equipo de soporte si un problema requiere experiencia adicional.

Capítulo 2: Cambios en esta versión

Esta sección describe las nuevas funciones y los cambios en Avaya Contact Center Select versión 7.0.

Cambios de características en la compilación base de la versión 7.0

Consulte las siguientes secciones para obtener información sobre las nuevas funciones en la compilación base de la versión 7.0.

Inserción automática de un dígito inicial antes de marcar números usando Agent Desktop Phonebook

En Contact Center versión 7.0, los administradores pueden configurar una configuración que les da a los agentes la capacidad de agregar automáticamente un dígito inicial antes de marcar cualquier número usando la Agenda telefónica de Agent Desktop. Si los administradores habilitan esta función, el signo más (**+**) antes de que los números de teléfono de la Agenda se reemplacen con un código de acceso a troncal. El código de acceso a la troncal se agrega antes del número de teléfono. Por lo tanto, los agentes no necesitan agregar manualmente un dígito inicial para llamar externamente o desviar una llamada usando la Agenda telefónica.

Avaya Contact Center Select es compatible con Microsoft Windows Server 2012 R2

Avaya Contact Center Select versión 7.0 es compatible con el sistema operativo Microsoft Windows Server 2012 R2. Avaya Contact Center Select versión 7.0 no es compatible con Microsoft Windows Server 2008 R2. Los clientes que actualicen a Avaya Contact Center Select versión 7.0 deben migrar a un nuevo servidor Microsoft Windows Server 2012 R2.

Cambios en Avaya Media Server

Avaya Media Server ahora se llama Avaya Aura®Servidor multimedia. Avaya Contact Center Select versión 7.0 solo es compatible con Avaya Aura®Servidor multimedia versión 7.7.

Avaya Contact Center Select versión 7.0 ya no requiere ni utiliza el componente Contact Center Services para Avaya Media Server (CCSA). Avaya Contact Center Select Release 7.0 se integra directamente con Avaya Aura®Media Server versión 7.7 usando comunicación basada en Media Server Markup Language (MSML).

Avaya Contact Center Select y Avaya Aura®Media Server usa el lenguaje MSML para controlar cómo se anclan y tratan las llamadas de punto de ruta. Avaya Contact Center Select también utiliza MSML para controlar las funciones de llamada de punto de ruta, como los anuncios Interrumpir, Observar, Zip Tone y Whisper Skillset.

En Contact Center Manager Administration (CCMA)*Servicios de medios y rutas*configuración, Avaya Aura®Las instancias de Media Server versión 7.7 ahora brindan un nuevo tipo de servicio basado en MSML denominado ACC_APP_ID. Este nuevo tipo de servicio ACC_APP_ID reemplaza el tipo de servicio CONF proporcionado por Avaya Media Server versión 7.6.

Las siguientes funciones, previamente configuradas en Avaya Media Server Element Manager, ahora están configuradas en Contact Center Manager Administration (CCMA).

- Tono de irrupción
- Tono de observación
- Tono Zip de respuesta forzada de llamada
- Tonos Zip personalizados
- Anuncio de perfil de susurro

Habilitar o deshabilitar los tonos de intrusión y observación en CCMA*Configuración global*.

Cargue los archivos .WAV de tono y anuncio en CCMA*Gestión rápida*.

Configure el conjunto de aptitudes de tono zip y susurro de Call Force Answer en CCMA*Clases de presentación de llamadas*.

Aura de Avaya®Media Server solo admite las siguientes opciones de implementación:

- Co-residente con Avaya Contact Center Select en un servidor Windows Server 2012 R2
- Independiente en un servidor Red Hat Enterprise Linux 6.x de 64 bits

Aura de Avaya®Media Server también está disponible como paquete Open Virtual Appliance (OVA). Puede usar este archivo OVA para crear un Avaya Aura®Dispositivo virtual de Media Server en un host de VMware.

Aplicación del navegador del agente del Contact Center

Contact Center versión 7.0 incluye una aplicación Agent Browser. Los agentes de Contact Center solo de voz pueden usar la aplicación Agent Browser para iniciar sesión en Contact Center y realizar tareas básicas. La aplicación Agent Browser solo es compatible con soluciones de Contact Center habilitadas para SIP.

Caducidad de la contraseña de Contact Center Manager Administration

En Contact Center versión 7.0, los administradores pueden configurar que la contraseña utilizada para Contact Center Manager Administration (CCMA) caduque después de una duración específica. De forma predeterminada, la función de caducidad de la contraseña de CCMA está desactivada.

Si los administradores habilitan la función de caducidad de la contraseña, de forma predeterminada, la contraseña de CCMA caduca después de 30 días y CCMA también muestra una advertencia de caducidad de contraseña de CCMA 14 días antes de que caduque la contraseña. Los administradores pueden configurar tanto el período de caducidad como la duración de la advertencia de caducidad de la contraseña mediante el cuadro de diálogo Configuración de seguridad de CCMA.

Asistencia de Contact Center Manager Administration para la base de datos de Caché

En Contact Center versión 7.0, Contact Center Manager Administration (CCMA) almacena información en una base de datos de Caché. Contact Center versión 7.0 almacena información de agentes, usuarios, estadísticas, programación y generación de informes en las bases de datos de Caché. Esto simplifica la gestión, la migración y el mantenimiento de datos del Contact Center. Esto también simplifica los procesos de configuración de resiliencia.

En Contact Center versión 7.0, Contact Center Manager Administration (CCMA) no almacena información mediante los servicios de directorio ligero de Active Directory (AD-LDS) o las bases de datos de Microsoft Access.

Servicios de Contact Center asegurados por defecto

La versión base de Contact Center versión 7.0 incluye una serie de servicios y conexiones que puede proteger mediante Transport Layer Security (TLS). De forma predeterminada, Contact Center instala los servicios web y las conexiones de CTI más utilizados con la seguridad habilitada. Esta función incluye mejoras en la herramienta de gestión de certificados del Contact Center para facilitar la gestión de certificados de servidor y raíz.

En una nueva instalación de Contact Center, las siguientes conexiones y servicios utilizan TLS de forma predeterminada:

- Administración del administrador del centro de contacto (CCMA)
- Administración de Contact Center Multimedia (CCMM)
- Escritorio del agente
- Servicios Multimedia
- Diseñador de orquestación
- Herramienta de gestión de campañas salientes
- Servicios web del centro de contacto

Página102 de 3226.

- Administración web del kit de herramientas de control de comunicaciones (CCT)

Puede desactivar la seguridad de los servicios web después de la instalación y la configuración inicial. Si elige dejar habilitada la seguridad de los servicios web, reemplace el almacén de seguridad predeterminado de Contact Center con un nuevo almacén de seguridad que contenga un certificado de servidor firmado y un certificado raíz de su autoridad de certificación (CA).

Notificación de caducidad de licencia de emergencia

Cuando se proporciona una licencia de emergencia a un cliente, se genera un evento diario de Windows. El evento de Windows advierte al cliente de la cantidad de días que faltan para que caduque la licencia de emergencia. Luego, los clientes pueden abordar la situación en la que el representante de servicio al cliente de Avaya proporcionó la licencia de emergencia, antes de que caduque la licencia de emergencia. Por ejemplo, si su representante de servicio al cliente de Avaya activa el archivo de licencia de emergencia en su sistema porque la conexión entre Contact Center License Manager y Contact Center Manager Server no se puede reparar dentro del período de gracia de 30 días, entonces puede usar la licencia de emergencia para volver -establecer la conexión entre Contact Center License Manager y Contact Center Manager Server.

Forzar cambio de contraseña cuando los usuarios inicien sesión en Contact Center Manager Administration por primera vez

En Contact Center versión 7.0, los administradores pueden configurar una configuración mediante el cuadro de diálogo Configuración de seguridad de CCMA, que obliga a los usuarios a cambiar su contraseña cuando inician sesión en Contact Center Manager Administration (CCMA) por primera vez. En Contact Center versión 7.0, la función de forzar cambio de contraseña está deshabilitada de manera predeterminada.

Para instalaciones nuevas de Contact Center versión 7.0 Feature Pack 1, la configuración de seguridad de CCMA está habilitada de manera predeterminada. Si está actualizando desde la versión 7.0 de Contact Center, la configuración de seguridad existente de CCMA no cambia.

Las contraseñas no deben coincidir con la contraseña anterior y deben contener lo siguiente:

- Solo caracteres especiales e ingleses
- 8 a 20 caracteres
- Un número
- Una letra mayúscula
- Una letra minúscula
- No hay espacios

Nuevo dispositivo de hardware Avaya Contact Center Select

Avaya Contact Center Select versión 7.0 se ofrece como dispositivo de hardware.

Página103 de 3226.

La especificación del dispositivo de hardware de Avaya Contact Center Select versión 7.0 ha mejorado para cumplir con los mayores requisitos del sistema operativo Microsoft Windows Server 2012 R2 incluido. Los nuevos discos duros del dispositivo de hardware versión 7.0 admiten una mayor retención de datos multimedia fuera de línea.

Nuevas especificaciones mínimas de hardware de Avaya Contact Center Select

Avaya Contact Center Select Release 7.0 continúa admitiendo Platform Vendor Independence (PVI) para implementaciones de hardware de servidor físico. Avaya Contact Center Select Release 7.0 define tres nuevos niveles mínimos de especificación de hardware; una nueva especificación de hardware de servidor de nivel de entrada, una nueva gama media y una nueva gama alta. Para las instalaciones de Avaya Contact Center Select versión 7.0 en servidores físicos, solo se admiten las nuevas especificaciones de hardware del servidor PVI.

Nuevas especificaciones mínimas de máquina virtual de Avaya Contact Center Select

Avaya Contact Center Select Release 7.0 sigue siendo compatible con VMware y la virtualización. Avaya Contact Center Select Release 7.0 define tres nuevos niveles mínimos de especificación de máquinas virtuales; un nuevo nivel de entrada, un nuevo rango medio y una nueva especificación de máquina virtual de gama alta. Para las instalaciones virtualizadas de Avaya Contact Center Select versión 7.0 en máquinas virtuales, solo se admiten las nuevas especificaciones de máquina virtual.

Caducidad de la contraseña en Contact Center Manager Administration

La caducidad de la contraseña protege a las organizaciones de usuarios malintencionados que obtienen acceso no autorizado a Contact Center, ya que una contraseña robada es útil para el intruso solo durante un tiempo limitado.

Contact Center versión 7.0 contiene una configuración que implementa la caducidad de la contraseña para Contact Center Manager Administration (CCMA).

En Contact Center versión 7.0, la función de caducidad de la contraseña está deshabilitada de forma predeterminada. Si los administradores habilitan la función de caducidad de la contraseña, la antigüedad máxima de la contraseña se establece de forma predeterminada en 30 días. Los usuarios deben cambiar las contraseñas para CCMA cuando se alcanza la antigüedad máxima de la contraseña. Los administradores pueden configurar la antigüedad máxima de la contraseña para CCMA mediante el cuadro de diálogo Configuración de seguridad de CCMA.

Para las nuevas instalaciones de Contact Center versión 7.0 Feature Pack 1, la configuración de seguridad de Contact Center Manager Administration (CCMA) está activada de forma predeterminada. Si está actualizando desde Contact Center versión 7.0, su configuración de seguridad CCMA existente no se modifica.

Asistente para la creación de informes

Avaya Contact Center Select versión 7.0 ahora es compatible con el Asistente de creación de informes (RCW). RCW es una interfaz basada en web en la que puede crear y editar informes. Puede importar y programar los informes en Informes históricos. Puede acceder a RCW desde el componente Informes históricos de Contact Center Manager Administration.

Mejoras en la capacidad de servicio en Contact Center 7.0

Las siguientes son las mejoras de capacidad de servicio en Contact Center 7.0:

- Controles de terceros actualizados en Agent Desktop
- Seguridad mejorada en Contact Center Manager Administration
- Prevención de cambios en la aplicación de flujo de Orchestration Designer hasta que se inicien todos los servicios del Contact Center

Soporte para agregar imágenes y logotipos de la empresa a las firmas

Contact Center versión 7.0 admite la adición de imágenes y logotipos de empresas a firmas de correo electrónico y firmas de correo electrónico automáticas. Las firmas automáticas se agregan automáticamente en la parte inferior de un mensaje de correo electrónico saliente.

Soporte para copiar el CLID de un cliente usando Agent Desktop

En Contact Center Release 7.0, los agentes pueden utilizar el**Copiar CLID**en la barra de herramientas de Agent Desktop para copiar el número de identificación de la línea que llama (CLID) de un cliente en el portapapeles. Los agentes pueden copiar el número de teléfono de la persona que llama cuando los administradores configuran Agent Desktop para mostrar el nombre de la persona que llama mediante la integración del directorio de contactos.

Para las llamadas entrantes, Agent Desktop copia el valor de AD_CLID intrínseco cuando los agentes hacen clic en el **Copiar CLID**botón. Para las llamadas salientes, Agent Desktop copia el valor del intrínseco CALLED_NUMBER cuando los agentes hacen clic en el**Copiar CLID**botón.

Nota:

Los agentes pueden copiar el CLID de un cliente usando Agent Desktop solo para llamadas de voz en un Contact Center habilitado para SIP.

Soporte para mostrar el historial de inicio de sesión en Contact Center Manager Administration, Agent Desktop y Security Manager

En Contact Center versión 7.0, Contact Center Manager Administration, Agent Desktop y Security Manager muestran la fecha y la hora de su último inicio de sesión. Contact Center Manager Administration and Security Manager también muestra la cantidad de intentos fallidos de inicio de sesión antes de un inicio de sesión exitoso. Con la cantidad de intentos fallidos, los usuarios pueden identificar si un usuario malintencionado intentó iniciar sesión con sus credenciales después del último inicio de sesión exitoso.

De forma predeterminada, la función de salida del historial de inicio de sesión está deshabilitada. Los administradores pueden habilitar esta función mediante el cuadro de diálogo Configuración de seguridad de CCMA.

Compatibilidad con códigos de motivo No listo forzados

En Contact Center versión 7.0, los administradores pueden configurar una configuración que obligue a los agentes y supervisor/agentes a ingresar un código de motivo No listo cuando cambien su estado a No listo.

Nota:

El código predeterminado o ningún código se aplica cuando Contact Center devuelve el contacto a una cola porque el contacto no ha sido respondido dentro de las pautas de clase de presentación establecidas para el agente.

Cuando un agente que ha iniciado sesión sale de Agent Desktop haciendo clic en X en la barra superior, el agente pasa al estado Predeterminado No listo.

Compatibilidad con secuencias de comandos mediante CLID y Wild CLID en entornos SIP

Contact Center versión 7.0 admite la creación de secuencias de comandos mediante el ID de línea de llamada (CLID) y los elementos intrínsecos de CLID salvaje al crear flujos de trabajo o secuencias de comandos para una implementación SIP.

Bloqueo temporal de los usuarios de Contact Center Manager Administration

En Contact Center versión 7.0, los administradores pueden configurar una configuración que bloquea temporalmente a los usuarios de Contact Center Manager Administration (CCMA), si los usuarios ingresan incorrectamente la contraseña de la aplicación una cantidad específica de veces.

En Contact Center versión 7.0, la función de bloqueo temporal está deshabilitada de forma predeterminada. Si los administradores habilitan la función de bloqueo temporal, de forma predeterminada, los usuarios pueden ingresar la contraseña incorrectamente tres veces antes de que CCMA bloquee la cuenta de usuario durante tres minutos. Los administradores pueden

configure la cantidad de veces que los usuarios pueden ingresar una contraseña incorrecta y el período de bloqueo mediante el cuadro de diálogo Configuración de seguridad de CCMA.

Para instalaciones nuevas de Contact Center versión 7.0 Feature Pack 1, la configuración de seguridad de Contact Center Manager Administration (CCMA) está activada de forma predeterminada. Si está actualizando desde la versión 7.0 de Contact Center, la configuración de seguridad existente de CCMA no se modifica.

Cambios de funciones en la versión 7.0 Feature Pack 1

Consulte las siguientes secciones para obtener información sobre las nuevas funciones de la versión 7.0 Feature Pack 1.

Agent Desktop utiliza un directorio de usuario como directorio de exploración de archivos predeterminado

A partir de la versión 7.0 Feature Pack 1, Contact Center cambia el directorio predeterminado que utiliza Agent Desktop para la exploración de archivos a un directorio de usuario en lugar de un directorio del sistema. La exploración de archivos mediante un directorio de usuario garantiza que los agentes no puedan explorar una unidad oculta, comoC:\y mejora la seguridad en una estación de trabajo. Un directorio de usuario es el directorio que Agent Desktop abre de forma predeterminada, si un agente ha definido una carpeta de archivos adjuntos predeterminada. Si un agente no ha definido una carpeta de archivos adjuntos predeterminada o si la carpeta de archivos adjuntos predeterminada ya no existe, de forma predeterminada, Agent Desktop abre laDocumentoscarpeta en el equipo cliente.

Actualización automática de conjuntos de habilidades sin personal para informes en tiempo real

A partir de la versión 7.0 Feature Pack 1, los informes en tiempo real de Contact Center Manager Administration actualizan automáticamente cada 20 segundos la lista de perfiles sin personal con la información más reciente.

Avaya Contact Center Select es compatible con la versión 10 de IP Office

Avaya Contact Center Select es compatible con la versión 10 de IP Office. Las soluciones de Avaya Contact Center Select que usan la versión 10 de IP Office pueden beneficiarse de un aumento en el número de agentes al habilitar Direct Media en las líneas de IP Office (línea IP Office o línea SIP de IP Office) que tienen como objetivo llamadas entrantes en Avaya Contact Center Select.

Póngase en contacto con el SDK del servicio de control

A partir de la versión 7.0 Feature Pack 1, Contact Center incluye el SDK de Contact Control Service. Este SDK se basa en las capacidades de las API existentes de Contact Center al agregar soporte para llamadas de voz salientes en soluciones que integran Proactive Outreach Manager (POM). El SDK de Contact Control Service es compatible con el lenguaje de programación Java. Puede desarrollar clientes personalizados para Contact Center utilizando el SDK de Contact Control Service.

Los navegadores web integrados en Agent Desktop utilizan la última versión de Internet Explorer instalada en el sistema cliente

A partir de la versión 7.0 Feature Pack 1, Contact Center comprueba y utiliza la versión más reciente de Internet Explorer, hasta Internet Explorer 11, instalada en el sistema cliente para el navegador web integrado en Agent Desktop. Agent Desktop comprueba la versión de Internet Explorer instalada en su sistema y obliga a todos los navegadores integrados utilizados en Agent Desktop a utilizar la versión instalada hasta Internet Explorer 11. Al utilizar la última versión de Internet Explorer, las ventanas emergentes se muestran mejor y también puede tomar ventaja de HTML5.

Restricciones de extensión de archivo para archivos adjuntos

A partir de la versión 7.0 Feature Pack 1, los administradores de Contact Center pueden usar la utilidad de administración Contact Center Multimedia (CCMM) para configurar la lista admitida de extensiones de archivo que los agentes pueden adjuntar a los correos electrónicos. Cuando los agentes agregan un archivo adjunto a un correo electrónico, Agent Desktop muestra la lista configurada de extensiones de archivos adjuntos en el cuadro de diálogo Abrir. Si el tipo de archivo adjunto no está en la lista configurada, Agent Desktop muestra un mensaje de advertencia y no adjunta el archivo al correo electrónico.

Rendimiento operativo mejorado para la continuidad del negocio

A partir de la versión 7.0 Feature Pack 1, Contact Center mejora el rendimiento operativo de Business Continuity. Esto da como resultado que se muevan los archivos de la base de datos del diario de respaldo del servidor en espera a la partición del diario de la base de datos.

Este cambio no afecta el tamaño mínimo de partición de la unidad de diario de la base de datos.

La función de mensajería instantánea es compatible con Microsoft Skype for Business 2015

A partir de la versión 7.0 Feature Pack 1, la función Mensajería instantánea de Contact Center se integra con Microsoft Skype for Business 2015. La integración y el funcionamiento son idénticos a las versiones de Microsoft Lync que ya son compatibles con la versión básica de Contact Center 7.0.

Nueva aplicación para instalar Feature Packs y Service Packs

A partir de la versión 7.0 Feature Pack 1, Contact Center incluye una nueva aplicación, Release Pack Installer (RPI), para instalar Feature Packs y Service Packs.

Los archivos ZIP de Feature Pack y Service Pack incluyen el ejecutable Release Pack Installer (RPI). El RPI garantiza que no necesite desinstalar manualmente parches de software antes de actualizar Contact Center. También garantiza que las actualizaciones de software de terceros se mantengan constantes y facilita la reversión a una línea de parches anterior.

Las contraseñas de las cuentas multimedia deben cumplir con los criterios mínimos de complejidad

A partir de la versión 7.0 Feature Pack 1, Contact Center requiere cuentas multimedia para cumplir con los criterios mínimos de complejidad de la contraseña. Si es un agente o supervisor que maneja contactos multimedia, Agent Desktop lo obliga a cambiar su contraseña si inicia sesión con la contraseña predeterminada o si su contraseña no cumple con los criterios mínimos de complejidad de contraseña.

Las contraseñas deben cumplir los siguientes criterios de complejidad:

- Debe tener entre 8 y 20 caracteres
- Debe contener un número
- Debe contener al menos una letra mayúscula y al menos una letra minúscula
- No debe contener espacios
- No debe contener ninguno de estos caracteres: \ & : < > |

Los agentes pueden cambiar la contraseña de la cuenta multimedia utilizando el**preferencias**pestaña en la pantalla Preferencias del usuario. Los administradores también pueden cambiar las contraseñas de las cuentas multimedia mediante la utilidad Administración multimedia.

Provisión de agregar un nombre descriptivo para un agente de chat web

A partir de la versión 7.0 Feature Pack 1, los administradores de Contact Center pueden agregar un nombre descriptivo o un apodo para un agente de chat web. Si los administradores configuran la etiqueta Friendly Name, el apodo

Página109 de 3226.

del agente de chat web se muestra en las respuestas de los agentes a los mensajes de chat web. Los administradores también pueden elegir que el nombre descriptivo se muestre en los mensajes de bienvenida.

Eliminación de la contraseña predeterminada del panel de Agent Desktop

A partir de la versión 7.0 Feature Pack 1, Contact Center eliminó la contraseña predeterminada que se requería para acceder al panel de Agent Desktop. Puede recopilar y cargar archivos de registro o videos en el servidor del Contact Center sin ingresar una contraseña.

Lista de perfiles ordenada al crear una cartelera

A partir de la versión 7.0 Feature Pack 1, Contact Center ordena la lista de perfiles alfabéticamente cuando crea una cartelera. La lista desplegable del conjunto de habilidades se agrupa por tipo de contacto y luego se ordena alfabéticamente dentro del grupo de tipo de contacto.

Compatibilidad con la interfaz abierta de cola abierta

A partir de la versión 7.0 Feature Pack 1, Avaya Contact Center Select (ACCS) es compatible con Open Queue Open Interface.

La interfaz Open Queue Open ofrece funciones Open Queue existentes a aplicaciones de terceros que utilizan un servicio web. Las aplicaciones de terceros pueden agregar y eliminar contactos de un tipo específico en Contact Center.

Compatibilidad con VMware 6.0

A partir de la versión 7.0 Feature Pack 1, Contact Center admite entornos virtualizados en VMware 6.0. No se requieren cambios en las especificaciones del servidor virtual para ejecutar Contact Center en VMware 6.0.

Entrenamiento de susurro

A partir de la versión 7.0 Feature Pack 1, los Contact Centers habilitados para SIP amplían la función Supervisor Observe para incluir Whisper Coaching. Al usar Whisper Coaching, un supervisor puede hablar con un agente en una llamada de conjunto de habilidades con un cliente, sin que el cliente lo escuche. En el modo de entrenamiento, un supervisor puede escuchar todo lo que se dice en la llamada. Sin embargo, el consejo que brinda el supervisor solo es audible para el agente.

Whisper Coaching mejora la capacitación y el desempeño de los agentes porque los supervisores pueden capacitar al agente susurrando consejos al agente.

Página110 de 3226.

Cambios de funciones en la versión 7.0 Feature Pack 2

Consulte las siguientes secciones para obtener información sobre las nuevas funciones de la versión 7.0 Feature Pack 2.

Inicio de sesión integrado de Agent Desktop

A partir de la versión 7.0 Feature Pack 2, los agentes ya no necesitan iniciar sesión por separado en CCMM. Agent Desktop autentica a los usuarios según sus credenciales de sesión de Windows únicamente. Si sus credenciales de sesión de Windows no coinciden con sus credenciales de usuario de CCT, Agent Desktop le solicita que se autentique con sus credenciales de usuario de CCT.

Barandillas de asignación de conjunto de habilidades del agente

A partir de la versión 7.0 Feature Pack 2, no puede ejecutar la misma asignación de perfil de agente al mismo tiempo. Debe esperar hasta que se complete la asignación antes de volver a ejecutarla. Esto evita un posible impacto en el rendimiento de CCMA.

Aumento de la relación de contacto con el cliente de CCMM

A partir de la versión 7.0 Feature Pack 2, la relación entre clientes y contactos en Contact Center Multimedia (CCMM) se incrementó a 1:1000 (o 1 registro de cliente por cada 1000 contactos).

Tienda de seguridad sin conexión

A partir de la versión 7.0 Feature Pack 2, puede crear una tienda sin conexión mediante Security Manager. Esto le permite minimizar el tiempo de inactividad si desea reemplazar su almacén de seguridad actual. Cuando se crea su tienda fuera de línea, puede cambiar entre la tienda activa y la tienda fuera de línea. Puede convertir la tienda fuera de línea en la tienda activa en cualquier momento mediante el Administrador de seguridad. Debe detener los servicios de Contact Center antes de activar la tienda sin conexión.

Compatibilidad con servicios de escritorio remoto para Agent Desktop

A partir de la versión 7.0 Feature Pack 2, Contact Center admite el uso de Servicios de escritorio remoto en un servidor Windows Server 2012 R2 para alojar y publicar Agent Desktop.

Eliminación de la configuración de seguridad predeterminada

A partir de la versión 7.0 Feature Pack 2, para las nuevas instalaciones, Contact Center ya no proporciona un almacén de seguridad predeterminado ni certificados de seguridad predeterminados. En la etapa de instalación, ahora puede usar Ignition Wizard para crear un almacén de seguridad, generar una Solicitud de firma de certificado (CSR) e importar un certificado raíz de Autoridad de certificación. Como alternativa, puede optar por omitir la configuración de seguridad en la etapa de instalación y configurar sus certificados de seguridad más adelante en el proceso de puesta en marcha mediante Security Manager.

Integración API REST

A partir de la versión 7.0 Feature Pack 2, Contact Center le permite invocar REST API en un flujo de trabajo de Contact Center. REST (Transferencia de estado representacional) proporciona servicios escalables eficientes para comunicaciones web.

Un flujo de trabajo de Contact Center puede solicitar datos mediante comandos de secuencias de comandos, y el flujo de trabajo utiliza TfeRestService para solicitar y recuperar datos de la API de REST.

Sincronización de cambios de usuario accssync a IP Office

A partir de la versión 7.0 Feature Pack 2, Avaya Contact Center Select sincroniza los cambios de contraseña de usuario de accssync con IP Office. Cuando cambia la contraseña de usuario de accssync, Contact Center Manager Administration actualiza automáticamente la contraseña en IP Office.

Compatibilidad con VMware 6.5

A partir de la versión 7.0 Feature Pack 2, Contact Center admite entornos virtualizados en VMware 6.5. No se requieren cambios en las especificaciones del servidor virtual para ejecutar Contact Center en VMware 6.5.

Cambios de funciones en la versión 7.0 Feature Pack 3

Consulte las siguientes secciones para obtener información sobre las nuevas funciones de la versión 7.0 Feature Pack 3.

Capacidad para almacenar archivos adjuntos de correo electrónico en la base de datos

A partir de la versión 7.0 Feature Pack 3, hay una opción para guardar nuevos archivos adjuntos de correo electrónico en la base de datos MULTIMEDIA en lugar de en el sistema de archivos. Puede configurar esta opción mediante la utilidad Administración multimedia.

Cifrado de la base de datos del Contact Center

A partir de la versión 7.0 Feature Pack 3, puede cifrar y descifrar la base de datos de Contact Center mediante Security Manager. Para cifrar la base de datos, debe crear y activar una clave de cifrado y utilizarla para codificar los archivos en la base de datos de Contact Center Caché.

Gestión de datos - privacidad del cliente

A partir de la versión 7.0 Feature Pack 3, puede utilizar la utilidad de gestión de datos multimedia para actuar sobre las solicitudes de privacidad de los clientes del centro de contacto. Por ejemplo, si un cliente ejerce su derecho de acceso a la información o su derecho al olvido, puede utilizar la utilidad Gestión de datos multimedia para satisfacer estas solicitudes.

Mejoras de la API REST

A partir de la versión 7.0 Feature Pack 3, la API REST de Contact Center admite los métodos de solicitud GET, POST, PUT o DELETE. Usando TFE REST Configurator, ahora puede agregar entornos que permiten el uso de variables de entorno en solicitudes REST.

Los flujos de trabajo de Contact Center ahora admiten los comandos CONVERT y JSON GET ELEMENT.

Compatibilidad con Security Manager para certificados encadenados

A partir de la versión 7.0 Feature Pack 3, Security Manager admite la importación de certificados encadenados.

Soporte para aplicar un indicador de restricción a un cliente

A partir de la versión 7.0 Feature Pack 3, puede aplicar un indicador de restricción a un cliente mediante Agent Desktop. Esto puede ayudar a su Contact Center a cumplir con el Reglamento General de Protección de Datos (GDPR). Por ejemplo, agregue una marca restringida para indicar a los agentes que no envíen mensajes de correo electrónico no solicitados a los clientes sin su consentimiento.

Otros cambios en la versión 7.0

Consulte las siguientes secciones para obtener información sobre otros cambios en la compilación base de la versión 7.0.

Agent Desktop ya no admite la implementación como un cliente pesado

A partir de la versión 7.0, Contact Center no admite la implementación de Agent Desktop como un cliente pesado. Puede implementar Agent Desktop mediante la implementación de un clic o un archivo MSI.

El archivo OVA de Avaya Contact Center Select ya no está disponible

Avaya Contact Center Select versión 7.0 no está disponible como archivo OVA (Open Virtual Appliance). Puede usar el DVD o la imagen ISO de la versión 7.0 de Avaya Contact Center Select para crear una variedad de máquinas virtuales de VMware. Avaya Contact Center Select sigue siendo compatible con la virtualización, la productividad, la eficiencia y la flexibilidad de VMware. Avaya Contact Center Select versión 7.0 admite la integración con Avaya WebLM versión 7.0 y Avaya Aura®Media Server Release 7.7 OVA.

Versiones compatibles con IP Office

Avaya Contact Center Select versión 7.0 no admite la integración con IP Office 9.0.3 o 9.0.4.

Avaya Contact Center Select versión 7.0 admite la integración con IP Office 9.1.x, mínimo 9.1.4 o posterior. Para obtener más información sobre las versiones compatibles de IP Office, consulte las Notas de la versión de Avaya Contact Center Select.

Versiones compatibles con Microsoft Exchange Server

Contact Center versión 7.0 no es compatible con Microsoft Exchange Server 2003. Contact Center versión 7.0 solo es compatible con Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 y Microsoft Exchange Server 2013.

Las versiones de Microsoft Internet Explorer ya no son compatibles

Contact Center versión 7.0 no es compatible con las versiones 8.0 o 9.0 de Microsoft Internet Explorer. Contact Center versión 7.0 solo es compatible con Microsoft Internet Explorer 10.0 (solo versión de 32 bits) y 11.0 (solo versión de 32 bits).

Las comunicaciones de Secure Sockets Layer ya no son compatibles

Contact Center versión 7.0 no es compatible con Secure Sockets Layer (SSL) para conexiones seguras. Contact Center solo admite Seguridad de la capa de transporte (TLS). Esto es para eliminar las vulnerabilidades de seguridad que existen en SSL.

Las aplicaciones personalizadas o de terceros que se conectan a Contact Center deben ser compatibles con TLS 1.0 o posterior. La eliminación del soporte de SSL puede tener implicaciones para las aplicaciones personalizadas o de terceros existentes. Antes de migrar desde una versión anterior, verifique las aplicaciones personalizadas o de terceros que se conectaron de forma segura a Contact Center, para asegurarse de que estas aplicaciones admitan TLS.

Windows Server 2008 ya no es compatible

Avaya Contact Center Select versión 7.0 solo es compatible con Microsoft Windows Server 2012 R2. Avaya Contact Center Select versión 7.0 no es compatible con Microsoft Windows Server 2008 R2. Los clientes que actualicen a Avaya Contact Center Select versión 7.0 deben migrar a un nuevo servidor Microsoft Windows Server 2012 R2.

Otros cambios en la versión 7.0 Feature Pack 1

Consulte las siguientes secciones para obtener información sobre otros cambios en la versión 7.0 Feature Pack 1.

Mejoras en la seguridad del Contact Center

A partir de la versión 7.0 Feature Pack 1, Contact Center presenta mejoras de seguridad adicionales para mantenerse al día con los últimos estándares de la industria. Estas mejoras incluyen restricciones al acceso a servicios web, bloqueo de cuentas de usuario y cambios en la forma en que Contact Center administra contraseñas y claves. Muchas de estas mejoras son internas para la operación del Contact Center y no tienen impacto en las operaciones del usuario final.

Cualquier mejora de seguridad que sea visible para los usuarios finales, o que cambie la forma en que los usuarios trabajan con Contact Center, tiene un tema aparte en esta sección.

Firma del bloque de mensajes del servidor habilitada en Windows Server 2012

A partir de la versión 7.0 Feature Pack 1, tanto el DVD de Contact Center como el instalador del Release Pack modifican la política de grupo local de Windows Server 2012 para habilitar la firma del bloque de mensajes del servidor (SMB). La firma SMB coloca una etiqueta digital en cada bloque de mensajes del servidor, lo que ayuda a prevenir ataques de intermediarios en el uso compartido de archivos en la red.

Página115 de 3226.

Si no desea utilizar la firma SMB, puede deshabilitarla modificando la política de grupo local de Windows Server 2012.

Componentes de terceros actualizados

La versión 7.0 Feature Pack 1 actualiza los componentes de terceros de Contact Center Tomcat y Java a versiones recientes. Esto mejora la seguridad y garantiza que Contact Center se mantenga actualizado con las actualizaciones más recientes.

El instalador del paquete de lanzamiento actualiza automáticamente estos componentes.

Otros cambios en la versión 7.0 Feature Pack 2

Consulte las siguientes secciones para obtener información sobre otros cambios en la versión 7.0 Feature Pack 2.

Los usuarios de CCMA deben iniciar sesión antes de cambiar la contraseña

A partir de la versión 7.0 Feature Pack 2, los usuarios de CCMA deben iniciar sesión antes de cambiar su contraseña. Al cambiar una contraseña en CCMA, los usuarios ahora pueden cambiar la contraseña del usuario actualmente conectado únicamente.

Cuenta de instalación para la instalación de Contact Center

A partir de la versión 7.0 Feature Pack 2, puede usar cualquier cuenta con derechos administrativos locales para instalar Contact Center, siempre que deshabilite la función de seguridad Modo de aprobación de administrador en el servidor de Contact Center. También puede usar cualquier cuenta con derechos administrativos locales para actualizar y parchear Contact Center; no es necesario utilizar siempre la misma cuenta administrativa para realizar estas tareas.

Componentes de terceros actualizados

La versión 7.0 Feature Pack 2 actualiza varios componentes de terceros a versiones recientes, como Caché, Contact Center Tomcat y .NET Framework. Esto mejora la seguridad y garantiza que Contact Center se mantenga actualizado con las actualizaciones más recientes.

El instalador del paquete de lanzamiento actualiza automáticamente estos componentes.

Otros cambios en la versión 7.0 Feature Pack 3

Consulte las siguientes secciones para obtener información sobre otros cambios en la versión 7.0 Feature Pack 3.

Aura de Avaya®Actualización del servidor de medios

Contact Center versión 7.0 Feature Pack 3 es compatible con Avaya Aura®Servidor multimedia versión 7.8.

Desde Contact Center versión 7.0 Feature Pack 3, instalación de la versión para Windows de Avaya Aura® El Media Server co-residente con Voice and Multimedia Contact Server ya no es compatible. Cuando implementa un servidor de contactos multimedia y de voz con Avaya Aura®Media Server, Contact Center instala la versión Linux de Avaya Aura®Servidor de medios en una instancia de Hyper-V en su servidor de contactos de voz y multimedia.

Este proceso está totalmente automatizado por el instalador del software Contact Center para instalaciones nuevas y por el instalador del paquete de versión (RPI) de Contact Center para actualizaciones. En ambos casos, puede usar la utilidad Update Configurator para actualizar Avaya Aura®Media Server a la última versión compatible y aplique toda la configuración necesaria. Después de reiniciar después de una instalación o actualización, se inicia la utilidad Update Configurator.

Contact Center retrocompatibilidad con la versión anterior de Agent Desktop

A partir de la versión 7.0 Feature Pack 3, Contact Center es compatible con versiones anteriores del Feature Pack o Service Pack de Agent Desktop. Esto le permite actualizar el servidor de Contact Center sin el requisito de actualizar Agent Desktop en una sola ventana de mantenimiento. Por ejemplo, si actualiza a la versión 7.0 Feature Pack 3, puede usar la versión 7.0 Feature Pack 2 de Agent Desktop.

Las nuevas funciones de Agent Desktop agregadas en la última versión de Contact Center no están disponibles hasta que actualice Agent Desktop a esa versión.

La compatibilidad con versiones anteriores no es compatible con versiones principales o secundarias. Por ejemplo, si actualiza a la versión 7.1, no puede usar la versión 7.0 de Agent Desktop.

Versiones compatibles con IP Office

Avaya Contact Center Select versión 7.0 Feature Pack 3 no admite la integración con IP Office 9.1.

Avaya Contact Center Select versión 7.0 Feature Pack 3 admite la integración con IP Office 10.1 y 11.0. Para obtener más información sobre las versiones compatibles de IP Office, consulte las Notas de la versión de Avaya Contact Center Select.

Componentes de terceros actualizados

La versión 7.0 Feature Pack 3 actualiza varios componentes de terceros a versiones recientes, como Caché, Contact Center Tomcat y .NET Framework. Esto mejora la seguridad y garantiza que Contact Center se mantenga actualizado con las actualizaciones más recientes.

El instalador del paquete de lanzamiento actualiza automáticamente estos componentes.

Capítulo 3: Avaya Contact Center Select

visión general

Avaya Contact Center Select es una solución de experiencia del cliente sensible al contexto, colaborativa, de voz y multimedia que permite a las pequeñas y medianas empresas anticipar, acelerar y mejorar las interacciones con los clientes. Avaya Contact Center Select utiliza el sistema telefónico Avaya IP Office para proporcionar una plataforma de telefonía en tiempo real. Avaya IP Office es un sistema telefónico flexible y escalable diseñado específicamente para pequeñas y medianas empresas. IP Office es compatible con una amplia gama de teléfonos y dispositivos para uso en centros de contacto.

Avaya Contact Center Select utiliza interfaces SIP y CTI para comunicarse con la plataforma IP Office. Esta integración brinda a Avaya Contact Center Select acceso y control de una amplia gama de teléfonos y funciones de IP Office. Los clientes que integran Avaya Contact Center Select con la plataforma IP Office obtienen enrutamiento basado en habilidades, tratamientos de llamadas, informes, administración unificada de agentes y la utilidad gráfica Orchestration Designer. Agent Desktop admite teléfonos IP Office específicos y también admite tipos de contactos multimedia.

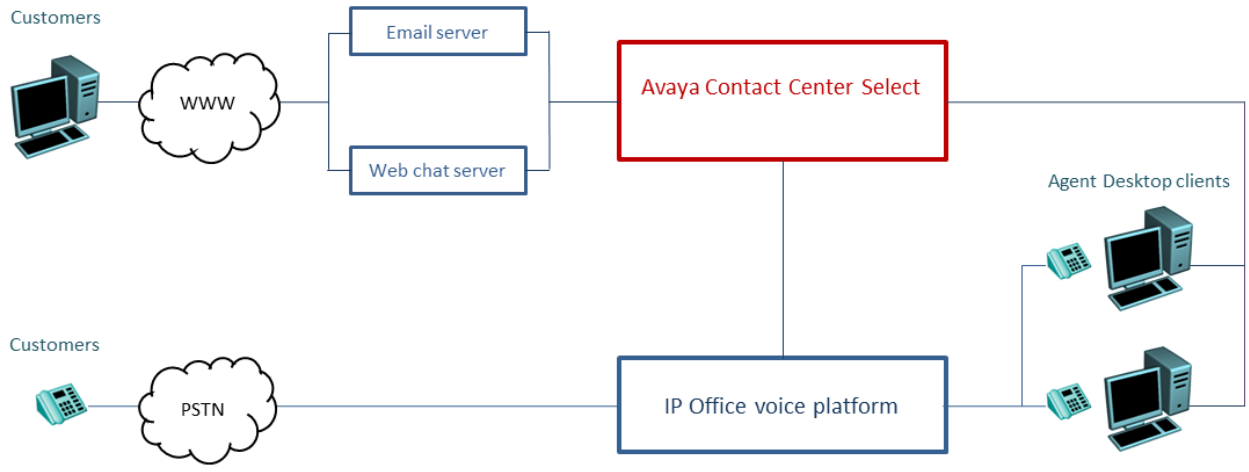


Figura 1: Solución típica de centro de contacto que utiliza Avaya Contact Center Select con voz y multimedia y el sistema telefónico de voz Avaya IP Office

Avaya Contact Center Select proporciona una solución multimedia y de voz rica en funciones con enrutamiento e informes integrados para las pequeñas y medianas empresas. Avaya Contact Center Select proporciona un centro de contacto unificado y administración de cuentas de usuario de teléfonos IP Office para agentes y supervisores.

Los agentes y supervisores habilitados para voz creados en Avaya Contact Center Select se agregan automáticamente a la plataforma IP Office. Avaya Contact Center Select sincroniza la información del usuario (agente y supervisor) entre Avaya Contact Center Select y la plataforma IP Office.

Avaya Contact Center Select se ofrece en los siguientes tipos de implementación:

- **DVD de Avaya Contact Center Select**; El DVD de Avaya Contact Center Select contiene el software de la aplicación. La opción de implementación de Avaya Contact Center Select DVD es compatible con Platform Vendor Independence (PVI). El cliente proporciona la licencia del sistema operativo Microsoft Windows 2012 R2 y el hardware del servidor que cumple con una de las especificaciones del servidor Avaya Contact Center Select PVI.
- **Dispositivo de software Avaya Contact Center Select**; El dispositivo de software Avaya Contact Center Select es un conjunto de servidores virtualizados de VMware; una máquina virtual Avaya Contact Center Select, un Avaya Aura®Media Server OVA y un WebLM OVA. El cliente proporciona los recursos de VMware y la licencia del sistema operativo para la máquina virtual de VMware (invitado).
- **Dispositivo de hardware Avaya Contact Center Select**; El dispositivo de hardware de Avaya Contact Center Select es un servidor físico con el software de la aplicación ya cargado y parcialmente preconfigurado. Avaya proporciona el hardware del servidor y una licencia para el sistema operativo Microsoft Windows 2012 R2.

Avaya Contact Center Select admite los siguientes tipos de contactos enrutados:

- Voz
- Correo electrónico
- Saliente
- Comunicaciones web (chat web)
- Mensajes de texto SMS
- Mensajes de fax
- Documentos escaneados
- Mensajes de correo de voz

Avaya Contact Center Select también es compatible con la mensajería instantánea punto a punto y las notificaciones de presencia. Para admitir los tipos de contacto basados en correo electrónico, debe agregar un servidor de correo electrónico a su solución. Para admitir el tipo de contacto de comunicaciones web, debe agregar un servidor de comunicaciones web a su solución.

El servidor de Avaya Contact Center Select se admite en un grupo de trabajo o en un dominio de Windows.

Avaya Contact Center Select se implementa rápidamente y ofrece una solución multimedia y de voz rica en funciones. Avaya Contact Center Select proporciona datos de configuración de muestra para respaldar una implementación e integración rápidas con IP Office. Puede modificar los datos de muestra para cumplir con los requisitos de su solución y agregarlos a medida que su solución se expande. También puede usar los datos de muestra para obtener más información sobre Avaya Contact Center Select. Los datos de muestra incluyen los siguientes datos:

- Supervisores y agentes

• Conjuntos de habilidades

• Aplicaciones de flujo de voz de Orchestration Designer

• Códigos de actividad

• CDN (puntos de ruta)

• Clases de presentación de multiplicidad

• Informes en tiempo real

• Informes históricos

• Cuenta de sincronización de datos de usuario para IP Office

Avaya Contact Center Select proporciona una utilidad de administración de mensajes de voz simplificada. El supervisor del centro de contacto puede realizar un trabajo de administración rápido sin necesidad de acceso de administrador a Avaya Aura.®Servidor del servidor de medios. Avaya Contact Center Select proporciona una serie de utilidades de monitoreo de estado para monitorear los puntos de integración con la plataforma IP Office. Avaya Contact Center Select también proporciona un tablero de resolución de problemas gráfico siempre activo que se ejecuta en el servidor.

Licencia

Avaya Contact Center Select admite los siguientes paquetes de agentes con licencia:

Nombre	Descripción	notas
Licencias de agente	Las licencias de agente determinan la cantidad de agentes que pueden iniciar sesión en Contact Center. La licencia está disponible para los siguientes tipos de agentes: • agente de voz • agente saliente • agente de correo electrónico (que cubre mensajes de FAX, mensajes de texto SMS, mensajes de correo de voz y mensajes de documentos escaneados) • Agente de comunicaciones web (o agente de chat web)	

Avaya Contact Center Select admite las siguientes funciones con licencia:

Nombre	Descripción	notas
Multiplicidad	La multiplicidad es la capacidad de un agente para manejar múltiples contactos multimedia concurrentes. En cualquier momento, un agente puede estar activo en un contacto de voz y multimedia. Sin embargo, cuando un contacto está activo; los demás quedan automáticamente en espera. El número máximo de contactos multimedia o no de voz simultáneos que se le puede asignar a un agente es cinco.	

La tabla continúa...

Nombre	Descripción	notas
Basado en la web Estadísticas	Si el servidor de informes web está habilitado, los agentes y supervisores pueden usar Agent Desktop para ver informes en tiempo real para el manejo de llamadas, datos de perfiles e información de estado en Agent Desktop.	
Agente remoto	Remote Agent es una solución que extiende un centro de contacto al entorno preferido de un agente, lo que le permite manejar llamadas de conjuntos de habilidades sin importar la ubicación. Las soluciones de Agente Remoto conectan las llamadas del centro de contacto al teléfono del agente (teléfono fijo o móvil), sin que el agente necesite hardware especial.	
Saliente	Utilice el servidor multimedia y la herramienta de administración de campañas salientes en Contact Center Manager Administration para crear campañas salientes progresivas en las que las llamadas se transfieren a los agentes y se realizan desde el Contact Center.	

Para la integración de Avaya Contact Center Select (ACCS) con IP Office Server Edition, IP Office Server Edition requiere las siguientes licencias:

- Una licencia de Avaya IP Endpoint para la integración de Avaya Contact Center Select.
- Una licencia de usuario avanzado para cada agente de ACCS o agente supervisor que esté configurado para cualquiera de los siguientes:
  - configurado para usar IP Office Avaya Communicator para Windows.
  - configurado para funcionar como un agente remoto ACCS.
  - configurado para usar un teléfono físico de IP Office con la funcionalidad de trabajador remoto de IP Office. Solo los teléfonos físicos de IP Office que utilizan la funcionalidad de trabajador remoto de IP Office requieren una licencia de usuario avanzado; otros usuarios de teléfonos físicos no requieren una licencia de usuario avanzado.
- Una licencia de Server Edition. Una licencia para cada nodo en la Small Community Network (SCN).
- Licencias de IP Endpoint: ya sea de Avaya o de terceros, según los teléfonos IP utilizados en su solución. Aprovisione una licencia IP Endpoint para cada punto final configurado.
  - Los usuarios de IP Office Avaya Communicator for Windows no requieren una licencia de terminal IP, solo una licencia de usuario de IP Office.
  - Si su solución usa teléfonos digitales solo de una expansión IP Office 500V2, entonces no necesita licencias para terminales.
- Una licencia de CTI Pro o una licencia de API de terceros para IP Office.
- Una licencia ACCS para IP Office.
- Canales de correo de voz adicionales de Voicemail Pro, hasta un máximo de 350.
- Licencias de troncales SIP o canales para admitir las troncales utilizadas en su solución.
- Administradores de grabación de Voicemail Pro. Una instancia en cada nodo del SCN desde el que se graban las llamadas. Si toda la grabación se va a realizar en el nodo principal, se requiere una instancia. Esta licencia habilita Contact Recorder.

Para la integración de Avaya Contact Center Select (ACCS) con IP Office 500V2 (non-Server Edition), IP Office 500V2 requiere las siguientes licencias:

- Una licencia de Avaya IP Endpoint para la integración de Avaya Contact Center Select.
- Una licencia de usuario avanzado para cada agente de ACCS o agente supervisor que esté configurado para cualquiera de los siguientes:
  - configurado para usar IP Office Avaya Communicator para Windows.
  - configurado para funcionar como un agente remoto ACCS.
  - configurado para usar un teléfono físico de IP Office con la funcionalidad de trabajador remoto de IP Office. Solo los teléfonos físicos de IP Office que utilizan la funcionalidad de trabajador remoto de IP Office requieren una licencia de usuario avanzado; otros usuarios de teléfonos físicos no requieren una licencia de usuario avanzado.
- Licencia de edición preferida.
- Licencia de Edición Esencial.
- Licencias de IP Endpoint: ya sea de Avaya o de terceros, según los teléfonos IP utilizados en su solución.
  - Los usuarios de IP Office Avaya Communicator for Windows no requieren una licencia de terminal IP, solo una licencia de usuario de IP Office.
  - Si su solución utiliza solo teléfonos digitales, entonces no necesita licencias de terminales.
- Una licencia CTI Pro.
- Canales de correo de voz adicionales de Voicemail Pro.
- Licencias de troncales SIP o licencias de canales para admitir las troncales utilizadas en su solución.
- Administradores de grabación de Voicemail Pro. Una instancia en cada nodo de la red comunitaria pequeña (SCN) desde la que se graban las llamadas. Si toda la grabación se va a realizar en el nodo principal, se requiere una instancia. Esta licencia habilita Contact Recorder. Contacto Recorder requiere un servidor de aplicaciones independiente.

Cuando se implementa Avaya Contact Center Select con un par IP Office Resilience, asegúrese de que el sistema secundario de IP Office contenga las siguientes licencias para habilitar la conectividad de Avaya Contact Center Select:

- Una licencia de punto final IP de Avaya
- Una licencia CTI Pro

Esto se aplica tanto a las configuraciones independientes de Avaya Contact Center Select como a Avaya Contact Center Select Business Continuity. El sistema secundario de IP Office no requiere la inclusión del sistema de licencias de administradores de grabaciones de Voicemail Pro o las licencias de Voicemail Pro, ya que la funcionalidad de grabación de llamadas tiene licencia del sistema primario de IP Office.

El paquete de software básico de Avaya Contact Center Select proporciona una licencia del sistema Contact Recorder más 1 puerto Voicemail Pro para cada agente de voz para la grabación de llamadas.

Una licencia de agente de voz de Avaya Contact Center Select proporciona un puerto de Voicemail Pro para grabación de llamadas.

Página123 de 3226.

Avaya Contact Center Select utiliza Avaya WebLM como proveedor de licencias. Cada instancia de Avaya WebLM admite un solo Avaya Contact Center Select.

Hotdesking / Asientos libres

Los entornos de escritorio compartido/de libre disposición son compatibles con los teléfonos físicos y softphones de ACCS e IP Office.

Hotdesking con teléfonos físicos

Cada teléfono IP físico requiere una licencia IP Endpoint.

No se requieren licencias de usuario avanzado para usar teléfonos físicos de IP Office a menos que use la función de trabajador remoto de IP Office.

Ejemplo:

Requisito: 100 asientos ACCS con 100 teléfonos físicos IP y 200 posibles agentes:

- Ordene 100 agentes de voz ACCS + 100 licencias de IP Endpoint.
- Si todos los agentes requieren la funcionalidad de trabajador remoto de IP Office, solicite también 200 licencias de usuario avanzado.

Escritorio compartido con softphones

Cada agente ACCS requiere una licencia de usuario avanzado. No se

requieren licencias de IP Endpoint para los softphones. **Ejemplo:**

Requisito: 100 asientos ACCS con 100 softphones y 200 posibles agentes:

- Solicite 100 agentes de voz ACCS + 200 licencias de usuario avanzado.

Número máximo de nodos admitidos

Avaya Contact Center Select admite la siguiente cantidad máxima de nodos de IP Office:

- Para IP Office 10.xo 11.0 Select (Server Edition) Switch R630 u OVA, ACCS admite 150 nodos en total, que consisten en un primario, un secundario y 148 expansiones.
- Para IP Office 10.xy 11.0 Select (Server Edition) con cualquier hardware que no sea R630/OVA, ACCS admite 32 nodos en total, que consisten en un primario, un secundario y 30 expansiones.

Sincronización de datos de usuario

Avaya Contact Center Select proporciona administración unificada para los agentes del centro de contacto y los usuarios de IP Office. Los usuarios (agentes y supervisores) que configura en Avaya Contact Center Select se reflejan automáticamente en la IP Office conectada.

Cuando crea un agente en Contact Center Manager Administration, puede optar por crear una cuenta de usuario de Windows local en el servidor de Avaya Contact Center Select o asignarla a una cuenta de usuario de dominio de Windows existente. Avaya Contact Center Select crea automáticamente una cuenta de usuario coincidente en IP Office.

Cuando modifica los detalles del agente en Avaya Contact Center Select, los detalles del usuario de IP Office correspondiente se actualizan automáticamente. Si elimina un agente en Avaya Contact Center Select, el usuario de IP Office correspondiente no se elimina.

El mecanismo de sincronización de datos funciona en una dirección; de Avaya Contact Center Select a IP Office. El administrador de Avaya Contact Center Select puede forzar manualmente la sincronización de datos desde Avaya Contact Center Select.

Topología

En una solución de centro de contacto que utiliza Avaya Contact Center Select y un sistema telefónico IP Office, se aplican las siguientes consideraciones de topología de red y conectividad.

Avaya Contact Center Select (ACCS) admite las siguientes opciones de implementación:

- DVD de Avaya Contact Center Select
- Dispositivo de software Avaya Contact Center Select
- Dispositivo de hardware Avaya Contact Center Select

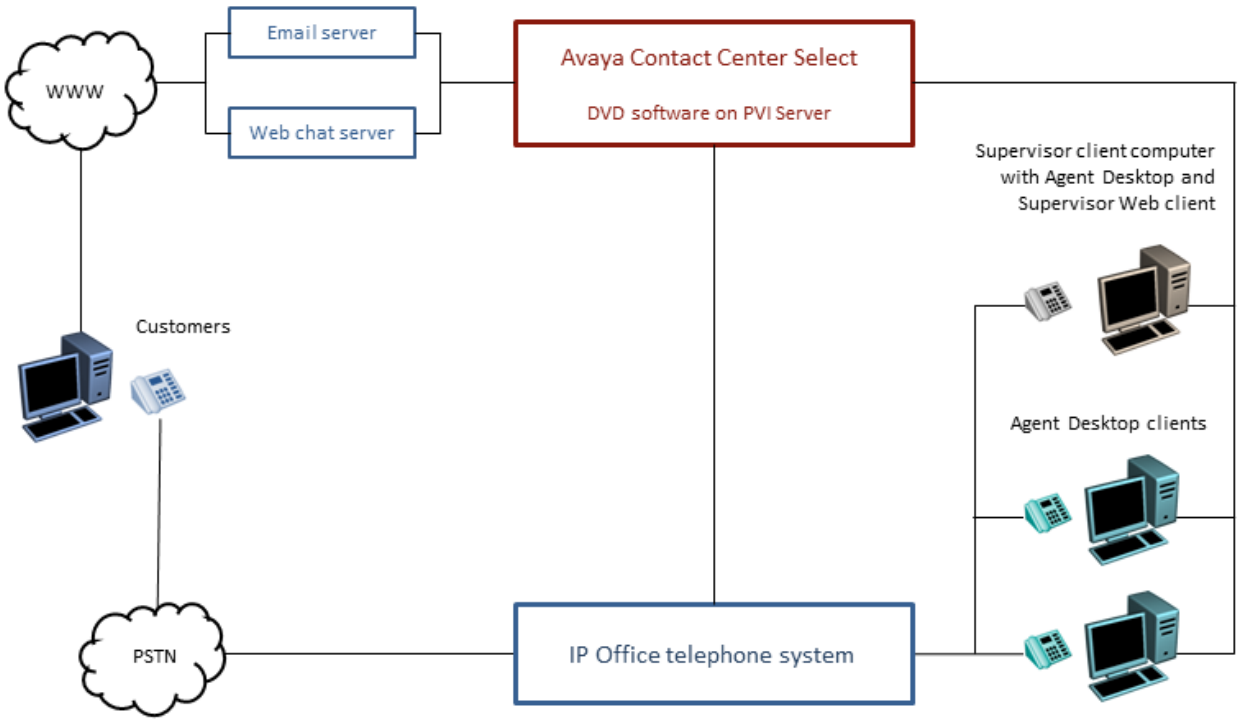


Figura 2: Implementación típica de Avaya Contact Center Select DVD

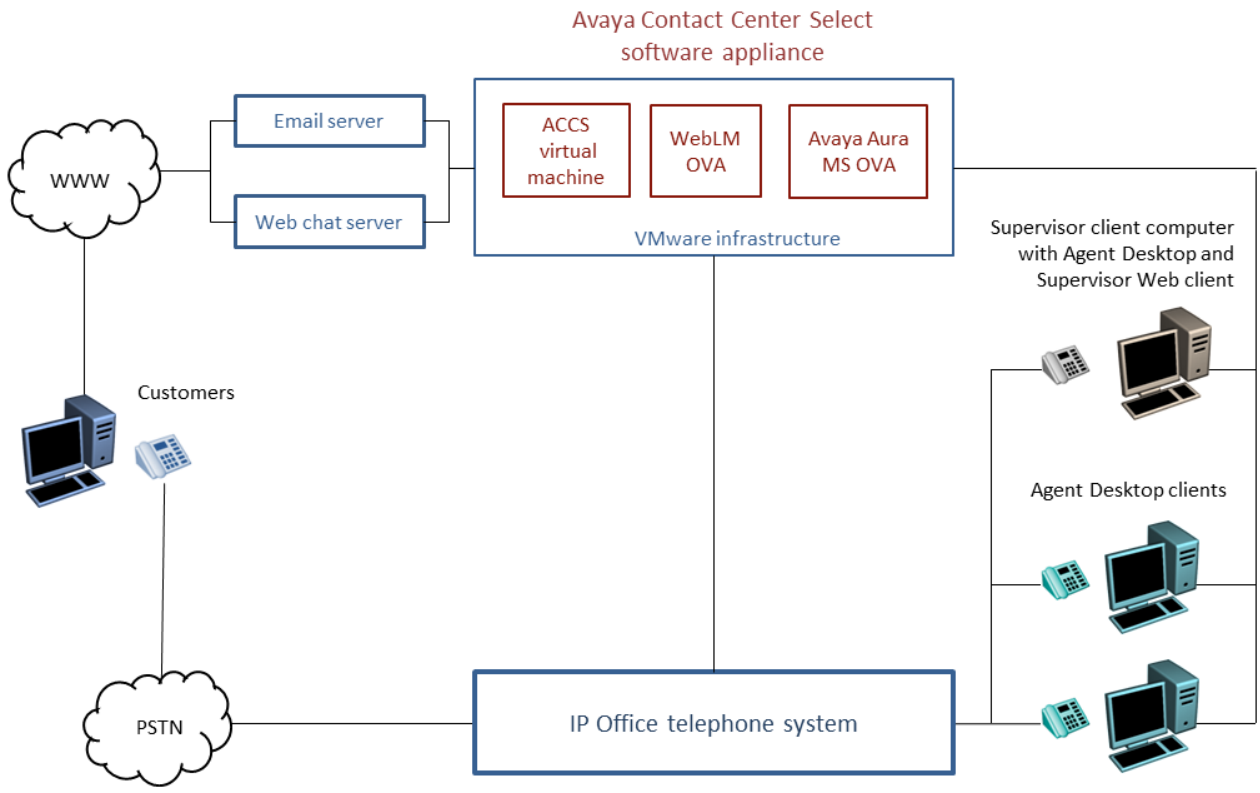


Figura 3: Solución típica de dispositivo de software de Avaya Contact Center Select

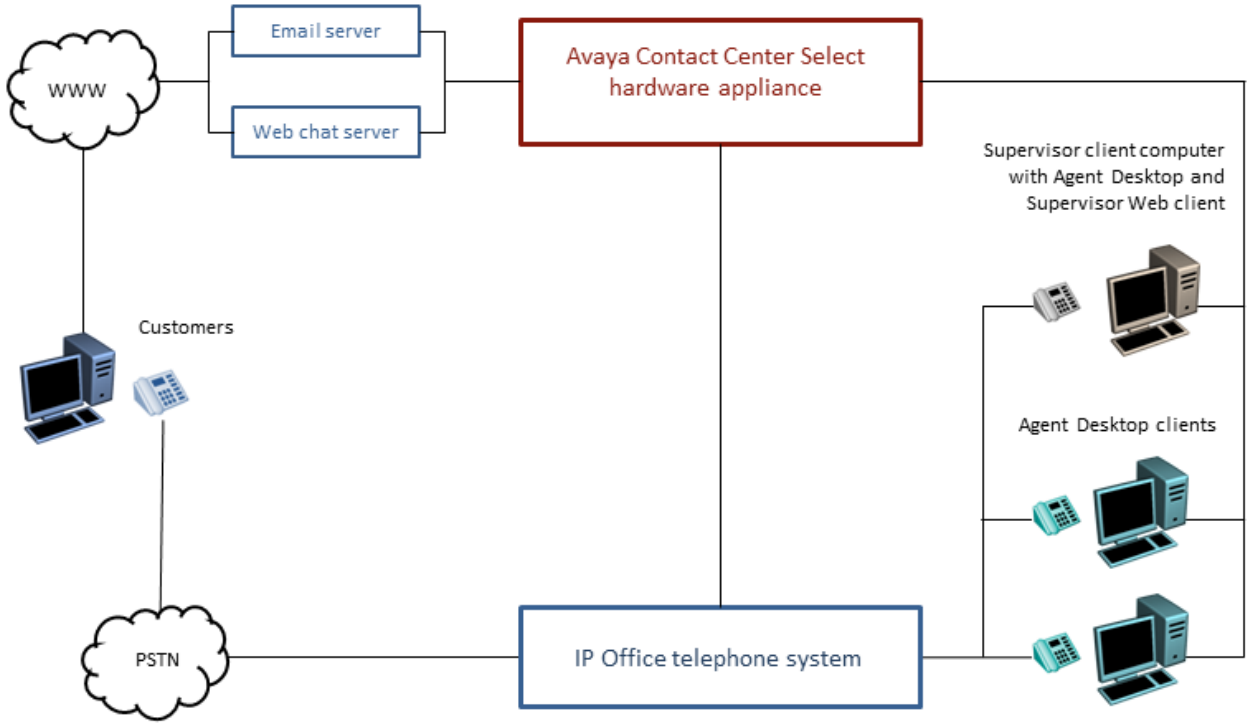


Figura 4: Solución típica de dispositivo de hardware de Avaya Contact Center Select

Las siguientes condiciones de conectividad y diseño de red se aplican a todas las soluciones de Avaya Contact Center Select:

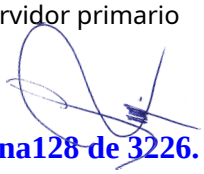
- El servidor Avaya Contact Center Select se admite en un grupo de trabajo o en un dominio de Windows.
- Cada Avaya Contact Center Select se conecta a un único servidor primario de IP Office Server Edition. Avaya Contact Center Select no admite la conexión a un servidor secundario de IP Office. De manera alternativa, cada Avaya Contact Center Select puede conectarse a un solo modo estándar de IP Office 500V2 con una licencia de edición avanzada.
- Una red comunitaria pequeña (SCN) es un sistema de sistemas telefónicos de IP Office en red que puede, entre otras funciones, compartir números de extensión y nombres de usuario. Cada IP Office SCN admite un solo Avaya Contact Center Select conectado. Avaya Contact Center Select se conecta al servidor primario de IP Office Server Edition del SCN.
- Para admitir una SCN de IP Office, Avaya Contact Center Select debe conectarse a un servidor primario de IP Office Server Edition en esa red SCN.
- El servidor Avaya Contact Center Select y el sistema telefónico IP Office conectado deben estar ubicados en la misma ubicación del campus.
- Para admitir los tipos de contactos multimedia basados en correo electrónico, debe instalar y poner en marcha un servidor de correo electrónico en su solución.
- Para admitir el tipo de contacto de comunicaciones web (chat web), debe instalar y poner en marcha un servidor de chat web en su solución.

- Cada instancia de Avaya WebLM admite un solo Avaya Contact Center Select.
- Cada Avaya Aura®La instancia de Media Server admite un solo Avaya Contact Center Select.
- Una sola instancia de Contact Center Manager Administration (CCMA) puede administrar solo un solo Avaya Contact Center Select.
- Si utiliza Avaya Contact Center Select Software Appliance, la máquina virtual Avaya Contact Center Select, la máquina virtual WebLM y Avaya Aura®Todas las máquinas virtuales de Media Server deben estar alojadas en servidores VMware ubicados en la misma ubicación del campus. El dispositivo de software Avaya Contact Center Select admite el alojamiento de la máquina virtual Avaya Contact Center Select, la máquina virtual WebLM y Avaya Aura.® Máquina virtual de Media Server en un servidor host de VMware. El servidor host de la máquina virtual de Avaya Contact Center Select y el sistema telefónico IP Office conectado deben estar ubicados en la misma ubicación del campus.
- Cada computadora cliente Supervisor se comunica con el servidor Avaya Contact Center Select. Cada equipo cliente de Agent Supervisor tiene instalado el software Agent Desktop y Microsoft Internet Explorer. El supervisor utiliza Internet Explorer para acceder al cliente web de Contact Center Manager Administration. El supervisor utiliza Contact Center Manager Administration para realizar la configuración básica del agente y ejecutar informes. El supervisor de agentes utiliza el software Agent Desktop para manejar llamadas de clientes, aceptar llamadas de emergencia o de supervisor de agentes y observar llamadas o contactos de comunicación web. Cada computadora Supervisor con Agent Desktop requiere un teléfono IP Office asociado.
- Cada equipo cliente del Agente se comunica con el servidor de Avaya Contact Center Select. Cada computadora del Agente tiene instalado el software Agent Desktop y Microsoft Internet Explorer. El agente utiliza Internet Explorer para descargar el software de cliente de Agent Desktop. El agente utiliza el software Agent Desktop para gestionar las llamadas de los clientes. Cada computadora del Agente requiere un teléfono IP Office asociado.
- La multidifusión o la unidifusión deben estar habilitadas en la red de datos subyacente entre los clientes y el servidor de Avaya Contact Center Select para el supervisor y los agentes.
- Avaya Contact Center Select Business Continuity agrega conectividad de red adicional y consideraciones de diseño a la solución. Para más información, ver*Continuidad comercial de Avaya Contact Center Select*.

Versiones compatibles con IP Office

Cada Avaya Contact Center Select se conecta a un único servidor primario de IP Office Server Edition. Las soluciones habilitadas para la continuidad comercial de Avaya Contact Center Select admiten la conexión a un servidor secundario de IP Office. Una red comunitaria pequeña (SCN) es un sistema de sistemas telefónicos IP Office en red que pueden compartir números de extensión y nombres de usuario. Cada IP Office SCN admite un solo Avaya Contact Center Select conectado. El servidor Avaya Contact Center Select y el servidor IP Office conectado deben estar ubicados en la misma ubicación del campus.

Para admitir una SCN de IP Office, Avaya Contact Center Select debe conectarse a un servidor primario de IP Office Server Edition en esa red SCN.



Avaya Contact Center Select admite solo las siguientes versiones de IP Office:

- IP Office Server Edition versión 10.1 u 11.0
- Software IP Office 500V2, versión 10.1 u 11.0, modo estándar, licencia de edición avanzada

Avaya Contact Center Select no es compatible con otras versiones de IP Office. Para obtener más información sobre las versiones compatibles de IP Office, consulte las Notas de la versión de Avaya Contact Center Select.

Avaya Contact Center Select no es compatible con el modo básico de IP Office 500V2.

Descripción general de la configuración de la solución

Esta sección proporciona una descripción general de cómo instalar y poner en marcha una solución basada en la plataforma Avaya Contact Center Select e IP Office. Al describir los pasos de puesta en marcha, esta sección también describe cómo Avaya Contact Center Select se integra con IP Office.

Avaya Contact Center Select utiliza la interfaz TAPID de IP Office y los estándares abiertos SIP para integrarse con la plataforma IP Office. Avaya Contact Center Select utiliza la interfaz TAPID de IP Office para monitorear y controlar los terminales de los agentes de la plataforma IP Office. La interfaz TAPID de IP Office brinda a Avaya Contact Center Select CTI control de llamadas de los usuarios y extensiones de IP Office que representan a los agentes de Avaya Contact Center Select. Avaya Contact Center Select utiliza un *Número de extensión de usuario SIP* para registrarse e integrarse con IP Office. Esto brinda a Avaya Contact Center Select la administración de sesiones SIP de las llamadas de voz de IP Office.

Configuración de IP Office para Avaya Contact Center Select

Configure IP Office para admitir la integración con Avaya Contact Center Select. Esta descripción general de la configuración no incluye la configuración básica de IP Office para la configuración del sistema, las licencias o las redes.

Uso del Administrador de IP Office:

1. Configure los detalles de la cuenta de usuario de Avaya Contact Center Select Service. En la pestaña Sistema > Contact Center, configure el *Dirección CCMA*, *Nombre de usuario CCMA*, y *Contraseña CCMA*.

2. Configure el nombre de dominio de voz sobre IP (VoIP) del sistema. El servidor de Avaya Contact Center Select utiliza este nombre de dominio para tratamientos y enrutamiento de contactos.

3. Agregue un usuario con las siguientes especificaciones. Avaya Contact Center Select utiliza este número de extensión de usuario de SIP para registrarse en IP Office:

   una. Tipo de dispositivo establecido en *Todos los demás tipos de teléfonos*.

   b. Tipo de extensión establecido en *Extensión SIP*. Por ejemplo, 6000.

   C. un numérico *Extensión de base* número.

   d. En Usuario, habilite *Llamada en espera activada*.

   mi. En la pestaña Usuario > Telefonía > Configuración de supervisor, configure el *Código de inicio de sesión*.

Página129 de 3226.

4. Configure un código corto de la solución IP Office para asignar un número de teléfono a Avaya Contact Center Select*Número de extensión de usuario SIP*. Por ejemplo, cree un código corto 6000|>>3000. Todas las llamadas de los clientes al número de teléfono 3000 se reenvían al 6000 y se enrutan a Avaya Contact Center Select. Si 3000 está configurado como un CDN (Punto de ruta), Avaya Contact Center Select trata la llamada del cliente y la enruta a un agente del centro de contacto.

5. Agregue una extensión H.323 o SIP para cada agente de Avaya Contact Center Select. Los agentes de Avaya Contact Center Select usan estas extensiones de IP Office para manejar contactos de voz.

Instalación de Avaya Contact Center Select

Durante la implementación, configure Avaya Contact Center Select para conectarse a IP Office. Uso

del Asistente de encendido de Avaya Contact Center Select (utilidad de configuración):

1. Configure los detalles de la plataforma IP Office.
2. Configure los detalles de la cuenta del usuario del servicio.
3. Configure el*Nombre de dominio*para que coincida con el nombre de dominio VoIP de IP Office.
4. Configure un número CDN (Punto de ruta) para que coincida con el*Código*número utilizado por el código corto de IP Office.
5. Configure el*Número de extensión de usuario SIP*para hacer coincidir el usuario de IP Office anterior con una extensión SIP.
6. Configure los detalles del servidor Avaya Contact Center Select, licencias y configuraciones multimedia opcionales.
7. Inicie Avaya Contact Center Select.

Al inicio, Avaya Contact Center Select usa los detalles del Número de extensión de usuario de SIP para registrarse como un dispositivo SIP con IP Office. Este registro permite la siguiente funcionalidad:

- Las llamadas entrantes destinadas a un punto de ruta de Avaya Contact Center Select se envían al servidor de Avaya Contact Center Select.
- Autoriza al servidor de Avaya Contact Center Select a enviar llamadas SIP salientes a IP Office (para el enrutamiento de agentes de llamadas de Avaya Contact Center Select).
- Habilita la funcionalidad específica de Avaya Contact Center Select en la plataforma IP Office.

Continúe con la puesta en servicio de Avaya Contact Center Select agregando funciones opcionales según corresponda. Instale el software Agent Desktop en todos los equipos del agente. Continúe manteniendo Avaya Contact Center Select haciendo copias de seguridad de datos frecuentes.

Para obtener más información sobre la implementación y configuración de Avaya Contact Center Select, incluidos los códigos cortos de IP Office, consulte:

- *DVD de implementación de Avaya Contact Center Select*
- *Implementación del dispositivo de software Avaya Contact Center Select*
- *Implementación del dispositivo de hardware de Avaya Contact Center Select*

Ejemplo de flujo de llamada de voz simple

El siguiente ejemplo muestra cómo Avaya Contact Center Select trata la llamada de un cliente a IP Office y luego la enruta a un agente. Al describir un flujo de llamadas de muestra, esta sección también describe cómo Avaya Contact Center Select se integra con IP Office.

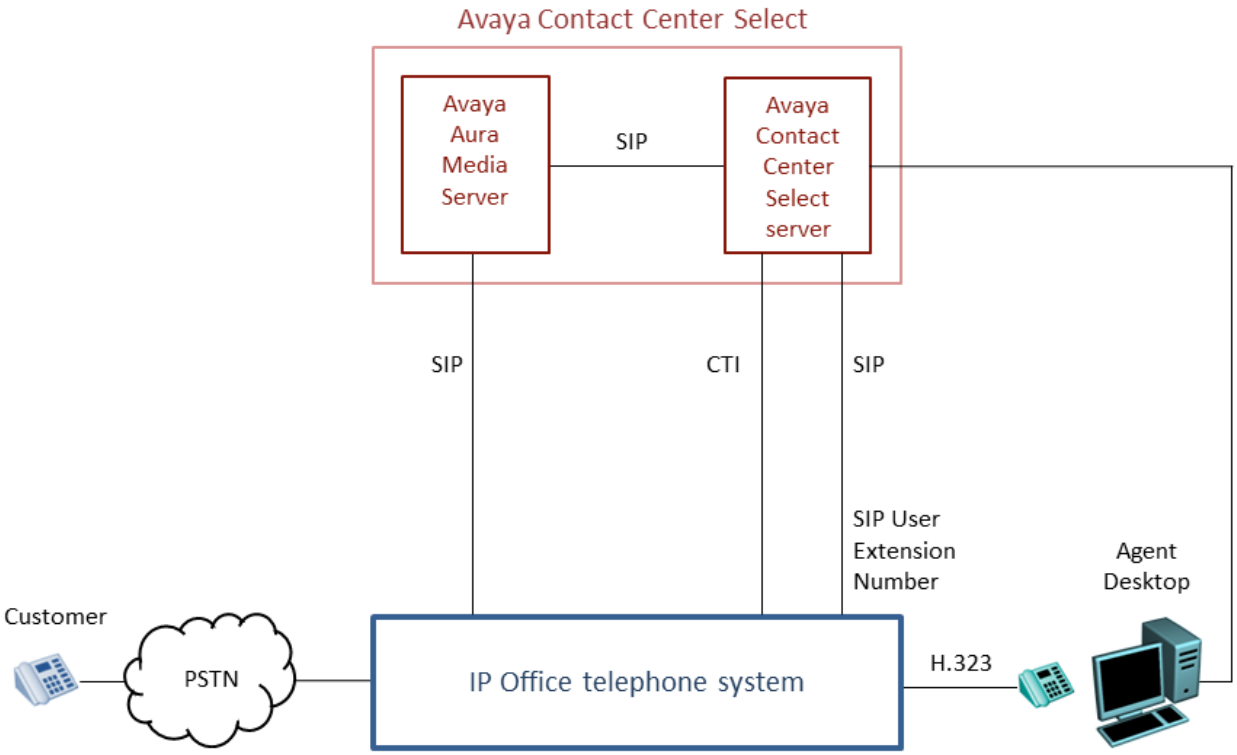


Figura 5: Enlaces de comunicación entre Avaya Contact Center Select e IP Office

1. Un Cliente marca un número y la llamada llega a una plataforma de IP Office. Por ejemplo, el cliente marca 3000.
2. Un código corto de IP Office (por ejemplo, 6000|>>3000) redirige la llamada del cliente a Avaya Contact Center Select.
3. IP Office envía un mensaje SIP INVITE a Avaya Contact Center Select.
4. Cuando el mensaje SIP INVITE llega a Avaya Contact Center Select, hace coincidir la llamada con uno de sus URI de punto de ruta configurados y luego ancla la llamada del cliente en un Avaya Aura®Puerto de conferencia del servidor multimedia.
5. El aura de Avaya®Media Server establece una ruta de voz y medios de Protocolo de transporte en tiempo real (RTP) con el cliente. Avaya Contact Center Select trata la llamada del cliente mediante este puerto de conferencia durante el resto de la duración de la llamada.
6. Cuando Avaya Contact Center Select haya identificado un agente adecuado disponible para manejar esta llamada, envía un mensaje SIP INVITE a IP Office. Cuando el mensaje SIP INVITE llega a IP Office, se envía al teléfono de escritorio H.323 del agente de destino.

Página131 de 3226.

7. IP Office envía una solicitud H.323 al teléfono de escritorio del agente para indicar que ha llegado una nueva llamada de cliente. El teléfono del agente suena e IP Office envía un mensaje de llamada SIP 180 (y un mensaje CTI de oferta de TAPID correspondiente) a Avaya Contact Center Select. Avaya Contact Center Select usa este disparador para informar a Agent Desktop que una llamada está alertando en el teléfono de escritorio. De esta forma, tanto el teléfono de escritorio del agente como el cliente de software Agent Desktop muestran la llamada del cliente como si estuviera sonando.
8. Cuando el agente responde la llamada del cliente mediante el software Agent Desktop, Avaya Contact Center Select envía una solicitud TAPID AnswerCall a IP Office. Esto hace que el teléfono de escritorio del agente se descuelgue y responda la llamada. IP Office envía un mensaje SIP 200 OK (y el correspondiente mensaje TAPID Connected CTI) a Avaya Contact Center Select. Avaya Contact Center Select usa CTI para notificar a Agent Desktop que se respondió la llamada del cliente.
9. Cuando se responde la llamada, se envía el Protocolo de transporte en tiempo real (RTP) desde el teléfono de escritorio del agente a Avaya Aura.®Servidor multimedia. Aura de Avaya®Media Server hace una conferencia entre el agente y el cliente, el cliente y el agente ahora pueden comunicarse. El agente ha respondido a la llamada telefónica del cliente.
10. La llamada permanece activa hasta que el cliente o el agente libera la llamada.

Ejemplos de aplicaciones de flujo de voz de Orchestration Designer

Avaya Contact Center Select proporciona una serie de aplicaciones de flujo de Orchestration Designer de muestra que tratan y enrutan los contactos de voz de los clientes. Las aplicaciones de flujo de Orchestration Designer contienen instrucciones que determinan la secuencia de pasos que sigue un contacto después de que llega a Avaya Contact Center Select. Estos pasos pueden incluir tratamientos de llamadas (como música o devolución de llamada), enrutamiento de llamadas (como enrutamiento basado en habilidades) o interacción con la persona que llama (ingresar números de cuenta).

Las aplicaciones realizan dos funciones principales: definen la ruta que sigue un contacto y brindan tratamientos a un contacto a medida que el contacto se mueve a través de Contact Center. También puede usar las aplicaciones para rastrear y registrar información sobre cada paso en el progreso de un contacto y usar esta información para analizar cómo funciona su centro de contacto para mejorar el servicio. Las aplicaciones de flujo de Orchestration Designer se almacenan en una base de datos de Avaya Contact Center Select. Task Flow Executor, un componente y servicio de Avaya Contact Center Select, ejecuta las aplicaciones de flujo para tratar los contactos de los clientes. Un contacto no siempre es respondido inmediatamente por un agente. Puede proporcionar tratamientos a los contactos de voz mientras esperan en una cola. Estos tratamientos pueden decirle a las personas que llaman la cantidad estimada de tiempo antes de que se responda su llamada, o reproduzca música para las personas que llaman mientras esperan en la cola. Además, puede usar la hora del día, el día de la semana o la actividad del centro de contacto para determinar cómo se maneja un contacto.

Avaya Contact Center Select proporciona una serie de aplicaciones de flujo de diseñador de orquestación de voz de muestra:

- Servicio al Cliente. Esta es la aplicación principal. Da la bienvenida al cliente al centro de contacto, realiza algunas comprobaciones básicas de límites y reproduce un menú que ofrece al cliente una

pequeña selección de opciones (hablar con la mesa de ayuda, hablar con soporte, ingresar su PIN o dejar un mensaje).

- Voice_Skill1. Esta aplicación reenvía las llamadas de los clientes al conjunto de habilidades de voz Skill1.
- Voice_Skill2. Esta aplicación reenvía las llamadas de los clientes al conjunto de habilidades de voz Skill2.
- Recopilar_Dígitos. Esta aplicación le pide al cliente que ingrese su número PIN utilizando los dígitos de su teléfono. Luego, la aplicación reproduce el número para el cliente y le pide que confirme el número PIN.

Avaya Contact Center Select también proporciona una cantidad de aplicaciones de flujo de diseñador de orquestación multimedia de muestra para los tipos de contactos multimedia admitidos.

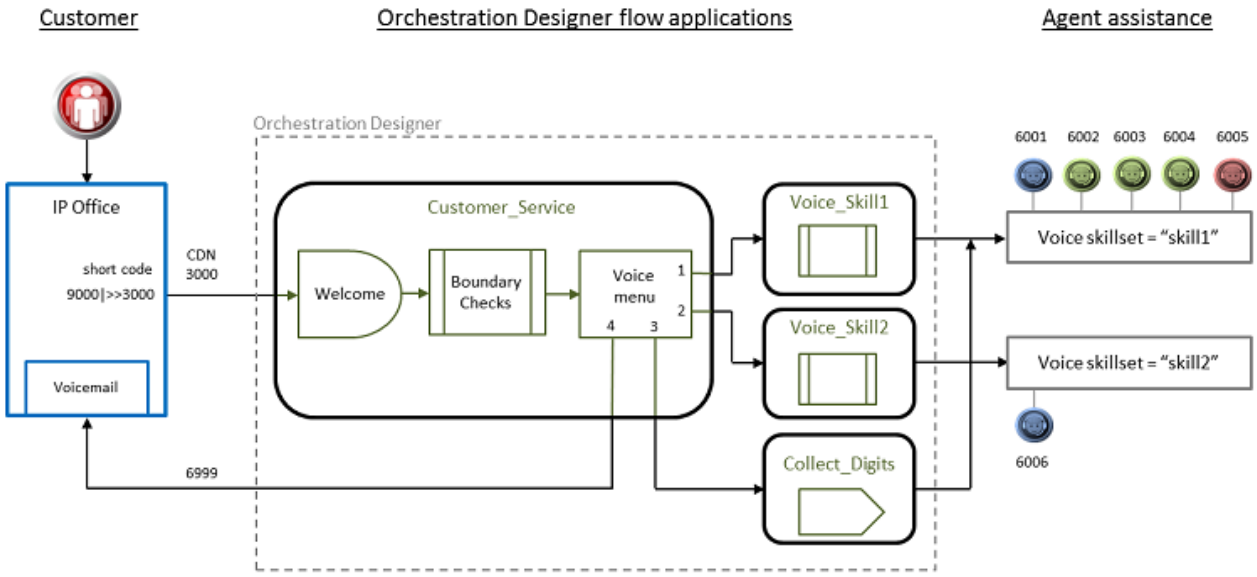


Figura 6: Tratamiento y enrutamiento de los contactos de voz del cliente a Avaya Contact Center Select por las aplicaciones de flujo de muestra de Orchestration Designer

Ejemplo de variables de indicaciones de voz

La siguiente tabla muestra los archivos multimedia de audio utilizados por las aplicaciones de flujo de muestra de Orchestration Designer. Orchestration Designer utiliza estos archivos de audio .WAV para reproducir mensajes (indicaciones) para el cliente. La tabla muestra qué aplicación de flujo de Orchestration Designer utiliza cada archivo multimedia. La tabla también proporciona una transcripción del audio en cada archivo multimedia.

Nombre rápido	Solicitar nombre de variable en Orquestación Diseñador	Transcripción rápida	Diseñador de orquestación flujo usando este mensaje
Bienvenido_CS	Bienvenido_CS	"Bienvenido al Centro de contacto".	Servicio al Cliente

La tabla continúa...

Página133 de 3226.

Nombre rápido	Solicitar nombre de variable en Orquestación Diseñador	Transcripción rápida	Diseñador de orquestación flujo usando este mensaje
Menu_Selection_CS	Menu_Selection_CS	• “Presione 1 para hablar con un agente en la mesa de ayuda. • Presione 2 para hablar con un agente en el centro de soporte. • Presione 3 para ingresar su número PIN o cualquier 8 dígitos de su eligiendo • Presione 4 para dejar un mensaje de voz. • Presione * para repetir este menú.”	Servicio al Cliente
Correo de voz_CS	Correo de voz_CS	“Espere mientras lo dirigimos a nuestro sistema de mensajes de voz buzón."	Servicio al Cliente
IntroduzcaDigits_CD	IntroduzcaDigits_CD	"Ingrese su número PIN o dígitos hasta un máximo de 8 dígitos seguidos de la tecla #".	Collect_Digits
Confirmar dígitos_CD	Confirmar dígitos_CD	"Los dígitos que ingresó fueron..."	Collect_Digits
ValidateDigits_CD	ValidateDigits_CD	"Si eso es correcto, presione 1 seguido de la tecla # o presione 2 si desea volver a intentarlo seguido de la tecla #".	Collect_Digits
Entrada no válida_CS	Entrada no válida_CS	"Esa es una entrada inválida, por favor inténtalo de nuevo".	Servicio al Cliente
NoData_Entry_CS	NoData_Entry_CS	"No ha ingresado ningún dato. Vuelva a intentarlo".	Servicio al Cliente
Emergencia_CS	Emergencia_CS	“El centro de contacto ahora está en modo de emergencia y cerrado. Lo haremos reabrir en breve.”	Servicio al Cliente
Fuera de horario_CS	Fuera de horario_CS	"El centro de contacto ahora está cerrado porque está fuera de horario".	Servicio al Cliente

La tabla continúa...

Nombre rápido	Solicitar nombre de variable en Orquestación Diseñador	Transcripción rápida	Diseñador de orquestación flujo usando este mensaje
Vacaciones_CS	Vacaciones_CS	"El centro de contacto ahora está cerrado por vacaciones".	Servicio al Cliente
Fuera de servicio_CS	Fuera de servicio_CS	"Todos los departamentos están fuera de servicio en este momento. Vuelva a llamar más tarde".	Servicio al Cliente
PromptSubmenu_CS	PromptSubmenu_CS	"Presione 0 para hablar con un agente, presione 1 para dejar un mensaje de voz, presione, presione 9 para volver al menú principal".	Servicio al Cliente - submenú 1 y 2
PrimeroRAN_CD	PrimeroRAN_CD	"Este es el primer anuncio. Por favor espere mientras tratamos de conectarlo con nuestros agentes".	Collect_Digits – Pestaña de colas
SegundoRAN_CD	SegundoRAN_CD	"Este es el segundo anuncio. Todo nuestro los agentes aún están ocupados, por favor espere".	Collect_Digits – Pestaña Iterar cola

Puede usar la administración del administrador del centro de contacto (CCMA)*Gestión rápida*para reemplazar estos archivos multimedia con sus propias grabaciones. Puede grabar sus propias indicaciones de voz para el cliente o grabar indicaciones de voz adecuadas para su región (idioma y dialecto). Avaya Contact Center Select proporciona un rendimiento de reproducción óptimo con archivos .WAV codificados como PCM lineal de 16 bits, mono de 8 KHz con una tasa de bits de 128 kbits/seg.

Procesamiento de contactos multimedia

Contact Center recibe contactos multimedia a través de dos puntos de interfaz externos: el servidor de correo electrónico y el servidor web externo.

Contactos del servidor de correo electrónico

Los contactos del servidor de correo electrónico se recuperan de un servidor de correo electrónico compatible con POP3 o IMAP mediante el controlador de mensajes entrantes (IMH). El IMH funciona a intervalos regulares. Puede configurar los ajustes para el IMH (como el tiempo entre intervalos y la cantidad de correos electrónicos recuperados de cada buzón durante cada ejecución) usando Contact Center Manager Administration.

El IMH inicia sesión en los buzones de correo del servidor de correo electrónico que se enumeran en el Administrador de correo electrónico. Analiza el correo electrónico en los buzones y los almacena en la base de datos de Contact Center Multimedia. Todos los archivos adjuntos asociados con un correo electrónico se almacenan en la carpeta de archivos adjuntos entrantes, como se especifica en Contact Center Manager Administration. Una vez que un correo electrónico se almacena correctamente en la base de datos de Contact Center Multimedia, se elimina del servidor de correo electrónico.

Traducido del inglés al español - www.onlinedoctranslator.com

El IMH pasa un correo electrónico recibido al motor de reglas de Contact Center Multimedia, que aplica reglas relevantes para el correo electrónico en función de la dirección Para e invoca el controlador de mensajes salientes (OMH) para enviar respuestas automáticas, si corresponde.

Contact Center versión 7.0 no es compatible con Microsoft Exchange Server 2003.

Contact Center versión 7.0 solo es compatible con las siguientes versiones de Microsoft Exchange Server:

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013

Transacciones del servidor web externo

Contact Center Multimedia recibe contactos del servidor web externo a través de los servicios web de Contact Center Multimedia. Los servicios web proporcionan una API de Java. Esto permite que los contactos se escriban en la base de datos de Contact Center Multimedia, se recuperen de la base de datos y se consulte su estado.

Los contactos recibidos a través de los servicios web no pasan por el motor de reglas. El servidor web externo determina el conjunto de habilidades y la prioridad asignada al contacto.

Se distribuye un conjunto de páginas de muestra a través de DevConnect para proporcionar ejemplos de cómo un servidor web puede acceder a los servicios web. Debe crear sus propias páginas web, con una apariencia y una lógica empresarial personalizadas.

Flujo de mensajes de correo electrónico simple

Avaya Contact Center Select proporciona soporte de contacto enrutado para mensajes de correo electrónico. Los clientes envían mensajes de correo electrónico solicitando información o soporte a una dirección de correo electrónico publicada. Avaya Contact Center Select se conecta al servidor de correo electrónico de alojamiento y analiza este buzón (dirección de correo electrónico publicada) a intervalos regulares. Avaya Contact Center Select recupera los mensajes de correo electrónico del cliente del servidor de correo electrónico, los procesa (por palabras clave) y los almacena en la base de datos. Luego, Avaya Contact Center Select genera un contacto multimedia (correo electrónico) para cada correo electrónico almacenado en la base de datos y lo enruta a un agente apropiado y disponible.

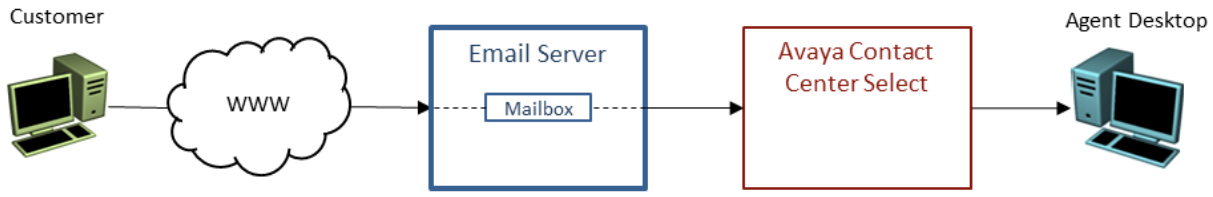


Figura 7: Proceso de Avaya Contact Center Select utilizado para recuperar mensajes de correo electrónico de clientes y enrutar los mensajes como contactos multimedia a los agentes del centro de contacto

Página136 de 3226.

Cuando instala Avaya Contact Center Select, configura el servidor de correo electrónico y un buzón de destinatario predeterminado. La configuración predeterminada garantiza que los mensajes de correo electrónico lleguen solo a un agente con la capacidad de manejar mensajes de correo electrónico. Puede personalizar su centro de contacto con conjuntos de habilidades adicionales, grupos de reglas y servidores de correo electrónico.

Para mejorar aún más su servicio al cliente, puede configurar reglas de enrutamiento para usar en grupos de reglas. Utilice grupos de palabras clave y grupos de remitentes para decidir cómo enrutar los contactos. Configure a qué perfil y prioridad se asigna el contacto de correo electrónico, en función de la entrada para el enrutamiento de contactos. Use sugerencias automáticas para que el agente responda rápidamente a un correo electrónico o respuestas automáticas para enviar una respuesta al cliente sin la interacción del agente. Puede cerrar el contacto inmediatamente después de la respuesta automática.

Avaya Contact Center Select admite interfaces abiertas de correo electrónico. Puede desarrollar un servicio web personalizado al que Avaya Contact Center Select Email Manager pueda llamar cuando se procesa un mensaje de correo electrónico. El servicio web personalizado puede realizar tareas personalizadas, como manipular el correo electrónico de origen y modificar las opciones de enrutamiento de reglas.

Para obtener más información sobre la configuración de los contactos de correo electrónico de Avaya Contact Center Select y la mejora de la experiencia del cliente, consulte*Administración avanzada de Avaya Contact Center Select*.

Grabacion de llamada

Avaya Contact Center Select es compatible con la grabación de llamadas de IP Office. La grabación de llamadas de IP Office proporciona grabación de tipo reglamentario, incluida la opción de pausar la grabación automática para el cumplimiento de la seguridad de la industria de tarjetas de pago (PCI). Avaya Contact Center Select admite la función de pausa y reanudación de la grabación de llamadas cuando se inicia desde un teléfono físico. De manera predeterminada, los agentes de Avaya Contact Center Select tienen habilitada la grabación de llamadas entrantes y salientes.

La grabación de llamadas de IP Office tiene dos componentes principales:

- La biblioteca de grabación de voz (VRL) de Voicemail Pro registra las llamadas entrantes y salientes del agente.
- IP Office Contact Recorder almacena las llamadas grabadas y los metadatos asociados.

Las llamadas grabadas se almacenan en archivos .WAV estándar de la industria. Cuando se completa cada llamada, Contact Recorder comprime el archivo de audio .wav y actualiza la base de datos con un registro de la llamada. Estos archivos se almacenan en una jerarquía de carpetas en el servidor de IP Office. Cada grabación da como resultado un archivo .wav y los metadatos asociados se almacenan en un archivo XML:

- Cada archivo .wav contiene el audio real de la grabación. Utilice la aplicación Contact Recorder Search and Replay para localizar y reproducir estas grabaciones.
- Cada archivo .xml contiene metadatos sobre el archivo de grabación .wav asociado. Los siguientes son algunos ejemplos de parámetros de metadatos de grabación de llamadas:

  - CLI original (P-Asserted-Identity)

  - Nombre del agente

  - Conjunto de habilidades

Página137 de 3226.

- Número de agente
- fiestas de conferencias
- hora de inicio de la llamada grabada
- hora de finalización de la llamada grabada

La grabación de llamadas de IP Office es una función con licencia. Las grabaciones consumen licencias de canal de Voicemail Pro.

Pausar la grabación cuando está en espera: si se está grabando una llamada de Avaya Contact Center Select y el agente pone la llamada en espera, IP Office Call Recording pone la grabación en un estado suspendido (no terminado), agrega un pitido breve a la grabación y cuando se recupera la llamada de espera se reanuda la grabación. Toda esta llamada se almacena en un solo archivo .wav.

Usuario Pausar grabación: si se está grabando una llamada de Avaya Contact Center Select y si el agente necesita recopilar los detalles de la tarjeta de pago de un cliente, el agente puede pausar la grabación para cumplir con los requisitos de la industria de tarjetas de pago (PCI). La grabación de llamadas de IP Office pone la grabación en un estado suspendido (no terminado) y agrega un pitido breve a la grabación. Después de recopilar los detalles de la tarjeta de pago, el agente reanuda la grabación de llamadas. Toda esta llamada se graba y almacena en un solo archivo .wav.

La interfaz de usuario de Agent Desktop no tiene un botón de pausa. Los agentes y los supervisores de agentes deben usar su teléfono físico para pausar y reanudar la grabación de contactos de voz.

Agentes Remotos

Avaya Contact Center Select (ACCS) admite agentes remotos. Esta función permite a los agentes en ubicaciones remotas usar un teléfono y el software Agent Desktop para manejar los contactos de voz del cliente enrutados desde ACCS.

ACCS admite los siguientes tipos de agentes remotos:

- Agentes remotos que utilizan un enrutador VPN de Avaya compatible con IPsec y un teléfono IP de escritorio de Avaya. El enrutador de Red Privada Virtual (VPN) compatible con Seguridad de Protocolo de Internet (IPsec) extiende la red ACCS a través de una red pública como Internet, brindando a los agentes remotos acceso seguro a la solución del centro de contacto. En este tipo de solución, el agente tiene una computadora, un teléfono de escritorio IP de Avaya y un enrutador VPN de Avaya en su hogar o en su lugar de trabajo remoto. El teléfono de escritorio IP de Avaya y la computadora Agent Desktop del agente se conectan al enrutador VPN de Avaya. El enrutador VPN se conecta a ACCS a través de Internet. El agente utiliza su teléfono de escritorio IP de Avaya y el software Agent Desktop para gestionar los contactos multimedia y de voz del cliente.

- Agentes remotos que utilizan un enrutador VPN de Avaya compatible con IPsec y un softphone de IP Office de Avaya. El enrutador de Red Privada Virtual (VPN) compatible con Seguridad de Protocolo de Internet (IPsec) extiende la red ACCS a través de una red pública como Internet, brindando a los agentes remotos acceso seguro a la solución del centro de contacto. En este tipo de solución, el agente tiene una computadora y un Avaya VPN Router en su hogar o en la ubicación de su lugar de trabajo remoto. La computadora Agent Desktop del agente y el softphone de IP Office se conectan a Avaya

Enrutador VPN. El enrutador VPN se conecta a ACCS a través de Internet. El agente utiliza el software Agent Desktop y el softphone de IP Office para manejar los contactos multimedia y de voz del cliente. ACCS Remote Agent es compatible con IP Office Avaya Communicator para Windows.

- Agentes remotos que utilizan sus teléfonos de terceros existentes. En este tipo de solución, el agente tiene un teléfono analógico residencial estándar y una computadora en su hogar o en su lugar de trabajo remoto. El teléfono del agente se conecta a ACCS mediante la red telefónica pública conmutada (PSTN) y el software Agent Desktop se conecta a ACCS mediante Internet. Este tipo de Remote Agent utiliza el modo de operación Telecommuter. El agente utiliza un teléfono analógico estándar y el software Agent Desktop para manejar los contactos multimedia y de voz del cliente.

Para habilitar el modo Teletrabajador de Remote Agent:

1. Habilite el*Agente externo*característica en*Configuración del servidor-Licencia*
2. Para cada agente remoto, habilite*Agente externo permitido*para cada agente remoto en CCMA.
3. Luego, los agentes pueden usar Agent Desktop para iniciar sesión desde casa o desde otra ubicación remota. Los agentes inician sesión con uno de sus números de teléfono remotos configurados.

Para usar Remote Agent, los agentes de ACCS deben tener una computadora portátil o de escritorio adecuada en su hogar o en su lugar de trabajo remoto. Los agentes instalan el software Agent Desktop en este equipo. Los agentes deben tener una conexión a Internet rápida y confiable a la solución del centro de contacto. Para más información, ver*Administrador de IP Office de Avaya*.

Los agentes remotos inician sesión en Agent Desktop mediante el*Otro teléfono*modo. Cuando inician sesión, suena el teléfono del agente. Esta es una llamada urgente. Los agentes deben responder esta llamada en su teléfono para completar el inicio de sesión en Agent Desktop. Una vez que se completa el inicio de sesión, el teléfono del agente se conecta y los agentes deben usar Agent Desktop para todas las operaciones de telefonía posteriores. Cuando el agente cierra la sesión de ACCS mediante el botón Cerrar sesión en Agent Desktop, ACCS desconecta la llamada fija. Los tipos de contactos multimedia aparecen para un agente remoto exactamente de la misma manera que lo hacen para un agente en el sitio.

Soporte para grupos de trabajo y dominios de Avaya Contact Center Select

El servidor de Avaya Contact Center Select se admite en un grupo de trabajo o en un dominio de Windows.

Después de implementar el dispositivo de hardware o el dispositivo de software de Avaya Contact Center Select, puede agregar el servidor de Avaya Contact Center Select a un dominio de Windows.

Puede agregar el servidor de Avaya Contact Center Select a un dominio de Windows antes o después de instalar el software de Avaya Contact Center Select mediante el DVD de Avaya Contact Center Select.

En una solución habilitada para la continuidad empresarial de Avaya Contact Center Select, los servidores de Avaya Contact Center Select deben estar en el mismo dominio de Windows. Para respaldar la resiliencia de Business Continuity, los agentes de Avaya Contact Center Select deben tener cada uno una cuenta de usuario de dominio de Windows asociada en el mismo dominio de Windows que los servidores activo y en espera. Los agentes de Avaya Contact Center Select también se admiten en dominios con una relación de confianza bidireccional con

Página139 de 3226.

el dominio del servidor de Avaya Contact Center Select. Avaya Contact Center Select Business Continuity no se admite en un grupo de trabajo.

Consideraciones sobre el dominio de Avaya Contact Center Select

Avaya Contact Center Select solo admite un dominio de Windows Server Active Directory. Avaya Contact Center Select admite una implementación de un solo bosque. Avaya Contact Center Select admite la integración de agentes solo dentro de aquellos dominios en el mismo bosque que el dominio de Avaya Contact Center Select. Avaya Contact Center Select no admite la integración de agentes en varios bosques o en dominios fuera del bosque de Avaya Contact Center Select.

Todos los servidores de Avaya Contact Center Select deben estar en el mismo dominio de Windows Active Directory. Todos los servidores de Avaya Contact Center Select deben estar registrados con el mismo controlador de dominio de Active Directory de Windows. Todos los clientes de Agent Desktop deben estar registrados en este dominio o en dominios con una relación de confianza bidireccional con este dominio de servidor de Avaya Contact Center Select.

La política de firewall de Avaya Contact Center Select define los servicios, los puertos de red y las cuentas de Windows necesarios para la funcionalidad multimedia y de voz del centro de contacto. Avaya Contact Center Select no proporciona ni instala una política de grupo. Una política de grupo administra y configura aplicaciones de software y configuraciones de usuario en un entorno determinado. Avaya Contact Center Select no se puede personalizar para adaptarse a estructuras de dominios corporativos individuales o políticas de grupo, por lo que los dominios corporativos deben cumplir con los requisitos de Avaya Contact Center Select.

Si planea aplicar una política de grupo corporativa o personalizada a los servidores y la solución de Avaya Contact Center Select (ACCS), primero debe realizar lo siguiente:

- Comprender los servicios, puertos y requisitos de cuentas de usuario de ACCS según lo especificado por el cortafuegos de ACCS. Para obtener más información, consulte Firewall de Microsoft Windows y seguridad avanzada en su servidor ACCS para ver las reglas de entrada/salida.
- Comprender los puertos de la red ACCS y los tipos de transporte. Para más información, verMatriz de puertos de Avaya Contact Center Select en la página 189.
- Diseñe o modifique su política de grupo para adaptarse a estos servicios ACCS, puertos, cuentas de usuario y requisitos de tipo de transporte existentes.
- Las políticas de grupo de dominio y las políticas de seguridad se pueden configurar para automatizar las actualizaciones de MS Windows, las copias de seguridad del servidor y las reglas de caducidad de la contraseña para los usuarios locales. Estas funciones automatizadas no son compatibles con ACCS. Si sus políticas de grupo o políticas de seguridad implementan estas funciones automatizadas, coloque los servidores ACCS en un contenedor de unidad organizativa (OU) de Active Directory que proteja a los servidores de estas funciones automatizadas.
- Durante la puesta en marcha de Avaya Contact Center Select o durante una ventana de mantenimiento, aplique y pruebe su política de grupo. Garantizar que se conserven las capacidades de control, administración y mantenimiento de llamadas de Avaya Contact Center Select. No aplique una política de grupo no probada a un entorno de producción de Avaya Contact Center Select. Si es necesario, modifique su política de grupo para conservar la funcionalidad de Avaya Contact Center Select.
- Después de una prueba exitosa, vuelva a poner ACCS en producción y continúe monitoreando el centro de contacto para detectar efectos secundarios adversos de su póliza de grupo.

Para obtener más información sobre la política de firewall de Avaya Contact Center Select y la compatibilidad con las políticas de grupos de dominios corporativos, consulte*Avaya Aura Contact Center Seguridad*.

Los servidores de Avaya Contact Center Select no admiten el Protocolo de configuración dinámica de host (DHCP). Todos los servidores Avaya Contact Center Select deben tener una dirección IP estática. Los equipos cliente de Agent Desktop admiten direcciones IP estáticas y DHCP.

Página140 de 3226.

Avisos de seguridad de Avaya

Los avisos de seguridad de Avaya se publican en el sitio web de soporte de seguridad de Avaya en https://support.avaya.com/security . Desde el sitio web de soporte de Avaya, puede registrarse para recibir notificaciones por correo electrónico de los avisos de seguridad de Avaya.

La cantidad de tiempo que lleva recibir un aviso de seguridad de Avaya varía según la clasificación de vulnerabilidad del aviso. Para obtener más información sobre clasificaciones de vulnerabilidades, respuestas y políticas de mantenimiento, consulte los siguientes documentos:

- *Política de respuesta a vulnerabilidades de seguridad de productos de Avaya*
- *Clasificación de vulnerabilidades de seguridad de Avaya*
- *Requisitos del contrato de mantenimiento de Avaya para soporte de productos*
- *Flujo de soporte de seguridad de productos de Avaya*

Continuidad comercial de Avaya Contact Center Select

Business Continuity es una función con licencia de Avaya Contact Center Select (ACCS). Las soluciones ACCS que admiten Business Continuity tienen dos servidores ACCS. Un servidor, denominado servidor activo, procesa los contactos de los clientes. El otro servidor ACCS (nodo geográfico en espera o remoto) hace sombra al servidor activo. Si el servidor activo falla, el otro servidor ACCS puede hacerse cargo del procesamiento de contactos. Por lo tanto, esta función proporciona redundancia ACCS, resiliencia de datos y recuperación ante desastres.

Para obtener más información sobre Avaya Contact Center Select Business Continuity, consulte *Continuidad comercial de Avaya Contact Center Select*.

Actualizaciones y migraciones

Avaya Contact Center Select Release 7.0 solo es compatible con el sistema operativo Microsoft Windows Server 2012 Release 2. El servidor y el sistema operativo Microsoft Windows Server 2012 R2 deben cumplir los requisitos especificados en *Descripción de la solución Avaya Contact Center Select*. Avaya Contact Center Select solo es compatible con las ediciones Microsoft Windows Server 2012 R2 Standard o Data Center.

Avaya Contact Center Select versión 6.4.2 solo es compatible con el sistema operativo Microsoft Windows Server 2008 R2. No puede actualizar directamente desde Avaya Contact Center Select versión 6.4.2 en Windows Server 2008 R2 a Avaya Contact Center Select versión 7.0 en Windows Server 2012 R2. Puede migrar información estadística y de agentes desde su solución Avaya Contact Center Select versión 6.x existente a Avaya Contact Center Select versión 7.0 en un servidor Windows Server 2012 R2.

Puede aplicar los parches más recientes de Avaya Contact Center Select para asegurarse de tener la versión más reciente del software de la aplicación para resolver problemas de software.

Puede aplicar parches a una solución Avaya Contact Center Select Business Continuity. Ambos servidores de Avaya Contact Center Select deben actualizarse al mismo nivel de parche. La actualización de una solución de continuidad comercial de Avaya Contact Center Select requiere una cuidadosa planificación inicial.

Para instalar un paquete de funciones o Service Pack de Avaya Contact Center Select, o para migrar un servidor de Avaya Contact Center Select, debe programar un ciclo de mantenimiento y reiniciar el centro de contactos. Para obtener más información, lea el archivo Léame de Feature Pack o Service Pack.

Migración de Avaya Contact Center Select a Avaya Aura®El centro de contacto no es compatible.

Se admite la migración de Avaya NES Contact Center a Avaya Contact Center Select.

Migración desde Avaya Aura®Se admite la solución basada en Contact Center AML para Avaya Contact Center Select.

La siguiente tabla resume las migraciones admitidas a Avaya Contact Center Select versión 7.0.

Existente	Nuevo
Avaya Contact Center Select versión 7.0 en Microsoft Windows Server 2012 versión 2	Avaya Contact Center Select versión 7.0 Feature Pack 3 en Microsoft Windows Server 2012 versión 2
Avaya Contact Center Select versión 6.4.2 en Microsoft Windows Server 2008 R2	
Aura de Avaya®Soluciones basadas en AML para centros de contacto	

Fuente de información de la desconexión de la llamada

Avaya Contact Center Select (ACCS) registra qué parte en una llamada del centro de contactos es la primera en desconectarse de la llamada. En una llamada típica del centro de contacto, la persona que desconecta o cuelga primero es la fuente de desconexión de la llamada (SOCD). ACCS admite el monitoreo y la generación de informes de SOCD para los contactos entrantes del centro de contacto. En algunos países, el agente no debe colgar a una persona que llama del centro de contacto. Por ejemplo, el Decreto Presidencial brasileño 6.523 exige que un agente no desconecte la llamada mientras habla con una persona que llamó al centro de contacto. Por lo tanto, ACCS registra la fuente de desconexión de la llamada (SOCD).

La información SOCD aparece en la*Datos asociados*en los informes Llamada por llamada y Resumen de contacto. La función SOCD proporciona la siguiente información sobre los contactos del centro de contactos enrutados:

- Parte llamada: identifica que el agente desconectó la llamada
- Parte que llama: identifica que la persona que llama desconectó la llamada
- Transferencia: identifica que un agente transfirió la llamada y completó la transferencia
- Participante de la conferencia: identifica que la persona que llama o un agente abandonó una llamada que el agente inicial realizó en conferencia

Página142 de 3226.

- Interrupción de la conferencia: identifica que la persona que llama o el último agente interrumpió una llamada que un agente realizó en conferencia
- Sistema: identifica que un evento generado por el sistema liberó la llamada
- Si un cliente abandona la llamada, la 'Fuente de desconexión' es DESCONOCIDA pero se completa una 'Disposición final' de abandono.

Las siguientes son algunas limitaciones de los informes SOCD:

- Para llamadas directas (que no sean del centro de contacto) hacia o desde agentes registrados, SOCD se muestra como Desconocido para todos estos tipos de llamadas.
- SOCD se registra solo para agentes ACCS registrados. SOCD no se registra si el agente ACCS no está conectado.
- Si el agente que recibió originalmente la llamada inicia una conferencia con otro agente y luego abandona la conferencia, todos los mensajes de información SOCD subsiguientes son Desconexión de conferencia. En este caso, los informes no pueden mostrar con precisión qué parte abandonó la llamada.

Reenviar automáticamente el correo de voz de IP Office a los agentes multimedia

En una solución Avaya Contact Center Select (ACCS) con licencia y configurada para admitir agentes multimedia, puede configurar IP Office y Voicemail Pro para reenviar automáticamente los mensajes de correo de voz a los agentes ACCS.

ACCS proporciona de muestra *Servicio al Cliente* menú con algunas opciones básicas. Este menú de muestra permite que la persona que llama deje un mensaje de correo de voz seleccionando la opción de correo de voz de la *Servicio al Cliente* menú. Luego, la persona que llama se enruta a un número de IP Office preconfigurado desde donde puede dejar un mensaje de correo de voz. Este número de correo de voz preconfigurado es el *Número de buzón de devolución de llamada* opción en el asistente de encendido ACCS. Los agentes pueden usar su teléfono y el sistema de correo de voz de IP Office para escuchar el mensaje de correo de voz de la persona que llama.

El administrador de IP Office puede configurar el número de buzón de devolución de llamadas de IP Office y Voicemail Pro para reenviar automáticamente el mensaje de correo de voz, como un mensaje de correo electrónico con un archivo .WAV adjunto, a una dirección de correo electrónico supervisada por ACCS. ACCS puede entonces tratar el contacto de correo electrónico y presentarlo a un agente multimedia disponible. El agente puede usar los auriculares de su computadora para escuchar el mensaje de correo de voz de la persona que llama en el archivo .WAV. Los agentes de ACCS no pueden escuchar archivos adjuntos .WAV con sus teléfonos IP Office.

Para obtener más información sobre el reenvío de mensajes de correo de voz a una dirección de correo electrónico, consulte la documentación de IP Office y Voicemail Pro.

Limitaciones

Las siguientes son algunas de las limitaciones de las soluciones Avaya Contact Center Select (ACCS):

- ACCS se registra en IP Office como usuario SIP. ACCS debe actualizar este registro activo repetidamente cada 180 segundos para evitar que caduque. Si ACCS no puede actualizar el registro, IP Office comienza a finalizar todas las llamadas ACCS activas.
  - En el caso de una interrupción del servicio ACCS o de la red de menos de 180 segundos, el registro SIP con IP Office podría caducar y las llamadas ACCS activas podrían comenzar a finalizar.
  - En el caso de una interrupción del servicio ACCS o de la red de más de 180 segundos, el registro de SIP con IP Office caduca y IP Office comienza a finalizar todas las llamadas ACCS activas.
- Si un agente ACCS forma parte directamente de una llamada de conferencia de IP Office y el agente invoca la espera en esta llamada, IP Office no transmite la música en espera incluso si la cantidad de participantes en esta conferencia se reduce a dos. Los agentes pueden identificar si son parte de este escenario revisando la pantalla de su teléfono para buscar la palabra clave 'Conferencia'.
- Agent Desktop siempre utiliza apariencia de 3 líneas con apariencia de reserva de última llamada, independientemente de la configuración de IP Office en el teléfono del agente. Cuando un agente inicia sesión con Agent Desktop, la configuración del teléfono de Agent Desktop anula la configuración del teléfono de IP Office.
- Para escenarios de conferencia de CDN a CDN, unión, irrupción o llamada de emergencia, si un agente de softphone de IP Office es una de las partes en esta llamada de conferencia multipartita e invoca la espera, la música en espera puede reproducirse en la multiconferencia activa. -Transmisión de audio de fiesta durante un período corto de aproximadamente 500 milisegundos antes de finalizar.
- Si un cliente llama a un agente y este primer agente inicia una consulta con un segundo agente, el teléfono del segundo agente muestra el número de teléfono del cliente mientras suena la llamada de consulta. Después de que el segundo agente responda la llamada de consulta, su teléfono muestra el número de teléfono del primer agente. Así es como IP Office procesa las consultas.
- Intrusión de llamadas: la función de intrusión de llamadas de IP Office permite que un agente se una o se infiltre en la llamada de otro agente. ACCS implementa Call Intrude como una conferencia de unión. La llamada del agente intruso se pone brevemente en espera para permitir que se complete la conferencia. La parte intrusa puede notar el cambio de estado En espera y consultar el segmento de la llamada que aparece brevemente a medida que se completa la operación. Es posible que la música de espera se reproduzca brevemente en la llamada de grupo intruso.
- Transferencia manual desde el softphone: Una transferencia completada manualmente en el softphone de IP Office aparece en Agent Desktop como una transferencia Unirse donde se lleva a cabo una unión en las llamadas principales y de consulta con la parte que realiza la transferencia y luego se desconecta de la llamada.
- IP Office admite integraciones de terceros mediante la interfaz TAPI de IP Office. Estas integraciones de terceros pueden interferir potencialmente con el funcionamiento de Avaya Contact Center Select. Debe configurar, implementar y monitorear integraciones de terceros para evitar interferir con Selección del centro de contacto de Avaya. Las aplicaciones de terceros que implementan la interfaz TAPID de IP Office no son compatibles con el control de dispositivos Agent.

- No todas las funciones invocadas en el teléfono físico se reflejan en Agent Desktop. Los siguientes escenarios son algunos ejemplos de esto:
  - Localización: los agentes que reciben una llamada de localización entrante no pueden responder a esta llamada mediante Agent Desktop. Una llamada de Page solo se puede responder en el teléfono del usuario. Una llamada de Anuncio que está alertando en el teléfono de un usuario se muestra en Agent Desktop como una llamada conectada. Agent Desktop muestra esta llamada como conectada si el usuario responde a la página. Agent Desktop abandona esta llamada de página si otro usuario responde a la página.
  - Recordatorio en espera: si una llamada permanece en estado En espera durante más tiempo que el ajuste de configuración de Tiempo de espera en espera para todo el sistema de IP Office, se muestra una notificación de Recordatorio en espera en el teléfono del usuario. Una notificación de recordatorio de espera puede ser una notificación de audio o visual. Agent Desktop no admite notificaciones de recordatorio de espera; en Agent Desktop, la llamada permanece en estado En espera. Los agentes pueden usar Agent Desktop para recuperar la llamada retenida.
- Cuando un agente de ACCS inicia sesión en un softphone de IP Office, hay un breve retraso antes de que el agente pueda usar el software Agent Desktop para controlar ese softphone. Este breve retraso puede durar hasta 12 segundos. Los agentes que utilizan un softphone de IP Office no pueden responder llamadas entrantes en Agent Desktop inmediatamente después de conectar el softphone a IP Office. Sin embargo, los agentes pueden contestar estas llamadas en su softphone. Esta limitación se aplica solo a las llamadas enrutadas al usuario en el período inmediato después de iniciar sesión en su softphone. Si un agente intenta responder una llamada en Agent Desktop durante el breve período de tiempo en el que la respuesta no está disponible, se muestra un mensaje de error en Agent Desktop. Después de que la función de respuesta esté disponible, todos los intentos posteriores de responder una llamada en Agent Desktop serán exitosos.
- Cuando un agente realiza una llamada saliente mediante Agent Desktop, el botón Espera de Agent Desktop está disponible de inmediato. Sin embargo, hasta que la parte remota responda la llamada y se conecte, cualquier intento de Retener la llamada en Agent Desktop generará un mensaje de error.
- Avaya Contact Center Select no admite la operación del agente solo desde el teléfono. Esto se conoce comúnmente como compatibilidad únicamente con el modo telefónico. Todos los agentes de Avaya Contact Center Select deben usar Agent Desktop para la funcionalidad de agente.

Los siguientes son flujos de llamadas que pueden experimentar limitaciones:

- Las llamadas iniciadas por el agente (originadas o transferidas) a un flujo de llamadas de Voicemail Pro que invoca la acción de telefonía de "transferencia asistida" a una CDN de punto de ruta son rechazadas por ACCS.
  - Una solución para esta limitación es usar "Transferir" (transferencia ciega) en Voicemail Pro.
- El agente que realiza una llamada en conferencia a un flujo de llamadas de Voicemail Pro que invoca cualquier acción de telefonía de transferencia ('transferencia asistida' o 'transferencia') a una CDN de punto de ruta, puede experimentar limitaciones de redirección como bucles, llamadas redirigidas rechazadas por ACCS, CLID incorrecto para la llamada redirigida.
- Las llamadas iniciadas por el agente a un experto remoto donde el experto remoto reenvía la llamada a un punto de ruta CDN, pueden ser rechazadas por ACCS. La llamada puede fallar y se puede volver a intentar.
- Un agente que pone en conferencia una llamada (llamada CC o llamada personal) al sonar a un usuario que posteriormente redirige la llamada a un punto de ruta CDN, hace que ACCS rechace esta llamada redirigida. El agente permanece en la llamada con la persona que llamó originalmente y puede volver a intentar la conferencia si lo desea.

- Un agente que transfiere una llamada (llamada CC o llamada personal) al sonar a un usuario que luego redirige la llamada a un punto de ruta CDN, puede causar que el CLID de la llamada redirigida sea intermitentemente incorrecto. El agente que enrutó esta llamada redirigida podría notar un CLID incorrecto.

ACCS no admite la transferencia de un solo paso de llamadas del centro de contacto (CDN) a otro agente de ACCS. El agente que recibe la llamada transferida puede contestar la llamada en su teléfono, pero la llamada no se presenta en Agent Desktop y el agente aparece inactivo en los informes.

- Agentes ACCS que utilizan Avaya Communicator.

  Cuando se trabaja en una llamada en Avaya Communicator, al seleccionar la opción 'Transferir' del menú desplegable asociado con la llamada, se obtiene una transferencia de un solo paso. Esto no es compatible con ACCS. La solución consiste en usar Agent Desktop para transferir llamadas de CDN. Alternativamente, en lugar de seleccionar la opción 'Transferir' del menú desplegable en Avaya Communicator, realice una llamada saliente no relacionada a la CDN. Luego, en Avaya Communicator, arrastre las dos llamadas juntas y seleccione "Transferir" en el menú que aparece.

- Agentes ACCS que utilizan teléfonos de escritorio 1140E/1230 SIP.

  Al transferir una llamada manualmente usando los teléfonos de escritorio SIP 1140E/1230, se le solicita al usuario Sí/No para consultar con la parte de destino. Seleccionar 'No' da como resultado una transferencia de un solo paso. Esto no es compatible con ACCS. La solución consiste en usar Agent Desktop para transferir llamadas de CDN. Alternativamente, cuando use teléfonos de escritorio SIP 1140E/1230 para transferir llamadas, seleccione 'Sí' para consultar con la parte de destino.

Los agentes de ACCS no deben configurar Reenviar si no hay respuesta (FONA) al DN de otro agente de ACCS. Una llamada del centro de contacto (CDN) transferida al sonar a un agente de ACCS con FONA configurado para otro agente de ACCS no es compatible con ACCS. Cuando se aplica FONA y se reenvía la llamada, el agente de ACCS que recibe la llamada reenviada puede responder la llamada en su terminal, pero la llamada no se presenta en Agent Desktop y el agente parece estar inactivo en la generación de informes.

Para los agentes ACCS que utilizan terminales SIP (teléfonos de escritorio 1140E/1230, Avaya Communicator for Windows o IP Office Softphone), una transferencia de consulta/llamada de conferencia iniciada desde el terminal SIP no se puede completar mediante Agent Desktop. Avaya recomienda que los agentes usen Agent Desktop tanto para iniciar como para completar transferencias y conferencias.

Los agentes de ACCS que utilizan Softphones de IP Office pueden experimentar algunas limitaciones al realizar Espera/Reactivación en Agent Desktop después de ser transferidos a otra parte. La limitación ocurre solo cuando un agente ACCS que usa IP Office Softphone se transfiere a un usuario de IP Office que también usa IP Office Softphone o teléfonos de escritorio Avaya 1140E/1230. En Agent Desktop, la solicitud de espera/reactivación no funciona, el estado de la llamada no cambia en IP Office Softphone y Agent Desktop no muestra un mensaje de error. En una cantidad limitada de casos, debido a una limitación de IP Office Softphone, la llamada puede interrumpirse después de un período de tiempo. Esta limitación no se aplica a las llamadas de los clientes o cuando cualquiera de los tramos de la operación de transferencia es una llamada del Centro de contacto (CDN/Punto de ruta). Para evitar esta limitación,

Nota:

Asegúrese de que Avaya Contact Center Select*Redirección*la característica está habilitada. Para habilitar la redirección, inicie sesión en Contact Center Manager Administration y navegue hasta**Configuración**>**Configuración global**>**Configuración de redirección**>**Reproducción aleatoria de medios en la transferencia**.

Capítulo 4: Avaya Contact Center Select DVD

El software Avaya Contact Center Select DVD proporciona una solución de experiencia del cliente sensible al contexto, colaborativa, de voz y multimedia que permite a las pequeñas y medianas empresas anticipar, acelerar y mejorar las interacciones con los clientes. Avaya Contact Center Select utiliza el sistema telefónico Avaya IP Office para proporcionar una plataforma de telefonía en tiempo real. Avaya IP Office es un sistema telefónico flexible y escalable diseñado específicamente para pequeñas y medianas empresas. IP Office es compatible con una amplia gama de teléfonos y dispositivos para uso en centros de contacto.

La opción de implementación de Avaya Contact Center Select DVD es compatible con Platform Vendor Independence (PVI). PVI brinda al cliente la flexibilidad de comprar un servidor que cumpla con los requisitos del servidor Avaya Contact Center Select y se ajuste a los estándares corporativos del cliente. Para utilizar la opción de implementación de DVD de Avaya Contact Center Select, el cliente debe proporcionar lo siguiente:

- Hardware de servidor que cumple con la especificación Avaya Contact Center Select Platform Vendor Independence (PVI).
- Licencia y sistema operativo Microsoft Windows 2012 Release 2 Standard o Datacenter Edition.

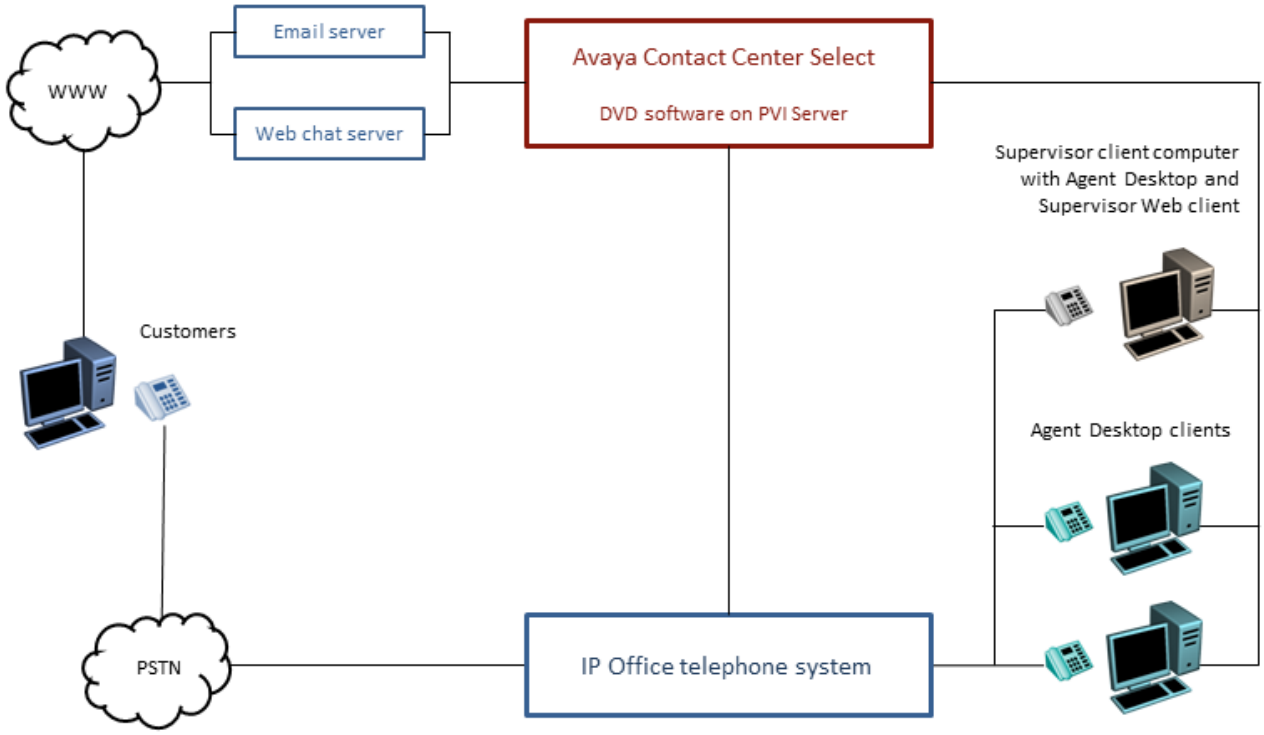


Figura 8: Topología de una solución típica de Avaya Contact Center Select

Avaya Contact Center Select está precargado con usuarios de muestra, conjuntos de habilidades y parámetros del centro de contacto. Puede utilizar estos datos de muestra para poner en marcha rápidamente la solución y realizar la primera llamada enrutada y contacto por correo electrónico. Avaya Contact Center Select ofrece una implementación de centro de contacto rápida y simplificada. Una vez que las funciones básicas de telefonía están funcionando, puede configurar contactos multimedia, multiplicidad, indicaciones personalizadas y otras funciones y funciones mejoradas para mejorar la experiencia de sus clientes.

Para implementar el software Avaya Contact Center Select mediante el software de DVD, realice lo siguiente:

- Obtener un servidor que cumpla con los requisitos de Avaya Contact Center Select PVI.
- Configure el servidor y formatee las particiones del disco duro según las especificaciones requeridas.
- Instale el sistema operativo Microsoft Windows 2012 Release 2 Standard o Datacenter edition.
- Obtenga la licencia y active el sistema operativo Microsoft Windows 2012 R2.
- Obtenga un DVD y una licencia de Avaya Contact Center Select.
- Utilice el DVD de Avaya Contact Center Select para instalar los componentes y las aplicaciones del software.
- Utilice el asistente de inicio de configuración de Avaya Contact Center Select para implementar rápidamente una solución de centro de contacto funcional.

El DVD Avaya Contact Center Select solo es compatible con el sistema operativo Microsoft Windows 2012 Release 2 Standard o Datacenter edition.

El servidor de Avaya Contact Center Select se admite en un grupo de trabajo o en un dominio de Windows.

Página149 de 3226.

Nota:

Avaya Contact Center Select con Avaya Aura®La opción de implementación del DVD del servidor multimedia no es compatible con VMware.

Especificación del servidor de la independencia del proveedor de la plataforma

La opción de implementación de Avaya Contact Center Select DVD es compatible con Platform Vendor Independence (PVI). PVI brinda al cliente la flexibilidad de comprar un servidor que cumpla con los requisitos del servidor Avaya Contact Center Select y se ajuste a los estándares corporativos del cliente. Para utilizar la opción de implementación de DVD de Avaya Contact Center Select, el cliente debe proporcionar hardware de servidor que cumpla con la especificación PVI de Avaya Contact Center Select.

La opción de implementación de DVD de Avaya Contact Center Select es compatible con las siguientes especificaciones de servidor PVI:

- Especificación de servidor de nivel de entrada en la página 65
- Especificación de servidor de gama media en la página 66
- Especificación de servidor de gama alta en la página 68

Las especificaciones del servidor de gama alta admiten la misma capacidad máxima de agente y las mismas cifras de tasa de llamadas. La especificación de servidor de gama media admite una capacidad de agente y una tasa de llamadas reducidas.

Para obtener información sobre cómo lograr el máximo rendimiento del hardware de su servidor, consulte Rendimiento del servidor y configuración del BIOS en la página 70.

Especificación de servidor de nivel de entrada

En la tabla siguiente se enumeran las especificaciones mínimas para un servidor único de 4 núcleos de nivel de entrada.

Especificación	Configuración	Comentario
UPC	Intel Xeon E3-1275L v3 único de 4 núcleos a 2,70 GHz	Seleccione una CPU que cumpla o supere la calificación de referencia para la CPU Intel Xeon E3-1275L v3 de 2,70 GHz. Las comparaciones comparativas relativas solo se aplican a las CPU con la misma cantidad de núcleos. Puede hacer comparaciones de CPU al ver las clasificaciones de aprobación de CPU de gama alta comparadas aquí:http://www.cpubenchmark.net • Los procesadores AMD no son compatibles.
CPU: velocidad de reloj mínima	2400 MHz	La velocidad de reloj de la CPU debe alcanzar o superar la velocidad de reloj mínima de 2400 MHz.

La tabla continúa...

Especificación	Configuración	Comentario
CPU - Requerido Tecnologías	Hyper-Threading	• 1 núcleo lógico adicional por cada núcleo físico. • Hyper-Threading debe estar habilitado.
RAM	mínimo de 32 GB	Para obtener el máximo rendimiento, Avaya recomienda que todas las ranuras DIMM estén ocupadas.
Tipo de disco y velocidad	SATA, SAS, mínimo 10000 RPM	• Avaya recomienda usar discos de 15000 RPM. • Las unidades de estado sólido (SSD) no son compatibles.
Tamaño total del disco	• 900 GB mínimo • Se recomienda 1,2 TB	• Se requieren discos de 900 GB para la partición multimedia de 300 GB. • Se requieren discos de 1,2 TB para la partición multimedia de 600 GB. Avaya recomienda una partición multimedia de 600 GB para admitir una retención de datos fuera de línea más prolongada. • Para obtener información sobre las particiones del disco duro, consulteTamaños de partición del disco duro de Contact Center en la página 69.
REDADA	Hardware RAID 1, RAID 5 o RAID 10	• Controlador RAID de hardware respaldado por batería con un mínimo de 512 MB de caché. • Requiere unidades duplicadas con especificaciones idénticas.
Unidad de DVD	Una unidad de DVD de doble capa	• 16X o más rápido recomendado • Se admiten unidades combinadas de DVD/Blu-Ray.
Interfaz de red	Dual NIC 1 Gbit/s o más rápido	• La NIC debe ser compatible con Receive Side Scaling (RSS) con un mínimo de 4 colas y un tamaño de búfer de recepción mínimo de 500. • Solo se admite Ethernet.

Para obtener información sobre cómo lograr el máximo rendimiento del hardware de su servidor, consulte Rendimiento del servidor y configuración del BIOS en la página 70.

Especificación de servidor de gama media

La siguiente tabla enumera las especificaciones mínimas para un servidor dual de 6 núcleos de gama media.

Página151 de 3226.

Especificación	Configuración	Comentario
UPC	Intel Xeon X5660 doble de 6 núcleos a 2,80 GHz	Seleccione una CPU que supere la calificación de referencia para el Xeon dual Intel Xeon X5660 de 2,80 GHz de 6 núcleos. Las comparaciones comparativas relativas solo se aplican a las CPU con la misma cantidad de núcleos. Puede hacer comparaciones de CPU al ver las clasificaciones de aprobación de CPU de gama alta comparadas aquí: http://www.cpubenchmark.net • Los procesadores AMD no son compatibles.
CPU: velocidad de reloj mínima	2400 MHz	La velocidad de reloj de la CPU debe alcanzar o superar la velocidad de reloj mínima de 2400 MHz.
CPU - Requerido Tecnologías	Hyper-Threading	• 1 núcleo lógico adicional por cada núcleo físico. • Hyper-Threading debe estar habilitado.
RAM	mínimo de 32 GB	Para obtener el máximo rendimiento, Avaya recomienda que todas las ranuras DIMM estén ocupadas.
Tipo de disco y velocidad	SAS, mínimo 10000 RPM	• Avaya recomienda usar discos de 15000 RPM. • Las unidades de estado sólido (SSD) no son compatibles.
Tamaño total del disco	• 900 GB mínimo • Se recomienda 1,2 TB	• Se requieren discos de 900 GB para la partición multimedia de 300 GB. • Se requieren discos de 1,2 TB para la partición multimedia de 600 GB. Avaya recomienda una partición multimedia de 600 GB para admitir una retención de datos fuera de línea más prolongada. • Para obtener información sobre las particiones del disco duro, consulteTamaños de partición del disco duro de Contact Center en la página 69.
REDADA	Hardware RAID 1, RAID 5 o RAID 10	• Controlador RAID de hardware respaldado por batería con un mínimo de 512 MB de caché. • Requiere unidades duplicadas con especificaciones idénticas.
Unidad de DVD	Una unidad de DVD de doble capa	• 16X o más rápido recomendado • Se admiten las unidades combinadas de DVD y Blu-Ray.

La tabla continúa...

Especificación	Configuración	Comentario
Interfaz de red	Dual NIC 1 Gbit/s o más rápido	• La NIC debe ser compatible con Receive Side Scaling (RSS) con un mínimo de 4 colas y un tamaño de búfer de recepción mínimo de 500. • Solo se admite Ethernet.

Para obtener información sobre cómo lograr el máximo rendimiento del hardware de su servidor, consulte Rendimiento del servidor y configuración del BIOS en la página 70.

Especificación de servidor de gama alta

La siguiente tabla enumera las especificaciones mínimas para un servidor de gama alta con CPU dual de 8 núcleos.

Especificación	Configuración	Comentario
UPC	Intel Xeon E5-2670 dual de 8 núcleos a 2,60 GHz	Seleccione una CPU que iguale o supere la calificación de referencia para la CPU dual de 8 núcleos Intel Xeon E5-2670 de 60 GHz. Las comparaciones comparativas relativas solo se aplican a las CPU con la misma cantidad de núcleos. Puede hacer comparaciones de CPU al ver la CPU de gama alta comparada clasificaciones de passmark aquí:http://www.cpubenchmark.net **Nota:** No se admiten CPU basadas en más de 12 núcleos • Los procesadores AMD no son compatibles.
CPU: velocidad de reloj mínima	2400 MHz	La velocidad de reloj de la CPU debe alcanzar o superar la velocidad de reloj mínima de 2400 MHz.
CPU - Requerido Tecnologías	Hyper-Threading	• 1 núcleo lógico adicional por cada núcleo físico. • Hyper-Threading debe estar habilitado.
RAM	mínimo de 32 GB	Para obtener el máximo rendimiento, Avaya recomienda que todas las ranuras DIMM estén ocupadas.
Tipo de disco y velocidad	SAS, mínimo 10000 RPM	• Avaya recomienda usar discos de 15000 RPM. • Las unidades de estado sólido (SSD) no son compatibles.

La tabla continúa...

Página153 de 3226.

Especificación	Configuración	Comentario
Tamaño total del disco	• 900 GB mínimo • Se recomienda 1,2 TB	• Se requieren discos de 900 GB para la partición multimedia de 300 GB. • Se requieren discos de 1,2 TB para la partición multimedia de 600 GB. Avaya recomienda una partición multimedia de 600 GB para admitir una retención de datos fuera de línea más prolongada. • Para obtener información sobre las particiones del disco duro, consulteTamaños de partición del disco duro de Contact Center en la página 69.
REDADA	Hardware RAID 1, RAID 5 o RAID 10	• Controlador RAID de hardware respaldado por batería con un mínimo de 512 MB de caché. • Requiere unidades duplicadas con especificaciones idénticas.
Unidad de DVD	Una unidad de DVD de doble capa	• Se recomienda 16X o más rápido. • Se admiten las unidades combinadas de DVD y Blu-ray.
Interfaz de red	Dual NIC 1 Gbit/s o más rápido	• La NIC debe ser compatible con Receive Side Scaling (RSS) con un mínimo de 4 colas y un tamaño de búfer de recepción mínimo de 500. • Se requieren NIC cuádruples para entornos virtualizados donde este servidor es un host VMware ESXi. • Solo se admite Ethernet.

Para obtener información sobre cómo lograr el máximo rendimiento del hardware de su servidor, consulte Rendimiento del servidor y configuración del BIOS en la página 70.

Tamaños de partición del disco duro de Contact Center

Seleccione el tamaño de su disco duro y configure las particiones requeridas. Para cada partición, especifique un tamaño de volumen en MB que, cuando se formatee, dé como resultado una partición de disco igual o mayor que el tamaño de partición mínimo requerido.

Para mejorar la retención de datos multimedia sin conexión, Avaya recomienda utilizar discos duros de 1,2 TB con una partición de 600 GB para el almacenamiento multimedia.

Tabla 1: Tamaños mínimos de partición del disco duro de Contact Center

Descripción de la partición de la unidad de disco duro	Conducir carta	Disco duro de 900 GB Tamaño mínimo dividir	Disco duro de 1,2 TB Tamaño mínimo dividir
Unidad del sistema operativo Excluyendo el cargador de arranque de Windows de 350 MB *Sistema reservado*dividir.	C:	80GB NTFS dividir	80GB NTFS dividir
Unidad de aplicación	D:	NTFS de 120GB dividir	NTFS de 120GB dividir
Unidad de DVD Para lograr continuidad y consistencia, Avaya recomienda usar la letra de unidad E: para la unidad de DVD. Sin embargo, Contact Center admite cualquier letra de unidad de DVD, excepto las letras de unidad enumeradas aquí para las particiones del disco duro.	MI:	—	—
Unidad de base de datos del servidor de contactos de voz	F:	NTFS de 200GB dividir	NTFS de 200GB dividir
Unidad de base de datos del servidor de contactos multimedia	GRAMO:	NTFS de 300 GB dividir	600GB NTFS dividir
Unidad de diario de base de datos	H:	NTFS de 100GB dividir	NTFS de 100GB dividir
	Total	801 GB de NTFS particiones en un formateado 900GB disco duro.	1101 GB de NTFS particiones en un formateado 1.2 TB disco duro.

Contact Center requiere hardware RAID-1 con unidades de disco duro duplicadas con especificaciones idénticas. Por lo tanto, como mínimo, el servidor de Contact Center debe tener dos discos duros de 900 GB o dos discos duros de 1,2 TB con especificaciones idénticas.

Configuración de rendimiento y firmware del servidor

El sistema básico de entrada y salida (BIOS) de un servidor configura los componentes de hardware y arranca el sistema operativo desde un dispositivo de almacenamiento. El sistema operativo (SO) del servidor luego usa el BIOS para controlar el hardware del servidor. Debe configurar los ajustes del BIOS del servidor para garantizar un rendimiento óptimo del hardware del servidor subyacente. Para la mayoría de las configuraciones del BIOS, debe elegir entre optimizar un servidor para ahorrar energía o para el rendimiento del servidor. Para aplicaciones en tiempo real como Avaya Contact Center Select, siempre debe elegir la configuración del BIOS del servidor que garantice el rendimiento óptimo del hardware del servidor subyacente.

Los fabricantes de servidores proporcionan sus propias placas base, BIOS, hardware y firmware. Determinar la configuración del BIOS para el hardware de su servidor puede ser un desafío. Hay varias configuraciones de BIOS que pueden afectar significativamente el rendimiento del sistema. Al optimizar para

Página155 de 3226.

rendimiento del sistema, debe seleccionar la configuración del BIOS que mejore el rendimiento del sistema sobre aquellas que contribuyen al ahorro de energía. Otras configuraciones y recomendaciones del BIOS no son tan sencillas. Comience consultando los datos técnicos del fabricante de su servidor. Avaya recomienda que luego pruebe su solución para tomar las mejores decisiones de configuración del BIOS.

Configure el hardware del servidor, el firmware y la configuración del sistema operativo para seleccionar el rendimiento del sistema sobre el ahorro de energía.

Firmware del servidor

El firmware es un programa informático que se almacena en la placa base del servidor o en un controlador de hardware adicional. El firmware almacenado en la placa base del servidor se denomina Sistema básico de entrada y salida (BIOS). El BIOS es responsable del comportamiento del sistema cuando se enciende por primera vez y de pasar el control del servidor al sistema operativo. El firmware también se almacena en componentes de hardware como los controladores Redundant Array of Independent Disks (RAID).

Consulte periódicamente los datos técnicos del fabricante de sus servidores y, en su caso, aplique las actualizaciones más recientes de BIOS y firmware. Los pasos necesarios para actualizar el firmware o el BIOS de un sistema varían según el proveedor de hardware y el componente que se va a actualizar. Normalmente, el fabricante proporciona una utilidad de actualización de firmware. Mantener el BIOS y el firmware de su servidor en un nivel compatible puede mejorar la confiabilidad, la capacidad de servicio y ayudar a garantizar un rendimiento óptimo.

Interfase Extensible de Firmware Unificado

La especificación de la interfaz de firmware extensible unificada (UEFI) define la interfaz entre el sistema operativo y el firmware del servidor. Al igual que el BIOS, el fabricante del servidor instala UEFI y es el primer programa que se ejecuta cuando se enciende el servidor. El firmware UEFI ofrece algunas ventajas técnicas sobre el sistema BIOS tradicional.

El software Contact Center, cuando se implementa en servidores físicos, es compatible con UEFI.

El software Contact Center, cuando se implementa en máquinas virtuales de VMware, no es compatible con UEFI.

Contact Center no es compatible con la función UEFI Secure Boot.

Seleccione la opción de inicio de firmware, BIOS o UEFI, en el servidor antes de instalar el sistema operativo Windows Server 2012 R2 y el software Contact Center. Consulte la documentación de su proveedor de hardware sobre cómo cambiar e implementar la opción de arranque de firmware requerida. Cambiar la opción de inicio del firmware después de que se haya instalado el sistema operativo hace que el servidor no se pueda iniciar y esto no es compatible.

Gestión de potencia y rendimiento

Para aplicaciones en tiempo real como Avaya Contact Center Select, siempre debe seleccionar la configuración de hardware, BIOS, firmware y sistema operativo que mejore el rendimiento del sistema sobre aquellas que contribuyen al ahorro de energía.

Las CPU Intel Xeon ofrecen dos opciones principales de administración de energía: C-states e Intel Turbo Boost.

- La desactivación de los estados C reduce las latencias para activar las CPU desde estados detenidos o inactivos hasta el encendido completo.
- Intel Turbo Boost aumenta la frecuencia interna del procesador si la carga de trabajo requiere más potencia.

Esta configuración depende de la marca y el modelo del OEM del servidor. La terminología de los parámetros del BIOS para los servidores Dell y HP actuales se describe a continuación. Otras marcas y modelos de servidores pueden tener otra terminología pero configuraciones de BIOS equivalentes.

Las siguientes son las configuraciones de BIOS recomendadas para los servidores Dell PowerEdge:

- Establezca el Modo de administración de energía en Máximo rendimiento.
- Establezca el Modo de administración de rendimiento y energía de la CPU en Rendimiento máximo.
- Configuración del procesador: establece el Modo Turbo en habilitado
- Configuración del procesador: establece C States en deshabilitado

Las siguientes son las configuraciones de BIOS recomendadas para los servidores HP ProLiant:

- Establezca el modo de regulador de potencia en modo estático alto.
- Deshabilitar la compatibilidad con el estado C del procesador
- Deshabilitar la compatibilidad con el procesador C1E
- Deshabilitar la administración de energía de QPI
- Habilitar Intel Turbo Boost

Configure el hardware del servidor, el firmware y la configuración del sistema operativo para seleccionar el rendimiento del sistema sobre el ahorro de energía.

Caché de disco y RAID

Las unidades de disco duro utilizan la memoria caché para mejorar el acceso de lectura y escritura a las unidades de disco. En el almacenamiento en caché del modo de reescritura, el disco o el controlador RAID escribe datos del servidor en la memoria caché y reconoce la finalización de la escritura en el servidor. El servidor puede realizar otras tareas mientras el controlador de disco transfiere los datos de la memoria caché de escritura a las unidades de disco. Este enfoque aumenta significativamente el rendimiento de escritura.

Avaya Contact Center Select admite hardware RAID-1, RAID-5 y RAID-10. La tecnología RAID proporciona redundancia de datos de disco, así como detección y corrección de errores. Para obtener la máxima seguridad y soluciones de misión crítica, Avaya recomienda que todos los servidores de Contact Center contengan un RAID

Página157 de 3226.

controlador. Hardware RAID-1, RAID-5 y RAID-10 son los únicos niveles y tipos de RAID admitidos.

Lea la documentación del hardware de su servidor para determinar cómo configurar el almacenamiento en caché del disco. Por lo general, el almacenamiento en caché del disco se puede configurar como una configuración del BIOS, una configuración de RAID, una configuración de la controladora RAID o como una configuración del sistema operativo. Algunos controladores RAID exponen la capacidad de manipular la política de almacenamiento en caché a través del sistema operativo y, por lo tanto, la configuración del nivel del sistema operativo puede anular la configuración del nivel del BIOS. Consulte la documentación de su hardware para obtener más información sobre la configuración del almacenamiento en caché del disco. Avaya Contact Center Select no es compatible con el almacenamiento en caché de disco a nivel del sistema operativo, el almacenamiento en caché de disco de software o RAID de software. Avaya Contact Center Select requiere almacenamiento en caché RAID de hardware respaldado por batería para evitar la pérdida de datos y la posible corrupción de la base de datos en caso de corte de energía.

Memoria y arquitectura de memoria no uniforme

El acceso a memoria no uniforme (NUMA) es un diseño de memoria de computadora que se utiliza en el multiprocesamiento, donde el tiempo de acceso a la memoria depende de la ubicación de la memoria en relación con el procesador. Con NUMA, un procesador puede acceder a su propia memoria local más rápido que a la memoria no local (memoria local a otro procesador o memoria compartida entre procesadores). Para Avaya Contact Center Select, el servidor debe admitir e implementar NUMA.

En la configuración del BIOS del servidor, configure el modo de funcionamiento de la memoria para optimizar el rendimiento y desactive la intercalación de nodos. Por ejemplo, para un servidor Dell, configure el "Modo operativo de memoria" como "Modo optimizador" y configure "Entrelazado de nodos" como "Deshabilitado". Consulte la documentación de su hardware para obtener más información sobre NUMA y el rendimiento de la memoria.

Hyper-Threading

Hyper-Threading es la tecnología patentada de Intel para aumentar la potencia computacional paralela (procesador multitarea) al permitir que el sistema operativo (SO) vea y aborde cada núcleo de procesador físico como si fueran dos procesadores virtuales. También permite que el sistema operativo y las aplicaciones compartan el trabajo entre esos procesadores virtuales siempre que sea posible, haciendo así un uso completo de los recursos disponibles.

Habilite Hyper-Threading en el servidor de Avaya Contact Center Select.

Dispositivos de hardware no utilizados

En el servidor, desconecte o deshabilite los dispositivos de hardware físicos innecesarios y no utilizados, como: puertos COM, puertos LPT, controladores USB, interfaces de red y controladores de almacenamiento. Debe conservar algunos dispositivos USB para el mouse y el teclado. La desactivación de dispositivos de hardware innecesarios mejora el rendimiento y la seguridad del servidor. Consulte los datos técnicos del fabricante de sus servidores para obtener información sobre cómo deshabilitar los dispositivos de hardware no utilizados en el BIOS.

Resumen

Para aplicaciones en tiempo real como Avaya Contact Center Select, elija la configuración del BIOS del servidor que optimice el rendimiento en lugar del ahorro de energía. Comience consultando los datos técnicos del fabricante de su servidor. Avaya recomienda que luego pruebe su solución para tomar las mejores decisiones de configuración del BIOS. Avaya recomienda habilitar CPU Hyper-Threading. Al habilitar opciones de BIOS como CPU Prefetchers y CPU Hyper-Threading, el rendimiento del sistema se puede mejorar de manera efectiva. Al ajustar la configuración del BIOS del sistema para el rendimiento, debe tener en cuenta las diversas opciones de procesador y memoria. Experimente con otras opciones para encontrar la configuración óptima para su solución específica de hardware y Contact Center.

Configure el hardware del servidor, el BIOS, el firmware y los ajustes del sistema operativo para seleccionar el rendimiento del sistema sobre el ahorro de energía.

Especificación del software Avaya Contact Center Select DVD

El DVD Avaya Contact Center Select contiene los siguientes componentes de software:

- Servidor del administrador del centro de contacto (CCMS)
- Administración del administrador del centro de contacto (CCMA)
- Conjunto de herramientas de control de comunicaciones (CCT)
- Administrador de licencias del centro de contacto (LM)
- Utilidad del servidor Contact Center Manager (SU)
- Diseñador de orquestación (OD)
- Centro de Contacto Multimedia (CCMM)
- Aura de Avaya®Instancia de Media Server Hyper-V en el servidor de Windows Server 2012
- Política de cortafuegos de Avaya Contact Center Select
- Datos de configuración predeterminados de Avaya Contact Center Select
- Asistente de encendido de configuración

El DVD Avaya Contact Center Select solo es compatible con el sistema operativo Microsoft Windows 2012 Release 2 Standard o Datacenter edition.

Requisitos de nomenclatura del servidor

Los nombres de servidor deben cumplir con RFC1123 (Requisitos para hosts de Internet), que especifica que un nombre de host debe cumplir con lo siguiente:

- Solo se pueden usar caracteres de la a a la z, de la A a la Z y del 0 al 9 en un nombre de host.

Página159 de 3226.

- Puede utilizar un guión (-), pero no para iniciar o finalizar el nombre de host.
- Los nombres de host deben tener entre 6 y 15 caracteres de longitud.
- Los nombres de host no deben comenzar con un número.
- No utilice el carácter de subrayado (_) ni el carácter de punto (.).
- No utilice espacios en el nombre de host.

El servidor de Contact Center debe poder resolver el nombre de host o el nombre de la computadora de todos los demás servidores dentro de la configuración. Si tiene un servidor de Servicio de nombres de dominio (DNS), asegúrese de que exista una entrada para cada servidor. Si no tiene un servidor DNS, actualice manualmente el archivo HOSTS en cada servidor con el nombre de host o el nombre de la computadora de todos los demás servidores para asegurarse de que todos los clientes puedan interpretar los nombres de los servidores.

Si la conectividad de red en su red requiere el uso de nombres de dominio completos (FQDN), entonces el FQDN de cada computadora debe poder resolverse entre todos los servidores asociados con Contact Center.

Revisiones de seguridad de Microsoft

Debe operar su servidor con los parches más recientes de Microsoft.

- Revisa el *Lista de aplicabilidad de hotfixes de seguridad y compatibilidad de paquetes de servicios de cartera de Contact Center* (disponible en el sitio web de soporte técnico) para ver la lista de revisiones de seguridad de Microsoft aplicables.
- Realice una copia de seguridad de todo el servidor y luego apague todos los servicios de Contact Center antes de aplicar las revisiones de seguridad de Microsoft siguiendo las instrucciones de Microsoft.
- Aplicar las actualizaciones de seguridad de Microsoft en el momento oportuno.

Actualizaciones del sistema operativo

Las actualizaciones del sistema operativo incluyen actualizaciones de servicio y paquetes de servicio.

Actualizaciones de servicio

Dada la cantidad de actualizaciones del servicio de seguridad del sistema operativo y la complejidad inherente a cualquier red, cree un proceso sistemático y responsable para identificar y aplicar las actualizaciones del servicio. Para ayudar a crear dicho proceso, puede seguir una serie de pautas de mejores prácticas, como se documenta en el Boletín especial 800-40 del Instituto Nacional de Estándares y Tecnología (NIST), Procedimientos para el manejo de parches de seguridad.

Este boletín sugiere que si una organización no tiene un grupo central para coordinar el almacenamiento, la evaluación y el registro crónico de las actualizaciones del servicio de seguridad en una biblioteca, los administradores del sistema o el administrador del centro de contacto deben cumplir esta función. Además de estas pautas, siempre que sea posible, siga las recomendaciones de Microsoft con respecto a las vulnerabilidades descubiertas recientemente y que instale de inmediato las actualizaciones del servicio de seguridad de Microsoft.

Siempre que sea posible, Avaya incorpora las recomendaciones de seguridad del sistema operativo y las actualizaciones de servicio más recientes en una estrategia de prueba de soluciones integradas durante cada prueba.

ciclo. Sin embargo, debido a la naturaleza urgente de las actualizaciones del servicio de seguridad cuando se descubren vulnerabilidades, siga las pautas de Microsoft a medida que se emiten, incluidos los procedimientos de instalación de Microsoft y los procesos de reversión de actualizaciones del servicio de seguridad.

Finalmente, debe realizar una copia de seguridad completa del sistema antes de actualizar el sistema para asegurarse de que sea posible una reversión, si es necesario. Si una aplicación de Contact Center no funciona correctamente después de aplicar una actualización del servicio de seguridad de Microsoft, debe eliminar la actualización del servicio y volver a la versión anterior de la aplicación (desde la copia de seguridad que realizó antes de aplicar la actualización del servicio). Para mayor seguridad, siempre determine si Avaya verificó la actualización del servicio de Microsoft para compatibilidad con Contact Center Manager.

Para obtener más información acerca de la actualización, consulte la*Lista de compatibilidad de hotfixes de seguridad y compatibilidad de paquetes de servicio de cartera de Contact Center*enhttp://soporte.avaya.com .

paquetes de servicios

Avaya tiene una política para implementar pruebas de co-residencia de todos los paquetes de servicios operativos nuevos para verificar la compatibilidad con el conjunto de aplicaciones de Contact Center tan pronto como estén disponibles. En la práctica, debido a que un paquete de servicio puede contener una cantidad significativa de contenido nuevo, Avaya requiere que espere hasta que se complete la prueba de compatibilidad antes de aplicar el paquete de servicio. Tenga en cuenta que los service packs del sistema operativo generalmente se prueban con el SP de la aplicación Contact Center más reciente y, por lo tanto, una actualización a un nuevo service pack requiere una actualización al SP de Avaya más reciente.

Antes de cargar un nuevo Service Pack, debe realizar una copia de seguridad completa del sistema (para revertir el sistema como en el escenario de actualización).

Importante:

La compatibilidad del Service Pack para todas las aplicaciones de Contact Center está documentada en el*Lista de aplicabilidad de hotfixes de seguridad y compatibilidad de paquetes de servicios de cartera de Contact Center*en el sitio web enhttp://soporte.avaya.com .

Actualizaciones del entorno de tiempo de ejecución de Java

Contact Center solo admite versiones específicas de Java Runtime Environment (JRE). Durante la instalación, Contact Center desactiva las actualizaciones automáticas de JRE en los servidores del centro de contacto.

Importante:

La actualización a una versión no compatible de JRE puede hacer que el centro de contacto deje de funcionar y puede requerir la reinstalación del servidor del centro de contacto.

Compatibilidad con el protocolo de configuración de host dinámico

Aplicaciones de Contact Center (CCMS, CCMA, CCT, CCMM, LM y Avaya Aura®Media Server) no son compatibles con el Protocolo de configuración dinámica de host (DHCP). Todos los servidores de Contact Center deben tener una dirección IP estática.

Los equipos cliente de Agent Desktop admiten direcciones IP estáticas y DHCP.

Requisitos de software de terceros

Debido al procesamiento en tiempo real y de misión crítica que realizan las aplicaciones de Contact Center, no debe instalar ningún otro tipo de software de aplicación en el servidor. Puede instalar cierto software de clase de utilidad en el servidor, siempre que cumpla con las pautas de esta sección.

El software de clase de aplicación generalmente requiere una cierta cantidad de recursos del sistema y no debe instalarse en un servidor que ejecute aplicaciones de Contact Center. La instalación de aplicaciones de terceros puede hacer que las aplicaciones de Contact Center funcionen fuera de los límites de ingeniería conocidos y puede crear posibles problemas desconocidos del sistema (por ejemplo, contenciones de CPU, mayor carga de tráfico de red y degradaciones de acceso al disco).

Ciertas aplicaciones de software de clase de utilidad de terceros, como diagnósticos de hardware o herramientas de copia de seguridad, generalmente requieren menos recursos del sistema durante el funcionamiento normal de las aplicaciones del Contact Center y están permitidas. Las excepciones son las utilidades, como los protectores de pantalla, que pueden causar problemas en el sistema y degradar el rendimiento.

El software antivirus se clasifica como una utilidad y está sujeto a las pautas genéricas de la siguiente sección.

Pautas genéricas para aplicaciones de software de clase de utilidad

Las siguientes son pautas genéricas para el software de clase de utilidad:

- Durante el tiempo de ejecución, la utilidad no debe degradar la aplicación del centro de contacto más allá de un porcentaje promedio de uso de CPU (consulte cada sección específica de la aplicación en este documento para conocer el nivel de uso de CPU máximo recomendado). Además, la utilidad no debe reducir la cantidad mínima de espacio libre en el disco duro requerido por la aplicación del centro de contacto y el sistema operativo Windows.
- La utilidad no debe causar apagados de software inadecuados o apagados fuera de secuencia.
- La empresa de servicios públicos no debe administrar la aplicación del centro de contacto.
- Si la utilidad tiene una base de datos, no debe afectar la base de datos de la aplicación del centro de contacto.
- No se deben utilizar las utilidades de compresión de disco.
- No se deben utilizar las utilidades de ajuste de memoria utilizadas para recuperar la memoria que Microsoft no utiliza.
- La instalación o desinstalación del software de terceros no debe afectar ni entrar en conflicto con la aplicación del centro de contacto (por ejemplo, no debe causar conflictos de DLL). Si se descubren tales conflictos, podría ser necesaria una reconstrucción del servidor.
- El personal de implementación debe realizar pruebas para garantizar que se cumplan estas condiciones y recomendaciones antes de poner en producción la aplicación Contact Center. El personal de soporte puede solicitar los resultados de las pruebas durante el diagnóstico de fallas. Como parte del diagnóstico de fallas, se le puede solicitar al distribuidor o al usuario final que elimine el software de terceros.
- No se debe instalar HyperTerminal en el servidor ya que interfiere con el funcionamiento del Contact Center.

Directrices para el uso de software antivirus

Esta sección describe los requisitos del software antivirus Avaya Contact Center Select.

Avaya Contact Center Select es compatible con los siguientes productos antivirus:

- Antivirus de Symantec
- McAfee

Para obtener más información sobre las consideraciones antivirus de Avaya Contact Center Select y las versiones admitidas, consulte *Guía de referencia de seguridad de Avaya Contact Center Select* disponible en el sitio web de soporte de Avaya en http://soporte.avaya.com .

Puede implementar productos antivirus de otros proveedores sujeto a las siguientes pautas:

- Política de cuarentena de archivos infectados en el servidor y el cliente: el software antivirus se puede configurar para limpiar el virus detectado automáticamente y los archivos se deben poner en cuarentena si no se pueden limpiar los archivos infectados. Comuníquese con Avaya para verificar si el archivo de cuarentena es parte de nuestros archivos de productos o un archivo de sistema dependiente. Si se detecta un virus, elimine el servidor de la red inmediatamente durante la erradicación del virus para evitar una mayor propagación del virus.
- No conecte una plataforma de aplicación del centro de contacto directamente a Internet para descargar definiciones de virus o archivos actualizados. Además, Avaya recomienda que no use una PC cliente de aplicación de centro de contacto para conectarse a Internet. En su lugar, descargue las definiciones de virus y los archivos actualizados a otra ubicación en la red del cliente y cárguelos manualmente desde esta ubicación provisional a la plataforma de la aplicación del centro de contacto.
- Realice los pasos anteriores para descargar los Service Packs (SP) de la aplicación Contact Center. Este método limita el acceso a Internet y, por lo tanto, reduce el riesgo de descargar archivos infectados.
- Escanee todos los archivos SP, DVD-ROM y disquetes antes de cargarlos o instalarlos en el servidor. Esta práctica minimiza cualquier exposición a archivos infectados de fuentes externas.
- Consideraciones de capacidad: la ejecución de un software de detección de virus puede generar una carga adicional en la plataforma de una aplicación del centro de contacto. El personal de implementación debe ejecutar la herramienta de supervisión de rendimiento en el servidor para medir el uso de la CPU. Si la exploración del software antivirus hace que el uso promedio de la CPU de la plataforma supere el porcentaje recomendado durante más de 20 minutos, el software antivirus no debe cargarse en la plataforma de la aplicación del centro de contacto.
- El Soporte de productos no brinda soporte para la configuración del software antivirus, pero ofrece orientación cuando es posible. Dirija las preguntas o problemas sobre el software antivirus al proveedor adecuado.
- Si se plantean problemas de rendimiento o funcionalidad al personal de soporte de Avaya como parte del diagnóstico de fallas, es posible que se le pida que elimine el software de utilidades o el software antivirus de terceros.

Varias tareas de mantenimiento se activan automáticamente a las 12:00 de la noche. Por lo tanto, debe programar análisis de virus en un momento distinto de la medianoche.

Página163 de 3226.

Avaya recomienda que excluya los siguientes archivos y carpetas de los análisis (tanto en tiempo real como programados):

- F:\Avaya\Contact Center\Bases de datos\
- *<unidad de base de datos adicional>*:\Avaya\Centro de contacto\Bases de datos\
- Archivos TSM_OAM ubicados en las siguientes carpetas:
  - D:\Avaya\Contact Center\Manager Server\iccm\bin\data
  - D:\Avaya\Contact Center\Manager server\iccm\data
  - D:\Avaya\Contact Center\Manager Server\iccm\sdm\log
- D:\Avaya\Contact Center\Manager Server\bin\tools2.exeSe producen errores de acceso a archivos en el registro de actividad de análisis si no excluye este archivo del análisis.
- D:\Avaya\Contact Center\Manager Server\iccm\logs (registros SIP)
- D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\ (archivos de configuración de registro SIP)
- D:\Avaya\Contact Center\Componentes comunes\CMF
- D:\Avaya\Contact Center\Manager Administration\Apps\ (incluyendo subdirectorios)
- La carpeta donde almacena Service Packs y parches

Contact Center Multimedia interactúa con un sistema de correo electrónico externo y permite a los agentes enviar archivos adjuntos desde sus computadoras al servidor de Avaya Contact Center Select. Ambos métodos de recuperación de datos son fuentes potenciales de infección de software.

Avaya recomienda las siguientes pautas para el software antivirus:

- El software antivirus debe instalarse en el servidor de correo electrónico para garantizar que los problemas se detecten en el origen.
- Las computadoras de los agentes requieren un software antivirus para garantizar que los archivos adjuntos enviados al servidor de Avaya Contact Center Select no tengan virus. Contact Center Multimedia no bloquea tipos de archivos adjuntos específicos. El software antivirus de terceros debe instalarse en el Portal Server de acuerdo con las pautas de este documento para dichas utilidades.
- Asegúrese de que el software antivirus esté configurado para permitir mensajes de correo electrónico salientes. Por ejemplo, configure el software antivirus McAfee*Protección de acceso*opción de no bloquear *Evite que los gusanos de correo masivo envíen correo*. Como alternativa, agregue el proceso "EmailManager.exe" de Contact Center Multimedia al McAfee*Procesos a excluir*lista.

  Excluya la partición de la base de datos de Contact Center Multimedia del análisis.
- Si los cortafuegos en equipos individuales están habilitados en el equipo de Agent Desktop, el detector de informes podría estar marcado como tratando de acceder a Internet. Las propiedades deben configurarse para permitir el acceso de Report Listener a Contact Center Multimedia a través del firewall.
- No debe habilitar Microsoft Updater para la ejecución automática. Microsoft Updater está configurado en el nivel de alerta para que pueda programar actualizaciones para las horas de menor actividad.

Advertencia:

Ejecutar un análisis de virus en la carpeta de archivos adjuntos de Contact Center Multimedia, que contiene miles de archivos, puede usar un tiempo de CPU significativo en un servidor y puede causar una ralentización drástica en los tiempos de respuesta del agente. Avaya recomienda ejecutar análisis, si es necesario, durante las horas de menor actividad.

Para evitar problemas de integridad de la base de datos, Avaya recomienda que excluya todos los archivos CACHE.DAT, los archivos de diario, el archivo cache.cpf y cualquier archivo relacionado con Caché de los análisis antivirus.

El software Caché está instalado en *<Unidad_de_instalación>*:\Avaya\Cache\CacheSys.Las bases de datos y los archivos de diario se instalan en *<Unidad_de_instalación>*:\Avaya\Contact Center\Bases de datos.

Excluya la carpeta de archivos de Caché Journal;G:\Avaya\

Para Avaya Aura®Media Server, debe excluir los siguientes archivos y carpetas de los análisis (tanto en tiempo real como programados):

- D:\Avaya\MAS\Multimedia_Applications\MAS\platdata
- D:\Avaya\MAS\Multimedia_Applications\MAS\common\log

Licencias de DVD de Avaya Contact Center Select

La opción de implementación de Avaya Contact Center Select DVD requiere una licencia de Nodal Enterprise entregada como un archivo WebLM XML. Este archivo de licencia se utiliza para controlar el acceso a funciones con licencia, como contactos multimedia y multiplicidad.

Contact Center License Manager brinda control central y administración de licencias para Avaya Contact Center Select. Cada Contact Center License Manager incluye una instancia local de WebLM. Cuando se inicia el servicio Contact Center License Manager, extrae las claves de licencia de WebLM de la instancia local de WebLM. Luego, Contact Center License Manager convierte las claves de licencia de WebLM en claves de licencia PLIC locales y distribuye las claves a las aplicaciones de Avaya Contact Center Select según sea necesario.

- Obtenga la ID de host de WebLM para su servidor Avaya Contact Center Select.
- Utilice el ID de host de WebLM para obtener un archivo de licencia nodal de WebLM del Sistema de entrega y licencias de productos (PLDS) de Avaya.
- Carga el archivo de licencia en el servidor de Avaya Contact Center Select mientras ejecuta la utilidad de configuración cuando implementa el servidor de Avaya Contact Center Select. También puede cargar el archivo de licencia después del proceso de configuración. Cuando Contact Center License Manager carga la licencia, si el número único de la licencia no coincide con la ID de host de WebLM, License Manager se cierra y Avaya Contact Center Select no puede procesar los contactos. Si el número exclusivo de la licencia coincide con la ID de host de WebLM, License Manager proporciona las claves de licencia y Avaya Contact Center Select procesa los contactos de los clientes.

Capítulo 5: Avaya Contact Center Select dispositivo de software

Para una mayor productividad, eficiencia y flexibilidad, Avaya Contact Center Select es compatible con la virtualización de VMware.

Puede utilizar un único paquete de dispositivo virtual abierto (OVA) para distribuir un dispositivo virtual. Por ejemplo, un Avaya Aura®El paquete Media Server OVA incluye toda la información de Open Virtualization Format (OVF) requerida para crear un Avaya Aura®Dispositivo virtual de Media Server en un host de VMware. Un dispositivo virtual contiene un sistema operativo preinstalado y preconfigurado y una pila de aplicaciones optimizada para proporcionar un conjunto específico de servicios.

Avaya Contact Center Select ofrece un paquete de dispositivo de software que consta de los siguientes componentes:

- Máquina virtual Avaya Contact Center Select
- Aura de Avaya®servidor de medios OVA
- Avaya WebLM OVA

El aura de Avaya®Media Server y Avaya WebLM OVA están empaquetados y listos para su implementación. Para la máquina virtual de Avaya Contact Center Select, debe crear una máquina virtual adecuadamente especificada y luego instalar el software del producto desde el DVD o la imagen ISO de Avaya Contact Center Select.

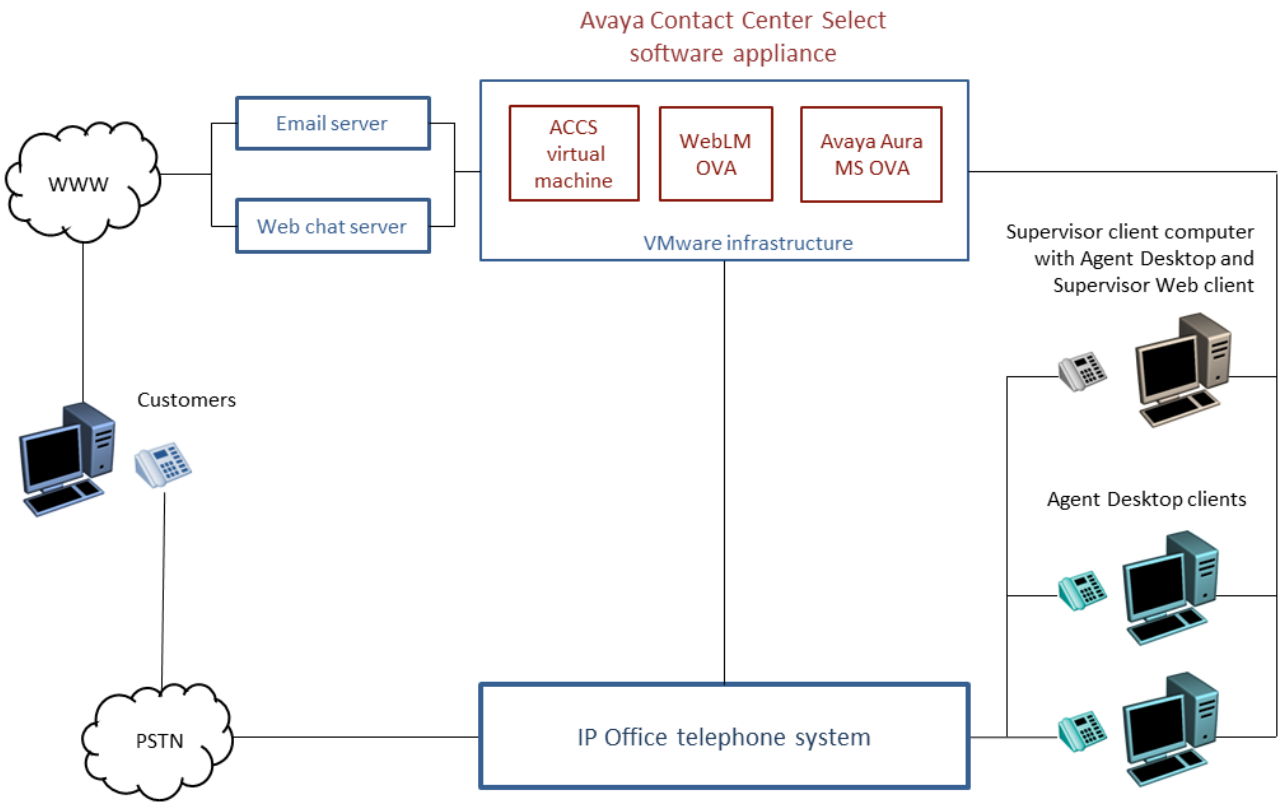


Figura 9: Solución típica de centro de contacto virtualizado con Avaya Contact Center Select, Avaya Aura® Media Server y Avaya WebLM implementados en un único servidor host de VMware

Puede usar VMware vSphere o vCenter y estos componentes para crear máquinas virtuales en su entorno virtualizado. Los paquetes OVA se crean como archivos de la versión 8 del hardware de VMware.

El dispositivo de software Avaya Contact Center Select solo es compatible con los siguientes entornos de virtualización:

- ESXi 5.5
- ESXi 6.0
- ESXi 6.5

Nota:

Se requiere VMFS 5.54 o posterior para todas las versiones compatibles de ESXi.

Avaya Contact Center Select es compatible con la máquina virtual Avaya WebLM co-residente en el mismo servidor host de VMware o implementada en un servidor host de VMware independiente.

Avaya Contact Center Select es compatible con Avaya Aura®Máquina virtual de Media Server co-residente en el mismo servidor de host de VMware o implementada en un servidor de host de VMware separado.

Para obtener más información sobre los componentes del dispositivo de software Avaya Contact Center Select, consulte lo siguiente:

- Máquina virtual Avaya Contact Center Select en la página 83
- Servidor multimedia Avaya Aura OVA en la página 90
- Avaya WebLM OVA en la página 91

Máquina virtual Avaya Contact Center Select

Cree la máquina virtual Avaya Contact Center Select para proporcionar enrutamiento sensible al contexto y basado en habilidades para los contactos multimedia y de voz del cliente.

La máquina virtual Avaya Contact Center Select (invitado) contiene el siguiente software de aplicación de centro de contacto.

- Servidor del administrador del centro de contacto (CCMS)
- Administración del administrador del centro de contacto (CCMA)
- Conjunto de herramientas de control de comunicaciones (CCT)
- Centro de Contacto Multimedia (CCMM)
- Administrador de licencias del centro de contacto (LM)
- Utilidad del servidor Contact Center Manager (SU)
- Diseñador de orquestación (OD)
- Datos de configuración predeterminados de Avaya Contact Center Select
- Política de cortafuegos

Para crear la máquina virtual Avaya Contact Center Select, realice lo siguiente:

1. Cree una máquina virtual VMware con las características de hardware:
2. Instale el sistema operativo en inglés Windows Server 2012 Release 2 Standard o Datacenter edition en la máquina virtual.
3. Obtenga la licencia y active el sistema operativo Microsoft Windows 2012 R2.
4. Configure el servidor y formatee las particiones del disco duro según las especificaciones requeridas.
5. Instale VMware Tools en el servidor.
6. Obtenga un DVD o una imagen ISO de Avaya Contact Center Select.
7. Obtenga un archivo de licencia de Avaya Contact Center Select.
8. Utilice el DVD o la imagen ISO de Avaya Contact Center Select para instalar los componentes y las aplicaciones del software.
9. Utilice el Asistente de encendido de configuración de Avaya Contact Center Select para implementar rápidamente una solución de centro de contacto funcional.

Página168 de 3226.

10. Continúe monitoreando los recursos en tiempo real de VMware.

Cada máquina virtual Avaya Contact Center Select requiere un Avaya Aura basado en Linux®Servidor multimedia. Cada máquina virtual Avaya Contact Center Select también requiere un servidor administrador de licencias Avaya WebLM adicional e independiente.

Particiones y discos duros de máquinas virtuales de Contact Center

Cree discos duros virtuales individuales para cada una de las particiones requeridas para su máquina virtual de Contact Center. Al crear un disco duro virtual para la partición del sistema operativo, cree un tamaño de disco duro 1 GB mayor que el tamaño de partición requerido para dar cabida a la creación de particiones de Windows adicionales que podrían crearse automáticamente como parte de la instalación de Windows Server 2012 R2.

Por ejemplo, para un requisito de tamaño de partición del sistema operativo de 80 GB, cree un disco duro virtual de 81 GB. Para cada partición adicional requerida por Contact Center, cree un disco duro virtual mayor o igual al requisito de tamaño de partición. El disco duro virtual debe tener un tamaño suficiente para que, cuando se cree y formatee la partición asociada, tenga un tamaño que coincida con el tamaño de partición requerido para la instalación.

Para mejorar la retención de datos multimedia fuera de línea, Avaya recomienda utilizar una partición de 600 GB para el almacenamiento multimedia. La partición multimedia de 600 GB requiere almacenamiento SAN.

Tabla 2: Tamaños mínimos de partición del disco duro de la máquina virtual de Contact Center

Descripción de la partición de la unidad de disco duro	Conducir carta	Mínimo tamaños de partición	Recomendado tamaños de partición, 300 GB multimedios dividir	Recomendado tamaños de partición, 600 GB multimedios dividir
Unidad del sistema operativo	C:	80GB NTFS dividir	80GB NTFS dividir	80GB NTFS dividir
Unidad de aplicación	D:	NTFS de 100GB dividir	NTFS de 120GB dividir	NTFS de 120GB dividir
Unidad de DVD	MI:	—	—	—
Unidad de base de datos del servidor de contactos de voz	F:	NTFS de 180GB dividir	NTFS de 200GB dividir	NTFS de 200GB dividir
Unidad de base de datos del servidor de contactos multimedia	GRAMO:	NTFS de 200GB dividir	NTFS de 300 GB dividir	600GB NTFS dividir
Unidad de diario de base de datos	H:	80GB NTFS dividir	NTFS de 100GB dividir	NTFS de 100GB dividir
	Total	641 GB de espesor disco aprovisionado espacio en un vmware Almacén de datos.	801 GB de espesor disco aprovisionado espacio en un almacén de datos de VMware.	1101 GB de disco de aprovisionamiento grueso espacio en una SAN Almacén de datos.

Si usa discos Raid–1 de 900 GB, use la opción de Tamaño mínimo de partición anterior.

Contact Center requiere hardware RAID-1 con unidades de disco duro duplicadas con especificaciones idénticas. Por lo tanto, el servidor host de VMware debe implementar Hardware RAID-1 o superior.

Requisitos de nomenclatura del servidor

Los nombres de servidor deben cumplir con RFC1123 (Requisitos para hosts de Internet), que especifica que un nombre de host debe cumplir con lo siguiente:

- Solo se pueden usar caracteres de la a a la z, de la A a la Z y del 0 al 9 en un nombre de host.
- Puede utilizar un guión (-), pero no para iniciar o finalizar el nombre de host.
- Los nombres de host deben tener entre 6 y 15 caracteres de longitud.
- Los nombres de host no deben comenzar con un número.
- No utilice el carácter de subrayado (_) ni el carácter de punto (.).
- No utilice espacios en el nombre de host.

El servidor de Contact Center debe poder resolver el nombre de host o el nombre de la computadora de todos los demás servidores dentro de la configuración. Si tiene un servidor de Servicio de nombres de dominio (DNS), asegúrese de que exista una entrada para cada servidor. Si no tiene un servidor DNS, actualice manualmente el archivo HOSTS en cada servidor con el nombre de host o el nombre de la computadora de todos los demás servidores para asegurarse de que todos los clientes puedan interpretar los nombres de los servidores.

Si la conectividad de red en su red requiere el uso de nombres de dominio completos (FQDN), entonces el FQDN de cada computadora debe poder resolverse entre todos los servidores asociados con Contact Center.

Revisiones de seguridad de Microsoft

Debe operar su servidor con los parches más recientes de Microsoft.

- Revisa el*Lista de aplicabilidad de hotfixes de seguridad y compatibilidad de paquetes de servicios de cartera de Contact Center*(disponible en el sitio web de soporte técnico) para ver la lista de revisiones de seguridad de Microsoft aplicables.
- Realice una copia de seguridad de todo el servidor y luego apague todos los servicios de Contact Center antes de aplicar las revisiones de seguridad de Microsoft siguiendo las instrucciones de Microsoft.
- Aplicar las actualizaciones de seguridad de Microsoft en el momento oportuno.

Actualizaciones del sistema operativo

Las actualizaciones del sistema operativo incluyen actualizaciones de servicio y paquetes de servicio.

Actualizaciones de servicio

Dada la cantidad de actualizaciones del servicio de seguridad del sistema operativo y la complejidad inherente a cualquier red, cree un proceso sistemático y responsable para identificar y aplicar el servicio.

actualizaciones Para ayudar a crear dicho proceso, puede seguir una serie de pautas de mejores prácticas, como se documenta en el Boletín especial 800-40 del Instituto Nacional de Estándares y Tecnología (NIST), Procedimientos para el manejo de parches de seguridad.

Este boletín sugiere que si una organización no tiene un grupo central para coordinar el almacenamiento, la evaluación y el registro crónico de las actualizaciones del servicio de seguridad en una biblioteca, los administradores del sistema o el administrador del centro de contacto deben cumplir esta función. Además de estas pautas, siempre que sea posible, siga las recomendaciones de Microsoft con respecto a las vulnerabilidades descubiertas recientemente y que instale de inmediato las actualizaciones del servicio de seguridad de Microsoft.

Siempre que sea posible, Avaya incorpora las recomendaciones de seguridad del sistema operativo y las actualizaciones de servicio más recientes en una estrategia de prueba de soluciones integradas durante cada ciclo de prueba. Sin embargo, debido a la naturaleza urgente de las actualizaciones del servicio de seguridad cuando se descubren vulnerabilidades, siga las pautas de Microsoft a medida que se emiten, incluidos los procedimientos de instalación de Microsoft y los procesos de reversión de actualizaciones del servicio de seguridad.

Finalmente, debe realizar una copia de seguridad completa del sistema antes de actualizar el sistema para asegurarse de que sea posible una reversión, si es necesario. Si una aplicación de Contact Center no funciona correctamente después de aplicar una actualización del servicio de seguridad de Microsoft, debe eliminar la actualización del servicio y volver a la versión anterior de la aplicación (desde la copia de seguridad que realizó antes de aplicar la actualización del servicio). Para mayor seguridad, siempre determine si Avaya verificó la actualización del servicio de Microsoft para compatibilidad con Contact Center Manager.

Para obtener más información acerca de la actualización, consulte la*Lista de compatibilidad de hotfixes de seguridad y compatibilidad de paquetes de servicio de cartera de Contact Center*enhttp://soporte.avaya.com .

paquetes de servicios

Avaya tiene una política para implementar pruebas de co-residencia de todos los paquetes de servicios operativos nuevos para verificar la compatibilidad con el conjunto de aplicaciones de Contact Center tan pronto como estén disponibles. En la práctica, debido a que un paquete de servicio puede contener una cantidad significativa de contenido nuevo, Avaya requiere que espere hasta que se complete la prueba de compatibilidad antes de aplicar el paquete de servicio. Tenga en cuenta que los service packs del sistema operativo generalmente se prueban con el SP de la aplicación Contact Center más reciente y, por lo tanto, una actualización a un nuevo service pack requiere una actualización al SP de Avaya más reciente.

Antes de cargar un nuevo Service Pack, debe realizar una copia de seguridad completa del sistema (para revertir el sistema como en el escenario de actualización).

Importante:

La compatibilidad del Service Pack para todas las aplicaciones de Contact Center está documentada en el*Lista de aplicabilidad de hotfixes de seguridad y compatibilidad de paquetes de servicios de cartera de Contact Center*en el sitio web enhttp://soporte.avaya.com .

Actualizaciones del entorno de tiempo de ejecución de Java

Contact Center solo admite versiones específicas de Java Runtime Environment (JRE). Durante la instalación, Contact Center desactiva las actualizaciones automáticas de JRE en los servidores del centro de contacto.

Importante:

La actualización a una versión no compatible de JRE puede hacer que el centro de contacto deje de funcionar y puede requerir la reinstalación del servidor del centro de contacto.

Compatibilidad con el protocolo de configuración de host dinámico

Aplicaciones de Contact Center (CCMS, CCMA, CCT, CCMM, LM y Avaya Aura®Media Server) no son compatibles con el Protocolo de configuración dinámica de host (DHCP). Todos los servidores de Contact Center deben tener una dirección IP estática.

Los equipos cliente de Agent Desktop admiten direcciones IP estáticas y DHCP.

Requisitos de software de terceros

Debido al procesamiento en tiempo real y de misión crítica que realizan las aplicaciones de Contact Center, no debe instalar ningún otro tipo de software de aplicación en el servidor. Puede instalar cierto software de clase de utilidad en el servidor, siempre que cumpla con las pautas de esta sección.

El software de clase de aplicación generalmente requiere una cierta cantidad de recursos del sistema y no debe instalarse en un servidor que ejecute aplicaciones de Contact Center. La instalación de aplicaciones de terceros puede hacer que las aplicaciones de Contact Center funcionen fuera de los límites de ingeniería conocidos y puede crear posibles problemas desconocidos del sistema (por ejemplo, contenciones de CPU, mayor carga de tráfico de red y degradaciones de acceso al disco).

Ciertas aplicaciones de software de clase de utilidad de terceros, como diagnósticos de hardware o herramientas de copia de seguridad, generalmente requieren menos recursos del sistema durante el funcionamiento normal de las aplicaciones del Contact Center y están permitidas. Las excepciones son las utilidades, como los protectores de pantalla, que pueden causar problemas en el sistema y degradar el rendimiento.

El software antivirus se clasifica como una utilidad y está sujeto a las pautas genéricas de la siguiente sección.

Pautas genéricas para aplicaciones de software de clase de utilidad

Las siguientes son pautas genéricas para el software de clase de utilidad:

- Durante el tiempo de ejecución, la utilidad no debe degradar la aplicación del centro de contacto más allá de un porcentaje promedio de uso de CPU (consulte cada sección específica de la aplicación en este documento para conocer el nivel de uso de CPU máximo recomendado). Además, la utilidad no debe reducir la cantidad mínima de espacio libre en el disco duro requerido por la aplicación del centro de contacto y el sistema operativo Windows.
- La utilidad no debe causar apagados de software inadecuados o apagados fuera de secuencia.
- La empresa de servicios públicos no debe administrar la aplicación del centro de contacto.
- Si la utilidad tiene una base de datos, no debe afectar la base de datos de la aplicación del centro de contacto.
- No se deben utilizar las utilidades de compresión de disco.
- No se deben utilizar las utilidades de ajuste de memoria utilizadas para recuperar la memoria que Microsoft no utiliza.

- La instalación o desinstalación del software de terceros no debe afectar ni entrar en conflicto con la aplicación del centro de contacto (por ejemplo, no debe causar conflictos de DLL). Si se descubren tales conflictos, podría ser necesaria una reconstrucción del servidor.
- El personal de implementación debe realizar pruebas para garantizar que se cumplan estas condiciones y recomendaciones antes de poner en producción la aplicación Contact Center. El personal de soporte puede solicitar los resultados de las pruebas durante el diagnóstico de fallas. Como parte del diagnóstico de fallas, se le puede solicitar al distribuidor o al usuario final que elimine el software de terceros.
- No se debe instalar HyperTerminal en el servidor ya que interfiere con el funcionamiento del Contact Center.

Directrices para el uso de software antivirus

Esta sección describe los requisitos del software antivirus Avaya Contact Center Select.

Avaya Contact Center Select es compatible con los siguientes productos antivirus:

- Antivirus de Symantec
- McAfee

Para obtener más información sobre las consideraciones antivirus de Avaya Contact Center Select y las versiones admitidas, consulte *Guía de referencia de seguridad de Avaya Contact Center Select* disponible en el sitio web de soporte de Avaya en http://soporte.avaya.com .

Puede implementar productos antivirus de otros proveedores sujeto a las siguientes pautas:

- Política de cuarentena de archivos infectados en el servidor y el cliente: el software antivirus se puede configurar para limpiar el virus detectado automáticamente y los archivos se deben poner en cuarentena si no se pueden limpiar los archivos infectados. Comuníquese con Avaya para verificar si el archivo de cuarentena es parte de nuestros archivos de productos o un archivo de sistema dependiente. Si se detecta un virus, elimine el servidor de la red inmediatamente durante la erradicación del virus para evitar una mayor propagación del virus.
- No conecte una plataforma de aplicación del centro de contacto directamente a Internet para descargar definiciones de virus o archivos actualizados. Además, Avaya recomienda que no use una PC cliente de aplicación de centro de contacto para conectarse a Internet. En su lugar, descargue las definiciones de virus y los archivos actualizados a otra ubicación en la red del cliente y cárguelos manualmente desde esta ubicación provisional a la plataforma de la aplicación del centro de contacto.
- Realice los pasos anteriores para descargar los Service Packs (SP) de la aplicación Contact Center. Este método limita el acceso a Internet y, por lo tanto, reduce el riesgo de descargar archivos infectados.
- Escanee todos los archivos SP, DVD-ROM y disquetes antes de cargarlos o instalarlos en el servidor. Esta práctica minimiza cualquier exposición a archivos infectados de fuentes externas.
- Consideraciones de capacidad: la ejecución de un software de detección de virus puede generar una carga adicional en la plataforma de una aplicación del centro de contacto. El personal de implementación debe ejecutar la herramienta de supervisión de rendimiento en el servidor para medir el uso de la CPU. Si la exploración del software antivirus hace que el uso promedio de la CPU de la plataforma supere el porcentaje recomendado durante más de 20 minutos, el software antivirus no debe cargarse en la plataforma de la aplicación del centro de contacto.

Página173 de 3226.

- El Soporte de productos no brinda soporte para la configuración del software antivirus, pero ofrece orientación cuando es posible. Dirija las preguntas o problemas sobre el software antivirus al proveedor adecuado.
- Si se plantean problemas de rendimiento o funcionalidad al personal de soporte de Avaya como parte del diagnóstico de fallas, es posible que se le pida que elimine el software de utilidades o el software antivirus de terceros.

Varias tareas de mantenimiento se activan automáticamente a las 12:00 de la noche. Por lo tanto, debe programar análisis de virus en un momento distinto de la medianoche.

Avaya recomienda que excluya los siguientes archivos y carpetas de los análisis (tanto en tiempo real como programados):

- F:\Avaya\Contact Center\Bases de datos\
- *<unidad de base de datos adicional>*:\Avaya\Centro de contacto\Bases de datos\
- Archivos TSM_OAM ubicados en las siguientes carpetas:
  - D:\Avaya\Contact Center\Manager Server\iccm\bin\data
  - D:\Avaya\Contact Center\Manager server\iccm\data
  - D:\Avaya\Contact Center\Manager Server\iccm\sdm\log
- D:\Avaya\Contact Center\Manager Server\bin\tools2.exeSe producen errores de acceso a archivos en el registro de actividad de análisis si no excluye este archivo del análisis.
- D:\Avaya\Contact Center\Manager Server\iccm\logs (registros SIP)
- D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\ (archivos de configuración de registro SIP)
- D:\Avaya\Contact Center\Componentes comunes\CMF
- D:\Avaya\Contact Center\Manager Administration\Apps\ (incluyendo subdirectorios)
- La carpeta donde almacena Service Packs y parches

Contact Center Multimedia interactúa con un sistema de correo electrónico externo y permite a los agentes enviar archivos adjuntos desde sus computadoras al servidor de Avaya Contact Center Select. Ambos métodos de recuperación de datos son fuentes potenciales de infección de software.

Avaya recomienda las siguientes pautas para el software antivirus:

- El software antivirus debe instalarse en el servidor de correo electrónico para garantizar que los problemas se detecten en el origen.
- Las computadoras de los agentes requieren un software antivirus para garantizar que los archivos adjuntos enviados al servidor de Avaya Contact Center Select no tengan virus. Contact Center Multimedia no bloquea tipos de archivos adjuntos específicos. El software antivirus de terceros debe instalarse en el Portal Server de acuerdo con las pautas de este documento para dichas utilidades.
- Asegúrese de que el software antivirus esté configurado para permitir mensajes de correo electrónico salientes. Por ejemplo, configure el software antivirus McAfee*Protección de acceso*opción de no bloquear *Evite que los gusanos de correo masivo envíen correo*. Como alternativa, agregue el proceso "EmailManager.exe" de Contact Center Multimedia al McAfee*Procesos a excluir*lista.

Excluya la partición de la base de datos de Contact Center Multimedia del análisis.

- Si los cortafuegos en equipos individuales están habilitados en el equipo de Agent Desktop, el detector de informes podría estar marcado como tratando de acceder a Internet. Las propiedades deben configurarse para permitir el acceso de Report Listener a Contact Center Multimedia a través del firewall.
- No debe habilitar Microsoft Updater para la ejecución automática. Microsoft Updater está configurado en el nivel de alerta para que pueda programar actualizaciones para las horas de menor actividad.

Advertencia:

Ejecutar un análisis de virus en la carpeta de archivos adjuntos de Contact Center Multimedia, que contiene miles de archivos, puede usar un tiempo de CPU significativo en un servidor y puede causar una ralentización drástica en los tiempos de respuesta del agente. Avaya recomienda ejecutar análisis, si es necesario, durante las horas de menor actividad.

Para evitar problemas de integridad de la base de datos, Avaya recomienda que excluya todos los archivos CACHE.DAT, los archivos de diario, el archivo cache.cpf y cualquier archivo relacionado con Caché de los análisis antivirus.

El software Caché está instalado en *<Unidad_de_instalación>*:\Avaya\Cache\CacheSys.Las bases de datos y los archivos de diario se instalan en *<Unidad_de_instalación>*:\Avaya\Contact Center\Bases de datos.

Excluya la carpeta de archivos de Caché Journal;G:\Avaya\

Para Avaya Aura®Media Server, debe excluir los siguientes archivos y carpetas de los análisis (tanto en tiempo real como programados):

- D:\Avaya\MAS\Multimedia_Applications\MAS\platdata
- D:\Avaya\MAS\Multimedia_Applications\MAS\common\log

Aura de Avaya®servidor de medios OVA

Aura de Avaya®Media Server es una plataforma de procesamiento de medios basada en software. Implemente Avaya Aura ®Media Server OVA para proporcionar los servicios de conferencia requeridos por Avaya Contact Center Select.

El aura de Avaya®Media Server OVA crea y configura una máquina virtual que contiene Avaya Aura®Software de servidor de medios. La máquina virtual resultante contiene un sistema operativo Linux, una unidad de disco duro, componentes de terceros, configuración del sistema, configuración del firewall y Avaya Aura.® Software de aplicación de servidor de medios.

Puede implementar Avaya Aura®Media Server OVA en el mismo servidor host de VMware que la máquina virtual Avaya Contact Center Select y Avaya WebLM OVA. Como alternativa, puede implementar Avaya Aura®Media Server OVA independiente en un servidor de host VMware independiente.

El aura de Avaya®Media Server OVA contiene información sobre la especificación de la máquina virtual, el sistema operativo y el software de la aplicación. Este OVA contiene los siguientes componentes:

- Red Hat Enterprise Linux 6.x - 64 bits

- Aura de Avaya®Software de servidor multimedia versión 7.8
- Aplicación de archivo de firewall de tablas IP
- Herramientas de VMware. No actualice el software VMware Tools en esta máquina virtual a menos que Avaya se lo indique.

El aura de Avaya®El paquete Media Server OVA tiene la siguiente configuración de hardware predeterminada:

vCPU	Mínimo velocidad de la CPU	Memoria virtual requerido	Número de NIC	Se requiere almacenamiento en disco virtual	
4	2400 MHz	4,5 GB (4608 MB)	1 VMXNET3	Tamaño	50GB
				Implemente Avaya Aura®Media Server OVA usando Thick Provision Lazy Zeroed. Aura de Avaya®Media Server no es compatible con el aprovisionamiento ligero.	

Nota:

Avaya Contact Center Select no es compatible con Avaya Aura®Media Server utilizando esta configuración de implementación predeterminada. Después de implementar Avaya Aura®Media Server OVA, vuelva a configurar la máquina virtual para que tenga 4 u 8 CPU y al menos 8 GB de RAM.

En un entorno virtualizado de Avaya Contact Center Select, puede usar VMware para cargar Avaya Aura®Paquete Media Server OVA en una máquina virtual en su solución de centro de contacto. El servidor virtualizado de Avaya Contact Center Select puede usar el servidor virtualizado de Avaya Aura®Media Server como procesador de medios de voz.

Implemente Avaya Aura®Media Server OVA usando formato de disco - Aprovisionamiento grueso Lazy Zeroed. Aura de Avaya®Media Server no es compatible con el aprovisionamiento ligero.

Avaya WebLM OVA

Implemente Avaya WebLM versión 7.1 OVA para proporcionar licencias de soluciones. Puede implementar Avaya WebLM OVA en el mismo servidor host de VMware que la máquina virtual Avaya Contact Center Select y Avaya Aura®Servidor multimedia OVA. Como alternativa, también puede implementar Avaya WebLM OVA independiente en un servidor host de VMware independiente.

Cada Avaya Contact Center Select admite un servidor de administrador de licencias WebLM. Cada servidor del administrador de licencias de WebLM admite un Avaya Contact Center Select. Para una mayor eficiencia y flexibilidad, el administrador de licencias de WebLM es compatible con los mecanismos de implementación VMware Virtual Appliance y Open Virtualization Archive (OVA). En un entorno virtualizado de Avaya Contact Center Select, puede usar VMware para cargar el paquete WebLM OVA en una máquina virtual separada en su solución de centro de contacto. El servidor virtualizado de Avaya Contact Center Select puede usar el servidor WebLM virtualizado como administrador de licencias.

WebLM OVA contiene un sistema operativo Linux reforzado.

Avaya WebLM OVA requiere lo siguiente:

Página176 de 3226.

vCPU	Velocidad mínima de la CPU	Memoria virtual reserva	Número de NIC	Almacenamiento en disco virtual reserva
1	—	2GB	1 compartido	35GB

Nota:

No cambie ninguna de estas configuraciones de máquina virtual Avaya WebLM OVA

VMware. WebLM OVA utiliza la siguiente asignación de red:

Interfaz de máquina virtual del servidor WebLM	Solicitud
Eth0	Gestión de licencias

El servidor WebLM para VMware se empaqueta como un dispositivo virtual listo para su implementación mediante VMware vSphere Client o VMware vCenter.

Implemente el OVA de WebLM mediante el formato de disco - Aprovisionamiento grueso Lazy Zeroed. WebLM no admite el aprovisionamiento ligero en entornos de producción.

Especificaciones y creación de perfiles del servidor host de VMware

Esta sección especifica los recursos de VMware necesarios para admitir el dispositivo de software Avaya Contact Center Select para varios tamaños de solución. El dispositivo de software Avaya Contact Center Select (ACCS) consta de los siguientes componentes:

- Máquina virtual Avaya Contact Center Select
- Aura de Avaya®servidor de medios OVA
- Avaya WebLM OVA

Avaya Contact Center Select, Avaya Aura®Las máquinas virtuales Media Server y Avaya WebLM son compatibles con un solo host de VMware o en hosts de VMware separados.

Especificación mínima de CPU del servidor host de VMware

Configure cada máquina virtual de VMware con los recursos de la CPU para admitir un componente de dispositivo de software ACCS. Para cada máquina virtual y número de agentes necesarios, configure una cantidad específica de núcleos de vCPU y reservas de CPU en MHz. Cada núcleo de vCPU debe tener un núcleo de CPU físico subyacente correspondiente en el host de VMware. El rendimiento de cada núcleo de CPU físico y el núcleo de vCPU correspondiente está determinado por el hardware y el procesador del servidor de VMware.

La creación de perfiles de ACCS VMware utiliza una CPU Intel Xeon E5-2670 de 2,60 GHz de doble núcleo como CPU de referencia. Este procesador de referencia tiene 16 núcleos de CPU físicos. Cada uno de estos 16 núcleos tiene un valor de referencia individual que es un dieciseisavo de la puntuación de referencia general del procesador de referencia. Utilice este valor de referencia de núcleo individual para comparar los núcleos de diferentes procesadores y seleccionar el hardware de host de VMware adecuado para la virtualización de ACCS.

El valor de referencia del núcleo individual para el procesador en su servidor host de VMware debe ser igual o superior al 90 % del valor de referencia del núcleo individual para el procesador de referencia ACCS.

Siga estos pasos para asegurarse de que las CPU host de VMware propuestas cumplan con los requisitos mínimos de ACCS.

- Utilizando elhttps://cpubenchmark.net sitio web, determine el valor de referencia del núcleo individual para la CPU de referencia: Intel Xeon E5-2670 dual de 8 núcleos a 2,60 GHz.

  Valor de referencia de núcleo individual de referencia = (Referencia de referencia de CPU del sitio web/ Número de núcleos en la CPU de referencia)
- Utilizando elhttps://cpubenchmark.net sitio web, determine el valor de referencia central individual para la CPU del servidor host de VMware.

  Valor de referencia de núcleo individual = (la referencia de CPU de su servidor host del sitio web/Número de núcleos en la CPU del servidor host)
- Para admitir la virtualización de ACCS, el valor de referencia del núcleo individual de su host VMware debe ser igual o superior al 90 % del valor de referencia del núcleo individual de referencia.

Para admitir un componente de dispositivo de software de Avaya Contact Center Select, su host VMware debe tener una cantidad suficiente de núcleos de CPU, cada uno con al menos el valor de referencia de núcleo individual mínimo.

Recursos mínimos del servidor host de VMware

Utilice las siguientes tablas para determinar los recursos mínimos de VMware necesarios para admitir una variedad de recuentos de agentes y tasas de contacto del sistema.

Tabla 3: Requisitos de recursos de VMware de la máquina virtual de Avaya Contact Center Select

Número máximo de agentes admitidos	**250**	**400**
Tasa máxima de contacto del sistema (contactos del sistema por hora)	**5000**	**8000**
Tasa de contacto de correo electrónico (correos electrónicos por hora)	750	750
Tasa de contacto de WebChat (WebChats por hora)	375	375
Número de CPU (velocidad de reloj de CPU mínima 2400 MHz)	4	6
Reserva de CPU (MHz)	9560	14340
RAM mínima (GB)	dieciséis	dieciséis
Reserva mínima de RAM (MB)	16384	16384
Tamaño mínimo de disco (GB): aprovisionamiento perezoso grueso	641	641
Tarjetas de interfaz de red virtual (1 GB) VMXNET3	1	1

Nota 1: La tasa de contacto del sistema es la tasa de contacto combinada máxima total en todos los tipos de contacto admitidos.

Nota 2: Las tarifas de contacto multimedia son aplicables solo si la multimedia es parte de la solución. Contactos de correo electrónico por hora (Eph). Chats web estándar por hora (WCph). La capacidad máxima del chat web estándar se basa en una duración promedio de chat de 5 minutos. El número máximo de sesiones simultáneas de Web Chat es 50.

Tabla 4: Avaya Aura®Requisitos de recursos de VMware de la máquina virtual del servidor de medios

Número máximo de agentes admitidos	**200**	**400**
Máximo de sesiones admitidas	**500**	**1000**
Número de CPU (velocidad de reloj de CPU mínima 2400 MHz)	4	8
Reserva de CPU (MHz)	9560	19120
RAM mínima (GB)	8	8
Reserva mínima de RAM (MB)	8192	8192
Tamaño mínimo de disco (GB): aprovisionamiento perezoso grueso	50	50
Tarjetas de interfaz de red virtual (1 GB) VMXNET3	1	1

Aura de Avaya®Media Server solo es compatible con máquinas virtuales con 4 u 8 CPU.

Tabla 5: Requisitos de recursos de VMware de la máquina virtual Avaya WebLM

Máximo de solicitudes de licencia admitidas	**5000**
Número de CPU (velocidad de reloj de CPU mínima 2300 MHz)	1
Reserva de CPU (MHz)	2290
RAM mínima (GB)	2
Reserva mínima de RAM (MB)	2048
Tamaño mínimo de disco (GB)	35
Tarjetas de interfaz de red virtual (1 GB) VMXNET3	1

Supervisión y gestión de recursos del servidor host de VMware

Cuando el dispositivo de software Avaya Contact Center Select esté virtualizado y puesto en marcha, continúe monitoreando y administrando sus recursos de VMware en tiempo real.

- El servidor host de VMware no debe estar sobreasignado. La cantidad total de CPU virtuales asignadas en todas las máquinas virtuales debe ser menor que el número de núcleos físicos del host.
- Los requisitos de recursos de CPU virtual (vCPU) se refieren solo a los núcleos físicos y no a los núcleos lógicos asociados con Hyper-Threading.
- Asegúrese de que VMware Tools esté instalado en todas las máquinas virtuales. Esto es necesario para la compatibilidad con VMXNET3 y la supervisión y gestión del rendimiento de VMware.
- 16 GB de RAM es el espacio mínimo de RAM para implementaciones con un número reducido de agentes. Según los requisitos de su solución, su máquina virtual ACCS podría necesitar 20 GB de RAM.
- Si el uso promedio total de la CPU supera el 50 % durante períodos sostenidos, agregue recursos de CPU adicionales a la máquina virtual de Contact Center.
- Si el monitoreo de la máquina virtual del dispositivo de software ACCS indica escasez de recursos, agregue recursos adicionales según sea necesario.
- Según la complejidad de las llamadas de su solución, es posible que deba agregar recursos de VMware adicionales según sea necesario.

Página179 de 3226.

- Según los requisitos de generación de informes y administración de su solución, es posible que deba agregar recursos de VMware adicionales según sea necesario. Avaya recomienda ejecutar informes grandes o complejos durante las horas de menor actividad.
- La cifra mínima de Reserva de CPU (MHz) se basa en la velocidad de reloj mínima admitida. Para reservar completamente cada CPU, reserve la cantidad de CPU multiplicada por la velocidad de reloj central del host de virtualización.
- Los recuentos de agentes admitidos y el procesamiento de contactos asociado se modelan utilizando un procesamiento de contactos simple con informes y administración moderados.

Ayuda laboral

La especificación del servidor PVI de gama alta de Avaya Contact Center Select (consulteEspecificación de servidor de gama alta en la página 68), configurado como un host de VMware, puede admitir el dispositivo de software Avaya Contact Center Select hasta la cantidad máxima de agentes y la tasa de contacto del sistema.

Ejemplos de creación de perfiles de VMware

Esta sección proporciona algunos ejemplos prácticos de creación de perfiles de soluciones ACCS para la virtualización mediante VMware.

Ejemplo 1

Una solución ACCS es admitir 230 agentes a una tasa de llamadas de 4600 contactos de voz por hora.

Utilizando las tablas de la**Recursos mínimos del servidor host de VMware**sección, calcule el número mínimo de CPU. La siguiente tabla especifica la cantidad mínima de CPU de VMware para esta solución de ejemplo.

Máquina virtual	CPU
máquina virtual ACCS	4
máquina virtual AAMS	8
Máquina virtual WebLM	1
Total de dispositivos de software ACCS:	**13**
Hipervisor ESXi	1
Mínimo de host ESXi:	**14**

El número mínimo de núcleos de CPU necesarios es 14 en total. Esto significa que el host de VMware debe tener al menos una CPU dual de 8 núcleos (16 núcleos físicos). Cada uno de estos núcleos de CPU debe tener un valor de referencia de núcleo individual igual o superior al 90 % del valor de referencia de núcleo individual para el procesador de referencia ACCS.

El siguiente paso es determinar si una CPU de servidor propuesta es adecuada.

- Utilizando elhttps://cpubenchmark.net sitio web, determine el valor de referencia del núcleo individual para el procesador de referencia ACCS: Intel Xeon E5-2670 dual de 8 núcleos a 2,60 GHz.

  Valor de referencia del núcleo individual de referencia = (Referencia del procesador de referencia del sitio web/Número de núcleos en la CPU de referencia)

  Por ejemplo:

Página180 de 3226.

Uso de la CPU Intel Xeon E5-2670 de 2,60 GHz dual de 8 núcleos de referencia

La CPU dual de 8 núcleos de referencia tiene un puntaje de referencia de, por ejemplo, 18653.

Valor de referencia de núcleo individual de referencia = (18653 / 16)

Valor de referencia básico individual de referencia = 1165 90 % del valor

de referencia básico individual de referencia = 1050

- Utilizando elhttps://cpubenchmark.net sitio web, determine el valor de referencia central individual para el procesador de servidor host de VMware propuesto.

  Valor de referencia del núcleo individual = (La referencia del procesador del servidor host del sitio web/Número de núcleos en el procesador del servidor host)

  Por ejemplo:

  Usando un procesador Intel Xeon E5-2640 v3 de 8 núcleos dual propuesto a 2,60 GHz. La

  CPU dual de 8 núcleos tiene una puntuación de referencia de, por ejemplo, 20885. Valor

  de referencia de núcleo individual = (20885 / 16)

  Valor de referencia central individual = 1305

  1305 > 1050, por lo que el Intel Xeon E5-2640 v3 2,60 GHz dual de 8 núcleos propuesto es adecuado. La

siguiente tabla enumera los recursos mínimos totales necesarios para esta solución de ejemplo.

Máquina virtual	CPU	RAM mínima	Tamaño mínimo de disco
máquina virtual ACCS	4	16 GB	641 GB
máquina virtual AAMS	8	8GB	50GB
Máquina virtual WebLM	1	2GB	35GB
Recursos mínimos del dispositivo de software ACCS:	13	26GB	726GB

Ejemplo 2

Una solución ACCS es admitir 50 agentes a una tasa de llamadas de 1000 contactos de voz por hora.

Utilizando las tablas de la**Recursos mínimos del servidor host de VMware**sección, calcule el número mínimo de CPU. La siguiente tabla especifica la cantidad mínima de CPU de VMware para esta solución de ejemplo.

Máquina virtual	CPU
máquina virtual ACCS	4
máquina virtual AAMS	4
Máquina virtual WebLM	1
Total de dispositivos de software ACCS:	**9**
Hipervisor ESXi	1
Mínimo de host ESXi:	**10**

El número mínimo de núcleos de CPU necesarios es 10 en total. Esto significa que el host de VMware debe tener al menos una CPU dual de 6 núcleos (12 núcleos físicos).

Página181 de 3226.

Cada uno de estos núcleos de CPU debe tener un valor de referencia de núcleo individual igual o superior al 90 % del valor de referencia de núcleo individual para el procesador de referencia ACCS.

El siguiente paso es determinar si una CPU de servidor propuesta es adecuada.

- Utilizando elhttps://cpubenchmark.net sitio web, determine el valor de referencia del núcleo individual para el procesador de referencia ACCS: Intel Xeon E5-2670 dual de 8 núcleos a 2,60 GHz.

  Valor de referencia del núcleo individual de referencia = (Referencia del procesador de referencia del sitio web/Número de núcleos en la CPU de referencia)

  Por ejemplo:

  Uso de la CPU Intel Xeon E5-2670 de 2,60 GHz dual de 8 núcleos de referencia

  La CPU dual de 8 núcleos de referencia tiene un puntaje de referencia de, por ejemplo, 18653.

  Valor de referencia de núcleo individual de referencia = (18653 / 16)

  Valor de referencia central individual de referencia = 1165

  90% del valor de referencia del núcleo individual de referencia = 1050

- Utilizando elhttps://cpubenchmark.net sitio web, determine el valor de referencia central individual para el procesador de servidor host de VMware propuesto.

  Valor de referencia del núcleo individual = (La referencia del procesador del servidor host del sitio web/Número de núcleos en el procesador del servidor host)

  Por ejemplo:

  Usando un Intel Xeon X5690 de 6 núcleos dual propuesto a 3,47 GHz

  La CPU dual de 6 núcleos tiene una puntuación de referencia de, por ejemplo, 9239.

  Valor de referencia de núcleo individual = (14363 / 12)

  Valor de referencia central individual = 1197

  1197> 1050, por lo que la CPU Dual de 6 núcleos propuesta es adecuada.

La siguiente tabla enumera los recursos mínimos totales necesarios para esta solución de ejemplo.

Máquina virtual	CPU	RAM mínima	Tamaño mínimo de disco
máquina virtual ACCS	4	16 GB	641 GB
máquina virtual AAMS	4	8GB	50GB
Máquina virtual WebLM	1	2GB	35GB
Recursos mínimos del dispositivo de software ACCS:	9	26GB	726GB

Consideraciones de virtualización

El uso de la virtualización en una solución empresarial de centro de contacto requiere una cuidadosa planificación, ingeniería e implementación por adelantado. Si bien las ventajas técnicas y comerciales son claras, la virtualización impone consideraciones adicionales al diseñar la solución del centro de contacto

Página182 de 3226.

arquitectura. El aislamiento ambiental permite que varios sistemas operativos se ejecuten en la misma máquina host de VMware. Si bien la virtualización ofrece estas formas de aislamiento, los entornos de virtualización no brindan aislamiento de rendimiento. El comportamiento de una máquina virtual puede afectar negativamente el rendimiento de otra máquina virtual en el mismo host. La mayoría de los entornos de virtualización modernos proporcionan mecanismos que puede utilizar para detectar y reducir la interferencia en el rendimiento. Debe diseñar cuidadosamente su solución de centro de contacto virtualizado para evitar interferencias en el rendimiento.

Si planea instalar aplicaciones de software que no sean de Contact Center en los otros invitados de un servidor host con Contact Center instalado, debe analizar cuidadosamente el impacto de estas aplicaciones en la solución de Contact Center y proporcionar un aislamiento de rendimiento adicional para salvaguardar la funcionalidad de Contact Center.

Importante:

Implemente Contact Center en un entorno virtual de nivel empresarial con el hardware más reciente que admita la virtualización asistida por hardware. Avaya recomienda que aplique la planificación, la ingeniería y la implementación de la virtualización con soporte organizacional completo para la virtualización en lugar de hacer crecer orgánicamente una infraestructura de virtualización.

Funciones de VMware

Avaya Contact Center Select es una colección de aplicaciones en tiempo real que se ejecutan en el sistema operativo MS Windows Server 2012 R2. Avaya Contact Center Select proporciona control de llamadas en tiempo real, gestión multimedia e informes estadísticos.

Aura de Avaya®Media Server es una aplicación de procesamiento de medios en tiempo real que se ejecuta en el sistema operativo Red Hat Enterprise Linux (RHEL). Aura de Avaya®Media Server proporciona capacidades de procesamiento de medios y conferencias en tiempo real para Avaya Contact Center Select.

Algunas características de VMware requieren CPU, E/S de disco o recursos de red para funcionar. La ejecución de estas funciones de VMware puede causar limitaciones de recursos y afectar el rendimiento en tiempo real de Avaya Contact Center Select y Avaya Aura.®Máquinas virtuales de servidor de medios (VM). Por lo tanto, estas funciones no son compatibles mientras Avaya Contact Center Select o Avaya Aura®El servidor multimedia está activo.

Algunas funciones de VMware no son compatibles con Avaya Contact Center Select o Avaya Aura®Servidor multimedia. Algunas otras funciones de VMware son compatibles solo mientras Avaya Contact Center Select o Avaya Aura®Las máquinas virtuales del servidor de medios se detienen por mantenimiento.

La siguiente tabla muestra Avaya Contact Center Select y Avaya Aura®Nivel de soporte de Media Server para funciones de VMware.

Característica de VMware	Compatible con Avaya activo Contacto Seleccionar centro máquina virtual	Apoyado durante Contacto Avaya Máquina virtual de selección central mantenimiento ventana	Compatible con Avaya activo Aura®Medios de comunicación Máquina virtual del servidor	Apoyado durante Aura de Avaya® Máquina virtual del servidor de medios mantenimiento ventana
Clonación	No	Sí	No	No
Potencia Distribuida Gestión (DPM)	No	Sí	No	Sí
Recursos distribuidos Programador (DRS)	No	Sí	No	Sí
Conmutador distribuido	Sí	Sí	Sí	Sí
Tolerancia a fallos	No	No	No	No
Alta disponibilidad (HA)	No	No	No	No
Instantáneas	No	Ver Contacto Avaya Seleccionar centro Instantánea de VMware consideraciones en página 104	No	Ver Aura de Avaya Servidor multimedia Instantánea de VMware consideraciones en página 105
DRS de almacenamiento	No	Sí	No	Sí
Almacenamiento delgado Aprovisionamiento	No	N / A	No	N / A
Almacenamiento vMotion	No	Sí	No	Sí
Suspender y reanudar	No	N / A	No	N / A
vMotion	No	Sí	No	No

Consideraciones sobre el host de VMware vSphere

Al planificar máquinas virtuales (invitados) en su sistema host, los recursos totales que necesitan las máquinas virtuales que se ejecutan en el servidor host no deben exceder la capacidad total del host. Es una buena práctica no comprometer los recursos de memoria y CPU en el host. Si la capacidad de la CPU del host está sobrecargada, Contact Center no funciona correctamente.

Importante:

Avaya Contact Center Select no es compatible con un host comprometido en exceso donde los recursos virtuales totales de todas las máquinas virtuales alojadas superan los recursos físicos del host.

Virtualización asistida por hardware

Los procesadores de nivel empresarial más recientes de Intel admiten la virtualización. Hay dos generaciones de soporte de virtualización: la primera generación introdujo la virtualización de CPU; la segunda generación incluyó virtualización de CPU y virtualización de unidad de administración de memoria (MMU) agregada. Para obtener el mejor rendimiento, asegúrese de que su sistema utilice procesadores con al menos funciones de asistencia de hardware de segunda generación.

Página184 de 3226.

Sistema de archivos de máquina virtual (VMFS)

Las instantáneas y las máquinas virtuales de VMware se almacenan en un almacén de datos del sistema de archivos de máquina virtual (VMFS). Para admitir Avaya Contact Center Select en una máquina virtual, el almacén de datos de VMware que contiene Contact Center debe ser VMFS 5.54 o posterior. Si actualiza un servidor host de VMware existente, asegúrese de que el almacén de datos asociado esté actualizado a VMFS 5.54 o posterior.

Virtualización de CPU asistida por hardware (Intel VT-x)

La primera generación de asistencia de virtualización de hardware incluye VT-x de Intel. Estas tecnologías atrapan automáticamente las interrupciones sensibles, eliminando la sobrecarga requerida para hacerlo en el software. Esto permite el uso de un monitor de máquina virtual (VMM) de virtualización de hardware (HV).

Virtualización de MMU asistida por hardware (Intel EPT)

Los procesadores de nivel empresarial más recientes también incluyen una función que aborda los gastos generales debido a la virtualización de la unidad de administración de memoria (MMU) al proporcionar soporte de hardware para virtualizar la MMU. VMware vSphere es compatible con esta función en los procesadores Intel, donde se denomina Tablas de páginas extendidas (EPT).

Red de área de almacenamiento (SAN)

Una red de área de almacenamiento (SAN) es una red de almacenamiento dedicada que proporciona acceso al almacenamiento de nivel de bloque consolidado. Las SAN se utilizan para hacer que los dispositivos de almacenamiento, como las matrices de discos, sean accesibles para los servidores, de modo que los dispositivos aparezcan como conectados localmente al sistema operativo.

Cuando Avaya Contact Center Select está instalado en máquinas virtuales, admite una SAN. Debe monitorear la demanda del Contact Center en el dispositivo de almacenamiento SAN. Cumpla con las recomendaciones de configuración de SAN específicas de su proveedor para garantizar que el dispositivo de almacenamiento SAN satisfaga las demandas de Contact Center.

Aprovisionamiento de unidades de disco

Aprovisione suficiente espacio en el disco duro en el servidor host para admitir todas las máquinas virtuales invitadas, una biblioteca ISO y aprovisione espacio adicional para el almacenamiento de imágenes de instantáneas.

Configuración de rendimiento y firmware del servidor

El sistema básico de entrada y salida (BIOS) de un servidor configura los componentes de hardware y arranca el sistema operativo desde un dispositivo de almacenamiento. El sistema operativo (SO) del servidor luego usa el BIOS para controlar el hardware del servidor. Debe configurar los ajustes del BIOS del servidor para garantizar un rendimiento óptimo del hardware del servidor subyacente. Para la mayoría de las configuraciones del BIOS, debe elegir entre optimizar un servidor para ahorrar energía o para el rendimiento del servidor. Para aplicaciones en tiempo real como Avaya Contact Center Select, siempre debe elegir la configuración del BIOS del servidor que garantice el rendimiento óptimo del hardware del servidor subyacente.

Los fabricantes de servidores proporcionan sus propias placas base, BIOS, hardware y firmware. Determinar la configuración del BIOS para el hardware de su servidor puede ser un desafío. Hay varias configuraciones de BIOS que pueden afectar significativamente el rendimiento del sistema. Al optimizar el rendimiento del sistema, debe seleccionar la configuración del BIOS que mejore el rendimiento del sistema sobre aquellas que contribuyen al ahorro de energía. Otras configuraciones y recomendaciones del BIOS no son tan

Traducido del inglés al español - www.onlinedoctranslator.com

directo. Comience consultando los datos técnicos del fabricante de su servidor. Avaya recomienda que luego pruebe su solución para tomar las mejores decisiones de configuración del BIOS.

Configure el hardware del servidor, el firmware y la configuración del sistema operativo para seleccionar el rendimiento del sistema sobre el ahorro de energía.

Firmware del servidor

El firmware es un programa informático que se almacena en la placa base del servidor o en un controlador de hardware adicional. El firmware almacenado en la placa base del servidor se denomina Sistema básico de entrada y salida (BIOS). El BIOS es responsable del comportamiento del sistema cuando se enciende por primera vez y de pasar el control del servidor al sistema operativo. El firmware también se almacena en componentes de hardware como los controladores Redundant Array of Independent Disks (RAID).

Consulte periódicamente los datos técnicos del fabricante de sus servidores y, en su caso, aplique las actualizaciones más recientes de BIOS y firmware. Los pasos necesarios para actualizar el firmware o el BIOS de un sistema varían según el proveedor de hardware y el componente que se va a actualizar. Normalmente, el fabricante proporciona una utilidad de actualización de firmware. Mantener el BIOS y el firmware de su servidor en un nivel compatible puede mejorar la confiabilidad, la capacidad de servicio y ayudar a garantizar un rendimiento óptimo.

Gestión de potencia y rendimiento

Para aplicaciones en tiempo real como Avaya Contact Center Select, siempre debe seleccionar la configuración de hardware, BIOS, firmware y sistema operativo que mejore el rendimiento del sistema sobre aquellas que contribuyen al ahorro de energía.

Las CPU Intel Xeon ofrecen dos opciones principales de administración de energía: C-states e Intel Turbo Boost.

- La desactivación de los estados C reduce las latencias para activar las CPU desde estados detenidos o inactivos hasta el encendido completo.
- Intel Turbo Boost aumenta la frecuencia interna del procesador si la carga de trabajo requiere más potencia.

Esta configuración depende de la marca y el modelo del OEM del servidor. La terminología de los parámetros del BIOS para los servidores Dell y HP actuales se describe a continuación. Otras marcas y modelos de servidores pueden tener otra terminología pero configuraciones de BIOS equivalentes.

Las siguientes son las configuraciones de BIOS recomendadas para los servidores Dell PowerEdge:

- Establezca el Modo de administración de energía en Máximo rendimiento.
- Establezca el Modo de administración de rendimiento y energía de la CPU en Rendimiento máximo.
- Configuración del procesador: establece el Modo Turbo en habilitado
- Configuración del procesador: establece C States en deshabilitado

Las siguientes son las configuraciones de BIOS recomendadas para los servidores HP ProLiant:

- Establezca el modo de regulador de potencia en modo estático alto.
- Deshabilitar la compatibilidad con el estado C del procesador
- Deshabilitar la compatibilidad con el procesador C1E

Página186 de 3226.

- Deshabilitar la administración de energía de QPI
- Habilitar Intel Turbo Boost

Configure el hardware del servidor, el firmware y la configuración del sistema operativo para seleccionar el rendimiento del sistema sobre el ahorro de energía.

Caché de disco y RAID

Las unidades de disco duro utilizan la memoria caché para mejorar el acceso de lectura y escritura a las unidades de disco. En el almacenamiento en caché del modo de reescritura, el disco o el controlador RAID escribe datos del servidor en la memoria caché y reconoce la finalización de la escritura en el servidor. El servidor puede realizar otras tareas mientras el controlador de disco transfiere los datos de la memoria caché de escritura a las unidades de disco. Este enfoque aumenta significativamente el rendimiento de escritura.

Avaya Contact Center Select admite hardware RAID-1, RAID-5 y RAID-10. La tecnología RAID proporciona redundancia de datos de disco, así como detección y corrección de errores. Para obtener la máxima seguridad y soluciones de misión crítica, Avaya recomienda que todos los servidores de Contact Center contengan un controlador RAID. Hardware RAID-1, RAID-5 y RAID-10 son los únicos niveles y tipos de RAID admitidos.

Lea la documentación del hardware de su servidor para determinar cómo configurar el almacenamiento en caché del disco. Por lo general, el almacenamiento en caché del disco se puede configurar como una configuración del BIOS, una configuración de RAID, una configuración de la controladora RAID o como una configuración del sistema operativo. Algunos controladores RAID exponen la capacidad de manipular la política de almacenamiento en caché a través del sistema operativo y, por lo tanto, la configuración del nivel del sistema operativo puede anular la configuración del nivel del BIOS. Consulte la documentación de su hardware para obtener más información sobre la configuración del almacenamiento en caché del disco. Avaya Contact Center Select no es compatible con el almacenamiento en caché de disco a nivel del sistema operativo, el almacenamiento en caché de disco de software o RAID de software. Avaya Contact Center Select requiere almacenamiento en caché RAID de hardware respaldado por batería para evitar la pérdida de datos y la posible corrupción de la base de datos en caso de corte de energía.

Memoria y arquitectura de memoria no uniforme

El acceso a memoria no uniforme (NUMA) es un diseño de memoria de computadora que se utiliza en el multiprocesamiento, donde el tiempo de acceso a la memoria depende de la ubicación de la memoria en relación con el procesador. Con NUMA, un procesador puede acceder a su propia memoria local más rápido que a la memoria no local (memoria local a otro procesador o memoria compartida entre procesadores). Para Avaya Contact Center Select, el servidor debe admitir e implementar NUMA.

En la configuración del BIOS del servidor, configure el modo de funcionamiento de la memoria para optimizar el rendimiento y desactive la intercalación de nodos. Por ejemplo, para un servidor Dell, configure el "Modo operativo de memoria" como "Modo optimizador" y configure "Entrelazado de nodos" como "Deshabilitado". Consulte la documentación de su hardware para obtener más información sobre NUMA y el rendimiento de la memoria.

Gestión del rendimiento y VMware

Para los servidores host de VMware, para permitir que el kernel de VMware controle el ahorro de energía de la CPU mientras maximiza el rendimiento del servidor cuando sea necesario, es posible configurar la administración de energía en el BIOS en "Modo de control del sistema operativo". Entonces, el hipervisor de VMware puede proporcionar un rendimiento y una administración de energía equilibrados. Esta combinación de configuración de BIOS y función de VMware no cumple con los requisitos de rendimiento en tiempo real de Avaya Contact Center Select. Avaya Contact Center Select no es compatible con la configuración del "Modo de control del sistema operativo" del BIOS o sus equivalentes.

Tecnología de virtualización

Cuando la tecnología de virtualización está habilitada, el BIOS habilita las funciones de virtualización del procesador y brinda soporte de virtualización al sistema operativo a través de la tabla DMAR. En general, solo los entornos virtualizados como VMware aprovechan estas funciones.

Para los servidores host de VMware, habilite todas las opciones de tecnología de virtualización disponibles en el BIOS del hardware. Para hosts basados en Intel: habilite la virtualización de Intel (VT-x) y, si está disponible, habilite las tablas de páginas extendidas (EPT). La configuración de virtualización disponible varía según el proveedor de hardware y la versión del BIOS. Lea los documentos de su proveedor de hardware que cubren el soporte de virtualización para determinar qué ajustes configurar.

Hyper-Threading

Hyper-Threading es la tecnología patentada de Intel para aumentar la potencia computacional paralela (procesador multitarea) al permitir que el sistema operativo (SO) vea y aborde cada núcleo de procesador físico como si fueran dos procesadores virtuales. También permite que el sistema operativo y las aplicaciones compartan el trabajo entre esos procesadores virtuales siempre que sea posible, haciendo así un uso completo de los recursos disponibles.

Habilite Hyper-Threading en el servidor de Avaya Contact Center Select.

Dispositivos de hardware no utilizados

En el servidor, desconecte o deshabilite los dispositivos de hardware físicos innecesarios y no utilizados, como: puertos COM, puertos LPT, controladores USB, interfaces de red y controladores de almacenamiento. Debe conservar algunos dispositivos USB para el mouse y el teclado. La desactivación de dispositivos de hardware innecesarios mejora el rendimiento y la seguridad del servidor. Consulte los datos técnicos del fabricante de sus servidores para obtener información sobre cómo deshabilitar los dispositivos de hardware no utilizados en el BIOS.

Resumen

Para aplicaciones en tiempo real como Avaya Contact Center Select, elija la configuración del BIOS del servidor que optimice el rendimiento en lugar del ahorro de energía. Comience consultando los datos técnicos del fabricante de su servidor. Avaya recomienda que luego pruebe su solución para tomar las mejores decisiones de configuración del BIOS. Avaya recomienda habilitar CPU Hyper-Threading. Al habilitar opciones de BIOS como CPU Prefetchers y CPU Hyper-Threading, el rendimiento del sistema se puede mejorar de manera efectiva. Al ajustar la configuración del BIOS del sistema para el rendimiento, debe tener en cuenta las diversas opciones de procesador y memoria. Experimente con otras opciones para encontrar la configuración óptima para su solución específica de hardware y Contact Center.

Configure el hardware del servidor, el BIOS, el firmware y los ajustes del sistema operativo para seleccionar el rendimiento del sistema sobre el ahorro de energía.

Prácticas recomendadas de redes de VMware

Hay muchas formas diferentes de configurar la red en un entorno de VMware. Revise la documentación de mejores prácticas de redes de VMware antes de implementar aplicaciones de Avaya en un

host ESXi. Esta sección no reemplaza la documentación de VMware. Para mejorar el rendimiento y las mejores prácticas, Contact Center utiliza el adaptador de red tipo VMXNET 3.

Las siguientes son algunas de las mejores prácticas de redes sugeridas:

- Separar los servicios de red para lograr una mayor seguridad y rendimiento. Crear una vSphere *Interruptor estándar*con NIC dedicadas para cada servicio. Separe VMware Management, iSCSI (tráfico SAN) y redes de VM para separar NIC físicas. Si no es posible cambiar por separado, considere grupos de puertos con ID de VLAN diferentes.
- Todas las NIC físicas que están conectadas al mismo vSphere*Interruptor estándar*debe estar conectado a la misma red física.
- Configure todas las vNIC de VMkernal en la misma MTU (unidad de transmisión máxima de IP).
- Configure Contact Center para usar el adaptador de red tipo VMXNET 3.

Para obtener más información sobre las mejores prácticas de redes de VMware, consulte la documentación de VMware.

Consideraciones sobre la instantánea de Avaya Contact Center Select VMware

Las instantáneas de VMware guardan el estado actual de la máquina virtual para que pueda volver a ella en cualquier momento. Las instantáneas son útiles cuando necesita revertir una máquina virtual repetidamente al mismo estado, pero no desea crear varias máquinas virtuales.

Las siguientes consideraciones se aplican al usar instantáneas con Avaya Contact Center Select en VMware:

- Las instantáneas se deben tomar durante una ventana de mantenimiento de Avaya Contact Center Select. No tome una instantánea de una máquina virtual de Contact Center mientras se está ejecutando Contact Center. Las instantáneas tienen un impacto negativo en el rendimiento de una máquina virtual a lo largo del tiempo. Debe Eliminar todas las instantáneas al final de la ventana de mantenimiento y*Consolidar*instantáneas si es necesario, antes de volver a poner en producción la máquina virtual de Contact Center. Para obtener más información sobre la consolidación de instantáneas, consulte la documentación de VMware. Antes de tomar la instantánea, apague todos los servicios del Contact Center y detenga la instancia de la base de datos de Caché usando Caché Cube.
- Cree una instantánea para las máquinas virtuales de Contact Center al mismo tiempo. Del mismo modo, cuando restaure una instantánea, restaure todas las instantáneas para asegurarse de que los datos sean coherentes en todo el conjunto de Contact Center.
- Al restaurar instantáneas, considere detenidamente el posible impacto de las definiciones de antivirus desactualizadas, las actualizaciones de seguridad y del sistema operativo Microsoft Windows perdidas y las cuentas de dominio caducadas en el centro de contacto. Aísle la máquina virtual restaurada hasta que se resuelvan estos problemas.
- De forma predeterminada, la contraseña de una cuenta de máquina de Windows Server 2012 R2 se cambia cada 30 días. Esta es una consideración importante al volver a una instantánea de una máquina virtual que ha estado en uso durante más de 30 días, ya que puede hacer que la máquina pierda su conexión con el dominio de Windows. Si ocurre este problema, vuelva a unir la máquina virtual de Windows Server 2012 R2 al dominio.

Las instantáneas de VMware no reemplazan los procedimientos y prácticas de copia de seguridad (y restauración) de la base de datos de Avaya Contact Center Select. Debe seguir realizando copias de seguridad periódicas y frecuentes del Contact Center. Para obtener más información sobre el mantenimiento, consulte*Implementación del dispositivo de software Avaya Contact Center Select*.

Aura de Avaya®Consideraciones sobre la instantánea de VMware del servidor de medios

Las instantáneas de VMware guardan el estado actual de la máquina virtual para que pueda volver a ella en cualquier momento. Las instantáneas son útiles cuando necesita revertir una máquina virtual repetidamente al mismo estado, pero no desea crear varias máquinas virtuales.

Las siguientes consideraciones se aplican al usar instantáneas con Avaya Aura®Servidor multimedia en VMware:

- Las instantáneas deben tomarse durante un Avaya Aura®Ventana de mantenimiento del servidor multimedia. No tome una instantánea de un Avaya Aura®Máquina virtual Media Server mientras se ejecuta el centro de contacto. Las instantáneas tienen un impacto negativo en el rendimiento de una máquina virtual a lo largo del tiempo. Debe Eliminar todas las instantáneas al final de la ventana de mantenimiento y*Consolidar* instantáneas, si es necesario, antes de instalar Avaya Aura®La máquina virtual Media Server vuelve a la producción. Para obtener más información sobre la consolidación de instantáneas, consulte la documentación de VMware.

- Al restaurar instantáneas, considere detenidamente el posible impacto de las definiciones de antivirus desactualizadas, las actualizaciones de seguridad y las actualizaciones del sistema operativo Linux perdidas. Aísle la máquina virtual restaurada hasta que se resuelvan estos problemas.

Las instantáneas de VMware no reemplazan a Avaya Aura®Procedimientos y prácticas de copia de seguridad (y restauración) de la base de datos del servidor multimedia. Para obtener más información sobre el mantenimiento, consulte*Implementación del dispositivo de software Avaya Contact Center Select*.

Orientación para los requisitos de almacenamiento

Entrada/salida por segundo (IOPS) es una medida del número máximo de lecturas y escrituras en *no contiguo* ubicaciones de almacenamiento realizadas por segundo. Las mediciones de IOPS están asociadas con archivos más pequeños y cambios más continuos, y comprenden las cargas de trabajo más típicas en aplicaciones empresariales en tiempo real, como Avaya Contact Center Select.

En un entorno virtualizado, cualquier arreglo de almacenamiento debe estar diseñado para tener una capacidad de IOPS que exceda la suma de los IOPS requeridos para todas las aplicaciones residentes.

Para una instancia de Avaya Contact Center Select completamente cargada, el IOPS es:

- Promedio: 105
- Máximo: 1488

Estas cifras de IOPS incluyen Avaya Contact Center Select y las cargas del sistema operativo subyacente.

Página190 de 3226.

Supervisión y gestión del rendimiento

Debe supervisar y medir continuamente el rendimiento del servidor host de Contact Center. Puede usar VMware vSphere vCenter para medir las métricas críticas de rendimiento del host en tiempo real. VMware vCenter agrega y archiva datos de rendimiento para que los datos se puedan visualizar y generar informes.

Configure la recopilación de estadísticas de VMware vCenter para recopilar datos de duración de intervalo de 5 minutos y 30 minutos para el host en el nivel de estadísticas 3. Conserve los datos de duración de intervalo de 5 minutos durante 3 días y conserve la duración de intervalo de 30 minutos durante 1 semana.

Genere informes de rendimiento con vCenter Report Performance y archive estos informes para proporcionar una referencia de rendimiento de referencia. Genere y almacene informes de 1 día y de 1 semana. Almacene el Resumen de informes de vCenter asociado con los informes de rendimiento. Debe analizar los informes de rendimiento después de los cambios en el host para evaluar el impacto del cambio en el host.

Supervise, reconozca y resuelva las alarmas de VMware vCenter. En particular, debe investigar y resolver de inmediato el uso de la CPU del host y las alarmas de uso de la memoria del host.

Además, las herramientas de línea de comandos "esxtop" y "resxtop" están disponibles para proporcionar una visión detallada de las métricas en tiempo real. Hay una serie de contadores críticos relacionados con la CPU a tener en cuenta:

- Si el promedio de carga que aparece en la primera línea del Panel de CPU es igual o mayor que la cantidad de procesadores físicos en el sistema, esto indica que el sistema está sobrecargado.
- El porcentaje de uso de CPU físicas en la línea PCPU puede indicar una condición de sobrecarga. En general, el 80 por ciento de uso es un límite razonable en entornos de producción. Utilice el 90 por ciento como una alerta para el administrador de VMware de que las CPU se están acercando a una condición de sobrecarga, que debe abordarse.
- %RDY: el porcentaje de tiempo que una entidad programable estuvo lista para ejecutarse pero no está programada para un núcleo. Si %RDY es superior al 10 por ciento, esto puede indicar una contención de recursos.
- %CSTP: el porcentaje de tiempo que se detiene la ejecución de una entidad programable para permitir que otras vCPU en la máquina virtual se pongan al día. Si el %CSTP es superior al 5 %, normalmente significa que la carga de trabajo de la máquina virtual no utiliza las VCPU de forma equilibrada. Un %CSTP alto puede ser un indicador de un sistema que se ejecuta en una instantánea no consolidada.

Para obtener más información sobre el uso de esxtop o resextop, consulte la *Guía de administración de recursos de VMware*.

Reservas de memoria

Utilice las reservas de VMware para especificar la cantidad mínima de memoria para una máquina virtual de Contact Center. Las reservas de VMware mantienen suficiente memoria de host para cumplir con todas las garantías de reserva. ESX no enciende una máquina virtual si al hacerlo reduce la cantidad de memoria disponible a menos de la cantidad reservada. El uso de reservas puede reducir la cantidad total de máquinas virtuales que se pueden alojar en un servidor host de VMware. Una vez que se han cumplido todas las reservas de recursos, ESX asigna los recursos restantes según la cantidad de recursos compartidos y los límites de recursos configurados para su máquina virtual.

Solución de problemas de VMware

Los problemas de rendimiento de la plataforma de virtualización pueden resultar en problemas de rendimiento del Contact Center. La plataforma de virtualización incluye el host y las máquinas virtuales en ejecución en el host. Los problemas de rendimiento del Contact Center pueden incluir (pero no se limitan a) un alto uso de la CPU, inestabilidad del enlace, llamadas incumplidas o abandonadas.

Debe investigar de forma lógica y sistemática cualquier problema de rendimiento del Contact Center para descartar problemas de rendimiento de virtualización. Todas las desviaciones de las especificaciones publicadas deben investigarse y resolverse antes de que se inicie la investigación del software del Contact Center. Para obtener más información, consulte la documentación de VMware vSphere.

Para ayudar a solucionar problemas de recursos de VMware, recopile información sobre los siguientes indicadores clave de rendimiento (KPI) de VMware.

KPI de host de VMware vSphere:

- CPU física
  - PCPU - Uso de CPU física.
  - Promedio de carga de CPU - Promedio promedio de carga de CPU del host.
- Memoria física
  - SWAP/MB - Estadísticas de uso de intercambio de memoria.

KPI de máquina virtual (VM) de VMware vSphere:

- vCPU
  - CPU RDY: la hora en que la máquina virtual estuvo lista para ejecutarse, pero no se le proporcionó el recurso de la CPU.
  - CPU WAIT - Porcentaje de tiempo pasado en el estado de espera bloqueado u ocupado.
  - AMIN - Reserva asignada.
  - ASHRS - cuotas de CPU asignadas.
  - CPU CSTP: cantidad de tiempo que una máquina virtual de procesamiento múltiple simétrico (SMP) estuvo lista para ejecutarse, pero se retrasó debido a la contención de programación de co-vCPU.
- E/S de disco
  - GAVG: latencia de lectura promedio del sistema operativo invitado por operación de lectura.
  - DAVG/rd: latencia de lectura promedio del dispositivo por operación de lectura.
  - DAVG/wr: latencia de escritura de dispositivo promedio por operación de escritura.
  - RESETS/s - Número de comandos reseteados por segundo.
  - ABRTS/s - Número de comandos de disco abandonados por segundo.
- La red
  - %DRPTX - Porcentaje de paquetes descartados al transmitir.

Página192 de 3226.

- %DRPRX - Porcentaje de paquetes descartados al recibir.

• Memoria

- MCTLSZ: cantidad de estadísticas de globo de memoria recuperada de memoria física.

Licencias de dispositivos de software

Contact Center License Manager solo admite la implementación del entorno virtualizado del servidor Avaya WebLM.

Cuando se inicia Contact Center License Manager, extrae las claves de licencia de WebLM del servidor WebLM remoto. Luego, Contact Center License Manager convierte las claves de licencia de WebLM en claves de licencia PLIC locales y distribuye las claves a las aplicaciones de Avaya Contact Center Select según sea necesario. Contact Center License Manager distribuye claves de licencia PLIC a Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia y Avaya Aura®Servidor multimedia según sea necesario.

Cuando Contact Center License Manager solicita licencias de un servidor Avaya WebLM remoto, reserva todas las licencias de Contact Center disponibles en ese servidor. Por lo tanto, Contact Center solo admite el tipo de archivo de licencia estándar (SLF) PLDS. Avaya Contact Center Select no es compatible con el modelo WebLM Enterprise. Contact Center es compatible con WebLM en centros de contacto nodales. WebLM no es compatible con las licencias corporativas de Contact Center.

Contact Center License Manager distribuye claves de licencia nodal a todos los Avaya Aura configurados® Servidores multimedia en la solución. Configurar Avaya Aura®Servidor multimedia como servidor multimedia en Contact Center Manager Administration. Contact Center License Manager, cuando se reinicia, envía claves de licencia a ese Avaya Aura®Servidor multimedia. No configure las licencias de WebLM en Avaya Aura®Servidores de servidor de medios.

Cómo obtener una licencia

Avaya Contact Center Select utiliza un servidor WebLM remoto para proporcionar control de licencias nodales.

1. Obtenga el ID de host de Avaya WebLM desde la interfaz de usuario de WebLM.
2. Utilice la ID de host de WebLM para obtener las claves de licencia de WebLM del Sistema de entrega y licencias de productos (PLDS) de Avaya.
3. Ingrese estas claves de licencia en el servidor Avaya WebLM remoto. Contact Center License Manager se conecta al servidor WebLM remoto y utiliza las claves de licencia específicas de Contact Center para controlar las funciones con licencia de Contact Center. Contact Center no importa el archivo de licencia a un servidor de Contact Center; WebLM almacena el archivo de licencia en el servidor WebLM.

Puede utilizar la Utilidad de configuración del administrador de licencias para verificar qué funciones de Contact Center tienen licencia y cuántas licencias de agente están disponibles.

Capítulo 6: Avaya Contact Center Select dispositivo de hardware

Esta sección describe el dispositivo de hardware de Avaya Contact Center Select. El dispositivo de hardware Avaya Contact Center Select es un servidor físico de montaje en rack con el software de la aplicación ya cargado y parcialmente preconfigurado.

Para implementar el dispositivo de hardware de Avaya Contact Center Select, debe activar el sistema operativo Windows con la clave de producto de MS Windows provista, configurar la red del servidor y luego usar un asistente de configuración simple para poner en marcha rápidamente la solución. En el momento de la instalación, el servidor del dispositivo de hardware de Avaya Contact Center Select inicia automáticamente un asistente de configuración simple que se utiliza para implementar rápidamente una solución de centro de contacto funcional. El servidor del dispositivo de hardware de Avaya Contact Center Select está precargado con usuarios de muestra, conjuntos de habilidades y parámetros del centro de contacto. Puede utilizar estos datos de muestra para poner en marcha rápidamente la solución y realizar la primera llamada enrutada y contacto por correo electrónico. El servidor de dispositivo de hardware de Avaya Contact Center Select ofrece una implementación de centro de contacto rápida y simplificada.

Debe activar el sistema operativo Microsoft Windows en el dispositivo de hardware de Avaya Contact Center Select utilizando la clave de producto de Microsoft Windows provista. La clave de producto de Microsoft Windows proporcionada se muestra en una etiqueta adherida a la parte superior del servidor del dispositivo de hardware de Avaya Contact Center Select.

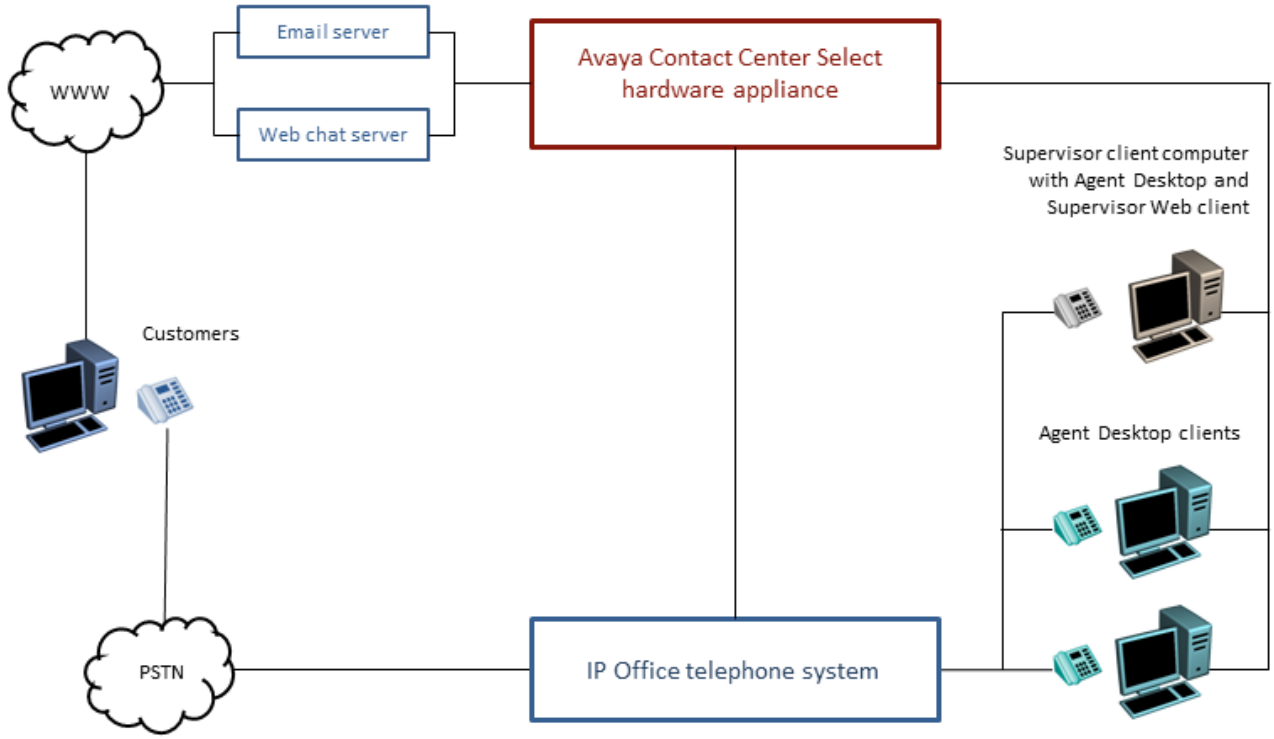


Figura 10: Topología de una solución típica de dispositivo de hardware de Avaya Contact Center Select

- Especificaciones del servidor del dispositivo de hardware en la página 110
- Especificaciones de software del dispositivo de hardware de Avaya Contact Center Select en la página 112
- Licencias de dispositivos de hardware en la página 118

Especificación del servidor del dispositivo de hardware

Contact Center Hardware Appliance es un servidor de montaje en bastidor preconfigurado para admitir Contact Center.

Contact Center es una colección de aplicaciones en tiempo real que se ejecutan en el sistema operativo Microsoft Windows Server 2012 R2. Contact Center proporciona control de llamadas en tiempo real, manejo de multimedia e informes estadísticos en tiempo real.

Importante:

El servidor Contact Center Hardware Appliance suministrado por Avaya está optimizado para proporcionar los recursos computacionales, de red y de registro en tiempo real que requiere Contact Center. No debe modificar el servidor del dispositivo de hardware, a menos que Avaya se lo indique:

- No agregue dispositivos de hardware internos adicionales a este servidor.

Página195 de 3226.

- No cambie ni actualice la configuración o la versión del BIOS del servidor.
- No cambie la configuración del hardware del servidor.
- No actualice el firmware del servidor.
- No cambie ni actualice los controladores del dispositivo.
- No modifique las particiones del disco duro.
- No cambie el*actualizacion de Windows*configuración de la aplicación en el servidor.
- No actualice Java Runtime Environment (JRE) suministrado en el dispositivo de hardware.

Debido al procesamiento en tiempo real que realizan las aplicaciones de Contact Center, no debe instalar ningún otro tipo de software de aplicación en el servidor. Solo puede instalar el software de clase de utilidad de soporte remoto y antivirus compatible en este servidor.

Instale solo los parches y revisiones del sistema operativo Microsoft Windows Server 2012 R2 compatibles con Contact Center. Para obtener más información acerca de los parches del sistema operativo admitidos, consulte la*Lista de compatibilidad de hotfixes de seguridad y compatibilidad de paquetes de servicio de cartera de Contact Center*enhttp://soporte.avaya.com .

La siguiente tabla enumera las especificaciones del servidor para el servidor Contact Center Hardware Appliance.

Especificación	Cantidad	Configuración	Comentario
Factor de forma	1	Montaje en rack, chasis 1U	Servidor de montaje en rack PowerEdge R630.
UPC	2	2,6 GHz E5-2640v3	—
RAM	12	4GB DDR4 RDIMM	—
Disco duro	2	Unidades SAS de 2,5" de 1,2 TB y 10 000 unidades	—
Controlador RAID	1	RAID1 PERC 730 1 GB	—
Unidad óptica	1	Unidad de DVD +/-RW 16X SATA	—
Interfaz de red	2	NIC PCIe de doble puerto de 1 GbE	Solo admite Ethernet.
Fuente de alimentación	2	750 vatios CA	—
Cables de poder	2	Cables de poder	Localizado a la región.
Adicional interfaces		• 2 puertos USB frontales • 2 puertos USB traseros • Conector de vídeo frontal	—
Adicional hardware	1	kit de montaje en bastidor	—
Peso	—	47.5 libras aproximadamente 21,5 kilogramos aproximadamente	—

Especificaciones de software del dispositivo de hardware de Avaya Contact Center Select

Avaya Contact Center Select se ofrece como un servidor de dispositivo de hardware. El servidor del dispositivo de hardware de Avaya Contact Center Select contiene el siguiente software:

- Sistema operativo Microsoft Windows 2012 R2 Standard Edition. El sistema operativo no se activa hasta que el cliente final aplica la licencia de Microsoft Windows adjunta al servidor.
- Servidor del administrador del centro de contacto (CCMS)
- Administración del administrador del centro de contacto (CCMA)
- Conjunto de herramientas de control de comunicaciones (CCT)
- Administrador de licencias del centro de contacto (LM)
- Utilidad del servidor Contact Center Manager (SU)
- Diseñador de orquestación (OD)
- Centro de Contacto Multimedia (CCMM)
- Aura de Avaya®Servidor multimedia con parches de Quick Fix Engineering (QFE)
- Datos de configuración predeterminados de Avaya Contact Center Select
- Paquetes de servicios
- Política de cortafuegos
- Asistente de configuración

El sistema operativo Windows 2012 R2 en el servidor del dispositivo de hardware enviado no está activado. El dispositivo de hardware de Contact Center proporciona una clave de licencia de producto de Microsoft Windows Server 2012 R2. La clave de licencia del producto Microsoft Windows Server 2012 R2 está impresa en una etiqueta adherida a la parte superior del servidor Contact Center Hardware Appliance. Debe activar el sistema operativo Microsoft Windows dentro de los 30 días posteriores al encendido inicial. De lo contrario, el servidor del dispositivo de hardware de Avaya Contact Center Select deja de funcionar.

La siguiente tabla muestra el sistema operativo en el servidor del dispositivo de hardware de Avaya Contact Center Select.

Sistema operativo	**Internacional** **Versiones compatibles**	**Paquete de servicio mínimo** **Soportado**
Windows Server 2012 Versión 2 Edición estándar	inglés	

Requisitos de nomenclatura del servidor

Los nombres de servidor deben cumplir con RFC1123 (Requisitos para hosts de Internet), que especifica que un nombre de host debe cumplir con lo siguiente:

- Solo se pueden usar caracteres de la a a la z, de la A a la Z y del 0 al 9 en un nombre de host.
- Puede utilizar un guión (-), pero no para iniciar o finalizar el nombre de host.
- Los nombres de host deben tener entre 6 y 15 caracteres de longitud.
- Los nombres de host no deben comenzar con un número.
- No utilice el carácter de subrayado (_) ni el carácter de punto (.).
- No utilice espacios en el nombre de host.

El servidor de Contact Center debe poder resolver el nombre de host o el nombre de la computadora de todos los demás servidores dentro de la configuración. Si tiene un servidor de Servicio de nombres de dominio (DNS), asegúrese de que exista una entrada para cada servidor. Si no tiene un servidor DNS, actualice manualmente el archivo HOSTS en cada servidor con el nombre de host o el nombre de la computadora de todos los demás servidores para asegurarse de que todos los clientes puedan interpretar los nombres de los servidores.

Si la conectividad de red en su red requiere el uso de nombres de dominio completos (FQDN), entonces el FQDN de cada computadora debe poder resolverse entre todos los servidores asociados con Contact Center.

Revisiones de seguridad de Microsoft

Debe operar su servidor con los parches más recientes de Microsoft.

- Revisa el*Lista de aplicabilidad de hotfixes de seguridad y compatibilidad de paquetes de servicios de cartera de Contact Center*(disponible en el sitio web de soporte técnico) para ver la lista de revisiones de seguridad de Microsoft aplicables.
- Realice una copia de seguridad de todo el servidor y luego apague todos los servicios de Contact Center antes de aplicar las revisiones de seguridad de Microsoft siguiendo las instrucciones de Microsoft.
- Aplicar las actualizaciones de seguridad de Microsoft en el momento oportuno.

Actualizaciones del sistema operativo

Las actualizaciones del sistema operativo incluyen actualizaciones de servicio y paquetes de servicio.

Actualizaciones de servicio

Dada la cantidad de actualizaciones del servicio de seguridad del sistema operativo y la complejidad inherente a cualquier red, cree un proceso sistemático y responsable para identificar y aplicar las actualizaciones del servicio. Para ayudar a crear dicho proceso, puede seguir una serie de pautas de mejores prácticas, como se documenta en el Boletín especial 800-40 del Instituto Nacional de Estándares y Tecnología (NIST), Procedimientos para el manejo de parches de seguridad.

Página198 de 3226.

Este boletín sugiere que si una organización no tiene un grupo central para coordinar el almacenamiento, la evaluación y el registro crónico de las actualizaciones del servicio de seguridad en una biblioteca, los administradores del sistema o el administrador del centro de contacto deben cumplir esta función. Además de estas pautas, siempre que sea posible, siga las recomendaciones de Microsoft con respecto a las vulnerabilidades descubiertas recientemente y que instale de inmediato las actualizaciones del servicio de seguridad de Microsoft.

Siempre que sea posible, Avaya incorpora las recomendaciones de seguridad del sistema operativo y las actualizaciones de servicio más recientes en una estrategia de prueba de soluciones integradas durante cada ciclo de prueba. Sin embargo, debido a la naturaleza urgente de las actualizaciones del servicio de seguridad cuando se descubren vulnerabilidades, siga las pautas de Microsoft a medida que se emiten, incluidos los procedimientos de instalación de Microsoft y los procesos de reversión de actualizaciones del servicio de seguridad.

Finalmente, debe realizar una copia de seguridad completa del sistema antes de actualizar el sistema para asegurarse de que sea posible una reversión, si es necesario. Si una aplicación de Contact Center no funciona correctamente después de aplicar una actualización del servicio de seguridad de Microsoft, debe eliminar la actualización del servicio y volver a la versión anterior de la aplicación (desde la copia de seguridad que realizó antes de aplicar la actualización del servicio). Para mayor seguridad, siempre determine si Avaya verificó la actualización del servicio de Microsoft para compatibilidad con Contact Center Manager.

Para obtener más información acerca de la actualización, consulte la*Lista de compatibilidad de hotfixes de seguridad y compatibilidad de paquetes de servicio de cartera de Contact Center*enhttp://soporte.avaya.com .

paquetes de servicios

Avaya tiene una política para implementar pruebas de co-residencia de todos los paquetes de servicios operativos nuevos para verificar la compatibilidad con el conjunto de aplicaciones de Contact Center tan pronto como estén disponibles. En la práctica, debido a que un paquete de servicio puede contener una cantidad significativa de contenido nuevo, Avaya requiere que espere hasta que se complete la prueba de compatibilidad antes de aplicar el paquete de servicio. Tenga en cuenta que los service packs del sistema operativo generalmente se prueban con el SP de la aplicación Contact Center más reciente y, por lo tanto, una actualización a un nuevo service pack requiere una actualización al SP de Avaya más reciente.

Antes de cargar un nuevo Service Pack, debe realizar una copia de seguridad completa del sistema (para revertir el sistema como en el escenario de actualización).

Importante:

La compatibilidad del Service Pack para todas las aplicaciones de Contact Center está documentada en el*Lista de aplicabilidad de hotfixes de seguridad y compatibilidad de paquetes de servicios de cartera de Contact Center*en el sitio web enhttp://soporte.avaya.com .

Actualizaciones del entorno de tiempo de ejecución de Java

Contact Center solo admite versiones específicas de Java Runtime Environment (JRE). Durante la instalación, Contact Center desactiva las actualizaciones automáticas de JRE en los servidores del centro de contacto.

Importante:

La actualización a una versión no compatible de JRE puede hacer que el centro de contacto deje de funcionar y puede requerir la reinstalación del servidor del centro de contacto.

Página199 de 3226.

Compatibilidad con el protocolo de configuración de host dinámico

Aplicaciones de Contact Center (CCMS, CCMA, CCT, CCMM, LM y Avaya Aura®Media Server) no son compatibles con el Protocolo de configuración dinámica de host (DHCP). Todos los servidores de Contact Center deben tener una dirección IP estática.

Los equipos cliente de Agent Desktop admiten direcciones IP estáticas y DHCP.

Requisitos de software de terceros

Debido al procesamiento en tiempo real y de misión crítica que realizan las aplicaciones de Contact Center, no debe instalar ningún otro tipo de software de aplicación en el servidor. Puede instalar cierto software de clase de utilidad en el servidor, siempre que cumpla con las pautas de esta sección.

El software de clase de aplicación generalmente requiere una cierta cantidad de recursos del sistema y no debe instalarse en un servidor que ejecute aplicaciones de Contact Center. La instalación de aplicaciones de terceros puede hacer que las aplicaciones de Contact Center funcionen fuera de los límites de ingeniería conocidos y puede crear posibles problemas desconocidos del sistema (por ejemplo, contenciones de CPU, mayor carga de tráfico de red y degradaciones de acceso al disco).

Ciertas aplicaciones de software de clase de utilidad de terceros, como diagnósticos de hardware o herramientas de copia de seguridad, generalmente requieren menos recursos del sistema durante el funcionamiento normal de las aplicaciones del Contact Center y están permitidas. Las excepciones son las utilidades, como los protectores de pantalla, que pueden causar problemas en el sistema y degradar el rendimiento.

El software antivirus se clasifica como una utilidad y está sujeto a las pautas genéricas de la siguiente sección.

Pautas genéricas para aplicaciones de software de clase de utilidad

Las siguientes son pautas genéricas para el software de clase de utilidad:

- Durante el tiempo de ejecución, la utilidad no debe degradar la aplicación del centro de contacto más allá de un porcentaje promedio de uso de CPU (consulte cada sección específica de la aplicación en este documento para conocer el nivel de uso de CPU máximo recomendado). Además, la utilidad no debe reducir la cantidad mínima de espacio libre en el disco duro requerido por la aplicación del centro de contacto y el sistema operativo Windows.
- La utilidad no debe causar apagados de software inadecuados o apagados fuera de secuencia.
- La empresa de servicios públicos no debe administrar la aplicación del centro de contacto.
- Si la utilidad tiene una base de datos, no debe afectar la base de datos de la aplicación del centro de contacto.
- No se deben utilizar las utilidades de compresión de disco.
- No se deben utilizar las utilidades de ajuste de memoria utilizadas para recuperar la memoria que Microsoft no utiliza.
- La instalación o desinstalación del software de terceros no debe afectar ni entrar en conflicto con la aplicación del centro de contacto (por ejemplo, no debe causar conflictos de DLL). Si se descubren tales conflictos, podría ser necesaria una reconstrucción del servidor.
- El personal de implementación debe realizar pruebas para garantizar que se cumplan estas condiciones y recomendaciones antes de poner en producción la aplicación Contact Center.

El personal de soporte puede solicitar los resultados de las pruebas durante el diagnóstico de fallas. Como parte del diagnóstico de fallas, se le puede solicitar al distribuidor o al usuario final que elimine el software de terceros.

- No se debe instalar HyperTerminal en el servidor ya que interfiere con el funcionamiento del Contact Center.

Directrices para el uso de software antivirus

Esta sección describe los requisitos del software antivirus Avaya Contact Center Select. Avaya

Contact Center Select es compatible con los siguientes productos antivirus:

- Antivirus de Symantec
- McAfee

Para obtener más información sobre las consideraciones antivirus de Avaya Contact Center Select y las versiones admitidas, consulte*Guía de referencia de seguridad de Avaya Contact Center Select*disponible en el sitio web de soporte de Avaya enhttp://soporte.avaya.com .

Puede implementar productos antivirus de otros proveedores sujeto a las siguientes pautas:

- Política de cuarentena de archivos infectados en el servidor y el cliente: el software antivirus se puede configurar para limpiar el virus detectado automáticamente y los archivos se deben poner en cuarentena si no se pueden limpiar los archivos infectados. Comuníquese con Avaya para verificar si el archivo de cuarentena es parte de nuestros archivos de productos o un archivo de sistema dependiente. Si se detecta un virus, elimine el servidor de la red inmediatamente durante la erradicación del virus para evitar una mayor propagación del virus.
- No conecte una plataforma de aplicación del centro de contacto directamente a Internet para descargar definiciones de virus o archivos actualizados. Además, Avaya recomienda que no use una PC cliente de aplicación de centro de contacto para conectarse a Internet. En su lugar, descargue las definiciones de virus y los archivos actualizados a otra ubicación en la red del cliente y cárguelos manualmente desde esta ubicación provisional a la plataforma de la aplicación del centro de contacto.
- Realice los pasos anteriores para descargar los Service Packs (SP) de la aplicación Contact Center. Este método limita el acceso a Internet y, por lo tanto, reduce el riesgo de descargar archivos infectados.
- Escanee todos los archivos SP, DVD-ROM y disquetes antes de cargarlos o instalarlos en el servidor. Esta práctica minimiza cualquier exposición a archivos infectados de fuentes externas.
- Consideraciones de capacidad: la ejecución de un software de detección de virus puede generar una carga adicional en la plataforma de una aplicación del centro de contacto. El personal de implementación debe ejecutar la herramienta de supervisión de rendimiento en el servidor para medir el uso de la CPU. Si la exploración del software antivirus hace que el uso promedio de la CPU de la plataforma supere el porcentaje recomendado durante más de 20 minutos, el software antivirus no debe cargarse en la plataforma de la aplicación del centro de contacto.
- El Soporte de productos no brinda soporte para la configuración del software antivirus, pero ofrece orientación cuando es posible. Dirija las preguntas o problemas sobre el software antivirus al proveedor adecuado.
- Si se plantean problemas de rendimiento o funcionalidad al personal de soporte de Avaya como parte del diagnóstico de fallas, es posible que se le pida que elimine el software de utilidades o el software antivirus de terceros.

Página201 de 3226.

Varias tareas de mantenimiento se activan automáticamente a las 12:00 de la noche. Por lo tanto, debe programar análisis de virus en un momento distinto de la medianoche.

Avaya recomienda que excluya los siguientes archivos y carpetas de los análisis (tanto en tiempo real como programados):

- F:\Avaya\Contact Center\Bases de datos\
- *<unidad de base de datos adicional>*:\Avaya\Centro de contacto\Bases de datos\
- Archivos TSM_OAM ubicados en las siguientes carpetas:
  - D:\Avaya\Contact Center\Manager Server\iccm\bin\data
  - D:\Avaya\Contact Center\Manager server\iccm\data
  - D:\Avaya\Contact Center\Manager Server\iccm\sdm\log
- D:\Avaya\Contact Center\Manager Server\bin\tools2.exeSe producen errores de acceso a archivos en el registro de actividad de análisis si no excluye este archivo del análisis.
- D:\Avaya\Contact Center\Manager Server\iccm\logs (registros SIP)
- D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\ (archivos de configuración de registro SIP)
- D:\Avaya\Contact Center\Componentes comunes\CMF
- D:\Avaya\Contact Center\Manager Administration\Apps\ (incluyendo subdirectorios)
- La carpeta donde almacena Service Packs y parches

Contact Center Multimedia interactúa con un sistema de correo electrónico externo y permite a los agentes enviar archivos adjuntos desde sus computadoras al servidor de Avaya Contact Center Select. Ambos métodos de recuperación de datos son fuentes potenciales de infección de software.

Avaya recomienda las siguientes pautas para el software antivirus:

- El software antivirus debe instalarse en el servidor de correo electrónico para garantizar que los problemas se detecten en el origen.
- Las computadoras de los agentes requieren un software antivirus para garantizar que los archivos adjuntos enviados al servidor de Avaya Contact Center Select no tengan virus. Contact Center Multimedia no bloquea tipos de archivos adjuntos específicos. El software antivirus de terceros debe instalarse en el Portal Server de acuerdo con las pautas de este documento para dichas utilidades.
- Asegúrese de que el software antivirus esté configurado para permitir mensajes de correo electrónico salientes. Por ejemplo, configure el software antivirus McAfee*Protección de acceso*opción de no bloquear *Evite que los gusanos de correo masivo envíen correo*. Como alternativa, agregue el proceso "EmailManager.exe" de Contact Center Multimedia al McAfee*Procesos a excluir*lista.

  Excluya la partición de la base de datos de Contact Center Multimedia del análisis.
- Si los cortafuegos en equipos individuales están habilitados en el equipo de Agent Desktop, el detector de informes podría estar marcado como tratando de acceder a Internet. Las propiedades deben configurarse para permitir el acceso de Report Listener a Contact Center Multimedia a través del firewall.

- No debe habilitar Microsoft Updater para la ejecución automática. Microsoft Updater está configurado en el nivel de alerta para que pueda programar actualizaciones para las horas de menor actividad.

Advertencia:

Ejecutar un análisis de virus en la carpeta de archivos adjuntos de Contact Center Multimedia, que contiene miles de archivos, puede usar un tiempo de CPU significativo en un servidor y puede causar una ralentización drástica en los tiempos de respuesta del agente. Avaya recomienda ejecutar análisis, si es necesario, durante las horas de menor actividad.

Para evitar problemas de integridad de la base de datos, Avaya recomienda que excluya todos los archivos CACHE.DAT, los archivos de diario, el archivo cache.cpf y cualquier archivo relacionado con Caché de los análisis antivirus.

El software Caché está instalado en *<Unidad_de_instalación>*:\Avaya\Cache\CacheSys.Las bases de datos y los archivos de diario se instalan en *<Unidad_de_instalación>*:\Avaya\Contact Center\Bases de datos.

Excluya la carpeta de archivos de Caché Journal;G:\Avaya\

Para Avaya Aura®Media Server, debe excluir los siguientes archivos y carpetas de los análisis (tanto en tiempo real como programados):

- D:\Avaya\MAS\Multimedia_Applications\MAS\platdata
- D:\Avaya\MAS\Multimedia_Applications\MAS\common\log

Licencias de dispositivos de hardware

La opción de implementación del dispositivo de hardware de Avaya Contact Center Select utiliza una licencia de Nodal Enterprise entregada como un archivo WebLM XML. Este archivo de licencia se utiliza para controlar el acceso a funciones con licencia, como contactos multimedia y multiplicidad.

Contact Center License Manager brinda control central y administración de licencias para Avaya Contact Center Select. Cada Contact Center License Manager incluye una instancia local de WebLM. Cuando se inicia el servicio Contact Center License Manager, extrae las claves de licencia de WebLM de la instancia local de WebLM. Luego, Contact Center License Manager convierte las claves de licencia de WebLM en claves de licencia PLIC locales y distribuye las claves a las aplicaciones de Avaya Contact Center Select según sea necesario.

- Obtenga la ID de host de WebLM para su servidor Avaya Contact Center Select.
- Utilice el ID de host de WebLM para obtener un archivo de licencia nodal de WebLM del Sistema de entrega y licencias de productos (PLDS) de Avaya.
- Carga el archivo de licencia en el servidor de Avaya Contact Center Select mientras ejecuta la utilidad de configuración cuando implementa el servidor de Avaya Contact Center Select. También puede cargar el archivo de licencia después del proceso de configuración. Cuando Contact Center License Manager carga la licencia, si el número único de la licencia no coincide con la ID de host de WebLM, entonces License Manager se cierra y Avaya Contact Center Select no puede procesar los contactos. Si el número exclusivo de la licencia coincide con el ID de host de WebLM, la licencia

Manager proporciona claves de licencia y Avaya Contact Center Select procesa los contactos de los clientes.

Capítulo 7: Límites de capacidad de la solución y funciones admitidas

Esta sección especifica los límites de capacidad máxima de Avaya Contact Center Select. Esta sección también especifica las funciones de telefonía y los dispositivos admitidos por Avaya Contact Center Select.

- Límites de capacidad máxima de Avaya Contact Center Select en la página 120
- Límites máximos de configuración de Avaya Contact Center Select en la página 123
- Funciones admitidas de Avaya Contact Center Select en la página 123
- Funciones de telefonía admitidas en la página 129
- Dispositivos de telefonía compatibles en la página 138
- Soporte de acceso remoto en la página 140
- Funcionalidad compatible con Communication Control Toolkit en la página 140

Límites de capacidad máxima de Avaya Contact Center Select

La capacidad máxima para su solución está determinada por su implementación de Avaya Contact Center Select y la plataforma de grabación de llamadas y voz de IP Office y su versión.

Puede instalar el DVD de Avaya Contact Center Select en cualquier servidor que cumpla con las especificaciones de servidor de independencia de proveedores de plataforma (PVI). El DVD Avaya Contact Center Select admite tres niveles de especificación de servidor PVI; Especificación de servidor PVI de nivel de entrada, de gama media y de gama alta. Las cifras de capacidad máxima para Avaya Contact Center Select DVD dependen de la especificación de servidor PVI que se utilice. La especificación de gama alta es compatible con Avaya Contact Center Select en su máxima capacidad nominal.

El dispositivo de software Avaya Contact Center Select es un conjunto de servidores virtualizados; una máquina virtual Avaya Contact Center Select, un Avaya Aura®Media Server OVA y un WebLM OVA. Puede implementar el dispositivo de software Avaya Contact Center Select en un servidor host VMware ESXi que proporcione los recursos necesarios.

El dispositivo de hardware Avaya Contact Center Select es un servidor físico de montaje en rack con el software de la aplicación ya cargado y parcialmente preconfigurado. El servidor de montaje en rack suministrado es compatible con Avaya Contact Center Select en su máxima capacidad nominal.

Página205 de 3226.

La siguiente tabla especifica los valores de capacidad máxima admitidos por los tipos de implementación de Avaya Contact Center Select para cada configuración de IP Office admitida.

Servidor escribe	Maxima capacidad	Configuración de IP Office (IPO)					
		OPI SE 10.1 o 11.0 R630, R620, DL360	OPI SE - DL120	oferta pública inicial 500V2 SORBO bañador sin CR	oferta pública inicial 500V2 SORBO bañador con CR	oferta pública inicial 500V2 TDM bañador sin CR	oferta pública inicial 500V2 TDM bañador con CR
Entrada-Nivel Servidor	Máximo de iniciados sesión agentesVer nota 3	60	60	60	30	40	30
	Máxima CCMA supervisores	10	10	10	10	10	10
	Sistema Máximo Tasa de contactoVer nota 1	1200	1200	1200	600	800	600
	máxima multimedia tasa (WCph / Eph)Ver Nota 2	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300
Rango medio Servidor	Máximo de iniciados sesión agentesVer nota 3	150	125	60	30	40	30
	Máxima CCMA supervisores	30	30	30	30	30	30
	Sistema Máximo Tasa de contactoVer nota 1	3000	2500	1200	600	800	600
	máxima multimedia tasa (WCph / Eph)Ver Nota 2	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600
Gama alta Servidor y Software Aparato	Máximo de iniciados sesión agentesVer nota 3	400Ver Nota 4	125	60	30	40	30
	Máxima CCMA supervisores	80	50	50	30	40	30
	Sistema Máximo Tasa de contactoVer nota 1	8000	2500	1200	600	800	600
	máxima multimedia tasa (WCph / Eph)Ver Nota 2	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200
Hardware Aparato	Máximo de iniciados sesión agentesVer nota 3	400	125	60	30	40	30

La tabla continúa...

Servidor escribe	Maxima capacidad	Configuración de IP Office (IPO)					
		OPI SE 10.1 o 11.0 **R630, R620, DL360**	**OPI SE - DL120**	oferta pública inicial **500V2** SORBO **bañador sin CR**	oferta pública inicial **500V2** SORBO **bañador con CR**	oferta pública inicial **500V2 TDM bañador sin CR**	oferta pública inicial **500V2 TDM bañador con CR**
	Máxima CCMA supervisores	80	50	50	30	40	30
	Sistema Máximo Tasa de contactoVer nota 1	8000	2500	1200	600	800	600
	máxima multimedia tasa (WCph / Eph)Ver Nota 2	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200

- **Nota 1:**La tasa de contacto del sistema es la tasa de contacto combinada máxima total en todos los tipos de contacto admitidos.

  - Para los cálculos de la tasa de contacto del sistema, los contactos de chat web tienen una ponderación equivalente a 2 mensajes de correo electrónico. Un chat web equivale a dos mensajes de correo electrónico.

  - Para los cálculos de la Tasa de contacto del sistema, el número máximo total de contactos admitidos por hora = (Voz + Correo electrónico + (Chat web * 2))

  - *Ruta a CDN*y *Transferencia/Conferencia a CDN*cada cuenta como dos llamadas.

  - Los flujos de llamadas complejos con escenarios de transferencia y conferencia reducen la cantidad admitida de contactos simultáneos.

- **Nota 2:**Las tarifas de contacto multimedia solo se aplican si Contact Center Multimedia (CCMM) es parte de la solución. Contactos de correo electrónico por hora (Eph). Chats web por hora (WCph). La capacidad de chat web se basa en un máximo de 500 sesiones de chat simultáneas con una duración promedio de chat de 5 minutos.
- **Nota 3**: Esta cifra es también el número máximo combinado para el uso simultáneo de Agent Desktop y la aplicación Agent Browser. Por ejemplo, en un servidor de gama alta, Avaya Contact Center Select admite 350 aplicaciones de Agent Desktop y 50 Agent Browser.
- **Nota 4**: Las líneas entrantes en IP Office (línea de IP Office o línea SIP de IP Office) que tienen como destino las llamadas entrantes en Avaya Contact Center Select deben tener Direct Media habilitado para admitir más de 250 agentes conectados simultáneamente.

  Con 400 agentes activos al mismo tiempo en llamadas simples (sin conferencias ni llamadas de transferencia), la cantidad máxima de llamadas en cola es 200. Esta cifra se basa en la cantidad máxima de sesiones disponibles en Avaya Aura®Servidor multimedia.

- La grabación de llamadas (CR) de IP Office es compatible con IP Office 500V2. Avaya Contact Center Select admite la grabación de llamadas hasta la cantidad máxima de agentes registrados admitidos. Por encima de este límite máximo, nadie puede dejar un mensaje de voz o grabar otras llamadas.

Server type	ACCS specification	IP Office platform						
		IPO SE R620/R630	IPO SE DL360	IPO SE DL120	IPO 500V2 SIP Trunks No CR	IPO 500V2 SIP Trunks With CR	IPO 500V2 TDM Trunks No CR	IPO 500V2 TDM Trunks With CR
Entry-level Server	Logged-in agents	60	60	60	60	30	40	30
	CCMA Supervisors	10	10	10	10	10	10	10
	System Contact Rate	1200	1200	1200	1200	600	800	600
	MM Rate (WCph/Eph)	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300
Mid-range Server	Logged-in agents	150	150	125	60	30	40	30
	CCMA Supervisors	30	30	30	30	30	30	30
	System Contact Rate	3000	3000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600
High-end Server	Logged-in agents	400	400	125	60	30	40	30
	CCMA Supervisors	80	80	50	50	30	40	30
	System Contact Rate	8000	8000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200
Hardware Appliance	Logged-in agents	400	400	125	60	30	40	30
	CCMA Supervisors	80	80	50	50	30	40	30
	System Contact Rate	8000	8000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200

Figura 11: Los valores de capacidad máxima admitidos por los tipos de implementación de ACCS para cada configuración de IP Office (IPO) admitida

Límites máximos de configuración de Avaya Contact Center Select

La siguiente tabla especifica los valores de configuración generales máximos admitidos por Avaya Contact Center Select.

Parámetro	Valor máximo
Máximo de agentes configurados	1500
Habilidades máximas de agentes	3000
Habilidades máximas por agente	20
Máximo de agentes por perfil	400
Máximo de supervisores por perfil	80
Máximo de supervisores por sistema	600

Funciones admitidas de Avaya Contact Center Select

La siguiente tabla especifica las funciones principales admitidas por Avaya Contact Center Select:

Rasgo	Soportado	Proveedor
Enrutamiento basado en habilidades de voz	Sí	Selección del centro de contacto de Avaya
Cola FIFO	Sí	Selección del centro de contacto de Avaya
Cola de agente inactivo más larga	Sí	Selección del centro de contacto de Avaya
Número ANI disponible	Sí	Selección del centro de contacto de Avaya
Enrutamiento del número ANI	Sí	Selección del centro de contacto de Avaya
Número DNIS disponible	Sí	
Enrutamiento de números DDI	Sí	Selección del centro de contacto de Avaya
Servicio Nocturno	Sí	Selección del centro de contacto de Avaya
Desbordamiento de umbral para habilidades	Sí	Selección del centro de contacto de Avaya
Alarma Visual Externa por umbral excedido	Sí	Selección del centro de contacto de Avaya
Clasificación de contacto de voz	Sí	Avaya Contact Center Select y Agent Desktop
Pantalla emergente multiparámetro por tipo de contacto por conjunto de habilidades	Sí	Selección del centro de contacto de Avaya
Música en espera	Sí	Oficina de PI
Música de múltiples fuentes en espera	No	
Anuncios en espera	No	
Anuncios de habilidades	Sí	Selección del centro de contacto de Avaya
Agente Ext In/Tecla DN	Sí	Avaya Contact Center Select e IP Office con tres líneas apariencia
Cobertura para Voicemail Pro	Sí	Las llamadas directas a una estación de agente reciben el tratamiento de cobertura configurado. Las llamadas enrutadas desde Avaya Contact Center Select a los agentes no reciben tratamiento de cobertura.
Reproducir aviso y recopilar dígitos	Sí	Selección del centro de contacto de Avaya
Tableros con API	Sí	Dev Connect y Avaya Contact Center Select
Códigos de actividad/trabajo	Sí	Selección del centro de contacto de Avaya
Códigos de motivo auxiliar/no listo	Sí	Selección del centro de contacto de Avaya
Códigos de trabajo después de la llamada	Sí	Selección del centro de contacto de Avaya
Indicación de pantalla en tiempo real Códigos ACW/Act/AUX/NotRdy	Sí	Selección del centro de contacto de Avaya
Operación de tres líneas (3 líneas de apariencia de llamada)	Sí	Avaya Contact Center Select e IP Office

La tabla continúa...

Rasgo	Soportado	Proveedor
Escritorio de agente basado en navegador	Sí	Avaya Contact Center Select y Agent Desktop El cliente de Agent Desktop se implementa mediante el clic una vez implementación o un archivo MSI.
Escritorio de supervisor basado en navegador	Sí	Avaya Contact Center Select y Agent Desktop El cliente de administración del supervisor utiliza CCMA basado en Internet Explorer. El cliente de Supervisor Agent se implementa mediante la implementación de ClickOnce o un archivo MSI.
Colas gratuitas	Sí	Selección del centro de contacto de Avaya
Operación en modo solo teléfono	No	
Tipo de transporte TLS	Sí	Entre IP Office y Avaya Contact Center Select
Asistente para la creación de informes	Sí	Selección del centro de contacto de Avaya
Zonificación del servidor de medios	No	
Enrutamiento basado en la red del centro de contacto	No	
Alta disponibilidad de misión crítica	No	Se admite Avaya Contact Center Select Business Continuity.
Soporte de agente remoto/fuera del sitio	Sí	Oficina de PI
Redes IPv6	No	
Personalización de la base de datos: importe nuevos campos definidos por el cliente	No	

La siguiente tabla especifica las funciones multimedia admitidas por Avaya Contact Center Select:

Rasgo	función secundaria	Soportado	Proveedor
Enrutamiento basado en habilidades multimedia		Sí	
Gestión Multimedia e informes		Sí	Centro de contacto de Avaya Seleccione
Multiplicidad		Sí	Centro de contacto de Avaya Seleccione
Manejo de contactos de correo electrónico		Sí	Centro de contacto de Avaya Seleccione

La tabla continúa...

Rasgo	función secundaria	Soportado	Proveedor
	Respuesta automática de correo electrónico	Sí	Centro de contacto de Avaya Seleccione
	Confirmación automática de correo electrónico	Sí	Centro de contacto de Avaya Seleccione
	Contacto con el cliente Historia	Sí	Centro de contacto de Avaya Seleccione
	Correo electrónico en tiempo real Informes	Sí	Centro de contacto de Avaya Seleccione
	Pantalla emergente basada en correo electrónico	Sí	Centro de contacto de Avaya Seleccione
	Tipos de contactos de fax	Sí	Centro de contacto de Avaya Seleccione
	Documentos escaneados	Sí	Centro de contacto de Avaya Seleccione
	Entrante de contacto de SMS	Sí	Centro de contacto de Avaya Seleccione
Comunicaciones Web		Sí	Centro de contacto de Avaya Seleccione
	Chat web	Sí	Centro de contacto de Avaya Seleccione
	Devolución de llamada web	Sí	Centro de contacto de Avaya Seleccione
	Co-navegación	No	
Saliente	Vista previa/progresivo	Sí	Centro de contacto de Avaya Seleccione
Integración de autoservicio			
	Autoservicio de datos y CTI a IVR externo	No	
	A bordo de Avaya Aura® Media Server IVR: reproducir aviso y recopilar dígitos	Sí	
Optimización de la fuerza laboral			
	Grabación de voz masiva	No	Centro de contacto de Avaya Seleccione
	Grabación selectiva	No	Usando el botón de IP Office
	Agente iniciado	No	Usando el botón de IP Office
	Monitoreo de calidad	No	
Administración de personal/ Pronóstico		No	

La tabla continúa...

Rasgo	función secundaria	Soportado	Proveedor
Umbral externo Alerta/Alarmas		No	
Informes de sitios múltiples		Sí	Para agentes distribuidos en una red SCN.
Supervisor/Agente Mensajería instantánea		No	
COLA ABIERTA Contacto Tipos		Sí	
SOA habilitado		No	
Contacto IM (enrutado) Tipos		No	
Saliente predictivo		No	
Escritorio del agente Softphone: H.323 o SIP		No	
Saludo del agente		No	

La siguiente tabla especifica las funciones de generación de informes admitidas por Avaya Contact Center Select:

Rasgo	función secundaria	Soportado	Proveedor
Multicanal unificado Informes históricos y en tiempo real		Sí	Centro de contacto de Avaya Seleccione
Tiempo real predefinido e Informes Históricos		Sí	Centro de contacto de Avaya Seleccione
Personalizable por el cliente Informes		Sí	Centro de contacto de Avaya Seleccione
Definible por el cliente Informes		Sí	Uso de herramientas de terceros que interactúan con Avaya Contact Center Select ODBC
Asistente para la creación de informes (RCW)		Sí	Centro de contacto de Avaya Seleccione
Informes históricos			
	Programado	Sí	Centro de contacto de Avaya Seleccione
	Intervalo	Sí	Centro de contacto de Avaya Seleccione
	Diariamente	Sí	Centro de contacto de Avaya Seleccione

La tabla continúa...

Rasgo	función secundaria	Soportado	Proveedor
	Semanalmente	Sí	Centro de contacto de Avaya Seleccione
	Mensual	Sí	Centro de contacto de Avaya Seleccione
	Trimestral	No	
	Conjunto de habilidades	Sí	Centro de contacto de Avaya Seleccione
	Tronco	No	
	Agentes	Sí	Centro de contacto de Avaya Seleccione
	Contactos abandonados	Sí	Centro de contacto de Avaya Seleccione
	Contactos de desbordamiento	Sí	Centro de contacto de Avaya Seleccione
	Umbral excedido	Sí	Centro de contacto de Avaya Seleccione
	Clasificación de contactos	Sí	Centro de contacto de Avaya Seleccione
	Fuente de desconexión	Sí	Centro de contacto de Avaya Seleccione
	Clave de estación de agente	No	
	Informe de correo electrónico Notificaciones	Sí	Centro de contacto de Avaya Seleccione
	Informes de estado del sistema	Sí	Centro de contacto de Avaya Seleccione

La siguiente tabla especifica la interoperabilidad del producto Avaya Contact Center Select:

Nombre del producto	Soportado
Aura de Avaya®Optimización de la fuerza laboral (WFO)	No. Utilice la grabación de llamadas de IP Office.
Selección de optimización de la fuerza laboral de Avaya (AWFOS)	Sí, versión 5.2, 5.2.1 y 5.3.
Gerente de alcance proactivo (POM)	No
Aura de Avaya®Portal de experiencia	Sí, versión 7.1, 7.2 y 7.2.1.
Informes de Avaya IQ	No
Administración de agentes y supervisores de Avaya Control Manager	No
Contacto proactivo de Avaya	No
Avaya one-X®Agente	No

La tabla continúa...

Nombre del producto	Soportado
Administrador de redes sociales	Sí (utilizando el tipo de contacto de correo electrónico). Liberar 6.2.13 o posterior.
Aura de Avaya®Servicios de presencia	No
Avaya Communicator para Windows	Sí, soporte de softphone.
Microsoft Lync (versión 2010 y 2013) y Microsoft Skype for Business 2015	Los MI punto a punto son soportado. Mensajes instantáneos enrutados no son compatibles.

La siguiente tabla especifica las interfaces abiertas admitidas por Avaya Contact Center Select:

Nombre de la interfaz abierta	Soportado
Multidifusión de estadísticas en tiempo real (RSM)	Sí
Visualización en tiempo real (RTD)	Sí
Asistente de integración de base de datos (DIW) e intercambio de datos de host (HDX)	Sí
Contact Center Multimedia (CCMM) Servicios avanzados de correo electrónico	Sí
Interfaces abiertas de Contact Center Manager Administration (CCMA)	Solo para sincronización de datos de usuario de IP Office con contacto de Avaya Seleccionar centro
Contact Center Multimedia Interfaces abiertas	Solo para comunicaciones estándar de Web Chat (no compatible con Agent Desktop).
Contact Center Multimedia Outbound Interfaces abiertas	Sí
Interfaces abiertas del kit de herramientas de control de comunicaciones (CCT)	No
cola abierta	Sí
Redes abiertas	No
Servicios de enlace de meridianos (MLS)	No
Kit de herramientas de control de comunicaciones .NET SDK	Sí
Póngase en contacto con el SDK del servicio de control	Sí
Contact Center Manager Server (CCMS) Interfaces abiertas	No
API de grabación de contactos de Avaya	No
Soporte del lado del servidor de Salesforce	Sí

Funciones de telefonía admitidas

Las siguientes tablas enumeran las funciones de telefonía de IP Office disponibles para un usuario de IP Office que no es agente y especifican qué funciones son compatibles con una estación de agente de Avaya Contact Center Select.

Página214 de 3226.

Manejo básico de llamadas:

Oficina de PI **telefonía** nombre de la característica	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente **apoyo**		**notas**
	Personal llamadas	**CC** llamadas	llamadas personales	llamadas CC	
Tonos	Sí	Sí	No	No	Agent Desktop no reproduce tonos específicos según la geografía.
Identificador de llamadas	Sí	Sí	Sí	Sí	
Filtrado de llamadas	Sí	No	No	No	
Mantener	Sí	Sí	Sí	Sí	
Alternar llamadas	Sí	Sí	No	No	Alternar llamadas no se aplica a los agentes de Avaya Contact Center Select con apariencia de 3 líneas.
llamada en espera Esperando	Sí	Sí	No	No	Igual que Permitido en espera automática.
Música en espera (Música encendida Mantener)	Sí	Sí	Sí	Sí	Proporcionado por IP Office.
Parque	Sí	No	No	No	
Automático Llamar de vuelta	Sí	No	No	No	
Directo hacia adentro Marcando (DID/ DDI)	Sí	Sí	Sí	Sí	
Transferir	Sí	Sí	Sí	Sí	
Distintivo y Personalizado El sonar	Sí	No	No	No	
Personalizado El sonar	Sí	Sí	No	No	
Mensaje Esperando Indicación (MWI)	Sí	No	No	No	Compatible con algunas estaciones físicas. No es compatible con Agent Desktop. Se evita que las llamadas del Centro de contacto (CC) vayan al correo de voz, por lo que no pueden resultar en una luz MWI en el teléfono. Sin embargo, un agente que maneja una llamada CC ve la luz MWI en su teléfono si un personal

La tabla continúa...

Oficina de PI **telefonía** nombre de la característica	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente **apoyo**		**notas**
	Personal llamadas	**CC** llamadas	llamadas personales	llamadas CC	
					la llamada da como resultado un nuevo mensaje de correo de voz mientras se maneja la llamada CC.
Voz visual	Sí	No	No	No	Compatible solo con algunas estaciones de IP Office y no con Agent Desktop. Se evita que las llamadas del centro de contacto (CC) vayan al correo de voz, por lo que no pueden resultar en mensajes que pueden ser procesado usando Visual Voice en el teléfono. Sin embargo, un agente que atiende una llamada CC puede usar Visual Voice en su teléfono mientras atiende la llamada CC.

Gestión avanzada de llamadas:

Oficina de PI función de telefonía **tu nombre**	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente **apoyo**		**notas**
	Personal llamadas	**CC** llamadas	llamadas personales	llamadas CC	
Texto de ausencia	Sí	Sí	No	No	
Etiquetado de llamadas	Sí	Sí	No	No	La función de etiquetado de llamadas es equivalente a la función de datos adjuntos de llamadas de Avaya Contact Center Select.
Reclamar llamada	Sí	No	No	No	
Grupo de caza Habilitar deshabilitar	Sí	Sí	No	No	Capacidad de un usuario para habilitar y deshabilitar su pertenencia a grupos de búsqueda.
Llamada en espera	Sí	N / A	Sí	N / A	Si un agente de Avaya Contact Center Select está activo en una llamada, no se enrutará otra llamada CC a ese agente. Si un agente de Avaya Contact Center Select está activo en

La tabla continúa...

Oficina de PI función de telefonía **tu nombre**	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente **apoyo**		**notas**
	Personal llamadas	**CC** llamadas	llamadas personales	llamadas CC	
					llamada personal, una llamada CC no se enruta al agente.
No molestar (NOM)	No	No	No	No	Los agentes de Avaya Contact Center Select usan NotReady (con código de motivo).
Plan de marcación	N / A	N / A	N / A	N / A	Se refiere a la configuración del plan de marcación en IP Office. Configure un plan de marcación para enrutar llamadas a extensiones y agentes
Paginación	Sí	Sí	No	No	El teléfono debe tener un altavoz.
Entrometerse	Sí	Sí	No	No	Los supervisores de Avaya Contact Center Select pueden usar las funciones Observar o Irrumpir.
Inclusión	Sí	Sí	No	No	
Llamada privada	Sí	Sí	No	No	
Escritorio compartido	Sí	Sí	N / A	N / A	Esta función permite el uso no exclusivo de una misma extensión por parte de varios usuarios. Una vez que haya iniciado sesión, cualquier llamada a ese usuario se enrutará a la extensión física en la que haya iniciado sesión.
Caliente remoto escritorio	Sí	Sí	N / A	N / A	Esta característica es la misma que 'Hot Desking' pero se refiere específicamente a un usuario configurado en un nodo en particular iniciando sesión en una extensión configurada en otro nodo en la red comunitaria pequeña (SCN).
Relé activado/desactivado/ Legumbres	N / A	N / A	N / A	N / A	
Levantar	Sí	No	No	No	
Grabacion de llamada	Sí	Sí	No	No	
teletrabajador Modo	No	No	No	No	
Hermanamiento y Movilidad	No	No	No	No	

Operación de teclas y lámparas:

Oficina de PI hazaña de telefonía tu nombre	**Soporte de estación de usuario de IP Office**		**Centro de contacto de Avaya Seleccionar estación de agente apoyo**		**notas**
	Personal llamadas	**CC** llamadas	**llamadas personales**	**llamadas CC**	
Apariencia Botones	N / A	N / A	N / A	N / A	
Línea Apariencia	N / A	N / A	N / A	N / A	Máximo tres líneas. Una apariencia de línea es una representación de una línea troncal en el sistema IP Office donde el indicador rastrea la actividad en la línea. Solo se pueden responder o realizar llamadas externas en Apariencias de línea.
Llamar Apariencia Botones	Sí	Sí	No*	No*	Las llamadas individuales son representado individualmente en Agent Desktop, pero no existe el concepto de seleccionar un botón de vista de llamada particular que corresponde al teléfono.
Alerta/Timbre tono para Llamadas cubiertas	Sí	No	No	No	IP Office bloquea las llamadas de Avaya Contact Center Select para que no las cubra.
puenteado Apariencia Botones	No	No	No	No	
Llamada externa Lámpara Indicación	Sí	No	No	No	
Cobertura de llamadas	Sí	No	Sí	No	IP Office bloquea las llamadas de Avaya Contact Center Select para que no las cubra.
Cobertura de llamadas Botones	Sí	N / A	No	N / A	

Manejo de llamadas salientes:

Oficina de PI hazaña de telefonía tu nombre	**Soporte de estación de usuario de IP Office**		**Centro de contacto de Avaya Seleccionar estación de agente apoyo**		**notas**
	Personal llamadas	**CC** llamadas	llamadas personales	llamadas CC	
Códigos de cuenta	Sí	Sí	No	No	
Autorización Códigos	Sí	Sí	No	No	
marcar emergencia	Sí	N / A	No	No	La función Marcar emergencia es equivalente al ACCS Función de llamada de emergencia.
Bloqueo de llamadas	N / A	N / A	N / A	N / A	Avaya Contact Center Select independiente

Selección de ruta alternativa (ARS):

Oficina de PI hazaña de telefonía tu nombre	**Soporte de estación de usuario de IP Office**		**Centro de contacto de Avaya Seleccionar estación de agente apoyo**		**notas**
	Personal llamadas	**CC** llamadas	llamadas personales	llamadas CC	
Llamada máxima Longitud	Sí	Sí	Sí	Sí	Avaya Contact Center Select independiente
Transferible Marcar hacia afuera Privilegio	Sí	N / A	No	N / A	Avaya Contact Center Select independiente
línea inactiva Preferencia	Sí	N / A	No	N / A	Avaya Contact Center Select independiente
Ruta alternativa Selección	N / A	N / A	N / A	N / A	Configure IP Office para seleccionar la troncal adecuada para enrutar las llamadas.

Reenvío:

Oficina de PI hazaña de telefonía tu nombre	**Soporte de estación de usuario de IP Office**		**Centro de contacto de Avaya Seleccionar estación de agente apoyo**		**notas**
	Personal llamadas	**CC** llamadas	**Personal** llamadas	llamadas CC	
Cobertura a Operador	Sí	No	No	No	
Reenviar en Ocupado	Sí	No	No	No	

La tabla continúa...

Oficina de PI hazaña de telefonía tu nombre	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente apoyo		notas
	Personal llamadas	CC llamadas	Personal llamadas	llamadas CC	
Reenviar en No Responder	Sí	No	No	No	
Delantero Incondicional	Sí	No	No	No	
Incondicional Reenviar a Mensaje de voz	Sí	No	No	No	
Caza delantera Grupo	Sí	No	No	No	
Sígueme	Sí	No	No	No	

Características del teléfono Avaya:

Oficina de PI hazaña de telefonía tu nombre	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente apoyo		notas
	Personal llamadas	CC llamadas	llamadas personales	llamadas CC	
Programable Botones	Sí	Sí	No	No	
Lámpara ocupada Campo (BLF) Indicadores	Sí	Sí	No	No	Avaya Contact Center Select independiente
Historial de llamadas	Sí	Sí	No	No	
Idioma	Sí	Sí	No	No	El idioma de Agent Desktop está determinado por la configuración del sistema operativo en el equipo cliente de Agent Desktop, no por el idioma configurado para la extensión de IP Office.
centralizado Personal Directorio	Sí	Sí	No	No	
centralizado Sistema Directorio	Sí	Sí	No	No	
Uno mismo- Administración	No	No	No	No	Los agentes de Avaya Contact Center Select no pueden modificar las propiedades del teléfono.

La tabla continúa...

Oficina de PI hazaña de telefonía tu nombre	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente apoyo		notas
	Personal llamadas	CC llamadas	llamadas personales	llamadas CC	
colgado Discado	Sí	Sí	Sí	Sí	

Manejo de llamadas entrantes. Se aplica solo en modo de conmutación por error a grupos de búsqueda de IP Office:

Oficina de PI hazaña de telefonía tu nombre	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente apoyo		notas
	Personal llamadas	CC llamadas	llamadas personales	llamadas CC	
Llamada entrante Enrutamiento	Sí	Sí	Sí	Sí	La configuración del sistema IP Office decide dónde se enrutan las llamadas entrantes. Una vez que se configura el enrutamiento de llamadas, las llamadas a los agentes se muestran en el teléfono y en Agent Desktop.
Grupos de búsqueda	Sí	N / A	Sí	N / A	
Multi-sitio Redes/ Pequeña Comunidad Redes (SCN) Repartido Caza	Sí	N / A	Sí	N / A	
Servicio Nocturno	Sí	N / A	Sí	N / A	
Perfiles de tiempo	Sí	No	Sí	No	
haciendo cola	Sí	N / A	Sí	N / A	Configure el sistema para limitar la cantidad de llamadas que pueden estar en espera de ser atendidas en un grupo de búsqueda. Por ejemplo, cuando todas las partes del grupo están ocupadas.
Anuncios	Sí	N / A	Sí	N / A	Configurar el sistema para reproducir anuncios en las llamadas esperando ser servicios en un grupo de caza.

Características del centro de contacto:

Oficina de PI hazaña de telefonía tu nombre	**Soporte de estación de usuario de IP Office**		**Centro de contacto de Avaya Seleccionar estación de agente apoyo**		**notas**
	Personal llamadas	**llamadas CC**	**Personal** llamadas	**llamadas CC**	
Adquirir llamada (Robo de llamadas)	Sí	No	No	No	Adquirir llamada puede comportarse como 'Reclamar llamada' o 'Captura de llamada' según cómo se invoque y el estado de los dos usuarios involucrados.
Supervisar llamadas	Sí	No	No	No	Un usuario puede monitorear las llamadas de otras partes escuchando.
Cola Alerta de umbral	N / A	N / A	N / A	N / A	La alerta de umbral de cola se aplica solo en el modo de conmutación por error a los grupos de búsqueda de IP Office.
Acceso	N / A	N / A	N / A	N / A	El inicio de sesión se aplica solo en el modo de conmutación por error para IP Office Hunt Grupos.

Códigos cortos del sistema:

Oficina de PI hazaña de telefonía tu nombre	**Soporte de estación de usuario de IP Office**		**Centro de contacto de Avaya Seleccionar estación de agente apoyo**		**notas**
	Personal llamadas	**llamadas CC**	**Personal** llamadas	**llamadas CC**	
Corto de usuario Códigos	Sí	Sí	No	No	
Cortocircuito del sistema Códigos	Sí	Sí	No	No	
Posmarcación Códigos cortos	Sí	Sí	No	No	
Entrante Número corto Códigos	Sí	Sí	No	No	

Características varias:

Oficina de PI hazaña de telefonía tu nombre	**Soporte de estación de usuario de IP Office**		**Centro de contacto de Avaya Seleccionar estación de agente apoyo**		**notas**
	Personal llamadas	**llamadas CC**	**Personal** llamadas	**llamadas CC**	
Conferencia Llamadas	Sí	Sí	Sí	Sí	

La tabla continúa...

Oficina de PI hazaña de telefonía tu nombre	Soporte de estación de usuario de IP Office		Centro de contacto de Avaya Seleccionar estación de agente apoyo		notas
	Personal llamadas	llamadas CC	Personal llamadas	llamadas CC	
Entrenamiento/Silencio Intrusión/ Página de susurro	Sí	Sí	No	No	
Marcar al recoger	No	No	No	No	Esta función de IP Office también se conoce como Hotline. La función marca automáticamente una extensión específica cuando se descuelga el teléfono. No configure esta función para los agentes de Avaya Contact Center Select.
Descolgado Operación	N / A	N / A	N / A	N / A	La función de estación analógica no es compatible con Avaya Contact Center Select.
E911 Llamada de emergencia	Sí	N / A	Sí	N / A	

Dispositivos de telefonía compatibles

Esta sección especifica los tipos de conexiones de telefonía y los dispositivos admitidos en una solución de Avaya Contact Center Select. La solución Avaya Contact Center Select es compatible con todos los tipos de troncales de la plataforma IP Office. No hay integración directa entre Avaya Contact Center Select e interfaces de enlace troncal de IP Office. La funcionalidad del centro de contactos de Avaya Contact Center Select es independiente de estas troncales de IP Office.

La siguiente tabla enumera las estaciones y los tipos de teléfonos admitidos por Avaya Contact Center Select.

Teléfono del agente	Modelo de teléfono	Centro de contacto de Avaya Seleccione Compatible	notas
Analógico – Todos los modelos		No	
Digital	Serie 9500	Sí	
	Serie 1400	Sí	
	Serie 5400 Serie 2400	Sí	La serie 5400 no es compatible con IP Office 10.xo posterior.

La tabla continúa...

Teléfono del agente	Modelo de teléfono	Centro de contacto de Avaya Seleccione Compatible	notas
IP: H.323	96x1	Sí	
	96x0	Sí	
	Teléfono de escritorio IP J129 Teléfono de escritorio IP J139 Teléfono de escritorio IP J169 Teléfono de escritorio IP J179	Sí	Compatible solo con IP Office 11.0 o posterior.
	Serie 1600	Sí	
	Serie 5600 4610/4620x	Sí	No compatible con IP Office 10.x o posterior.
IP: SORBO	Teléfono IP 1140E Modelo NTYS05 Teléfono IP 1230 Modelo NTYS20 Teléfono IP 1120e Teléfono IP 1220 Teléfono de escritorio IP J129 Teléfono de escritorio IP J139 Teléfono de escritorio IP J169 Teléfono de escritorio IP J179	Sí	Compatible cuando se ejecuta Firmware SIP de IP Office. Se admiten los teléfonos IP 1120e y 1220 solo con IP Office 10.xo posterior. IP de la serie J los teléfonos de escritorio son compatible solo con IP Office 11.0 o posterior.
DECT: todos los modelos		No	
Inalámbrico Wi-Fi – Todos los modelos		No	
Comunicador de Avaya para ventanas		Sí	Soporte de softphone con Oficina de PI.
Softphone de IP Office		Sí	Apoyado como co-softphone residente activado estación de trabajo de agente con Escritorio del agente. No compatible como softphone integrado.

La siguiente tabla muestra la experiencia del agente de Avaya Contact Center Select para varios tipos de teléfonos.

Tipo de telefono	Perfil en Agent Desktop		Conjunto de habilidades en el teléfono		RTPC Número	Grabación Indicación
	El sonar	Conectado	El sonar	Conectado		
96x0 (9640)	Sí	Sí	Sí	Sí	Sí	Sí

La tabla continúa...

Tipo de telefono	Perfil en Agent Desktop		Conjunto de habilidades en el teléfono		RTPC Número	Grabación Indicación
	El sonar	Conectado	El sonar	Conectado		
96x1 (9641)	Sí	Sí	Sí	Sí	Sí	Sí
J129	Sí	Sí	Sí	Sí	Sí	Sí
J139	Sí	Sí	Sí	Sí	Sí	Sí
J169	Sí	Sí	Sí	Sí	Sí	Sí
J179	Sí	Sí	Sí	Sí	Sí	Sí
56xx (5610)	Sí	Sí	Sí	No	Sí	Sí
46xx (4610)	Sí	Sí	Sí	No	Sí	Sí
16xx (1616)	Sí	Sí	Sí	Sí	Sí	Sí
softphone	Sí	Sí	Sí	Sí	Sí	No
95xx (9504)	Sí	Sí	Sí	Sí	Sí	No
54xx (5410)	Sí	Sí	Sí	No	Sí	Sí
24xx (2420)	Sí	Sí	Sí	No	Sí	Sí
14xx (1408)	Sí	Sí	Sí	Sí	Sí	Sí

Soporte de acceso remoto

Avaya Contact Center Select admite el acceso remoto mediante lo siguiente:

- Escritorio remoto de Microsoft Windows
- Servicios de soporte de IP Office (IPOSS)

Ambos admiten la resolución de problemas y el soporte técnico remotos.

Funcionalidad compatible con Communication Control Toolkit

Esta sección compara las funciones compatibles con Avaya Contact Center Select mediante Avaya IP Office con las funciones compatibles con Avaya Aura®Centro de contacto con Avaya Aura® Communication Manager o Avaya Communication Server 1000 (CS 1000).

Communication Control Toolkit y Agent Desktop implementan y utilizan estas funciones. Agent Desktop es un cliente de Communication Control Toolkit, por lo que admiten las mismas funciones.

Las siguientes tablas enumeran las funciones básicas de control de llamadas de Communication Control Toolkit.

Tabla 6: Funciones básicas de Communication Control Toolkit y Avaya Agent Desktop

Evento	Avaya compatible con SIP Aura®Centro de contacto con Avaya Aura®	Avaya basado en AML Aura®Centro de contacto con CS 1000	Centro de contacto de Avaya Seleccione usando IP Office
Hacer una llamada	Sí	Sí	Sí
Poner en espera la llamada actual	Sí	Sí No se admite la función de interruptor Swap Hold de CS 1000.	Sí
Reanudar llamada	Sí (Recuperar llamada)	Sí (Recuperar llamada)	Sí
Desconectar llamada actual (liberar)	Sí	Sí	Sí
Llamada de transferencia ciega	No	Sí	No
Iniciar transferencia supervisada	Sí	Sí	Sí
Transferencia completa	Sí	Sí	Sí
Iniciar llamada de conferencia	Sí	Sí (hasta seis partes)	Sí
Llamada de conferencia completa	Sí	Sí	Sí
Desvío de llamadas	No	Sí	No
Cancelar desvío de llamadas	No	Sí	No
Unirse a la conferencia	Sí, Avaya Aura®solamente	No	Sí
Desviar llamadas	No	No	No
Obtener el estado	Sí	Sí	Sí
Obtener capacidades de llamada	Sí	Sí	Sí
Obtener datos	Sí	Sí	Sí
Borrar datos	Sí	Sí	Sí
Agregar datos	Sí	Sí	Sí
Establecer ocupado (No molestar)	No	Sí (en Agente solo terminales)	No
Obtener/Establecer UUI	Sí	No (UUI adjunto como datos de llamada)	Sí
Enviar DTMF (por ejemplo, número de tarjeta de crédito a IVR)	Sí	Sí	Sí
Silenciar/Activar silencio	No	No	No
Consultar	Sí	Sí (pero debe designar como transferencia o conferencia)	Sí
Aparcar/Desaparcar	No	No	No
Indicador de mensaje en espera	No	No	No

La tabla continúa...

Evento	Avaya compatible con SIP Aura®Centro de contacto con Avaya Aura®	Avaya basado en AML Aura®Centro de contacto con CS 1000	Centro de contacto de Avaya Seleccione usando IP Office
HER (Host Enhanced Enrutamiento)	No	Sí	No
Responder	Sí	Sí	Sí

La funcionalidad de transferencia rápida no admite completar una llamada de transferencia rápida a un número de troncal externo. Esta funcionalidad es para entornos de marcación predictiva en los que la aplicación envía una solicitud MakeCall a un número de cliente externo y, cuando el cliente responde, la aplicación envía la solicitud FastTransfer para transferir ciegamente al cliente a un agente en vivo.

La siguiente tabla enumera las funciones específicas de Contact Center admitidas por Agent Desktop y Communication Control Toolkit.

Tabla 7: Funciones específicas del Contact Center

Evento	Avaya compatible con SIP Aura®Centro de contacto con Avaya Aura®	Avaya basado en AML Aura®Centro de contacto con CS 1000	Centro de contacto de Avaya Seleccione usando IP Office
Inicio de sesión del agente	Sí	Sí	Sí
Cierre de sesión del agente	Sí	Sí	Sí
Listo	Sí	Sí	Sí
Establecer no listo	Sí	Sí	Sí
Código de actividad de conjunto de ACD	Sí	Sí	Sí
Conjunto de ACD no listo/Código de motivo	Sí	Sí	Sí
Código de elemento de trabajo posterior a la llamada establecido de ACD	Sí	Sí	Sí
Soporte de llave lista para trabajar	No	No	No
agente susurro	No	No	No
Observar llamada	Sí	No	Sí
Establecer tratamiento de llamadas	No	Sí	No
Entrometerse	Sí	No	Sí
Supervisor de llamadas	Sí	Sí	Sí
Llave de emergencia	Sí	Sí	Sí
Redirigir a otro conjunto de habilidades	No, debe transferirse a un CDN (punto de ruta)	No	No, debe transferirse a un CDN (punto de ruta)
Devolver una llamada al perfil de la cola de donde provino	No	No	No
Redirigir a otro conjunto de habilidades	No	No	No
Devolver una llamada al perfil de la cola de donde provino	No	No	No

Página227 de 3226.

La siguiente tabla enumera los eventos entregados por Communication Control Toolkit.

Tabla 8: Eventos del kit de herramientas de control de comunicación

Evento	Avaya compatible con SIP Aura®Centro de contacto con Avaya Aura®	Avaya basado en AML Aura®Centro de contacto con CS 1000	Centro de contacto de Avaya Seleccione usando IP Office
Evento de llamada	Sí	Sí	Sí
Evento de tono de marcación	No	No	No
Evento ocupado	No	No	No
Evento de ofrenda	Sí	Sí	Sí
Evento de devolución de llamada	Sí	Sí	Sí
Evento conectado entrante	Sí	Sí	Sí
Evento conectado saliente	Sí	Parcial	Sí
Evento conectado	Sí	Sí	Sí
Evento desconectado	Sí	Sí	Sí
Evento realizado	Sí	Sí	Sí
Evento no realizado	Sí	Sí	Sí
Evento de conferencia pendiente en espera	Sí	Sí	Sí
Evento de transferencia pendiente en espera	Sí	Sí	Sí
Evento transferido	Sí	Sí	Sí
Evento de conferencia	Sí	Sí	Sí
Evento de transferencia iniciado	Sí	Sí	Sí
Evento de conferencia iniciado	Sí	Sí	Sí
Evento de desconexión de sesión (incluye apagado)	Sí	Sí	Sí
Evento de reenvío de dispositivo	No	No	No
Evento de cambio de estado	Sí	Sí	Sí
Mensaje de aviso en espera Evento	No	No	No
Aviso de evento sin mensaje en espera	No	No	No
Evento de cierre de sesión del agente	Sí	Sí	Sí
Evento de inicio de sesión del agente	Sí	Sí	Sí
Evento de agente listo	Sí	Sí	Sí
Evento de agente no listo	Sí	Sí	Sí
Evento de agente ocupado	No	No	No

La tabla continúa...

Evento	Avaya compatible con SIP Aura®Centro de contacto con Avaya Aura®	Avaya basado en AML Aura®Centro de contacto con CS 1000	Centro de contacto de Avaya Seleccione usando IP Office
Evento de trabajo listo del agente	No	No	No
Código de actividad ingresado	Sí	Sí	Sí
WalkAway activado	No	No	No
Regreso de WalkAway	No	No	No
Emergencia invocada	No	No	No
Supervisor de llamada invocado	No	No	No

Capítulo 8: Avaya Aura®Portal de experiencia Integración

Aura de Avaya®Experience Portal es una plataforma de software de autoservicio basada en estándares abiertos que ofrece confiabilidad y escalabilidad líderes en la industria para ayudar a reducir costos y simplificar las operaciones.

Aura de Avaya®Experience Portal se implementa en servidores Linux estándar y admite la integración con sistemas habilitados para SIP, incluidos Avaya Contact Center Select e IP Office.

El aura de Avaya®El sistema Experience Portal consta de un Experience Portal Manager (EPM), que controla el sistema Experience Portal y los servidores Media Processing Platform (MPP), que procesan todas las llamadas. El sistema Experience Portal generalmente incluye un servidor de reconocimiento automático de voz (ASR), servidores de voz de texto a voz (TTS) y servidores de aplicaciones.

Avaya Contact Center Select admite los siguientes tipos de integración con Avaya Aura®
Portal de experiencias:

- Interfaz Avaya Aura®Portal de experiencia
- Avaya Aura de back-end®Experience Portal utilizando la información del encabezado SIP
- Avaya Aura de back-end®Experience Portal utilizando la creación de contexto

En una interfaz Avaya Aura®Integración de Experience Portal, Avaya Aura procesa primero la llamada del cliente® Experience Portal y luego por Avaya Contact Center Select. En un back-end Avaya Aura®Integración de Experience Portal, la llamada del cliente es procesada primero por Avaya Contact Center Select y luego por Avaya Aura®Portal de experiencias. Avaya Contact Center Select es compatible con Avaya Aura front-end y back-end®Experimente la integración del Portal en una única solución.

Los siguientes mecanismos admiten la transferencia de llamadas y datos de llamadas entre Avaya Aura®Portal de Experiencia y Centro de Contacto:

- Información del encabezado SIP. SIP incluye una serie de encabezados de mensajes en cada mensaje SIP. Estos encabezados contienen información que permite al receptor comprender y utilizar el mensaje correctamente. En una solución de centro de contacto, los encabezados SIP se pueden usar para transferir pequeñas cantidades de información relacionada con llamadas entre aplicaciones habilitadas para SIP. Avaya Contact Center Select es compatible con el encabezado SIP de información de usuario a usuario (UUI) y el encabezado privado SIP P-Intrinsics personalizado de Avaya.
- Cuerpo del mensaje SIP INFO mediante la creación de contexto: si la información de contexto relacionada con la llamada no cabe en un encabezado de información de usuario a usuario (UUI) de SIP o en el encabezado P-Intrinsics más grande, puede usar la aplicación de ejemplo de creación de contexto para pasar más información de contexto de Avaya Aura®Experience Portal para Avaya Contact Center Select. Esta aplicación de ejemplo de creación de contexto puede devolver múltiples valores de Avaya Aura®Experience Portal, en lugar del valor único devuelto por la aplicación de muestra Play and Collect. El ejemplo de creación de contexto

La aplicación puede devolver información de contexto relacionada con la llamada en un cuerpo de mensaje SIP INFO. Un cuerpo de mensaje SIP INFO contiene y transfiere mucha más información que un encabezado SIP.

En una solución basada en la plataforma IP Office, Avaya Contact Center Select admite los siguientes métodos de integración con Avaya Aura®Portal de experiencias:

- Información del encabezado SIP
- Mensaje SIP INFO utilizando la creación de contexto

No hay requisitos de licencia adicionales para Avaya Contact Center Select y Avaya Aura® Integración del portal de experiencias.

Métodos de transferencia de datos

La siguiente tabla muestra la cantidad máxima de datos que admite cada tipo de transferencia:

Método de transferencia	Datos máximos admitidos por Contact Center
Encabezado UUI SIP usando ASAI	96 bytes máximo.
Encabezado SIP P-Intrinsics	Depende de tu solución.Nota 1
Cuerpo del mensaje SIP INFO mediante la creación de contexto	Máximo total de 8K bytes: • Máximo de 10 pares clave-valor ASCII. • Y 1K caracteres de datos adjuntos de llamadas (CAD) dentro de la aplicación CC.
Nota 1Las siguientes limitaciones se aplican a la información del encabezado SIP de P-Intrinsics: • La cantidad de información P-Intrinsics asociada con una llamada depende de los otros encabezados SIP en la llamada y en la ruta del flujo de la llamada. Por lo general, Contact Center admite hasta 10 pares clave-valor ASCII de P-Intrinsics.	

Contact Center admite pares clave-valor ASCII con un nombre de clave de hasta 25 caracteres y un tamaño de valor de hasta 80 caracteres.

Aura de Avaya®Diseñador de orquestación del portal de experiencia

Aura de Avaya®Experience Portal Orchestration Designer es un entorno de desarrollo de aplicaciones basado en Eclipse que admite el desarrollo de aplicaciones de voz Voice XML y CCXML. Orchestration Designer genera Avaya Aura®Experimente las aplicaciones basadas en XML compatibles con Portal que se implementan en servidores de aplicaciones de software como Apache Tomcat Server en una solución de autoservicio.

XML de voz

Voice XML (VXML) es un formato XML estándar para especificar diálogos de voz interactivos entre un humano y una computadora. Voice XML está diseñado para crear diálogos de audio que cuentan con voz sintetizada, audio digitalizado, reconocimiento de entrada hablada y tecla DTMF, grabación de entrada hablada, telefonía y conversaciones de iniciativa mixta. Una aplicación típica de reproducción y recopilación de XML de voz reproduce indicaciones de voz a los clientes pidiéndoles que ingresen dígitos usando su teléfono. Luego, la aplicación recopila los dígitos del cliente y los devuelve para su procesamiento al centro de contacto.

XML de control de llamadas

Call Control XML (CCXML) es un lenguaje de marcado estándar para controlar cómo se realizan, responden, transfieren, realizan conferencias y más las llamadas telefónicas. CCXML funciona con Voice XML para proporcionar una solución basada en XML para cualquier aplicación de telefonía. Voice XML y CCXML son dos idiomas separados y no se requieren en una implementación de ninguno de los dos. Por ejemplo, CCXML se puede integrar con un sistema de respuesta de voz interactiva (IVR) más tradicional y los sistemas de diálogo Voice XML se pueden integrar con otros sistemas de control de llamadas.

Avaya Contact Center Select compatible con SIP

Avaya Contact Center Select utiliza la arquitectura del Protocolo de inicio de sesión (SIP) para brindar la máxima interoperabilidad y flexibilidad. Avaya Contact Center Select habilitado para SIP simplifica la arquitectura de la solución y las implementaciones de CTI. La arquitectura habilitada para SIP de Avaya Contact Center Select y los datos intrínsecos de contacto facilitan el desarrollo de aplicaciones de pantalla emergente, lo que reduce el tiempo, el esfuerzo y el costo necesarios para lanzar nuevas capacidades.

Contact Center Manager Server (CCMS) contiene un componente SIP Gateway Manager (SGM) que es el procesador de llamadas en un Contact Center habilitado para SIP. SIP Gateway Manager es un elemento SIP independiente que puede recibir y procesar llamadas desde sistemas de comunicación habilitados para SIP como IP Office.

Avaya Contact Center Select admite información de encabezado SIP de información de usuario a usuario (UUI) e información de encabezado SIP intrínseco P. Contact Center utiliza la información del encabezado en cada llamada SIP para generar información intrínseca de contacto relacionada con la llamada y datos adjuntos de llamada (CAD). Estos datos intrínsecos de contacto pueden contener información relevante para esa llamada, el cliente que llama y otra información recuperada por aplicaciones de autoservicio o de terceros. Los intrínsecos de contacto son pares clave-valor de cantidades de datos relativamente pequeñas. Los datos adjuntos de llamadas son una cantidad de datos no estructurada más larga.

En una solución de centro de contacto habilitada para SIP, la información almacenada en algunos mensajes SIP INFO se puede usar para transferir información relacionada con llamadas entre componentes habilitados para SIP. Esta información relacionada con la llamada permite que el receptor comprenda y maneje mejor la llamada. Si la información de contexto relacionada con la llamada no cabe en un encabezado de información de usuario a usuario (UUI) de SIP o en el P-

Encabezado intrínseco, puede usar la aplicación de creación de contexto de muestra para pasar más información de contexto de Avaya Aura®Experience Portal para Avaya Contact Center Select. La aplicación de muestra de creación de contexto puede inyectar múltiples piezas de información de contexto (intrínsecos y datos adjuntos de llamadas) en Avaya Contact Center Select, mientras que la aplicación de muestra Play and Collect puede recuperar solo una pieza de datos, por ejemplo, dígitos recopilados. La información de contexto relacionada con la llamada se devuelve en un cuerpo de mensaje SIP INFO. Un cuerpo de mensaje SIP INFO contiene y transfiere mucha más información que un encabezado SIP.

Los datos intrínsecos de contacto enriquecen el contexto y la información que se presenta a los agentes con cada contacto con el cliente. Los datos intrínsecos de contacto facilitan el desarrollo de pantallas emergentes, lo que reduce el tiempo, el esfuerzo y el costo necesarios para lanzar nuevas capacidades. Avaya recomienda que utilice datos intrínsecos de contacto.

Encabezado SIP intrínseco P

Avaya Contact Center Select admite el encabezado privado P-Intrinsics personalizado. El Protocolo de inicio de sesión (SIP) incluye varios encabezados de mensajes en cada mensaje SIP. Estos encabezados contienen información que permite al receptor comprender y utilizar el mensaje correctamente. En una solución de centro de contacto, puede usar encabezados SIP para transferir pequeñas cantidades de información relacionada con llamadas entre aplicaciones habilitadas para SIP. La aplicación que recibe este mensaje SIP lee estos encabezados y realiza alguna acción basada en el contenido de los encabezados. La información del encabezado SIP puede proporcionar datos adicionales sobre una llamada que las aplicaciones pueden usar para procesar esa llamada.

Puede utilizar la información de encabezado de P-Intrinsics para pasar información de contexto entre aplicaciones habilitadas para SIP. Avaya Contact Center Select analiza la información del encabezado SIP de P-Intrinsics y la utiliza para crear datos adjuntos de llamadas o intrínsecos de contacto. Puede usar P-Intrinsics junto con información de usuario a usuario (UUI) si se requiere compatibilidad con versiones anteriores de aplicaciones existentes.

Los encabezados privados SIP (P-Headers) son puramente informativos. No crean nuevos comandos y no interfieren con la transmisión regular de mensajes SIP. Los encabezados privados SIP se usan solo para pasar información adicional que la aplicación receptora puede usar. Avaya Contact Center Select admite el encabezado SIP P-Intrinsics en los mensajes SIP INVITE entrantes.

Los componentes que admiten este encabezado privado incluyen sistemas IVR front-end como Avaya Aura® Experience Portal y otras entidades habilitadas para SIP en el flujo de llamadas.

La información de P-Intrinsics no está restringida por limitaciones heredadas como UUI. La información de P-Intrinsics puede crecer en tamaño, dependiendo de otros encabezados en la llamada y en la ruta del flujo de la llamada. También se puede usar para inyectar datos adjuntos de llamadas. Por lo tanto, es más flexible que los datos UUI. Puede usar ambos encabezados juntos y los clientes pueden conservar la compatibilidad con versiones anteriores con aplicaciones que ya usan datos de UUI.

Solución típica usando P-Intrinsics

Avaya Aura de front-end®El sistema Experience Portal utiliza aplicaciones de voz XML e información de encabezado SIP para integrarse con Avaya Contact Center Select. Una aplicación de voz XML de voz de autoservicio que se ejecuta en Avaya Aura®Experience Portal: el servidor de aplicaciones responde las llamadas de los clientes y recopila información asociada a las llamadas en función de las respuestas y entradas de los clientes.

Página233 de 3226.

Luego, Experience Portal transfiere la llamada del cliente, completa con esta información asociada a la llamada almacenada en el encabezado SIP de P-Intrinsics, a Avaya Contact Center Select.

Contact Center utiliza el encabezado P-Intrinsics para generar datos intrínsecos de contacto y/o datos adjuntos de llamada específicos para esa llamada. Si esta llamada finalmente es respondida por un agente, el agente puede usar los datos intrínsecos de contacto relacionados con la llamada para acceder a los detalles del cliente. Los agentes pueden recibir los datos intrínsecos del contacto en una pantalla emergente o pueden necesitar acceder a estos detalles manualmente mediante Agent Desktop.

Los P-Intrinsics reducen la cantidad de tiempo que los agentes dedican a cada llamada, mejoran la experiencia del cliente y hacen que el Contact Center sea más eficiente.

Información de usuario a usuario

Los sistemas habilitados para SIP pueden usar información de usuario a usuario (UUI) para transmitir pequeñas cantidades de datos entre sistemas dentro de mensajes de encabezado SIP.

Las aplicaciones XML de voz pueden utilizar la información del encabezado SIP para recopilar, almacenar y transportar información relacionada con las llamadas de los clientes. La aplicación Voice XML puede usar los datos de la entrevista del cliente para modificar el encabezado SIP y luego pasar la llamada del cliente junto con los datos del encabezado actualizados a la siguiente aplicación en la solución. Las aplicaciones XML de voz también pueden usar la información del encabezado SIP para tomar decisiones de procesamiento sobre la llamada de un cliente. Los ejemplos de datos UUI del encabezado SIP incluyen un número de cuenta de cliente obtenido durante una entrevista de autoservicio con el cliente.

Agent Desktop y Contact Center Orchestration Designer también pueden modificar la información de usuario a usuario.

Estos datos de UUI del encabezado SIP se pueden usar para admitir Avaya Aura®Secuenciación de aplicaciones.

Identificador de llamada universal

Universal Call Identifier (UCID) es un identificador de llamadas propiedad de Avaya que se utiliza para ayudar a correlacionar registros de llamadas entre diferentes sistemas. La información del identificador de llamada universal, cuando está habilitada, se agrega a los datos de información de usuario a usuario (UUI) en las llamadas SIP.

Este identificador puede ser generado por Avaya Aura®Servidor Experience Portal MPP. El identificador de llamada universal se puede pasar a Avaya Aura®Experience Portal a través de los encabezados SIP de una aplicación.

Interfaz Avaya Aura®Experience Portal y Contact Center habilitado para SIP

Un Avaya Aura combinado®El sistema de autoservicio Experience Portal y la solución Avaya Contact Center Select brindan a sus clientes un servicio excepcional y una eficiencia mejorada. La automatización de autoservicio front-end reduce los costos operativos del centro de contacto y mejora la satisfacción del cliente (CSAT).

Aura de Avaya®Experience Portal utiliza aplicaciones de voz XML e información basada en mensajería SIP para integrarse con Avaya Contact Center Select. Una aplicación de voz XML de voz de autoservicio que se ejecuta en Avaya Aura®El servidor de aplicaciones Experience Portal Tomcat responde a las llamadas de los clientes y modifica la información de usuario a usuario (UUI) asociada a la llamada en función de las respuestas y entradas de los clientes. Cuando las llamadas de los clientes se transfieren a los agentes de Contact Center, los agentes utilizan los datos intrínsecos de contacto relacionados con las llamadas para acceder a los detalles del cliente. Esto reduce la cantidad de tiempo que los agentes dedican a cada llamada, mejora la experiencia del cliente y hace que el Centro de contacto sea más eficiente.

Avaya recomienda que cree sus aplicaciones de voz XML con Avaya Aura®

Diseñador de orquestación. Aura de Avaya®Experience Portal incluye automáticamente todas las aplicaciones de Orchestration Designer en el informe de resumen de la aplicación y el informe de detalles de la aplicación. Si desea que estos informes muestren mensajes e información de estado de una aplicación desarrollada en una herramienta de terceros, debe registrar manualmente los mensajes y la información de estado de esa aplicación mediante el servicio web de registro de aplicaciones.

El siguiente diagrama muestra un diseño de solución típico de una interfaz Avaya Aura®Experimente la integración de autoservicio del Portal con Avaya Contact Center Select e IP Office.

Traducido del inglés al español - www.onlinedoctranslator.com

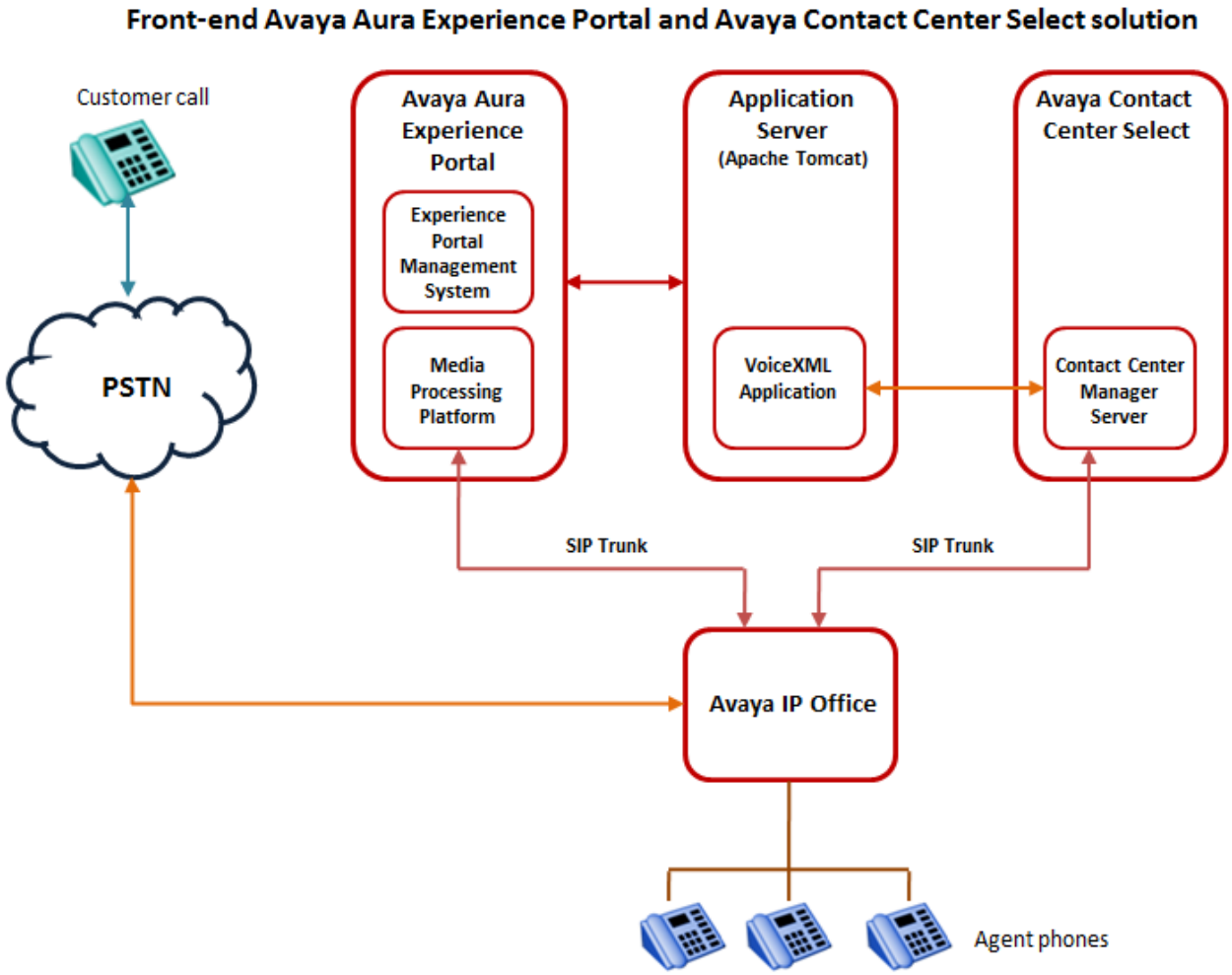


Figura 12: Ejemplo de interfaz Avaya Aura®Experience Portal y Contact Center habilitado para SIP

Ejemplo de flujo de llamadas para el front-end Avaya Aura®Experience Portal y Contact Center habilitado para SIP

Este ejemplo de flujo de llamadas muestra cómo Avaya Aura®El sistema Experience Portal interactúa con Avaya Contact Center Select para manejar una transacción de cliente de autoservicio de front-end automatizada típica.

1. Las llamadas entrantes de los clientes se enrutan a un servidor de plataforma de procesamiento de medios (MPP) en Avaya Aura®Sistema Portal de Experiencias.
2. El servidor MPP verifica el Servicio de identificación del número marcado (DNIS) para la llamada entrante y usa la información de configuración descargada del servidor Experience Portal Manager (EPM) para hacer coincidir el número con una aplicación de voz en Avaya Aura®
   Portal de experiencias.

3. Experience Portal Management System inicia una sesión de Avaya Voice Browser y le pasa el Indicador de recursos universal (URI) especificado para la aplicación de voz seleccionada.

4. Avaya Voice Browser se comunica con el servidor de aplicaciones y le pasa el URI.

5. El servidor de aplicaciones devuelve una página XML de voz a Avaya Voice Browser.

6. Según las instrucciones de la aplicación Voice XML, el MPP utiliza archivos de audio pregrabados, texto a voz (TTS) o ambos para reproducir un aviso para iniciar la interacción con la persona que llama.

7. Si el cliente responde ingresando dígitos de multifrecuencia de doble tono (DTMF), el MPP establece una conexión con un servidor TTS y el texto ASCII en la aplicación de voz se reenvía para su procesamiento. El servidor TTS presenta el texto como salida de audio en forma de voz sintetizada que luego el MPP reproduce para la persona que llama.

8. El cliente elige hablar con un agente.

9. La aplicación Voice XML se conecta al Contact Center Manager Server. La aplicación Voice XML especifica un número de directorio controlado (CDN) o agente de destino, el tipo de transferencia (transferencia ciega, en puente o consulta), el número de identificación del contacto y los datos de UUI generados por los datos intrínsecos del contacto.

10. El servidor de la Plataforma de procesamiento de medios (MPP) de Experience Portal completa la transferencia ciega de la llamada del cliente a la CDN de destino.

11. El Contact Center Manager Server SIP Gateway Manager (SGM) ahora controla la llamada del cliente. El SGM enruta la llamada a un perfil de agente apropiado.

12. Se ofrece la llamada a un agente del Contact Center. El agente puede acceder a los detalles del cliente y a los datos intrínsecos del contacto antes de responder la llamada.

13. El agente de Contact Center recibe la información de contexto (cliente y llamada) en una pantalla emergente y responde la llamada del cliente.

14. La aplicación XML finaliza la llamada cuando finaliza la ejecución o cuando la persona que llama cuelga.

Un Avaya Aura combinado®El sistema de autoservicio Experience Portal y la solución Avaya Contact Center Select brindan a los clientes un servicio excepcional y una mayor eficiencia. La automatización de autoservicio front-end reduce los costos operativos del centro de contacto y mejora la satisfacción del cliente (CSAT).

Aura de Avaya®Experience Portal utiliza aplicaciones XML de voz e información de encabezado SIP (UUI y P-Intrinsics) para integrarse con Avaya Contact Center Select. Esto brinda a las empresas flexibilidad y control completos de la solución integrada. La interfaz Avaya Aura®El sistema de autoservicio Experience Portal y la solución Avaya Contact Center Select son altamente flexibles y eficientes. Avaya suministra aplicaciones XML de voz de muestra para la rápida integración de un front-end Avaya Aura®
Experimente el sistema Portal con Avaya Contact Center Select.

Avaya Aura de back-end®Experience Portal y Contact Center habilitado para SIP

Aura de Avaya®Experience Portal proporciona servicios back-end de respuesta de voz interactiva (IVR) como texto a voz, recopilación de dígitos, música y reconocimiento de voz. Un Avaya Aura combinado®
El sistema Experience Portal y la solución Avaya Contact Center Select brindan a sus clientes un servicio excepcional y una eficiencia mejorada. La respuesta de voz interactiva (IVR) de back-end reduce los costos operativos del centro de contacto y mejora la satisfacción del cliente (CSAT).

En un back-end típico de Avaya Aura®solución Experience Portal, las llamadas de los clientes a Avaya Contact Center Select se enrutan a las aplicaciones Experience Portal para el procesamiento automatizado. Aura de Avaya®
Las aplicaciones de Experience Portal reproducen indicaciones de voz que le piden al cliente que seleccione elementos de un menú o que ingrese números de cuenta. El cliente responde ingresando dígitos en su teléfono o hablando (Experience Portal admite servidores opcionales de reconocimiento automático de voz). Las aplicaciones de Experience Portal luego recopilan la respuesta del cliente y la devuelven a Avaya Contact Center Select para tratamientos adicionales o enrutamiento al siguiente agente disponible y apropiado.

El siguiente diagrama muestra un diseño de solución típico de Avaya Contact Center Select con un backend Avaya Aura®Integración del portal de experiencias.

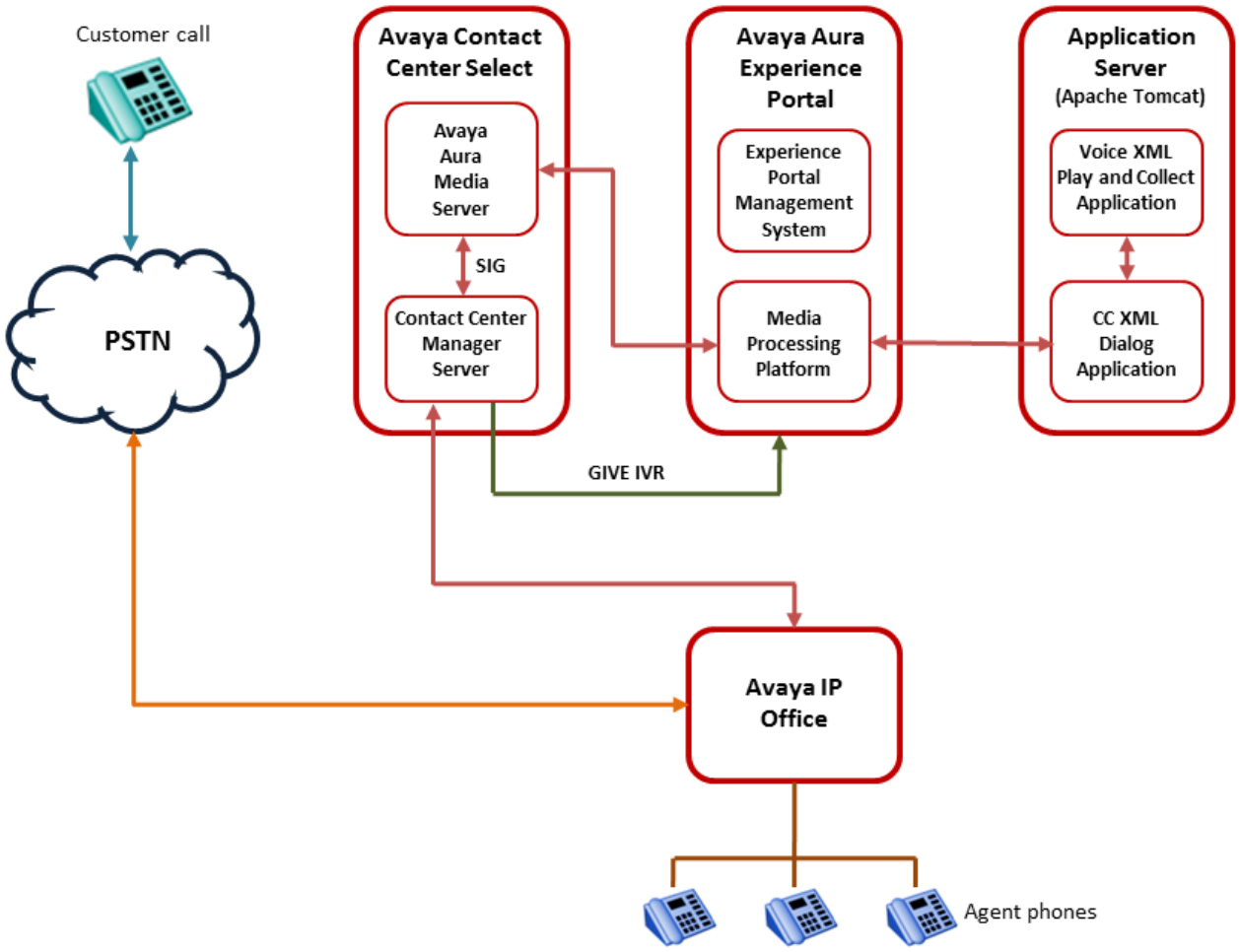


Figura 13: Ejemplo de back-end Avaya Aura®Experience Portal y Contact Center habilitado para SIP

Ejemplo de flujo de llamadas usando el back-end Avaya Aura®Experience Portal y Contact Center habilitado para SIP

Este ejemplo de flujo de llamadas muestra cómo Avaya Aura®El sistema Experience Portal interactúa con Avaya Contact Center Select para manejar una transacción típica de cliente de respuesta de voz interactiva (IVR) de back-end automatizada.

1. Las llamadas de clientes entrantes a IP Office se enrutan a Avaya Contact Center Select.
2. Avaya Contact Center Select responde la llamada y ejecuta una aplicación de flujo, un script y/o scripts principales opcionales. Un script principal es una aplicación ejecutada o referenciada por el Master Script. Contact Center Manager Server registra las acciones del script principal y del script principal en registros estadísticos.

3. El script de Avaya Contact Center Select emite unDAR IVRpara un servidor de medios externo (XDIALOG), proporcionando el identificador URI de Avaya Aura®Portal de experiencias.
4. Avaya Contact Center Select retiene el control de la llamada y envía unINVITACIÓN SIPmensaje a Avaya Aura®Portal de experiencias. Avaya Contact Center Select especifica los parámetros de tratamiento en el INVITACIÓN SIPmensaje.
5. Aura de Avaya®Experience Portal pasa la llamada a una aplicación de diálogo CCXML en el servidor de aplicaciones Apache Tomcat.
6. La aplicación de diálogo CCXML acepta y recupera los parámetros IVR delINVITACIÓN SIPmensaje.
7. La aplicación de diálogo CCXML invoca la aplicación XML Play and Collect Voice (PlayAndCollect) con los parámetros recuperados de Avaya Contact Center Select. Si está disponible, los datos UUI del encabezado SIP también se extraen y pasan a la aplicación Voice XML.
8. La aplicación Play and Collect Voice XML transmite flujos de protocolo de transporte en tiempo real (RTP) al Avaya Aura asociado®Conferencia de Media Server y solicita al cliente que ingrese dígitos en su teléfono.
9. La aplicación XML Play and Collect Voice recopila los dígitos ingresados por el cliente.
10. La aplicación XML Play and Collect Voice luego pasa los dígitos del cliente a la aplicación de diálogo CCXML.
11. La aplicación de diálogo CCXML devuelve los dígitos recopilados a Avaya Contact Center Select en un INFORMACIÓN SIPmensaje.
12. La aplicación de diálogo CCXML luego se cierra (ADIÓS).
13. El guión de Avaya Contact Center Select recupera los dígitos recopilados de IVR.

Una combinación de Avaya Contact Center Select y Avaya Aura®La solución Experience Portal brinda a los clientes un servicio excepcional y una mayor eficiencia. Avaya Aura de back-end®La automatización de Experience Portal reduce los costos operativos del centro de contacto y mejora la satisfacción del cliente (CSAT).

Avaya Contact Center Select utiliza las aplicaciones Call Control XML y Voice XML para integrarse con Avaya Aura® Portal de experiencias. Esto brinda a las empresas flexibilidad y control completos de la integración de la solución. El aura de Avaya®El sistema Experience Portal y la solución Avaya Contact Center Select son altamente flexibles y eficientes. Avaya proporciona aplicaciones XML de voz de muestra para la rápida integración de un back-end Avaya Aura®Experimente el sistema Portal con Avaya Contact Center Select.

Avaya Aura de back-end®Experience Portal usando Context Creation y Contact Center habilitado para SIP

Aura de Avaya®Experience Portal proporciona servicios back-end de respuesta de voz interactiva (IVR) como texto a voz, recopilación de dígitos, música y reconocimiento de voz. Un Avaya Aura combinado®

El sistema Experience Portal y la solución Avaya Contact Center Select brindan a sus clientes un servicio excepcional y una eficiencia mejorada.

Avaya Contact Center Select proporciona aplicaciones de muestra genéricas para demostrar cómo se integra con Avaya Aura®Portal de experiencias. Puede seleccionar una aplicación de muestra que se adapte a su integración, revisar el código de muestra y personalizarlo para su solución antes de implementarlo en producción.

En una solución de centro de contacto habilitada para SIP, la información almacenada en algunos mensajes SIP INFO se puede usar para transferir información relacionada con llamadas entre componentes habilitados para SIP. Esta información relacionada con la llamada permite que el receptor comprenda y maneje mejor la llamada. Si su información de contexto relacionada con la llamada no cabe en un encabezado de información de usuario a usuario (UUI) de SIP o en el encabezado más grande de P-Intrinsics, puede usar la aplicación de creación de contexto de muestra para pasar más información de contexto de Avaya Aura®Experience Portal para Avaya Contact Center Select.

La aplicación de muestra de creación de contexto puede inyectar múltiples piezas de información de contexto (intrínsecos y datos adjuntos de llamadas) en Avaya Contact Center Select, mientras que la aplicación de muestra Play and Collect puede recuperar solo una pieza de datos, por ejemplo, dígitos recopilados.

En un back-end típico de Avaya Aura®Solución Experience Portal, las llamadas de los clientes a Avaya Contact Center Select se enrutan a Avaya Aura®Aplicaciones Experience Portal para procesamiento automatizado. Aura de Avaya®Las aplicaciones de Experience Portal reproducen indicaciones de voz que le piden al cliente que seleccione elementos de un menú o que ingrese números de cuenta. El cliente responde ingresando dígitos en su teléfono o hablando (Avaya Aura®Experience Portal admite servidores de reconocimiento automático de voz opcionales). El aura de Avaya®Luego, las aplicaciones de Experience Portal recopilan la respuesta del cliente y la devuelven a Avaya Contact Center Select para tratamientos adicionales o enrutamiento al siguiente agente disponible y apropiado.

En una integración de back-end donde Avaya Aura®Experience Portal está utilizando la aplicación de muestra Context Creation, el script Avaya Contact Center Select Orchestration Designer envía un mensaje GIVR IVR (SIP INVITE) a Avaya Aura®Sistema Portal de Experiencias. El mensaje SIP INVITE tiene "tipo de tratamiento" establecido en "creación de contexto". Aura de Avaya®Experience Portal pasa la llamada SIP a una aplicación XML de Dialog CC de muestra. Las aplicaciones Dialog CC XML y Context Creation VoiceXML procesan la llamada y devuelven información relacionada con la llamada codificada en hexadecimal. Debido a que el "tipo de tratamiento" se configuró en "creación de contexto", la aplicación Dialog devuelve un mensaje SIP INFO del tipo "aplicación/x-aacc-info" al centro de contacto. El Contact Center SIP Gateway Manager (SGM) reconoce este tipo de mensaje SIP y convierte la información de contexto en la llamada en Contact Intrinsics. La secuencia de comandos de Orchestration Designer puede acceder y utilizar los Intrínsecos de contacto para la llamada, y Contact Center puede pasarlos a Agent Desktop.

Esta muestra de aplicaciones de creación de contextos y diálogos puede devolver múltiples valores de Avaya Aura ®Experience Portal, en lugar del valor único devuelto por la aplicación de ejemplo Avaya Contact Center Select Play and Collect VoiceXML. La aplicación de muestra Context Creation admite datos más complejos. La información de contexto relacionada con la llamada se devuelve en un cuerpo de mensaje SIP INFO. Un cuerpo de mensaje SIP INFO contiene y transfiere mucha más información que un encabezado SIP.

Cuando se utiliza la aplicación de muestra Context Creation, los datos del cuerpo del mensaje SIP tienen codificación hexadecimal y formato XML (usando la misma codificación que P-Intrinsics).

Ejemplo de un solo intrínseco en código VoiceXML (Nota: los espacios no son compatibles):

<cc>CUSTOMER_SESSION_ID=12345</cc>

Ejemplo del intrínseco único cuando está codificado en Hex:

3c63633e3c693e435553544f4d45525f53455353494f4e5f49443d31323334353c2f693e3c2f63633e

El siguiente diagrama muestra un diseño de solución típico de un Avaya Contact Center Select con un back-end Avaya Aura®Integración del portal de experiencias.

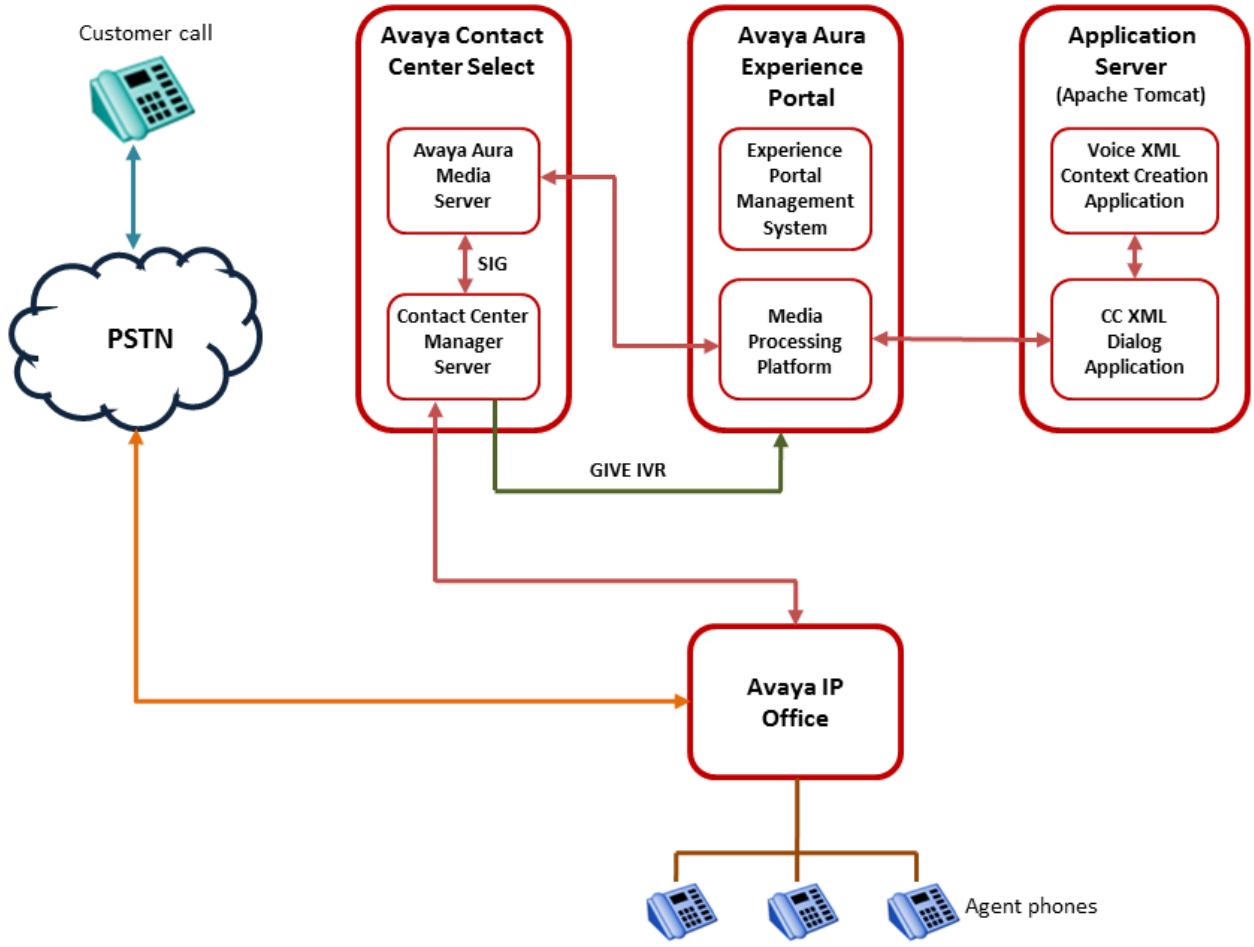


Figura 14: Ejemplo de back-end Avaya Aura®Experience Portal utilizando la aplicación de muestra Context Creation

Ejemplo de flujo de llamadas usando el back-end Avaya Aura®Experience Portal con la aplicación de muestra Context Creation

Este ejemplo de flujo de llamadas muestra cómo Avaya Aura®El sistema Experience Portal interactúa con Avaya Contact Center Select para manejar una transacción típica de cliente de respuesta de voz interactiva (IVR) de back-end automatizada.

1. Las llamadas de clientes entrantes a IP Office se enrutan a Avaya Contact Center Select.
2. Avaya Contact Center Select responde la llamada y ejecuta un guión y/o guiones principales opcionales. Un script principal es una aplicación ejecutada o referenciada por el Master Script. Contact Center Manager Server registra las acciones del script principal y del script principal en registros estadísticos.
3. El script de Avaya Contact Center Select emite unDAR IVRpara un servidor de medios externo (XDIALOG), proporcionando el identificador URI de Avaya Aura®Portal de experiencias.
4. Avaya Contact Center Select retiene el control de la llamada y envía unINVITACIÓN SIPmensaje a Avaya Aura®Portal de experiencias. Avaya Contact Center Select especifica los parámetros de tratamiento en el INVITACIÓN SIPmensaje. El mensaje SIP INVITE tiene "tipo de tratamiento" establecido en "creación de contexto".
5. Aura de Avaya®Experience Portal pasa la llamada a la aplicación de diálogo CCXML de ejemplo en el servidor de aplicaciones Apache Tomcat.
6. La aplicación de diálogo CCXML acepta y recupera los parámetros IVR delINVITACIÓN SIPmensaje.
7. La aplicación de diálogo CCXML invoca la aplicación Context Creation Voice XML con los parámetros recuperados de Avaya Contact Center Select.
8. La aplicación Context Creation Voice XML transmite flujos de protocolo de transporte en tiempo real (RTP) al Avaya Aura asociado®Conferencia de Media Server y solicita al cliente que ingrese dígitos en su teléfono.
9. La aplicación Context Creation Voice XML recopila los dígitos ingresados por el cliente.
   - Si los dígitos coinciden con el primer número de cuenta (AccountA=123123) en el archivo config.properties de la aplicación, la aplicación Context Creation usa los datos de "Context Data para la cuenta A" del archivo de configuración y los codifica hexadecimal.
   - Si los dígitos ingresados coinciden con la segunda cuenta (AccountB=456456) en el archivo config.properties de la aplicación, la aplicación Context Creation usa los datos de "Context Data para la cuenta B" del archivo de configuración y los codifica hexadecimal.

   La aplicación de creación de contexto de muestra utiliza los detalles del número de cuenta de los archivos de configuración con fines ilustrativos. En una solución real, puede extraer los datos de contexto desde cualquier lugar; ya sea una base de datos externa, un sistema de gestión de relaciones con el cliente (CRM) o del contexto recopilado dentro de la aplicación Orchestration Designer.
10. La aplicación Context Creation Voice XML luego pasa los datos hexadecimales codificados a la aplicación de diálogo CCXML.

11. La aplicación de diálogo CCXML devuelve los datos hexadecimales codificados a Avaya Contact Center Select en un mensaje SIP INFO. Debido a que "tipo de tratamiento" se estableció en "creación de contexto", la aplicación de diálogo establece el tipo del cuerpo del mensaje SIP en 'aplicación/x-aacc-info'.
12. La aplicación de diálogo CCXML luego se cierra (ADIÓS).
13. Avaya Contact Center Select SIP Gateway Manager (SGM) reconoce este tipo de mensaje SIP y crea información de contexto para la llamada al convertir los datos codificados hexadecimales en el cuerpo del mensaje SIP INFO en Contact Intrinsics.
14. El script de Avaya Contact Center Select registra el valor devuelto.

Avaya Contact Center Select utiliza las aplicaciones Call Control XML y Voice XML para integrarse con Avaya Aura® Portal de experiencias. Esto brinda a las empresas flexibilidad y control completos de la integración de la solución. El aura de Avaya®El sistema Experience Portal y la solución Avaya Contact Center Select son altamente flexibles y eficientes. Avaya proporciona aplicaciones XML de voz de muestra para la rápida integración de un back-end Avaya Aura®Experimente el sistema Portal con Avaya Contact Center Select.

Avaya DevConnect

El programa Avaya DevConnect proporciona una amplia gama de recursos para desarrolladores, incluido el acceso a API y SDK para productos de Avaya, herramientas para desarrolladores, opciones de soporte técnico y materiales de capacitación. La membresía registrada es gratuita para cualquier persona interesada en diseñar soluciones compatibles con Avaya. Las opciones de membresía mejorada ofrecen mayores niveles de soporte técnico, pruebas de cumplimiento y mercadeo conjunto de soluciones innovadoras compatibles con las soluciones basadas en estándares de Avaya.

Avaya Contact Center Select suministra muestra genérica Avaya Aura®Experimente las aplicaciones del Portal con fines de demostración. Si planea usar estas aplicaciones de muestra, debe revisar el código de muestra y personalizarlo para su solución antes de implementarla en producción.

Para obtener más información y descargar el Avaya Aura completo®Experience Portal front-end self-service y Avaya Contact Center Select usando archivos de muestra de encabezado SIP, consulte Aplicaciones de muestra de Orchestration Designer enwww.avaya.com/devconnect .

Capítulo 9: Equipo cliente de administración requisitos

Esta sección proporciona los requisitos de configuración para las computadoras cliente de administración de Avaya Contact Center Select basadas en navegador. Instale esta computadora cliente para configurar y administrar los recursos de Avaya Contact Center Select, monitorear el rendimiento y generar informes (históricos y en tiempo real). También puede usar esta computadora cliente para cargar y descargar datos usando las hojas de cálculo de la herramienta de configuración.

Requisitos de hardware de la computadora del administrador

La siguiente tabla enumera los requisitos mínimos de hardware para la computadora cliente del Administrador.

Tabla 9: Requisitos mínimos de hardware del equipo cliente

Artículo de ferretería	Requerimientos mínimos	Información Adicional
UPC	CPU de 1 gigahercio (GHz) o más rápida compatible con PAE, NX y SSE2	La extensión de dirección física (PAE), el bit de procesador NX (NX) y Streaming SIMD Extensions 2 (SSE2) son características del procesador. Estas características de la CPU son necesarias para ejecutar Microsoft Windows 7.0 y Microsoft Windows 8.1. Los sistemas de doble y cuádruple CPU son compatibles con o sin Hyper-Threading habilitado. También se admiten los procesadores AMD de la misma o superior especificación.
RAM	1 Gigabyte (GB) (32 bits) o 2 GB (64 bits)	Se requiere memoria adicional si ejecuta otras aplicaciones que requieren mucha memoria.
Espacio en disco duro	16 GB (32 bits) o 20 GB (64 bits)	
Particionamiento del disco duro	Sin requisitos de partición específicos	—
velocidad del disco duro	Velocidad mínima del disco de 2,5 pulgadas: 10000 RPM	—

La tabla continúa...

Artículo de ferretería	Requerimientos mínimos	Información Adicional
	Velocidad mínima del disco de 3,5 pulgadas: 7200 RPM	
Unidad de disquete	No requerido	Si se instala una unidad de disquete, debe ser A.
DVD ROM	No requerido	
Interfaz de red	Una tarjeta de interfaz de red	Se recomienda Ethernet de 100 Mb/s o superior.
Tarjeta de video	Dispositivo gráfico Microsoft DirectX 9 con controlador WDDM	Resolución mínima de 1024 x 768 píxeles
Teclado	un teclado	—
Ratón	un raton	—

Requisitos del sistema operativo del cliente

La siguiente tabla enumera los requisitos del sistema operativo para los equipos cliente.

Tabla 10: Requisitos del sistema operativo del cliente

Sistema operativo	Versiones internacionales soportado	paquete mínimo de servicios
Windows 7 (32 bits y 64 bits)	inglés Francés (FR) Alemán (DE) italiano (IT) Holandés (Holanda) Japonés (JA) Coreano (KO) Español latino (ES) Portugués brasileño (PT-BR) Ruso (RU) Chino simplificado (Zh-CN)	
Windows 8.1 (32 bits y 64 bits)	inglés Francés (FR) Alemán (DE) italiano (IT) Holandés (Holanda)	

La tabla continúa...

Sistema operativo	Versiones internacionales soportado	paquete mínimo de servicios
	Japonés (JA) Coreano (KO) Español latino (ES) Portugués brasileño (PT-BR) Ruso (RU) Chino simplificado (Zh-CN)	
Windows 10 (32 bits y 64 bits)	inglés Francés (FR) Alemán (DE) italiano (IT) Holandés (Holanda) Japonés (JA) Coreano (KO) Español latino (ES) Portugués brasileño (PT-BR) Ruso (RU) Chino simplificado (Zh-CN)	

Cliente de administración Soporte de Citrix

Contact Center Manager Administration (CCMA) es compatible con las implementaciones de Citrix. Una solución de servidor Citrix utiliza software para entregar aplicaciones de Windows bajo demanda a escritorios físicos. Esto permite a los usuarios del cliente acceder y utilizar programas que están disponibles en el sistema operativo Windows Server 2012 R2 del servidor Citrix. Contact Center Manager Administration admite las siguientes versiones del servidor Citrix:

- Citrix XenApp 6.5
- Citrix XenApp 7.x

Los usuarios acceden a Contact Center Manager Administration a través de un cliente Citrix en su computadora cliente, conectándose a través de un navegador Internet Explorer que se ejecuta en el servidor Citrix. El navegador está disponible para los usuarios a través de un cliente Citrix en su computadora cliente. En una implementación de cliente Citrix de CCMA, debe instalar controles ActiveX en el servidor Citrix. Para obtener más información sobre la instalación de controles ActiveX en el servidor Citrix, consulte*Administración avanzada de Avaya Contact Center Select*.

Para obtener más información sobre la publicación de aplicaciones de Citrix, consulte la documentación de Citrix. Para obtener más información sobre cómo configurar su servidor Citrix para permitir que los usuarios accedan a CCMA, consulte *Administración avanzada de Avaya Contact Center Select*.

Avaya Contact Center Select solo admite la opción de multidifusión para pantallas en tiempo real (RTD) en un entorno Citrix. Avaya Contact Center Select no admite la opción Unicast para pantallas en tiempo real (RTD) en un entorno Citrix.

Importante:

Ningún componente de cliente de Avaya Contact Center Select, aparte de Agent Desktop y Contact Center Manager Administration, es compatible con una implementación de Citrix. El diseñador de orquestaciones (OD), la herramienta de administración de campañas salientes (OCMT) y los componentes de cliente de la utilidad de administración de CCMM son compatibles con una implementación de Citrix.

Requisitos de software de terceros

En esta sección se describen los requisitos de software de terceros para el equipo cliente de administración.

Los siguientes componentes son necesarios en la PC del cliente de administración:

- Microsoft Internet Explorer 10.0 (solo versión de 32 bits) y 11.0 (solo versión de 32 bits).

  Nota:

  Debe ejecutar Internet Explorer en modo de compatibilidad para Contact Center Manager Administration and Communication Control Toolkit.

- Microsoft Excel 2007 o posterior (solo para la herramienta de configuración)

Contact Center Manager Administration solo admite la versión de 32 bits de Microsoft Internet Explorer.

Contact Center Manager Administration no es compatible con Microsoft Edge.

Capítulo 10: Computadora Agent Desktop requisitos

Esta sección proporciona los requisitos de configuración para los equipos cliente de Agent Desktop. Agent Desktop es una aplicación de cliente de interfaz única utilizada por los agentes del centro de contacto para interactuar con los clientes. Los agentes descargan e instalan el software de cliente Agent Desktop desde el servidor de Avaya Contact Center Select. Los agentes de Avaya Contact Center Select utilizan el software Agent Desktop junto con un teléfono provisto de IP Office.

Avaya Contact Center Select admite la compatibilidad con versiones anteriores de Feature Pack o Service Pack de Agent Desktop. Esto le permite actualizar el servidor de Avaya Contact Center Select sin el requisito de actualizar Agent Desktop en una sola ventana de mantenimiento. Por ejemplo, si actualiza a la versión 7.0 Feature Pack 3, puede usar la versión 7.0 Feature Pack 2 de Agent Desktop. Las nuevas funciones de Agent Desktop agregadas en la versión más reciente de Avaya Contact Center Select no están disponibles hasta que actualice Agent Desktop a esa versión. La compatibilidad con versiones anteriores no es compatible con versiones principales o secundarias. Por ejemplo, si actualiza a la versión 7.1, no puede usar la versión 7.0 de Agent Desktop.

Nota:

Agent Desktop no admite tabletas ni dispositivos con pantalla táctil.

Nota:

Agent Desktop no es compatible con la traducción de direcciones de red (NAT).

Idiomas localizados de Agent Desktop

Agent Desktop es compatible con los siguientes idiomas localizados:

- Inglés
- Francés
- Alemán
- Italiano
- japonés
- coreano

Página249 de 3226.

- español latino
- Portugués Brasileño
- ruso
- Chino simplificado

Una sola solución de Avaya Contact Center Select, con los parches de idioma de localización instalados, es compatible con todos los idiomas localizados de Agent Desktop. Por ejemplo, un único servidor de contacto de voz y multimedia en inglés es compatible con las versiones en inglés, chino, francés y ruso del software cliente Agent Desktop.

Avaya Contact Center Select es compatible con los sistemas operativos de cliente de Agent Desktop que utilizan una familia de idiomas diferente a la del servidor de Contact Center.

Requisitos de hardware de la computadora Agent Desktop

La siguiente tabla enumera los requisitos mínimos de hardware para una computadora que ejecuta el software Agent Desktop.

Tabla 11: Requisitos mínimos de hardware de la computadora Agent Desktop

Artículo de ferretería	Requerimientos mínimos	Información Adicional
UPC	CPU de 1 gigahercio (GHz) o más rápida compatible con PAE, NX y SSE2	La extensión de dirección física (PAE), el bit de procesador NX (NX) y Streaming SIMD Extensions 2 (SSE2) son características del procesador. Estas características de la CPU son necesarias para ejecutar Microsoft Windows 7.0 y Microsoft Windows 8.1. Los sistemas de doble y cuádruple CPU son compatibles con o sin Hyper-Threading habilitado.
RAM	1 Gigabyte (GB) (32 bits) o 2 GB (64 bits)	Se requiere memoria adicional si ejecuta otras aplicaciones que consumen mucha memoria al mismo tiempo que Agent Desktop.
Espacio en disco duro	16 GB (32 bits) o 20 GB (64 bits)	
Particionamiento del disco duro	Sin requisitos de partición específicos	—
velocidad del disco duro	Velocidad mínima del disco de 2,5 pulgadas: 10000 RPM Velocidad mínima del disco de 3,5 pulgadas: 7200 RPM	—
Unidad de disquete	No requerido	Si se instala una unidad de disquete, debe ser A.

La tabla continúa...

Artículo de ferretería	Requerimientos mínimos	Información Adicional
DVD ROM	No requerido	
Interfaz de red	Una tarjeta de interfaz de red	Se recomienda Ethernet de 100 Mb/s o superior.
Tarjeta de video	Dispositivo gráfico Microsoft DirectX 9 con controlador WDDM	Resolución mínima de 1024 x 768 píxeles
Teclado	un teclado	—
Ratón	un raton	—

Agent Desktop no admite tabletas ni dispositivos con pantalla táctil.

Requisitos del sistema operativo del cliente

La siguiente tabla enumera los requisitos del sistema operativo para los equipos cliente.

Tabla 12: Requisitos del sistema operativo del cliente

Sistema operativo	Versiones internacionales soportado	paquete mínimo de servicios
Windows 7 (32 bits y 64 bits)	inglés Francés (FR) Alemán (DE) italiano (IT) Holandés (Holanda) Japonés (JA) Coreano (KO) Español latino (ES) Portugués brasileño (PT-BR) Ruso (RU) Chino simplificado (Zh-CN)	
Windows 8.1 (32 bits y 64 bits)	inglés Francés (FR) Alemán (DE) italiano (IT) Holandés (Holanda) Japonés (JA)	

La tabla continúa...

Página251 de 3226.

Sistema operativo	Versiones internacionales soportado	paquete mínimo de servicios
	Coreano (KO) Español latino (ES) Portugués brasileño (PT-BR) Ruso (RU) Chino simplificado (Zh-CN)	
Windows 10 (32 bits y 64 bits)	inglés Francés (FR) Alemán (DE) italiano (IT) Holandés (Holanda) Japonés (JA) Coreano (KO) Español latino (ES) Portugués brasileño (PT-BR) Ruso (RU) Chino simplificado (Zh-CN)	

Requisitos de software de terceros

Esta sección describe los requisitos de software de terceros para los equipos cliente de Agent Desktop.

Agent Desktop solo admite Microsoft Internet Explorer 10.0 (solo versión de 32 bits) y 11.0 (solo versión de 32 bits).

Agent Desktop solo admite la versión de 32 bits de Microsoft Internet Explorer.

Agent Desktop no es compatible con Microsoft Edge.

Requisitos de infraestructura de red del cliente de Agent Desktop

Agent Desktop es una aplicación cliente que se comunica con el servidor de Avaya Contact Center Select. Para un funcionamiento óptimo de Agent Desktop, la infraestructura de red del centro de contactos subyacente debe proporcionar una latencia y un ancho de banda adecuados entre la computadora del agente y el servidor de Avaya Contact Center Select.

Esta sección proporciona una descripción general de alto nivel de los datos que se pasan entre Agent Desktop y el servidor de Avaya Contact Center Select. También establece los valores de red recomendados y los posibles impactos en los agentes si no se cumplen estos valores. Esta sección también describe el rendimiento de Agent Desktop en diferentes entornos de tiempo de ida y vuelta (RTT) y ancho de banda.

Importante:

El rendimiento de Agent Desktop se degrada a medida que aumenta el tiempo de ida y vuelta de la red y disminuye el ancho de banda de la red.

Latencia de conexion

La latencia de la red es una medida de la demora de tiempo experimentada en un sistema, medida en tiempo de ida y vuelta (RTT). RTT es el tiempo promedio de ida y vuelta (paquete) medido con el comando ping para un tamaño de datos de 1024 bytes (1 KB).

Para un rendimiento óptimo, Avaya recomienda un RTT de menos de 80 ms desde la computadora cliente de Agent Desktop a los siguientes componentes de Avaya Contact Center Select:

- Conjunto de herramientas de control de comunicaciones (CCT)
- Centro de Contacto Multimedia (CCMM)
- Servidor del administrador del centro de contacto (CCMS)

El RTT desde la PC cliente de Agent Desktop hasta el servidor de Avaya Contact Center Select debe ser inferior a 120 ms. Para entornos de red con un RTT superior a 120 ms, consulte las implementaciones de Citrix de Agent Desktop en la siguiente sección.

Impactos de RTT en el tráfico de voz

Esta sección describe cómo el RTT subyacente y la latencia de la red afectan la experiencia de manejar el tráfico de voz en Agent Desktop.

Agent Desktop utilizado con un teléfono de escritorio físico

El componente CCT envía señales de Integración de telefonía informática (CTI) a Agent Desktop, por ejemplo, para solicitar a Agent Desktop que avise a un contacto entrante. Estas señales CTI se transmiten a través de la red como datos. Sin embargo, si el agente utiliza un teléfono de escritorio físico, los paquetes de voz se transportan a través de una red.

La siguiente tabla detalla el tiempo que tarda el contacto en alertar en Agent Desktop, en comparación con el tiempo que tarda el mismo contacto en sonar en el teléfono del agente, donde el teléfono está sujeto a un RTT constante de 1 ms.

RTT (ms)	Retraso entre el timbre del teléfono de escritorio y la alerta de llamada en Agent Desktop	Retraso entre hacer clic en el botón Aceptar en Agent Desktop y la ruta de voz activa
LAN de 1 ms	<0,5 segundos	<0,5 segundos
50ms	0,5 segundos	1,0 segundos
120ms	1,0 segundos	2,5 segundos

Impacto de RTT en contactos multimedia

Los contactos de Contact Center Multimedia también se ven afectados por la latencia de la red. Agent Desktop descarga los contactos del cliente del servidor de Avaya Contact Center Select y muestra su contenido tan pronto como se recupera por completo.

La siguiente tabla muestra cómo los diferentes RTT afectan los tiempos de visualización de contactos multimedia (en este caso, contactos de correo electrónico) en Agent Desktop. La columna "Detalles del cliente/Visualización del historial del cliente" indica cuánto tiempo pasa entre la apertura del correo electrónico en Agent Desktop y la carga y visualización de la información de contexto adicional. Estos tiempos de muestra son para condiciones de laboratorio ideales.

RTT (ms)	Pantalla de correo electrónico	Visualización de detalles del cliente/historial del cliente
LAN de 1 ms	2 segundos	0 segundos
50ms	3 segundos	3 segundos adicionales
100ms	4 segundos	4 segundos adicionales
120ms	4 segundos	5 segundos adicionales

Estos datos se generaron utilizando un mensaje de correo electrónico de 20 KB, un historial de clientes que contiene 30 contactos de 20 KB cada uno, en una red donde el ancho de banda no limita la transferencia de datos. Los mensajes de correo electrónico de diferentes tamaños generan resultados diferentes.

Banda ancha

El ancho de banda de red disponible para las computadoras cliente de Agent Desktop para la comunicación con los servidores de Avaya Contact Center Select es fundamental para el rendimiento de Agent Desktop. Si el tráfico de voz se transporta en la misma red, este tráfico a menudo se prioriza por encima de otro tráfico de red; por lo tanto, este ancho de banda no está disponible para Agent Desktop. En muchos casos, los agentes utilizan otras aplicaciones de terceros en la misma red. Los requisitos de ancho de banda de estas aplicaciones de terceros deben considerarse como parte de los cálculos de ancho de banda general (además del ancho de banda asignado para softphones de voz y para Agent Desktop).

Varios factores afectan el ancho de banda recomendado para Agent Desktop. Según las funciones de Contact Center Multimedia (CCMM) que se utilicen en una implementación de Cliente determinada, no se aplican todos los factores. A continuación se presentan cálculos indicativos para estimar el uso real del ancho de banda para los diversos tipos de contactos y funciones. Para calcular el ancho de banda requerido, las cifras relevantes para las funciones implementadas y los tipos de contacto admitidos se pueden combinar para obtener una cifra general.

El uso de la red puede ser de dos tipos:

Constante tráfico	Estos requieren un uso de red dedicado y permanentemente disponible durante la vida útil del consumo. Los ejemplos de este tipo de tráfico incluyen; visualización de estadísticas en Agent Desktop, actualización de contactos de chat web en vivo. Muchos factores influyen en los niveles de tráfico constante, por ejemplo, la cantidad de agentes con una gran cantidad de conjuntos de habilidades asignados, la cantidad de supervisores activos que ejecutan RTD en modo de unidifusión y una gran cantidad de conjuntos de habilidades en uso (paquete de datos grande) incluso para multidifusión.
estallido tráfico	La visualización de contactos multimedia y el historial de contactos multimedia es un tráfico a ráfagas. Una cantidad significativa de datos se descarga en Agent Desktop durante varios segundos. La frecuencia de estas descargas depende de la actividad del agente.

La tabla continúa...

	Estos requieren un alto uso de la red disponible por tiempos cortos para descargar ráfagas de datos. La ventana de tiempo que tardan estos datos en descargarse depende del ancho de banda de red disponible en ese momento. Dado que este no es un consumo constante de la red, un valor de Kilobits por segundo no refleja el ancho de banda requerido y, en su lugar, se ha proporcionado un valor de Kilobits.

Impactos del ancho de banda en la voz

Si los agentes usan un teléfono de escritorio físico para voz o cualquier otra aplicación que utilice el ancho de banda de la red, esto debe tenerse en cuenta en la ingeniería de la red para cumplir con los niveles de rendimiento esperados en Agent Desktop.

Recuperar el historial del cliente en los contactos de voz

La función Historial de cliente de Agent Desktop permite a los agentes recuperar el historial de cliente multimedia de las personas que llaman, desde el servidor de Avaya Contact Center Select, cuando se acepta un contacto de voz. El historial de clientes de Agent Desktop es una función opcional que se habilita en la herramienta de administración de CCMM. Estos contactos históricos pueden ser de cualquier tipo de contacto multimedia. Agent Desktop Customer History requiere un ancho de banda adecuado para funcionar y debe incluirse en los cálculos de planificación del ancho de banda de su red.

Para calcular el impacto del historial de cliente multimedia de las personas que llaman por voz en el ancho de banda, considere los contactos de voz como un tipo de contacto multimedia adicional y agregue la cantidad de contactos de voz a su cálculo multimedia para los cálculos de ancho de banda.

Requisitos de ancho de banda de contacto multimedia

Esta sección detalla el requisito de ancho de banda del Historial de cliente de Agent Desktop para los siguientes tipos de contactos multimedia:

- Mensajes de correo electrónico
- Mensajes de fax
- Documentos escaneados (SD)
- Mensajes de texto SMS
- Contactos salientes
- Comunicaciones Web (WC)

Esta sección también detalla el requisito de ancho de banda para los tipos de contacto de voz si la visualización del historial multimedia está habilitada.

Algunos contactos multimedia admiten archivos adjuntos y estos archivos adjuntos también deben incluirse en los cálculos de la red:

- Los contactos de correo electrónico son de tamaño variable. El tamaño promedio del correo electrónico es una estimación razonable y se utiliza para los cálculos de Agent Desktop.
- Los mensajes de fax se entregan como archivos adjuntos de correo electrónico. Los mensajes de fax deben incluirse en las estimaciones de tamaño y tarifa del archivo adjunto.
- Los contactos salientes de la solución Avaya Contact Center Select no tienen archivos adjuntos.
- Mensajes SMS de prueba de los clientes. Los mensajes de prueba de SMS no tienen archivos adjuntos.

• Los mensajes de chat web no tienen archivos adjuntos.

La función Historial del cliente de Agent Desktop permite a los agentes recuperar el historial del cliente multimedia (que contiene hasta 30 contactos anteriores), desde el servidor de Avaya Contact Center Select, cuando se acepta un contacto multimedia. Agent Desktop Customer History requiere un ancho de banda adecuado para funcionar y debe incluirse en los cálculos de planificación del ancho de banda de su red. La recuperación del historial del cliente de Agent Desktop desde el servidor de Avaya Contact Center Select utiliza el tipo de datos de red en ráfagas y, cuando la función del historial del cliente está habilitada, debe incluirse en todos los cálculos del ancho de banda de la red.

Ejemplo de cálculo de los requisitos de ancho de banda de las descargas del historial del cliente de Agent Desktop (basado en condiciones de laboratorio ideales):

norte=Número de agentes trabajando en contactos multimedia (MM). Si la función para mostrar el historial multimedia con llamadas de voz está activada, entonces N debe incluir agentes de voz.

C=Número máximo de contactos multimedia por hora para toda la solución de contact center. Si se activa la función de mostrar el historial multimedia con llamadas de voz, entonces C debe incluir el tráfico de voz por hora a todos esos agentes.

avg_contact_size=tamaño promedio de un contacto en Kbits (no Kbytes). (Kbits = KBytes * 8). En muchos casos, este es el tamaño promedio del correo electrónico entrante o saliente.

att_rate_in=porcentaje de archivos adjuntos de contactos entrantes. Los archivos adjuntos de contacto se aplican a mensajes de correo electrónico y mensajes de fax.

att_rate_out=porcentaje de mensajes de correo electrónico entrantes que se responden con archivos adjuntos adjuntos del agente en la respuesta.

avg_att_size=tamaño promedio de un archivo adjunto en Kbits. Los archivos adjuntos de contacto se aplican a mensajes de correo electrónico y mensajes de fax.

Nota:

Los archivos adjuntos en línea también deben incluirse en los cálculos de ancho de banda como archivos adjuntos normales.

Un factor clave en el cálculo del ancho de banda mínimo para procesar contactos multimedia es una evaluación de la cantidad de agentes activos que aceptan contactos en cualquier período de un segundo. El ancho de banda disponible se comparte entre todos estos agentes en este período de tiempo.

El número promedio a largo plazo de agentes activos en cualquier segundo se calcula de la siguiente manera: ***norte***

promedio= Redondeo(C/3600)

Esto equivale a la cantidad promedio de agentes que hacen clic en el botón Aceptar en Agent Desktop en cualquier momento. Sin embargo, dado que el tiempo que tarda un agente en manejar un contacto es aleatorio, la cantidad de agentes que hacen clic en el botón Aceptar es aleatoria. Es incorrecto diseñar una solución de ancho de banda basada únicamente en este promedio, ya que casi el 50 % de las veces más de***norte***promedioslos agentes están haciendo clic en el botón Aceptar.

Por lo tanto, el número de agente activo por segundo se calcula con un factor F de la siguiente manera:

norteactivo= Redondeo (F* C / 3600)

donde F es un factor de ingeniería entre 3 y 10. Se debe usar un valor mayor para F cuando N, el número total de agentes que procesan contactos multimedia e historial multimedia con voz

contacto, es inferior a 50. La elección del valor F es su decisión. F refleja la cantidad de ancho de banda adicional para construir en su red para manejar tanto la distribución inherentemente aleatoria de la actividad de los agentes que da como resultado picos naturales de uso y cualquier evento de pico de datos atribuible a sus modelos comerciales particulares de Contact Center, como las horas de inicio del turno inicial, promociones y emergencias. Un valor más alto reduce el nivel de limitación de ancho de banda causado por la superposición de descargas de múltiples agentes de contactos multimedia.

Una vez que se define F, el ancho de banda mínimo (en Kbits por segundo) se puede estimar de la siguiente manera:

BWMMmin=

norteactivo* ((avg_contact_size * 64) + 2000) + avg_att_size * (att_rate_in% + att_rate_out%) / 100) Kbps

Importante:

El ancho de banda mínimo recomendado disponible para procesar contactos multimedia ***BWMM***mindebe ser superior a 10 Mbits por segundo.

El tiempo para descargar y mostrar contactos en Agent Desktop se ve directamente afectado por el ancho de banda disponible entre el servidor de Avaya Contact Center Select y Agent Desktop en el momento en que se acepta el contacto en Agent Desktop. El impacto de la limitación del ancho de banda se observa como una visualización retrasada de contactos e historial de contactos en Agent Desktop.

La siguiente tabla demuestra el impacto de limitar el ancho de banda en los tiempos de visualización de contactos multimedia en Agent Desktop. Los datos se generaron utilizando un mensaje de correo electrónico de 20 KB, un historial de clientes de 30 contactos de 20 KB de tamaño cada uno, con un RTT fijo de 80 ms.

Ancho de banda disponible	visualización de correo electrónico	Visualización de detalles del cliente/historial del cliente
1Mbps	3 segundos	6 segundos adicionales
3Mbps	3 segundos	3 segundos adicionales
5Mbps	3 segundos	2 segundos adicionales

Recuperar el historial del cliente en los contactos de voz

Esta función opcional permite que Agent Desktop recupere el historial multimedia del cliente de las personas que llaman (que contiene hasta 30 contactos anteriores), desde el servidor de Avaya Contact Center Select, en el momento en que se acepta un contacto de voz. Estos contactos históricos pueden ser de cualquier tipo de contacto multimedia. Si esta función está activada, el tamaño de este historial se puede agregar a la planificación de su red considerando la voz como un tipo de contacto multimedia adicional y agregando la cantidad de contactos de voz a su cálculo multimedia.

Cálculo del ancho de banda de la red de comunicación web (WC)

El procesamiento de las comunicaciones web, una vez recibidas por el agente, requiere un nivel constante de ancho de banda.

Tipo de uso de red: Constante c = Número

de contactos de WC por hora

avg_session_length = Duración promedio en segundos de la sesión de WC

Página257 de 3226.

Tamaño de datos: 50 Kbps por contacto de WC activo

Requisito de ancho de banda de red de WC (Kbps): $WC_{B/N}$= (c

* 50 Kbps * avg_session_length)/ 3600

Cálculo del ancho de banda de la red de presencia Las actualizaciones

de presencia requieren un nivel constante de ancho de banda. Tipo de

uso de red: Constante

N = Número de agentes que trabajan en contactos MM

avg_pres = Número promedio de actualizaciones de presencia por usuario por hora Tamaño

de datos: 7 Kb por actualización de presencia

Requisito de ancho de banda de la red de presencia (en Kbps) = (N* 7Kb * avg_pres)/ 3600

Cálculo del ancho de banda de la red de búsqueda CCMM

Se debe proporcionar ancho de banda para que un agente realice búsquedas

multimedia. Tipo de uso de red: Bursty

N = Número de agentes que realizan búsquedas promedio_búsqueda

= Número promedio de búsquedas por hora Datos transmitidos:

1280 Kb por búsqueda

Requisito de ancho de banda de búsqueda CCMM (en Kbps) = (1280 Kb * promedio_búsqueda * N)/3600

Cálculo del ancho de banda de la red CCMM Pull Mode

El modo Pull permite a los agentes trabajar fuera del modo de enrutamiento normal de Avaya Contact Center Select. Seleccionan personalmente los contactos individuales de las colas de Avaya Contact Center Select. Su vista de la cola de Avaya Contact Center Select se actualiza automáticamente utilizando los mismos servicios web que la función de búsqueda CCMM de Avaya Contact Center Select y, por lo tanto, utiliza el mismo ancho de banda.

N = Número de agentes trabajando en Modo Pull c

= Número de contactos por hora por agente Datos

transmitidos: 1280Kb por búsqueda

Requisito de ancho de banda de búsqueda CCMM Pull Mode (en Kbps) = (1280Kb * c * N)/3600

Cálculo del ancho de banda de la red de estadísticas

web Tipo de uso de red: Bursty N = Número de agentes

avg_skills = Número promedio de conjuntos de habilidades por agente

Datos transmitidos: 3,2 Kb por conjunto de habilidades una vez por minuto

Requisito de ancho de banda de estadísticas web: (3,2 Kb * avg_skills * N)/60

Descargas de Agent Desktop por agente

Agent Desktop es un cliente inteligente que se descarga desde el servidor de Avaya Contact Center Select a través de la red en cada computadora del agente en la instalación inicial. En cada actualización de software (paquete de servicio o parche), el Agent Desktop actualizado se vuelve a descargar en cada computadora del agente. Los requisitos de descarga de Agent Desktop deben tenerse en cuenta al planificar los requisitos de ancho de banda para los agentes remotos.

Resumen de los requisitos de ancho de banda total

Debe resumir todas las demandas de ancho de banda aplicables enumeradas anteriormente para llegar a un ancho de banda mínimo para el sitio. Calcule el ancho de banda acumulativo para todas las funciones multimedia.

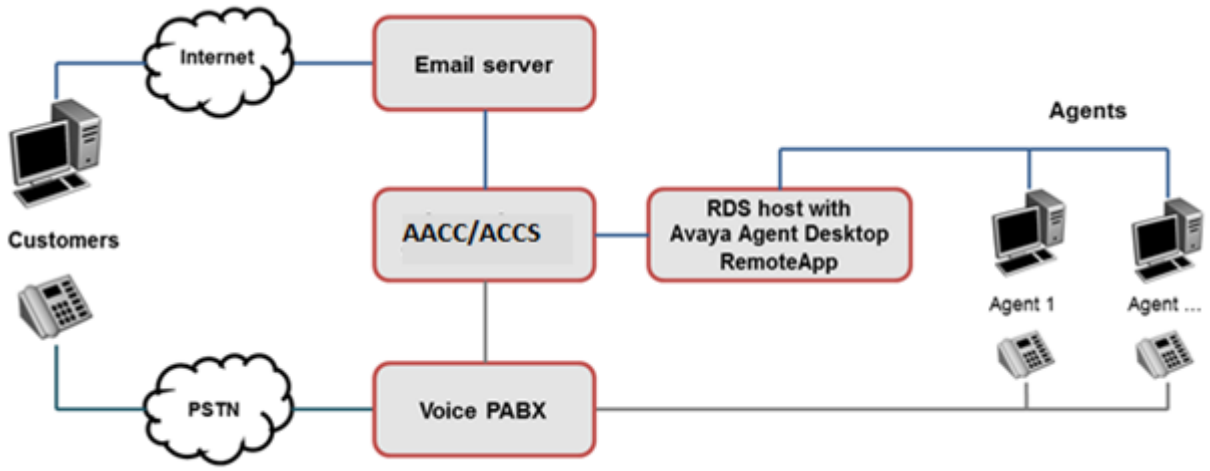
Soporte de servicios de escritorio remoto

Avaya Contact Center Select (ACCS) admite el uso de Servicios de escritorio remoto en un servidor Windows Server 2012 R2 para alojar y publicar Agent Desktop.

Los Servicios de escritorio remoto, anteriormente conocidos como Servicios de Terminal Server, permiten que un servidor aloje varias sesiones de clientes simultáneas. En el entorno de Servicios de escritorio remoto (RDS), una aplicación se ejecuta completamente en el servidor Host de sesión de Escritorio remoto (Host de sesión de RD). El cliente RDC no realiza ningún procesamiento local del software de la aplicación. El servidor transmite la interfaz gráfica de usuario al cliente. El cliente transmite la entrada del usuario al servidor. Con RDS, solo las interfaces de usuario del software se transfieren al sistema cliente. Toda la entrada del sistema del cliente se transmite al servidor, donde tiene lugar la ejecución del software.

Debe utilizar el paquete MSI de Agent Desktop para las implementaciones de Servicios de Escritorio remoto. La forma en que implementa y utiliza los clientes RDS de Agent Desktop depende de los requisitos de su solución y de la infraestructura de virtualización. Para obtener más información sobre cómo crear una infraestructura de cliente mediante RDS, consulte la documentación del producto Servicios de escritorio remoto de Microsoft.

El siguiente diagrama muestra una solución típica de Servicios de Escritorio remoto con Agent Desktop alojado en el servidor RDS Session Host.



Los servicios de escritorio remoto requieren una cuidadosa planificación e ingeniería por adelantado. Requiere algo de mantenimiento adicional y soporte organizacional completo para brindar una experiencia de agente y cliente de centro de contacto de nivel empresarial.

Aplicación remota:

RemoteApp le permite hacer que los programas a los que se accede de forma remota a través de Servicios de escritorio remoto aparezcan como si se estuvieran ejecutando en la computadora local del usuario final. Estos programas se denominan programas RemoteApp. En lugar de presentarse al usuario en el escritorio del servidor Host de sesión de Escritorio remoto (Host de sesión de Escritorio remoto), el programa RemoteApp se integra con el escritorio del cliente. El programa RemoteApp se ejecuta en su propia ventana de tamaño variable, se puede arrastrar entre varios monitores y tiene su propia entrada en la barra de tareas. Si un usuario está ejecutando más de un programa RemoteApp en el mismo servidor Host de sesión de Escritorio remoto, el programa RemoteApp comparte la misma sesión de Servicios de Escritorio remoto.

Limitaciones:

Las siguientes limitaciones se aplican cuando utiliza Servicios de Escritorio remoto en un servidor Windows Server 2012 R2 para alojar y publicar Agent Desktop:

- El modo de softphone integrado de Agent Desktop Mi PC no es compatible. Los agentes deben usar un teléfono de escritorio o usar un softphone compatible al mismo tiempo que Agent Desktop.
- Avaya recomienda que el servidor RDS que aloja Agent Desktop esté ubicado en la misma red de área local (LAN) que el servidor ACCS. Si el servidor RDS que aloja Agent Desktop no está en la misma LAN que el servidor ACCS, se aplican los requisitos de red, tiempo de ida y vuelta y ancho de banda ACCS.
- ACCS admite la opción de multidifusión solo para pantallas en tiempo real (RTD) en un entorno RDS. Unicast no es compatible con un entorno RDS.
- No puede utilizar el servidor ACCS como host RDS.
- Los agentes deben definir plantillas predeterminadas o carpetas de archivos adjuntos en las preferencias de Agent Desktop en una carpeta AppData en el host RDS. Los agentes no tienen acceso a unidades compartidas o asignadas. Para obtener más información sobre los ajustes de configuración de las carpetas temporales en el servidor host RDS, consulte la documentación del producto Servicios de escritorio remoto de Microsoft.

Para obtener información sobre cómo usar Servicios de Escritorio remoto en un servidor Windows Server 2012 R2 para alojar y publicar Agent Desktop, consulte*Administración avanzada de Avaya Contact Center Select*.

Asistencia al cliente Citrix

Agent Desktop es compatible como una aplicación publicada por Citrix. Una solución de servidor Citrix utiliza software para entregar aplicaciones de Windows bajo demanda a escritorios físicos. Esto permite a los usuarios del cliente (agentes en este caso) acceder y utilizar programas que están disponibles en el sistema operativo Windows Server 2012 R2 del servidor Citrix.

Agent Desktop es compatible con las siguientes versiones del servidor Citrix:

- Citrix XenApp 6.5
- Citrix XenApp 7.x

En el servidor de Avaya Contact Center Select, la carpeta de Agent Desktop normalmente se encuentra en: D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\cliente

Esta carpeta contiene toda la aplicación Agent Desktop. Copie esta carpeta en el servidor de Agent Desktop al servidor Citrix. Luego configure su servidor Citrix para publicar Agent Desktop como una aplicación publicada, a la que se accede desde esta carpeta de Agent Desktop en el servidor Citrix. En el servidor Citrix, seleccione los usuarios (agentes) autorizados para ejecutar la aplicación publicada de Agent Desktop. Para obtener más información sobre la publicación de aplicaciones de Citrix, consulte la documentación de Citrix. Para obtener más información sobre cómo configurar su servidor Citrix para publicar Agent Desktop como una aplicación publicada, consulte*Administración avanzada de Avaya Contact Center Select*.

El Agent Desktop de publicación del servidor Citrix debe estar ubicado en la misma red de área local (LAN) que el servidor Avaya Contact Center Select.

Avaya Contact Center Select solo admite la opción de multidifusión para pantallas en tiempo real (RTD) en un entorno Citrix. Avaya Contact Center Select no admite la opción Unicast para pantallas en tiempo real (RTD) en un entorno Citrix.

Puertos de red de Agent Desktop

Agent Desktop utiliza los siguientes puertos de red para comunicarse con los componentes de Contact Center.

Rasgo	Componente	Número de puerto
HTTP (servicios web)	CCMM	80
HTTP (servicios web)	CCMM	443 (si TLS está habilitado para CCMM)
CCT	CCT	29373
Historial de voz	CCMS	57772
Estadísticas web	CCMS	9086

Página261 de 3226.

Capítulo 11: Navegador de agentes de Contact Center requerimientos de aplicacion

Esta sección proporciona información sobre los requisitos de configuración para la aplicación Contact Center Agent Browser.

Los agentes de Contact Center solo de voz pueden usar la aplicación Agent Browser para iniciar sesión en Contact Center y realizar tareas básicas. La aplicación Agent Browser no proporciona control de llamadas, funciones multimedia ni funciones de supervisor. Los agentes deben usar un teléfono de escritorio compatible para el control de llamadas. La aplicación Agent Browser admite las siguientes tareas:

- iniciar y cerrar sesión
- cambiar el estado del agente
- configuración de códigos de motivo de no listo
- configuración de códigos de actividad
- configuración de códigos de elemento de trabajo después de la llamada
- llamar a su supervisor
- manejo de una emergencia

La aplicación Contact Center Agent Browser solo es compatible con soluciones de Contact Center habilitadas para SIP. Todos los agentes que utilizan Agent Browser requieren una cuenta de dominio de Windows asociada o una cuenta local de Widows, configurada en CCMA, para iniciar sesión en Agent Browser. Si usa un dominio, las cuentas de dominio del agente deben estar en el mismo dominio que el servidor de Contact Center.

Los agentes acceden a la aplicación Agent Browser a través de un navegador web, utilizando el nombre de dominio completo (FQDN) del servidor de Contact Center. En las soluciones Business Continuity, los agentes deben iniciar sesión en la aplicación Agent Browser utilizando el FQDN del par Business Continuity.

En el caso de un cambio a un servidor de nodo geográfico remoto (RGN), los agentes deben iniciar sesión en la aplicación Agent Browser utilizando el FQDN del servidor RGN.

La aplicación Agent Browser no es compatible con la función Remote Agent.

Debe acceder a la aplicación Agent Browser solo mediante HTTPS. También debe instalar un certificado TLS válido, emitido por una autoridad de certificación (CA) de confianza, en Security Manager. Para evitar las advertencias de seguridad del certificado, instale el certificado raíz de la CA en todos los dispositivos cliente utilizados para acceder a la aplicación Agent Browser. Para más información, verComunicaciones seguras TLS de Avaya Contact Center Select en la página 180.

Si usa un dispositivo móvil para acceder a la aplicación Agent Browser, Avaya recomienda usar una pantalla de tamaño mediano de 992 píxeles o más. Algunos dispositivos móviles se bloquean automáticamente después de un tiempo definido.

Página262 de 3226.

período de tiempo de espera: la aplicación Agent Browser no tiene control sobre el bloqueo automático de los dispositivos móviles.

Ayuda de idioma

La aplicación Contact Center Agent Browser admite los siguientes idiomas:

- Inglés
- Francés (FR)
- Alemán (DE)
- Italiano (IT)
- LA español (ES)
- Portugués brasileño (PT-BR)
- Ruso (RU)
- Chino simplificado (Zh-CN)
- Chino tradicional (Zh-TW)
- Japonés (JA)
- Coreano (KO)

Puede establecer el idioma de la aplicación en el menú Configuración de la aplicación Agent Browser.

Requisitos del navegador web

La aplicación Agent Browser está alojada en Internet Information Services (IIS) que se ejecuta en el servidor de Contact Center. Los agentes acceden a la aplicación a través de un navegador web. La siguiente tabla enumera los navegadores compatibles.

Navegador	Versiones compatibles	Sistema operativo
Microsoft Internet Explorer	11.0	• Windows 7 • Windows 8.1 • Windows 10
Borde de Microsoft	20.10240	• Windows 10
Google Chrome	43.0.23	• Windows 7 • Windows 8.1 • Windows 10 • Android 4.4.2 • Android 5.0.1 • iOS 8.3

La tabla continúa...

Navegador	Versiones compatibles	Sistema operativo
		• OS X Yosemite 10.10.3
Mozilla Firefox **Importante:** El navegador de agentes La aplicación no admite el uso de la función "Buscar texto cuando empiezo a escribir" en Firefox.	38.0.5	• Windows 7 • Windows 8.1 • Windows 10
Safari	8.0.5	• iOS 8.3 • OS X Yosemite 10.10.3

Capítulo 12: Avaya Contact Center Select comunicaciones TLS seguras

Avaya Contact Center Select (ACCS) incluye una serie de servicios que puede proteger mediante el protocolo HTTPS. En la etapa de instalación, puede usar Ignition Wizard para crear un almacén de seguridad, generar una solicitud de firma de certificado (CSR) e importar un certificado raíz de autoridad de certificación. Como alternativa, puede omitir la configuración de seguridad en la etapa de instalación y configurar sus certificados de seguridad más tarde mediante Security Manager.

Conceptos básicos de seguridad HTTPS

HTTPS es un protocolo seguro para las comunicaciones web. HTTPS proporciona tanto la autenticación del servidor web como el cifrado de las comunicaciones entre el servidor y el cliente en ambas direcciones. HTTPS utiliza conexiones cifradas por el protocolo Transport Layer Security (TLS).

Cuando un cliente inicia una conexión segura con un servidor, el servidor devuelve su clave criptográfica pública en un certificado de servidor. Para garantizar la integridad del certificado del servidor, debe estar firmado por un tercero, denominado Autoridad de certificación (CA). El cliente debe tener un certificado raíz de la CA que proporcionó el certificado de servidor firmado. Si el cliente tiene un certificado raíz coincidente, completa la conexión y se establece una comunicación segura.

Niveles de cifrado, versiones de TLS y SSL

Avaya Contact Center Select (ACCS) es compatible con las funciones hash criptográficas SHA1 y SHA2, con tamaños de clave de 1024, 2048 o 4096. Sin embargo, la función hash SHA1 y el tamaño de clave 1024 no proporcionan el nivel de cifrado actual recomendado por la industria. . ACCS admite SHA1 y un tamaño de clave 1024 solo para proporcionar compatibilidad con versiones anteriores.

Avaya recomienda que use solo SHA2, ya sea un tamaño de clave 2048 o 4096. Los valores predeterminados para los nuevos almacenes de seguridad son SHA2 con un tamaño de clave de 2048.

Secure Sockets Layer (SSL) también está obsoleto y tiene una serie de debilidades conocidas. Contact Center ahora usa solo Transport Layer Security (TLS) para comunicaciones seguras. Tenga en cuenta que TLS es una extensión del antiguo protocolo SSL, y la industria acepta y utiliza con frecuencia el término 'SSL' para referirse a TLS.

Contact Center implementa Transport Layer Security (TLS) versión 1.2 como la versión mínima predeterminada negociada para comunicaciones seguras. Esto es para evitar las vulnerabilidades de seguridad que existen en TLS 1.0. Para la compatibilidad con versiones anteriores y la interoperabilidad con aplicaciones personalizadas o de terceros que se conectan a Contact Center, los administradores pueden configurar versiones más bajas de TLS en ciertos

canales de comunicación. Cuando hay disponible una versión inferior de TLS, Contact Center aún negocia el nivel más alto de TLS que la otra aplicación puede admitir.

Certificado de servidor

El certificado del servidor, a veces llamado certificado firmado, es el certificado que el servidor envía a un cliente que solicita un servicio seguro (HTTPS). El certificado del servidor combina una clave pública utilizada para el cifrado con los detalles de una organización y está firmado por una autoridad de certificación para permitir que los clientes verifiquen que es válido. El cliente puede usar el certificado del servidor para cifrar los datos que envía al servidor.

Autoridad certificada

Una Autoridad de certificación (CA) es una organización de terceros que proporciona certificados digitales que certifican al propietario de una clave pública para criptografía utilizada en comunicaciones seguras. Si usa una sola CA para toda su configuración de seguridad, reduce su carga de trabajo para la configuración de seguridad, porque necesita copiar solo un único certificado raíz para todos los clientes. Con frecuencia, los certificados raíz de muchas CA bien conocidas ya están integrados en sistemas operativos comunes para clientes y servidores.

Certificado raíz

El certificado raíz prueba la autenticidad del certificado firmado. Contiene una firma digital de una Autoridad de Certificación (CA). Para confiar en el certificado del servidor que les envió el servidor, los clientes deben tener una copia del certificado raíz con la firma digital de la CA que firmó el certificado del servidor. Los certificados raíz exportados desde diferentes almacenes de seguridad funcionan de la misma manera si contienen una firma digital de la misma CA.

Nombre del certificado del servidor

Cada certificado de servidor tiene un nombre, que normalmente se deriva del nombre de dominio completo del servidor. Si el nombre de un certificado de servidor no coincide con el nombre del sitio web o servicio web al que se conectó el cliente, el cliente genera una advertencia. Esto impacta a ACCS de la siguiente manera:

- En los sistemas Business Continuity (BC), debe encargar sus propios certificados con nombres alternativos de sujeto (SAN) para usar el nombre administrado del par de alta disponibilidad del campus. Por lo tanto, debe decidir el nombre administrado antes de configurar sus propios certificados.

Nombre alternativo del sujeto

Un nombre alternativo del sujeto (SAN) es una extensión de HTTPS que permite asociar varios valores con un certificado de seguridad. Estos valores se denominan "Nombres alternativos del sujeto" o SAN. Hay varios tipos de valores SAN, pero para ACCS solo es relevante el tipo de nombre DNS.

En ACCS, utiliza SAN en los certificados de seguridad para incluir los nombres de BC activo, en espera y administrado en el certificado del servidor, de modo que las conexiones seguras continúen durante un cambio de BC y los clientes no vean mensajes de advertencia.

Cuando crea el almacén de seguridad ACCS en Security Manager, puede agregar SAN al certificado del servidor.

Tienda de seguridad de Avaya Contact Center Select

Avaya Contact Center Select (ACCS) incluye un almacén de seguridad para permitir comunicaciones seguras sobre Transport Layer Security (TLS), tanto entre aplicaciones ACCS como con clientes externos o

Aplicaciones de terceros. Los clientes deben crear un almacén de seguridad utilizando Ignition Wizard o Security Manager, con un certificado de servidor y un certificado raíz de una autoridad de certificación (CA).

ACCS también utiliza el almacén de seguridad de Internet Information Services (IIS) para algunos servicios. En un servidor ACCS, Security Manager controla tanto el almacén de seguridad de IIS como el almacén de seguridad de ACCS. Estas dos tiendas siempre usan el mismo certificado de servidor, que usted configura en Security Manager.

Aura de Avaya®Media Server también tiene un almacén de seguridad. Esta tienda se configura a través de Avaya Aura®

Administrador de elementos del servidor de medios.

Figura 15: Ejemplo de almacenes de seguridad en un único servidor ACCS con Avaya Aura corresidente®Servidor multimedia

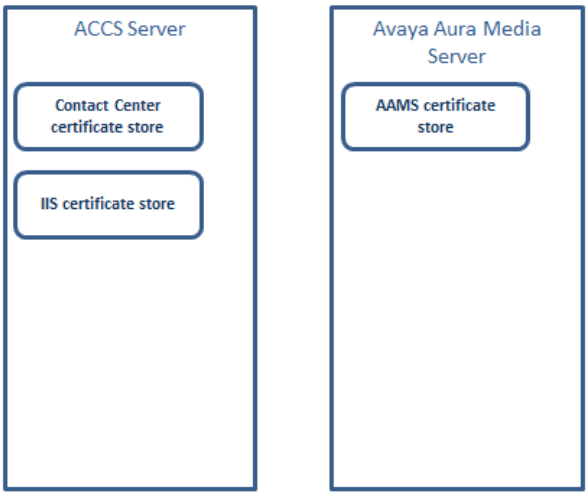


Figura 16: Ejemplo de almacenes de seguridad en un servidor ACCS con Avaya Aura independiente®Servidor multimedia

La siguiente tabla enumera los almacenes de seguridad en los servidores ACCS:

tienda de seguridad	Aplicaciones	Servicios que utiliza esta tienda	Gestionado por
Almacén de seguridad ACCS	CCMS, CCT	Enlace TAPI-D CTI	Gerente de seguridad de ACCS
Windows 2012 IIS tienda de seguridad	CCMA, CCMM	CCMA Administración CCMM Escritorio del agente Servicios multimedia Diseñador de orquestación Campaña saliente Herramienta de administracion Administración web de CCT	Gerente de seguridad de ACCS

Servicios ACCS que pueden usar la seguridad TLS

La siguiente tabla enumera todos los servicios ACCS que deben ser seguros o que pueden configurarse para que no lo sean.

Servicio ACCS	Siempre seguro	Seguridad opcional
Conexión TAPI-D CTI	Y	
Aplicación de navegador de agentes	Y	
Administración CCMA		Y
Administración CCMM		Y
Escritorio del agente		Y
Diseñador de orquestación		Y
Herramienta de gestión de campañas salientes		Y
Servicios web de ACCS		Y
Administración web de CCT		Y

- Todos estos servicios utilizan el certificado de servidor que configura en Security Manager. Si cambia este certificado, el cambio afecta a todos los servicios.
- Debe usar un certificado para los servicios TAPI-D CTI y la aplicación Agent Browser. Este certificado se genera en ACCS Security Manager. La conexión CTI entre ACCS e IPO requiere seguridad de capa de transporte mutuo (MTLS).

  El servidor IPO tiene un certificado de servidor y debe tener el certificado raíz ACCS. El servidor ACCS tiene un certificado de servidor y debe tener el certificado raíz IPO.
- Debe utilizar un certificado para los servicios web, a menos que desactive la seguridad de los servicios web. El certificado se usa en Security Manager.
- Debe usar un certificado para Avaya Aura®Servidor multimedia. En un ACCS con Avaya Aura Media Server, puede usar el certificado de servidor que creó en Security Manager.

Contact Center realiza automáticamente una copia de seguridad de un nuevo almacén de seguridad cuando lo crea. Esto le permite recuperarse de situaciones en las que el almacén está dañado o eliminado entre el envío de la Solicitud de firma de certificado (CSR) a una Autoridad de certificación (CA) y la recepción de un certificado firmado de vuelta.

la CA. La ubicación de esta copia de seguridad automática del almacén de seguridad esD:\Centro de contacto\autoBackUpCertStore.No sobrescriba ni elimine esta ubicación de copia de seguridad.

Administrador de seguridad de Avaya Contact Center Select

Avaya Contact Center Select (ACCS) incluye una serie de servicios que puede proteger mediante el protocolo HTTPS.

ACCS Security Manager proporciona una interfaz para administrar los certificados de seguridad en el almacén de seguridad de ACCS y el almacén de seguridad de IIS. ACCS admite la administración del almacén de seguridad de IIS solo a través de Security Manager: no use las funciones de IIS para administrar el almacén de seguridad de IIS en un servidor ACCS. Security Manager admite la importación de certificados encadenados y coloca estos certificados en el almacén de seguridad para su distribución en la solución.

Certificados de servidor

Cada almacén de seguridad debe tener un certificado de servidor firmado por una CA y un certificado raíz de la misma CA. En ACCS, puede usar el mismo certificado de servidor en todos los almacenes de seguridad en un solo servidor. También puede generar diferentes certificados de servidor para cada almacén de seguridad en un único servidor. No puede usar el mismo certificado de servidor en dos servidores diferentes.

Certificados raíz de la autoridad de certificación

Cuando un cliente inicia una conexión segura con un servidor, debe tener un certificado raíz de la CA que proporcionó el certificado de servidor firmado. Si el cliente no tiene un certificado raíz coincidente, no completa la conexión. Si el cliente tiene un certificado raíz de una CA determinada, puede confiar en cualquier certificado de servidor firmado por esa CA.

Avaya recomienda que utilice una sola CA para firmar todos los certificados en su centro de contacto. Esto simplifica el proceso de implementación, ya que solo necesita distribuir un único certificado raíz a todos los clientes.

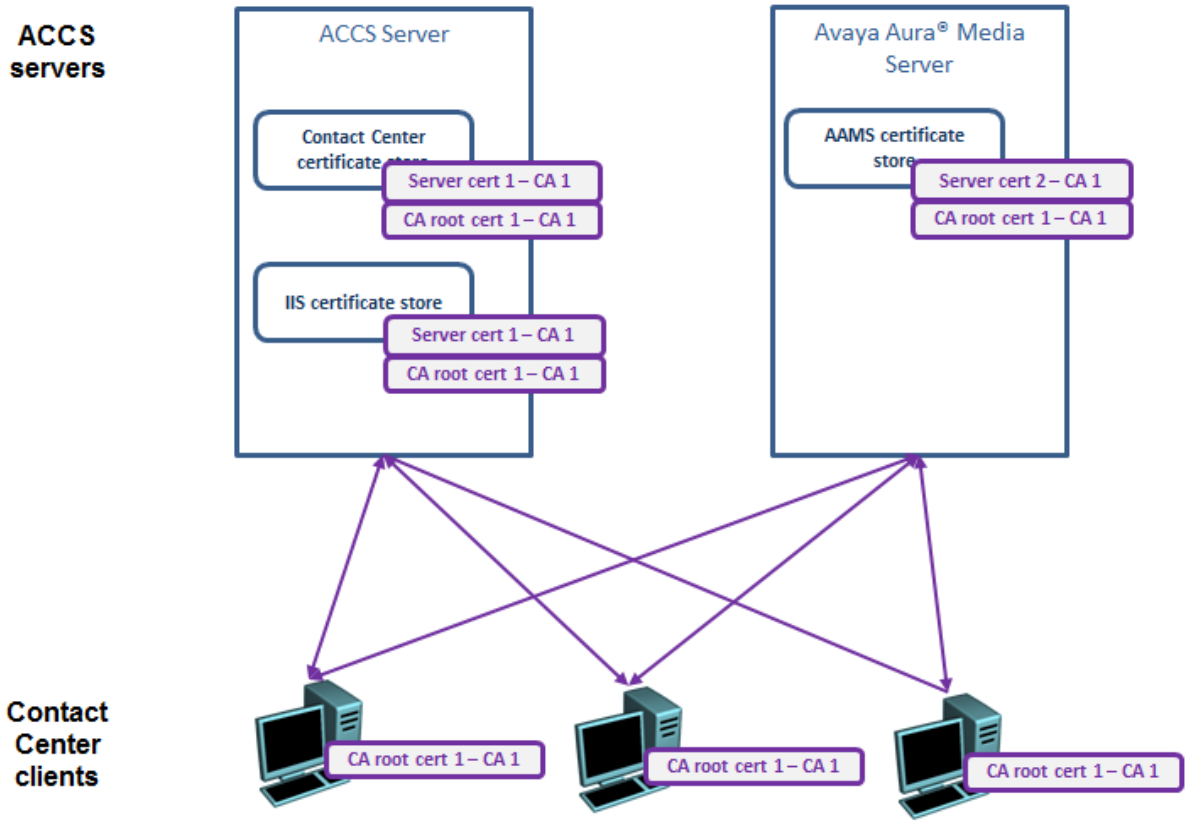


Figura 17: Ejemplo de cómo un único certificado raíz de CA puede funcionar con diferentes certificados de servidor firmados por la misma CA

Si desea utilizar diferentes CA para firmar certificados para sus diferentes servidores, debe copiar el certificado raíz de cada CA a todos los clientes de su centro de contacto. Para algunos servicios web de ACCS, los servidores de ACCS pueden actuar como clientes de otros servidores. Por lo tanto, debe asegurarse de que los servidores ACCS también tengan los certificados raíz de CA necesarios.

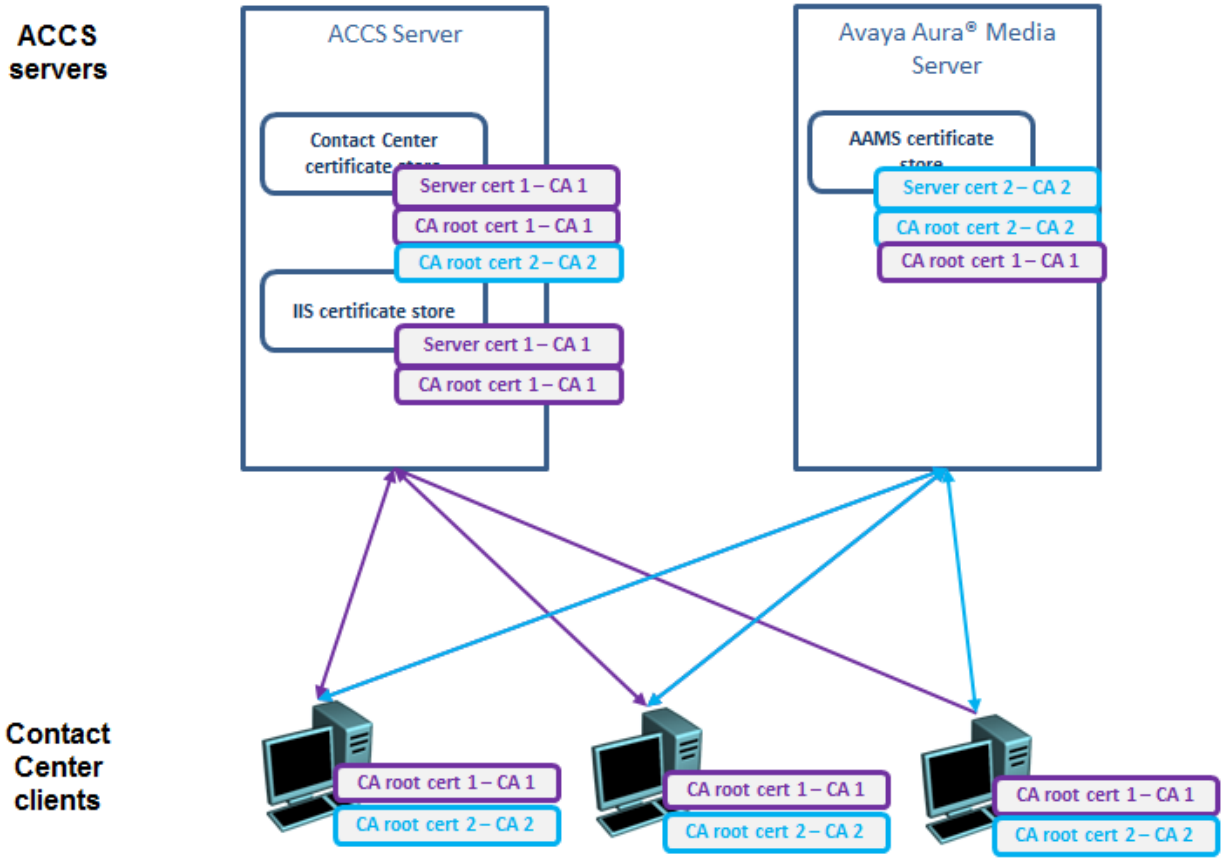


Figura 18: Ejemplo de cómo los clientes deben tener los certificados raíz de CA de cada CA que firmó un certificado de servidor, si el centro de contacto usa certificados de servidor firmados por diferentes CA

Puede distribuir certificados raíz a equipos cliente mediante una directiva de grupo en Microsoft Windows Server 2012.

Seguridad TLS en un entorno de continuidad empresarial

Si implementa Business Continuity (BC), los clientes y servidores de Avaya Contact Center Select (ACCS) deben poder comunicarse con el servidor del centro de contactos activo, el servidor del centro de contactos en espera y el nombre administrado del par de servidores BC.

En un sistema BC, cree un almacén de seguridad con nombres alternativos de sujeto (SAN). El almacén de seguridad para un par BC debe tener el nombre común del servidor ACCS y una SAN para:

- el nombre del servidor ACCS
- el nombre administrado del par BC

Página271 de 3226.

Esto garantiza que los clientes que se conectan a ACCS con el nombre administrado no reciban advertencias de que el nombre del certificado del servidor no coincide con el nombre del servidor.

ACCS admite el uso del mismo certificado tanto en el servidor activo como en el servidor en espera en el par BC.

Avaya recomienda planificar los nombres activos, administrados y en espera de su BC antes de crear un nuevo almacén de seguridad. De esta forma, puede crear sus certificados una vez utilizando SAN durante la puesta en marcha inicial, en lugar de volver a crear certificados cuando pone en marcha BC.

Migración de sistemas seguros de Contact Center

No puede migrar un almacén de seguridad de Contact Center de la versión 6.x a la versión 7.0. Si está migrando un sistema de Contact Center seguro desde la versión 6.x, debe crear un nuevo almacén de seguridad en el servidor de Contact Center de la versión 7.0.

Avaya Contact Center Select Security almacenar notificaciones

Los certificados de seguridad contienen una fecha de caducidad y no son válidos después de esta fecha. Si los certificados de seguridad utilizados por Avaya Contact Center Select (ACCS) caducan, el centro de contacto pierde el control de llamadas y deja de funcionar.

Security Manager proporciona una utilidad de inspección de almacenamiento de seguridad para ayudarlo a monitorear y mantener certificados de seguridad válidos. Puede utilizar Security Manager para programar una tarea de inspección del almacén de seguridad. Security Manager agrega la tarea programada al Programador de tareas de Windows subyacente. La tarea programada ejecuta la utilidad de inspección del almacén de seguridad una vez a la semana. La utilidad de inspección verifica el estado de los certificados de seguridad en el almacén de seguridad ACCS. Si alguno de los certificados de seguridad vence dentro de un mes, la utilidad de inspección envía una notificación por correo electrónico al administrador del centro de contacto. Luego, el administrador del centro de contacto debe actualizar los certificados de seguridad.

Security Manager proporciona el correo electrónico de notificación; no puede renovar los certificados de seguridad caducados. Para una funcionalidad ACCS ininterrumpida, si recibe un correo electrónico sobre las próximas fechas de vencimiento del certificado, debe renovar los certificados de seguridad antes de que caduquen. Security Manager utiliza el Programador de tareas de Microsoft Windows para programar la inspección semanal del almacén de seguridad. Debe asegurarse de que haya una cuenta de usuario de Microsoft Windows que tenga los privilegios necesarios desde la cual Security Manager pueda programar una tarea en el Programador de tareas de Windows. Puede usar la cuenta de administrador de Windows que usó para instalar ACCS para agregar una tarea al Programador de tareas de Windows.

Security Manager utiliza un servidor de Protocolo simple de transporte de correo (SMTP) para enviar los correos electrónicos de notificación a la dirección de correo electrónico del administrador. ACCS no proporciona este servidor SMTP. Debe aprovisionar este servidor SMTP y asegurarse de que el servidor ACCS pueda comunicarse con él en todo momento. ACCS no es compatible con la conectividad de Seguridad de la capa de transporte (TLS) con este servidor SMTP.

Firma del bloque de mensajes del servidor

Las instalaciones y actualizaciones de Contact Center modifican la política de grupo local de Windows Server 2012 para habilitar la firma del bloque de mensajes del servidor (SMB). La firma SMB coloca una etiqueta digital en cada bloque de mensajes del servidor, lo que ayuda a prevenir ataques de intermediarios en el uso compartido de archivos en la red.

Si no desea utilizar la firma SMB, puede deshabilitarla modificando la política de grupo local de Windows Server 2012.

Capítulo 13: Avaya Contact Center Select

matriz de puertos

Esta sección enumera los puertos utilizados por Avaya Contact Center Select. El servidor de Avaya Contact Center Select contiene los siguientes componentes:

- Servidor del administrador del centro de contacto (CCMS)
- Administración del administrador del centro de contacto (CCMA)
- Conjunto de herramientas de control de comunicaciones (CCT)
- Administrador de licencias del centro de contacto (LM)
- Utilidad del servidor Contact Center Manager (SU)
- Diseñador de orquestación (OD)
- Centro de Contacto Multimedia (CCMM)
- Aura de Avaya®Servidor multimedia

Estos componentes utilizan los siguientes puertos.

Requisitos de puerto del Contact Center Manager Server

Contact Center Manager Server utiliza puertos para la comunicación entre sus propios componentes. La mayoría de los puertos no tienen implicaciones para los componentes de la red externa, como los cortafuegos; sin embargo, algunos puertos pueden usarse externamente y, por lo tanto, pueden afectar un firewall externo. En particular, el puerto 10000 es un puerto codificado que se utiliza para permitir la interoperabilidad entre las aplicaciones del Contact Center y las aplicaciones externas de terceros (aplicaciones desarrolladas con la API de datos en tiempo real (RTD)).

Ninguna aplicación de terceros instalada en Contact Center Manager Server puede usar los puertos enumerados en la siguiente tabla, ya que puede provocar que la aplicación Contact Center Manager Server no funcione correctamente.

La siguiente tabla muestra los puertos que utiliza Contact Center Manager Server.

Tabla 13: Uso del puerto del Contact Center Manager Server

Número de puerto CCMS	Funcionalidad
445	El puerto TCP utilizaba el uso compartido de archivos e impresoras de Windows para redes Microsoft. Requerido al copiar datos entre servidores activos y en espera usando Windows File Sharing.
1550	CAPÍ HDX
1972	Base de datos de Caché y sombreado de Caché
4422	Servicio de nombres HDX
12668–12670	seguimiento de control
10000	Servicio de nombres del kit de herramientas codificado
10001–10082	Redes
10038	NCP_CHANNEL: este canal se utiliza para comunicarse entre el NCP de un nodo y el NCP de otro nodo. El NCP en un nodo envía mensajes de cordura al otro nodo a través de este puerto.
10039	ASM_CHANNEL: diferentes módulos como NCP y TFE envían mensajes a ASM a través de este canal.
10040	NCP_ASM_CHANNEL: ASM utiliza este canal para enviar mensajes a NCP.
10060	ASM_Service: el servicio ASM se ejecuta en este puerto. El administrador de control de servicios puede enviar mensajes como START, STOP y RESTART al servicio ASM a través de este puerto.
10062	NCP_Service: el servicio NCP se ejecuta en este puerto. El administrador de control de servicios puede enviar mensajes como START, STOP y RESTART a NCP en este puerto.
3998	Puerto de destino del administrador de licencias: este es el primero de 10 puertos consecutivos necesarios para la administración de licencias.
3999–4007	Puerto de origen del cliente del administrador de licencias
3389	Conexión de escritorio remoto para soporte
9080–9083	Interfaces abiertas de servicios web
9086	Estadísticas web CC
9100	Puerto del servidor del servicio web XMPP
9120	Puerto de cliente de servicio web XMPP
57012	Bandeja del sistema del componente de supervisión y administración del sistema (SMMC).

Requisitos del puerto de Contact Center Manager Administration

La siguiente tabla muestra los puertos que usa Contact Center Manager Administration.

Página275 de 3226.

Tabla 14: Uso del puerto de Contact Center Manager Administration

número de puerto CCMA	Funcionalidad
TCP 80	Para la comunicación de Internet Explorer.
TCP 443	Para comunicación HTTP segura (solo aplicable si SSL está habilitado para comunicación segura de Internet Information Services (IIS)).
Puerto TCP 445	Uso compartido de impresoras y archivos de Windows para redes Microsoft. Requerido al copiar datos entre servidores activos y en espera usando Windows File Sharing.
Puerto TCP 3389	Para conexión de escritorio remoto.
Puerto TCP 25 (SMTP)	Para que el componente Informes históricos envíe notificaciones por correo electrónico cuando se impriman y guarden los informes.
Puerto TCP 8200	Para el componente Ayuda de emergencia en la PC cliente.
Puertos UDP 6020, 6030, 6040, 6050, 6060, 6070, 6080, 6090, 6100, 6110, 6120, 6130	Para que el servidor CCMA reciba datos de multidifusión IP desde el servidor CCMA (necesario para los informes en tiempo real y las pantallas de Agent Desktop).
Puertos UDP 7020, 7030, 7040, 7050, 7060, 7070, 7080, 7090, 7100, 7110, 7120, 7130, 7140, 7150	Para que el servidor CCMA envíe datos de multidifusión IP a las PC cliente (necesario para los informes en tiempo real y las pantallas de Agent Desktop).
Puertos UDP 7025, 7035, 7045, 7055, 7065, 7075, 7085, 7095, 7105, 7115, 7125, 7135, 7145 y 7155	Para que el servidor CCMA envíe datos de unidifusión IP a las PC cliente. Este es un método opcional para enviar los datos necesarios para los informes en tiempo real. Si no utiliza el método de multidifusión, debe configurar la opción de unidifusión. También puede utilizar una combinación de los dos métodos.
Puerto TCP 10000	Utilizado por el proceso de servicio de nombres en el servidor CCMA (nbnmsrvc.exe). Permite la comunicación entre el servidor CCMA y el servidor en Contact Center Manager Server. **Importante:** El puerto predeterminado para el software de terceros. Esto entra en conflicto con el puerto predeterminado utilizado por CCMA Toolkit NameService. Para evitar problemas con la funcionalidad CCMA al utilizar Veritas Backup Exec, debe cambiar el puerto predeterminado de Veritas Backup Exec a otro número de puerto que no esté siendo utilizado por la red.
Puerto UDP predeterminado 3998	Puerto de destino del administrador de licencias.
Puertos UDP predeterminados 3999 - 4007	Puerto de origen de destino del administrador de licencias.

Requisitos de puerto de Communication Control Toolkit

La siguiente tabla muestra los números de puerto necesarios para Communication Control Toolkit (CCT).

Página276 de 3226.

Tabla 15: Uso del puerto de Communication Control Toolkit

número de puerto CCT	Funcionalidad
1972	Base de datos de Caché y soluciones de sombreado de Caché.
3998	Puerto de destino del administrador de licencias (LM), que es el primero de 10 puertos consecutivos necesarios para la administración de licencias.
3999 - 4007	Puertos de origen del cliente LM.
5000	Para conectarse al servidor en CCMS.
8081	Puerto predeterminado del servidor Apache Tomcat que aloja la administración web de CCT.
8085	Para que los servicios de CCT accedan a la base de datos de CCT.
8098	Para el marco de gestión de contactos en el servidor CCT.
8099	Para el marco de gestión de contactos en el servidor CCT.
8087	Para el componente CCT CMF.
9000	Para el componente CCT WebAdmin.
9010	Para el componente CCT CMF.
11110	Utilizado por el servicio del servidor CCT para el servicio web CMF: puerto de devolución de llamada.
11111	Utilizado por el servicio del servidor CCT para el servicio web CMF: puerto del servidor web.
29373	Escucha las solicitudes de las aplicaciones cliente de CCT.
29374	El servicio de capa de acceso a datos escucha las solicitudes de la consola de administración remota de CCT.

Requisitos del puerto de Contact Center Multimedia

La siguiente tabla enumera los puertos multimedia configurables.

Tabla 16: Puertos multimedia del Contact Center

Puerto	Anfitrión	Cliente	Interfaz de red	Funcionalidad
1972	Centro de contacto Multimedia	Centro de contacto Gerente Administración Servidor	Centro de contacto Caché multimedia base de datos	Puerto abierto el base de datos para informes Cache base de datos, y Sombreado de caché.
445	Archivo de Windows y Uso compartido de impresoras para microsoft Redes.	Archivo de Windows y Uso compartido de impresoras para microsoft Redes.	Archivo de Windows y Uso compartido de impresoras para microsoft Redes.	Archivo de Windows y Uso compartido de impresoras para microsoft Redes. Requerido cuando

La tabla continúa...

Página277 de 3226.

Puerto	Anfitrión	Cliente	Interfaz de red	Funcionalidad
				copiando datos entre activo y servidores en espera usando el archivo de Windows Intercambio.
110	servidor de correo electronico	Administrador de correo electrónico	Servidor de correo electrónico POP3	Recibir correo electrónico
143	servidor de correo electronico	Administrador de correo electrónico	Servidor de correo electrónico IMAP	Recibir correo electrónico
995	servidor de correo electronico	Administrador de correo electrónico	POP3 sobre SSL (opcional)	Recibir seguro email opcional)
993	servidor de correo electronico	Administrador de correo electrónico	IMAP sobre SSL (opcional)	Recibir seguro email opcional)
110	servidor de correo electronico	Administrador de correo electrónico	POP3 sobre TLS (opcional)	Recibir seguro email opcional)
143	servidor de correo electronico	Administrador de correo electrónico	IMAP sobre TLS (opcional)	Recibir seguro email opcional)
25	servidor de correo electronico	Administrador de correo electrónico	SMTP	Enviando correo electrónico
25	servidor de correo electronico	Administrador de correo electrónico	SMTP sobre TLS (opcional)	Envío seguro email opcional)
80	Centro de contacto servidor multimedia	Cualquier servicio web cliente (Agente Escritorio, OCMT, y de terceros Servicios web)	Protocolo SOAP	Accediendo a http servicios web
29373	Comunicación Kit de herramientas de control Servidor	Escritorio del agente	Comunicación Kit de herramientas de control	Acceso remoto de clientes a Comunicación Kit de herramientas de control servidor (para Agente Escritorio solicitud)
57012	Sistema Administración y Vigilancia Componente (SMMC) sistema bandeja	Sistema Administración y Vigilancia Componente (SMMC) sistema bandeja	Sistema Administración y Vigilancia Componente (SMMC) sistema bandeja	Base de datos sombreado

Aura de Avaya®Requisitos del puerto del servidor de medios

La siguiente tabla muestra los números de puerto necesarios para Avaya Aura®Servidor multimedia en Windows Server 2012 R2.

Tabla 17: Avaya Aura®Uso del puerto del servidor multimedia: Windows Server 2012 R2

Puerto	Escribe	Permiso en TCP Filtrar	Descripción
1027	TCP	Sí	Servidor de licencias
1028	TCP	No	Monitor de sistema mchb
3306	TCP	Sí	mysql
3389	TCP	Sí	Escritorio remoto
3867	SCTP	No	Diámetro sobre SCTP
3868	TCP	No	Diámetro sobre TCP
3869	TCP	No	Diámetro sobre TLS
4001	TCP	No	IvrMP MSLink
4004	TCP	No	Sip UA MSLink
4005	TCP	No	Gestor de recursos ExtSess
4014	TCP	No	SIP UA cmd i/f
4015	TCP	No	Administrador de recursos y i/f
6080	TCP	No	Saludo del agente
7080	TCP	No	ConfMP MSLink
7410	TCP	Sí	servidor de jabón
7411	TCP	Sí	SoapServer TLS
8080	TCP	Sí	EM HTTP
8443	TCP	Sí	HTTP(s) de EM
11004	TCP	No	DiamC MSLink
11014	TCP	No	DiamC y i/f
19899	TCP	Sí	Administrador de recursos CPLink
19999	TCP	Sí	datos ss de IvrMP
20005	TCP	Sí	CStore MSLink
20007	TCP	Sí	CAlmacenar RTFT
20009	TCP	Sí	IvrMP RTFT
21000	TCP	No	Intérprete XML de voz IPC
51000	TCP	No	Administrador de recursos IPC
51001	TCP	No	Demonio de alarma MPS heredado
51003	TCP	No	Intérprete CCXML IPC

La siguiente tabla muestra los números de puerto necesarios para Avaya Aura®Servidor multimedia en Linux.

Tabla 18: Avaya Aura®Uso del puerto del servidor multimedia: Linux

Puerto	Escribe	Permiso en TCP Filtrar	Descripción
1027	TCP	Sí	Servidor de licencias
1028	TCP	No	Monitor de sistema mchb
3306	TCP	Sí	mysql
3867	SCTP	No	Diámetro sobre SCTP
3868	TCP	No	Diámetro sobre TCP
3869	TCP	No	Diámetro sobre TLS
4001	TCP	No	IvrMP MSLink
4004	TCP	No	Sip UA MSLink
4005	TCP	No	Gestor de recursos ExtSess
4014	TCP	No	SIP UA cmd i/f
4015	TCP	No	Administrador de recursos cmd i/f
5060	TCP	Sí	SIP sobre TCP
5060	UDP	No	SIP sobre UDP
5061	TCP	Sí	SIP sobre TLS
6080	TCP	No	Saludo del agente
7080	TCP	No	ConfMP MSLink
7410	TCP	Sí	servidor de jabón
7411	TCP	Sí	SoapServer TLS
8080	TCP	Sí	EM HTTP
8443	TCP	Sí	HTTP(s) de EM
11004	TCP	No	DiamC MSLink
11014	TCP	No	DiamC y i/f
19899	TCP	Sí	Administrador de recursos CPLink
19999	TCP	Sí	datos ss de IvrMP
20005	TCP	Sí	CStore MSLink
20007	TCP	Sí	CAlmacenar RTFT
20009	TCP	Sí	IvrMP RTFT
20011	TCP	No	Administrador de recursos IPC
21000	TCP	No	Intérprete XML de voz IPC

Se requiere el rango de puertos UDP para el procesamiento de medios. Todos los puertos UDP iniciales son configurables.

Tabla 19: Intervalo de puertos UDP requerido

Sistema operativo	Intervalo de puertos UDP
Servidor Windows 2012 R2	20000 a 45499
linux	6000 a 32599

Índice

numericos

1,2 TB 69
1200GB 69
CPU de 8 núcleos 68
900 GB 69

A

agregar imágenes de la empresa
  firmas 20
agregar logotipos de empresas
  firmas 20
AD-LDS 17
agente
  Entrenamiento de susurros 25
aplicación de navegador de agente
  Compatibilidad del navegador 178
  requisitos 177
Escritorio del agente
  inserción automática de un dígito inicial 15
  Asistencia técnica de Citrix 176
  Mostrar el historial de inicio de sesión 21
  directorio de exploración de archivos cambiado a directorio de usuario 22
  forzar la complejidad de la contraseña para las cuentas Multimedia 24
  soporte para copiar CLID 20
  compatibilidad con códigos de motivo No listo forzados 21
Navegador web integrado de Agent Desktop
  utiliza la última versión de Internet Explorer instalada en el sistema cliente 23
Requisitos de Agent Desktop 164
software antivirus ..... 78 ,88 ,116
secuencia de aplicaciones 149
Portal de la experiencia Avaya Aura 145
Servidor multimedia Avaya Aura 90
Requisitos de puerto de Avaya Aura Media Server 193
Servidor de medios Avaya 15
Aviso de seguridad de Avaya 56

B

Tono de intrusión y observación 15
cartelera
  lista de conjuntos de habilidades ordenada 25
BIO ..... 70 ,100
compatibilidad del navegador
  aplicación de navegador del agente 178
Continuidad del negocio 56

C

Base de datos de caché 17
XML de control de llamadas 147
desconexión de llamada 57
Llamada Forzada Respuesta Zip Tono 15
grabacion de llamada 52
límites de capacidad 120
CCMA
  Citrix 162
  introducción incorrecta de una contraseña 21
  caducidad de la contraseña 19
  caducidad de la contraseña 17
  bloqueo temporal 21
Requisitos del puerto CCMA 190
Requisitos del puerto CCMM 192
Requisitos del puerto CCMS 189
CCSA 15
Requisitos del puerto CCT 191
Funcionalidad compatible con CCT 140
CCXML 147
cambios en esta versión 15
Soporte Citrix
  Escritorio del agente 176
CLI 21
requerimientos del cliente 160
configuración 44
Cuenta de instalación de Contact Center 31
Administración del administrador del centro de contacto
  mostrar los intentos de inicio de sesión fallidos 21
  Mostrar el historial de inicio de sesión 21
Servicios del centro de contacto 15
copiar CLID 20

D

Sincronización de datos 39
Transferencia de datos 146
DHCP ..... 76 ,87 ,115
almacenamiento en caché del disco ..... 72 ,
102 particiones de disco 84
mostrando
  intentos de inicio de sesión fallidos 21
  historial de inicio de sesión 21
dominio 54
DVD ..... 63,sesenta y cinco,74,80

mi

ejemplo de flujo de mensajes de correo electrónico 51
licencia de emergencia 18
Servidor de nivel de entrada ..... sesenta y cinco
Servidor de intercambio 29
Portal de la experiencia ..... 153 ,155
interacciones con servidores externos 50

F

funciones 7.0 Paquete de funciones 1
- agregar un nombre descriptivo para el agente de chat web 24
- Directorio de exploración de Agent Desktop 22
- restricción de tipo de archivo adjunto 23
- actualización automática de conjuntos de habilidades sin personal para informes en tiempo real 22
- forzar la complejidad de la contraseña 24
- última versión de Internet Explorer instalada en el sistema cliente para el navegador web integrado en Agent Desktop 23
- eliminación de la contraseña predeterminada del panel de Agent Desktop 25
  - lista de conjuntos de aptitudes ordenada para visualización en vallas publicitarias 25
- Entrenamiento de susurros 25

funciones 7.0 Paquete de funciones 2
- Inicio de sesión integrado de Agent Desktop 26
  - medidas de protección de asignación de conjunto de habilidades de agente 26
- cambiar la contraseña CCMA 31
- aumento de la relación de contacto con el cliente de CCMM 26
- sincronización de cambios de usuario accssync 27

firmware ....71 ,101
forzados códigos de motivo No listo 21
forzar cambio de contraseña
- el usuario inicia sesión en CCMA por primera vez 18

funciones del servidor de telefonía 140

GRAMO

nombre del servidor de requisitos globales ....74 ,85 ,113 Directrices para el entorno de tiempo de ejecución de Java ....76 ,86 ,114
Directrices para paquetes de servicios ....76 ,86 ,114
Directrices para las actualizaciones del servicio ....75 ,85 , 113 Directrices para el software de utilidad ....77 ,87 ,115

H

H.323 149
particiones del disco duro ....69 ,84
ferretería 109
dispositivo de hardware ....18 ,109 ,110
Aparato de hardware 118
virtualización asistida por hardware 99
Requisitos de hardware ....sesenta y cinco ,66 , 68 requisitos de hardware, Administrador 160
requisitos de hardware, Agent Desktop 165
Solución de gama alta 68
consideraciones sobre el host vmware 99
Hiperprocesamiento ....73 ,103

yo

interacciones con servidores multimedia externos 50
IOP 105
Soporte de IP Office 43
Versiones de IP Office 29,32

j

Directrices del entorno de tiempo de ejecución de Java ....76 ,86 ,114

L

Licencia ....80 ,108 ,118
Licencia 36
limitaciones 59
Idiomas localizados 164

METRO

maxima capacidad 120
Servidor de Microsoft Exchange 29
Servidor de gama media 66
especificaciones mínimas de hardware 19
especificación mínima de máquina virtual 19
cuentas multimedia
- forzar la complejidad de la contraseña 24
  - coincida con los criterios mínimos de complejidad de la contraseña 24

interacciones del servidor externo multimedia 50

norte

Requisitos del servidor de nombres 74,85,113
requisitos de la red 167
notificación
- caducidad de la licencia de emergencia 18

No soportado
- Implementación de cliente grueso de escritorio de agente 29

NUMA ....73 ,102

O

Tono de observación 15
almacén de seguridad fuera de línea 26
Pautas del entorno de ejecución de Java del sistema operativo ....76 ,86 ,114
Directrices sobre los paquetes de sistemas operativos ....76 ,86 ,114
requisitos del sistema operativo ....161 ,166 directrices de actualización del servicio del sistema operativo ....75 ,85 ,113

PAGS

antigüedad de la contraseña
- CMA 19

caducidad de la contraseña
- CMA 17

actuación ....70 ,100
gestión del rendimiento ....72 ,101 P-encabezado 148
Directorio telefónico
- inserción automática de un dígito inicial 15

Página283 de 3226.

P-Intrínsecos 148
matriz de puertos 189
requisitos de puerto Avaya Aura Media Server 193
requisitos de puerto CCMA 190
requisitos de puerto CCMM 192
requisitos de puerto CCMS 189
requisitos portuarios CCT 191
puertos 176
Encabezado privado 148
PVI ..... sesenta y cinco

R

REDADA ..... 72 ,102
documentación relacionada 11
soporte de acceso remoto 140
Agentes Remotos 53
Servicios de escritorio remoto Escritorio de agente
A ..... 26 ,174
Eliminación de la configuración de seguridad predeterminada 27
requisitos
aplicación de navegador del agente 177
requisitos Java Runtime Environments ..... 76 ,86 ,114
puerto de requisitos Avaya Aura Media Server 193
requisitos puerto CCMA 190
requisitos puerto CCMM 192
requisitos puerto CCMS 189
requisitos puerto CCT 191
nombre del servidor de requisitos ..... 74 ,85 ,113
Paquetes de servicio de requisitos ..... 76 ,86 ,114
actualizaciones del servicio de requisitos ..... 75 ,85 ,113
software de utilidad de requisitos ..... 77 ,87 ,115
Integración de la API REST 27
restricción
tipos de archivos adjuntos 23

S

flujos de muestra 47
Pantalla emergente 148
secuencias de comandos
CLID y CLID salvaje 21
seguridad 56
Gerente de seguridad
mostrar los intentos de inicio de sesión fallidos 21
Mostrar el historial de inicio de sesión 21
Firma del bloque de mensajes del servidor 188
requisitos del nombre del servidor ..... 74 ,85 ,113
mejoras de capacidad de servicio
Actualización de controles de terceros de Agent Desktop 20
mejoras de seguridad 20
Directrices de los paquetes de servicios ..... 76 ,86 ,114
Directrices de actualizaciones de servicio ..... 75 ,85 , 113 Protocolo de Iniciacion de Sesion 147
SGM 147
firmas
añadir imágenes de la empresa 20
firmas *(continuado)*
añadir logotipos de la empresa 20
SORBO 147
entorno SIP
CLID y CLID salvaje 21
Administrador de puerta de enlace SIP 147
señalización SIP 149
lista de conjuntos de habilidades ordenada 25
consideraciones de instantáneas ..... 104 ,105 SODC 57
software 109
dispositivo de software 81
especificaciones del software 112
directrices de la utilidad de software ..... 77,87, 115 apoyo 14
funciones principales admitidas 123
funciones multimedia admitidas 123
Funciones de informes admitidas 123

T

Dispositivos de telefonía 138
caracteristicas de telefono 129
funciones del servidor de telefonía 140
bloqueo temporal
CMA 21
software de terceros ..... 163 ,167
pantalla táctil 165
pantalla táctil 165

tu

UEFI 71
Identificador universal de llamadas 149
equipo sin usar ..... 73 ,103 el usuario inicia sesión en CCMA por primera vez
forzar cambio de contraseña 18
Directrices del software de utilidad ..... 77 ,87 , 115 IUU 149

V

vídeos 14
virtualización 103
virtualización 107
consideraciones de virtualización 97
máquina virtual ..... 83 ,84
Vmware 102
anfitrión vmware 99
VMXNET 103
XML de voz 147
VXML 147

W

WebLM 91

Conjunto de habilidades de susurro 15
CLID salvaje 21
grupo de trabajo 54

Traducido del inglés al español - www.onlinedoctranslator.com

Administración de la plataforma Avaya IP Office™ con Manager

Avisos

© 2021 derechos de autor

Usted puede, bajo su propio riesgo, reunir una colección de MyDocs únicamente para sus propios fines comerciales internos, lo que constituye una modificación de la versión original publicada de las publicaciones. Avaya no será responsable de ninguna modificación, adición o eliminación de la versión original publicada de las publicaciones. Usted acepta defender, indemnizar y eximir de responsabilidad a Avaya, a los agentes, servidores y empleados de Avaya contra todos los reclamos, juicios, demandas y juicios que surjan de, o en relación con, sus modificaciones, adiciones o eliminaciones de las publicaciones.

Un solo tema o una colección de temas puede provenir de varias publicaciones de Avaya. Todo el contenido de su colección está sujeto a los avisos legales y descargos de responsabilidad de las publicaciones a partir de las cuales reunió la colección. Para obtener información sobre licencias y tipos de licencias, marcas comerciales y declaraciones reglamentarias, consulte las publicaciones originales de las que copió los temas de su colección.

Salvo que Avaya indique expresamente lo contrario, no se debe hacer uso de los materiales proporcionados por Avaya en este sitio. Todo el contenido de este sitio y las publicaciones proporcionadas por Avaya, incluida la selección, disposición y diseño del contenido, son propiedad de Avaya y/o sus licenciantes y están protegidos por derechos de autor y otras leyes de propiedad intelectual, incluidos los derechos sui generis relacionados con la protección de bases de datos Avaya posee todos los derechos, títulos e intereses sobre cualquier modificación, adición o eliminación del contenido de las publicaciones de Avaya.

Resiliencia de la edición del servidor

Resiliencia

Un solo servidor Primario de Server Edition admite unidades de disco duro y fuentes de alimentación redundantes. También puede configurar la selección de ruta alternativa.

Agregue una Server Edition Secundaria para brindar resiliencia en cualquier nivel. El servidor secundario de Server Edition proporciona resiliencia para los usuarios del servidor primario de Server Edition, extensiones H.323 y SIP, grupos de búsqueda y correo de voz sin ninguna administración. El servidor secundario de Server Edition puede proporcionar resiliencia para Avaya one-X® Portal for IP Office.

Se puede realizar una copia de seguridad de un Sistema de expansión Server Edition en el Primario Server Edition, el Secundario Server Edition u otro Sistema de expansión Server Edition. La topología de red multisitio de doble estrella cuando hay un servidor secundario de Server Edition admite enrutamiento diverso entre todos los nodos.

Para las implementaciones de Server Edition Select, las líneas IP Office (troncales SCN) se pueden configurar entre los sistemas de expansión Server Edition. Los grupos de búsqueda se pueden configurar localmente para el sistema de expansión y se puede configurar la resiliencia para los grupos de búsqueda y los teléfonos, con conmutación por error a Server Edition Primary, Server Edition Secondary u otro Server Edition Expansion System.

En todo momento, no se obliga a ningún hardware de servidor a estar inactivo, lo que le permite decidir si proporciona redundancia real o resiliencia de recursos compartidos.

La solución IP Office Server Edition proporciona resiliencia para teléfonos H.323 compatibles, terminales SIP e implementaciones DECT R4. Las líneas de IP Office entre sistemas se pueden configurar para permitir que el control pase automáticamente a un IP Office de respaldo cuando el sistema doméstico no está disponible.

Componentes resilientes

Los siguientes componentes de IP Office Server Edition Solution son resistentes:

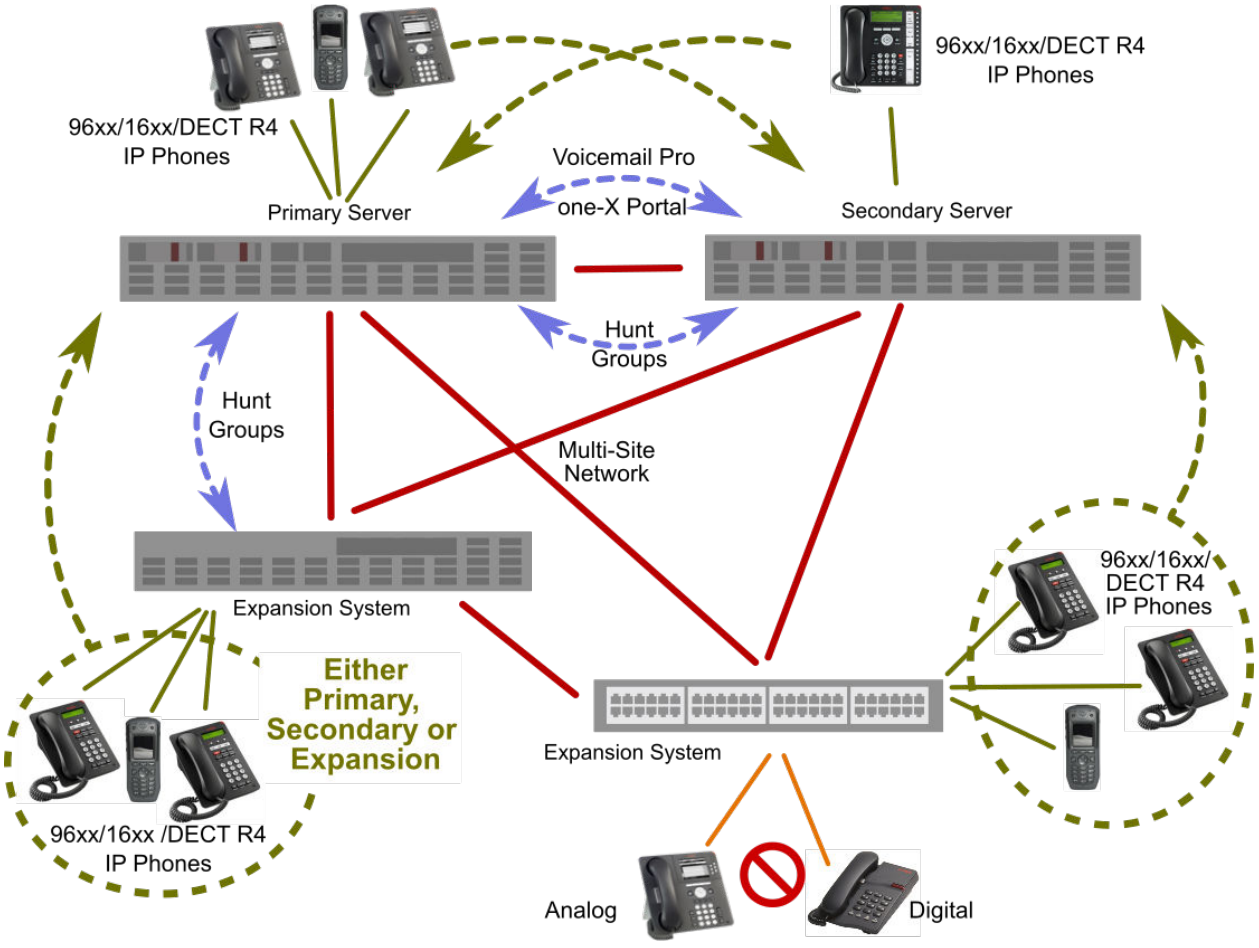
- Edición de servidor de IP Office
- Servidor Voicemail Pro
- Servidor Avaya one-X® Portal
- Teléfonos H.323
- terminales SIP
- DECT R4
- Grupos de búsqueda
- Enlaces entre dispositivos
- Baúles
- Rutas de llamadas entrantes
- Administración

Red multisitio

Una red multisitio mejora la resiliencia al proporcionar las siguientes capacidades:

- Transparencia para la mayoría de las funciones
- Resiliencia de usuarios y grupos de búsqueda
- Sistema de respaldo para Voicemail Pro
- La topología de red proporciona resiliencia
- Ningún hardware está inactivo
- Fácil de activar la resiliencia

Figura 1. Arquitectura de resiliencia



Gestión resiliente

Puede continuar administrando y administrando la falla del servidor y los dispositivos de IP Office Server Edition en una red de IP Office Server Edition Solution a través del servidor secundario de Server Edition. Esto proporciona administración sin la capacidad fuera de línea y una facilidad para realinear la configuración después de que se hayan resuelto las interrupciones. La función de resincronización destaca la hora y el origen del cambio de configuración y permite al administrador decidir qué conjunto de cambios conservar. Además, puede administrar directamente cada dispositivo y aplicación para permitir la configuración mientras está aislado. Puede utilizar la capacidad de resincronización para realinear las configuraciones después de volver a conectar los dispositivos.

Avaya IP Office™ Platform Feature Description

Versión 11.0 FP4
Febrero de 2019

© 2015-2019, Avaya Inc.
Todos los derechos reservados.

Aviso

Si bien se hicieron esfuerzos razonables para asegurar que la información contenida en este documento esté completa y sea exacta en el momento de su impresión, Avaya no se responsabiliza por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información contenida en este documento sin la obligación de notificar a ninguna persona u organización dichos cambios.

Exención de responsabilidad con respecto a la documentación

“Documentación” hace referencia a la información publicada en diversos medios (que puede incluir información del producto, instrucciones operativas y especificaciones de rendimiento) que se suele poner a disposición de los usuarios de los productos. La documentación no incluye material publicitario. Avaya no es responsable de ninguna modificación, incorporación ni eliminación en la versión original publicada de la Documentación a menos que dichas modificaciones, incorporaciones o eliminaciones hayan sido efectuadas por Avaya o en su representación. El usuario final acuerda indemnizar y eximir de toda responsabilidad a Avaya, agentes de Avaya y empleados con respecto a todo reclamo, acción judicial, demanda y juicio que surgiere de o en relación con modificaciones, incorporaciones o eliminaciones posteriores en esta documentación realizadas por el usuario final.

Exención de responsabilidad con respecto a los vínculos

Avaya no asume la responsabilidad del contenido ni de la fiabilidad de los enlaces a los sitios web incluidos en cualquier punto de este sitio o en Documentación proporcionada por Avaya. Avaya no es responsable de la confiabilidad de ninguna información, instrucción ni contenido proporcionado en estos sitios y no necesariamente aprueba los productos, los servicios o la información descritos u ofrecidos por los mismos. Avaya no garantiza que estos vínculos funcionarán todo el tiempo ni tiene control de la disponibilidad de las páginas vinculadas.

Garantía

Avaya ofrece una garantía limitada para sus productos de hardware y software. Consulte su contrato de compraventa para establecer las condiciones de la garantía limitada. Además, el idioma de la garantía estándar de Avaya, así como la información relacionada con el soporte técnico para este producto durante el período de vigencia de la garantía, está disponible, tanto para los clientes como para otras partes interesadas, en el sitio web de soporte técnico de Avaya: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 en el enlace “Warranty & Product Lifecycle” (Garantía y ciclo de vida del producto) o en el sitio web posterior a este designado por Avaya. Tenga en cuenta que si ha adquirido los productos de un Channel Partner de Avaya fuera de Estados Unidos y Canadá, la garantía es proporcionada por dicho Channel Partner y no por Avaya.

“Servicio alojado” hace referencia a una suscripción de servicio alojado de Avaya que usted adquiere ya sea de Avaya o de un Channel Partner autorizado de Avaya (según corresponda) y que se describe detalladamente en SAS alojado u otra documentación de descripción del servicio sobre el servicio alojado correspondiente. Si compra una suscripción de servicio alojado, la garantía limitada anterior podría no ser aplicable, pero puede tener derecho a servicios de soporte técnico relacionados con el servicio alojado como se describe más adelante en los documentos de descripción del servicio para el servicio alojado correspondiente. Comuníquese con Avaya o el Channel Partner de Avaya (según corresponda) para obtener más información.

Servicio alojado

LOS SIGUIENTES TÉRMINOS SE APLICAN SOLO SI COMPRA UNA SUSCRIPCIÓN DE SERVICIO ALOJADO DE AVAYA MEDIANTE AVAYA O UN CHANNEL PARTNER DE AVAYA (SEGÚN CORRESPONDA). LOS TÉRMINOS DE USO DE LOS SERVICIOS ALOJADOS SE ENCUENTRAN DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO EN EL ENLACE “Términos de uso de Avaya para los servicios alojados” U OTRO SITIO DESIGNADO POR AVAYA, Y SE APLICAN A CUALQUIER PERSONA QUE ACCEDA O UTILICE EL SERVICIO ALOJADO. SI ACCEDE O UTILIZA EL SERVICIO ALOJADO O AUTORIZA A TERCEROS PARA QUE LO HAGAN, USTED, EN REPRESENTACIÓN DE USTED MISMO Y LA ENTIDAD PARA LA QUE LO ESTÁ HACIENDO (DE AQUÍ EN ADELANTE “USTED” Y “USUARIO FINAL” DE MANERA INTERCAMBIABLE), ACEPTAN LOS TÉRMINOS DE USO. SI ACEPTA LOS TÉRMINOS DE USO EN REPRESENTANCIÓN DE UNA EMPRESA U OTRA ENTIDAD LEGAL, SIGNIFICA QUE USTED TIENE LA AUTORIDAD PARA VINCULAR A DICHA ENTIDAD A ESTOS TÉRMINOS DE USO. SI NO CUENTA CON TAL AUTORIDAD O SI NO DESEA ACEPTAR ESTOS TÉRMINOS DE USO, NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A TERCEROS A ACCEDER O UTILIZAR EL SERVICIO ALOJADO.

Licencias

LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO EN EL ENLACE “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” [TÉRMINOS DE LA LICENCIA DE SOFTWARE DE AVAYA (productos de Avaya)] O EN EL SITIO POSTERIOR A ESTE DESIGNADO POR AVAYA, SE APLICAN A CUALQUIER PERSONA QUE DESCARGUE, USE O INSTALE SOFTWARE DE AVAYA, ADQUIRIDO DE AVAYA INC., CUALQUIER SUBSIDIARIA DE AVAYA O UN CHANNEL PARTNER DE AVAYA (SEGÚN CORRESPONDA) BAJO UN ACUERDO COMERCIAL CON AVAYA O CON UN CHANNEL PARTNER DE AVAYA. A MENOS QUE AVAYA ACEPTE POR ESCRITO LO CONTRARIO, AVAYA NO EXTIENDE ESTA LICENCIA SI EL SOFTWARE SE OBTUVO DE UN TERCERO QUE NO SEA AVAYA, UN AFILIADO DE AVAYA O UN CHANNEL PARTNER DE AVAYA. AVAYA SE RESERVA EL DERECHO DE INICIAR ACCIONES LEGALES EN CONTRA SUYO O DE CUALQUIER PERSONA QUE UTILICE O VENDA EL SOFTWARE SIN LA LICENCIA. SI INSTALA, DESCARGA O UTILIZA EL SOFTWARE O SI AUTORIZA A UN TERCERO A QUE LO HAGA, USTED, EN REPRESENTACIÓN DE USTED MISMO Y DE LA ENTIDAD PARA LA CUAL INSTALA, DESCARGA O UTILIZA EL SOFTWARE (DE AQUÍ EN ADELANTE “USTED” Y “USUARIO FINAL”), ACEPTA ESTOS TÉRMINOS Y CONDICIONES Y ESTABLECE UN CONTRATO VINCULANTE ENTRE USTED Y AVAYA INC. O EL AFILIADO DE AVAYA CORRESPONDIENTE (“AVAYA”).

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el que se detalla el alcance de la licencia a continuación. Donde la documentación de la orden no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de sistema designado. La cantidad correspondiente de licencias y unidades de capacidad para la que se otorga la licencia será uno (1), a menos que una cantidad diferente de licencias o unidades de capacidad se especifique en la documentación u otros materiales disponibles para usted. “Software” significa programas de computadora en código objeto proporcionado por Avaya o un Channel Partner de Avaya, ya sea como productos independientes o preinstalados en productos de hardware, y cualquier mejora, actualización, revisión, corrección de falla o versiones modificadas del mismo. “Procesador designado” significa un dispositivo informático independiente único. “Servidor” significa un Procesador designado que aloja una aplicación de software a la que pueden acceder varios usuarios. “Instancia” significa una única copia del software que se ejecuta en un momento determinado: (i) en una máquina física, o (ii) en un software instalado en una máquina virtual (“VM”) o una implementación similar.

Tipos de licencia

Licencia de sistemas designados (DS). El usuario final puede instalar y utilizar cada copia o una instancia del software solo en el número de procesadores designados indicado en la orden. Avaya puede exigir que el procesador designado sea indicado en la orden por tipo, número de serie, tecla de función, instancia, ubicación u otra designación específica, o que el usuario final proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este propósito.

Licencia de usuarios simultáneos (CU). El usuario final puede instalar y utilizar el software en varios procesadores designados o en uno o más servidores, siempre y cuando solo las unidades con licencia accedan y utilicen el software en un momento dado. Una “unidad” se refiere a la unidad en la que Avaya, a su exclusivo criterio, fundamenta el precio de sus licencias y puede ser incluso, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o de correo de voz en nombre de una persona o función corporativa (por ejemplo, administrador web o centro de asistencia técnica) o una entrada de directorio en la base de datos administrativa utilizada por el software que permite que un usuario se conecte con el software. Las unidades pueden vincularse con un servidor específico identificado o una instancia del software.

Licencia de la base de datos (DL). El usuario final puede instalar y utilizar cada copia o una instancia del software en un servidor o en varios servidores, siempre y cuando cada servidor en el cual el software esté instalado se comunique con no más de una instancia de la misma base de datos.

Licencia de CPU (CP). El usuario final puede instalar y utilizar cada copia o instancia del software hasta la cantidad de servidores que indica la orden, siempre y cuando la capacidad de rendimiento de los servidores no exceda la capacidad de rendimiento especificada para el software. El usuario final no puede instalar nuevamente ni operar el software en servidores con una capacidad de rendimiento mayor sin el consentimiento previo de Avaya y sin pagar una tarifa por la actualización.

Licencia del usuario identificado (NU). Usted puede: (i) instalar y utilizar cada copia o instancia del software en un solo procesador designado o servidor por usuario identificado autorizado (se define a continuación); o (ii) instalar y utilizar cada copia o instancia del software en un servidor siempre y cuando únicamente los usuarios identificados autorizados obtengan acceso a él y lo utilicen. “Usuario identificado” se refiere a un usuario o un dispositivo que ha sido expresamente autorizado por Avaya para tener acceso al software y utilizarlo. A entera discreción de Avaya, un “usuario identificado” puede ser incluso, entre otros, designado por nombre, función corporativa (por ejemplo, administrador web o centro de asistencia técnica), una cuenta de correo electrónico o de correo de voz a nombre de una persona o función corporativa, o una entrada de directorio en la base de datos administrativa utilizada por el software que permite que un usuario se conecte con el software.

Licencia Shrinkwrap (SR). El cliente puede instalar y utilizar el software de acuerdo con los términos y las condiciones de los contratos de licencia vigentes, como las licencias “shrinkwrap” o “clickthrough” que acompañan o se aplican al software (“licencia Shrinkwrap”).

Heritage Nortel Software

“Heritage Nortel Software” significa el software que adquirió Avaya como parte de la compra de Nortel Enterprise Solutions Business en diciembre de 2009. El software Nortel heredado es el software que se incluye en la lista Heritage Nortel Products (Productos Nortel heredados) en https://support.avaya.com/LicenseInfo, en el enlace “Heritage Nortel Products” o en el sitio web posterior a este designado. Para el software Nortel heredado, Avaya otorga al cliente una licencia para utilizar el software Nortel heredado en virtud del presente documento únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la documentación y solamente como se incorpora, ejecuta o para comunicación con equipo Avaya. Los cargos por Heritage Nortel Software se podrían basar en el alcance de activación o el uso autorizado según se especifique en una orden o factura.

Copyright

Excepto donde se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, de la documentación, del software, del servicio alojado ni del hardware proporcionados por Avaya. Todo el contenido de este sitio, la documentación, el servicio alojado y los productos proporcionados por Avaya, incluida la selección, la disposición y el diseño del contenido, son de propiedad de Avaya o de sus licenciantes y están protegidos por leyes de derecho de autor y otras leyes de propiedad intelectual, incluidos los derechos de su género relacionados con la protección de las bases de datos. No debe modificar, copiar, reproducir, reeditar, cargar, publicar, transmitir ni distribuir de ninguna manera el contenido, en su totalidad o en parte, incluidos los códigos y el software, a menos que posea una autorización expresa de Avaya. La reproducción, transmisión, difusión, almacenamiento y/o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede considerarse un delito penal o civil según la ley vigente.

Virtualización

Si el producto se implementa en una máquina virtual, se aplica lo siguiente. Cada producto tiene su propio código de pedido y tipos de licencia. Tenga en cuenta que cada instancia de un producto debe tener una licencia aparte y pedirse por separado. Por ejemplo, si el cliente usuario final o el Channel Partner de Avaya prefieren instalar dos instancias del mismo tipo de producto, entonces se deben solicitar dos productos del mismo tipo.

Componentes de terceros

“Componentes de terceros” se refieren a ciertos programas de software y partes de estos incluidos en dicho software o servicio alojado que pueden contener software (incluido el software de código abierto) distribuido según contratos de terceros (“Componentes de terceros”), que incluyen condiciones sobre los derechos a utilizar ciertas partes del software (“Términos y condiciones de terceros”). Según se requiera, la información correspondiente al código fuente de SO Linux distribuido (para aquellos productos que tienen código fuente de SO Linux distribuido) y que identifique a los titulares de derechos de autor de los Términos y condiciones de los participantes, y los Términos y condiciones de terceros aplicables, está disponible en los productos, la documentación o en el sitio web de Avaya: https://support.avaya.com/Copyright o en el sitio web posterior a este designado por Avaya. Los términos de la licencia de software de código abierto que se proporcionan como Términos de terceros se corresponden con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del software de código abierto. Los Términos de terceros tienen prioridad sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables, en la medida en que estos Términos de la licencia de software impongan mayores restricciones que los Términos de terceros aplicables.

Se aplica lo siguiente únicamente si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO ESTÁ SUJETO A LA LICENCIA DE CARTERA DE PATENTES AVC PARA EL USO PERSONAL DE UN CONSUMIDOR Y OTROS USOS QUE NO IMPLIQUEN REMUNERACIÓN PARA (i) CODIFICAR VÍDEO QUE CUMPLA CON EL ESTÁNDAR AVC (“AVC VIDEO”) O (ii) DECODIFICAR VÍDEO AVC QUE UN CLIENTE CODIFICÓ DURANTE UNA ACTIVIDAD PERSONAL U OBTENIDO A TRAVÉS DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA SUMINISTRAR VÍDEO AVC. NINGUNA LICENCIA SE OTORGA O DEBE UTILIZARSE PARA OTRO FIN. PUEDE OBTENER MÁS POR PARTE DE MPEG LA, L.L.C. VISITE HTTP://WWW.MPEGLA.COM.

Proveedor de servicio

LO SIGUIENTE SE APLICA A LOS CHANNEL PARTNERS DE AVAYA QUE ALOJEN PRODUCTOS O SERVICIOS DE AVAYA. EL PRODUCTO O SERVICIO ALOJADO PUEDE USAR COMPONENTES DE TERCEROS SUJETOS A LOS TÉRMINOS DE TERCEROS Y REQUERIR QUE EL PROVEEDOR DE SERVICIOS UNA TENGA LICENCIA INDEPENDIENTE DIRECTA DE ESTOS TERCEROS. UN CHANNEL PARTER DE AVAYA QUE ALOJE PRODUCTOS DE AVAYA DEBE CONTAR CON AUTORIZACIÓN ESCRITA DE AVAYA, Y, EN CASO DE QUE DICHOS PRODUCTOS ALOJADOS UTILICEN O INCORPOREN SOFTWARE DE TERCEROS, LO QUE INCLUYE, A TÍTULO ENUNCIATIVO, SOFTWARE O CÓDECS DE MICROSOFT,EL CHANNEL PARTNER DE AVAYA DEBERÁ OBTENER DE FORMA INDEPENDIENTE Y A SU CARGO LOS ACUERDOS DE LICENCIA CORRESPONDIENTES, DIRECTAMENTE DEL PROVEEDOR DE TERCEROS.

CON RESPECTO A LOS CÓDECS, SI EL CHANNEL PARTNER DE AVAYA ALOJA PRODUCTOS QUE UTILIZAN O INCORPORAN LOS CÓDECS G.729, H.264 O H.265, EL CHANNEL PARTNER DE AVAYA RECONOCE Y MANIFIESTA ACUERDO CON QUE ES RESPONSABLE DE ASUMIR TODAS LAS TARIFAS Y/O REGALÍAS. EL CÓDEC G.729 TIENE LICENCIA DE SIPRO LAB TELECOM INC. CONSULTE WWW.SIPRO.COM/CONTACT.HTML. EL CÓDEC H.264 (AVC) ESTÁ SUJETO A LA LICENCIA DE CARTERA DE PATENTES AVC PARA EL USO PERSONAL DE UN CONSUMIDOR Y OTROS USOS QUE NO IMPLIQUEN REMUNERACIÓN PARA (i) CODIFICAR VIDEO QUE CUMPLA CON EL ESTÁNDAR AVC (“AVC VIDEO”) O (ii) DECODIFICAR VIDEO AVC QUE UN CLIENTE CODIFICÓ DURANTE UNA ACTIVIDAD PERSONAL U OBTENIDO A TRAVÉS DE UN PROVEEDOR DE VIDEO CON LICENCIA PARA SUMINISTRAR VIDEO AVC. NO SE OTORGA LICENCIA NI DEBERÁ CONSIDERARSE IMPLÍCITA PARA NINGÚN OTRO USO. SE PODRÁ OBTENER INFORMACIÓN ADICIONAL SOBRE LOS CÓDECS H.264 (AVC) Y H.265 (HEVC) DE MPEG LA, L.L.C. VISITE HTTP://WWW.MPEGLA.COM.

Cumplimiento de leyes

Usted reconoce y manifiesta su acuerdo en cuanto a que es responsable de cumplir con las leyes y normativas aplicables, lo que incluye, a título enunciativo, las leyes y normativas

relacionadas con la grabación de llamadas, la privacidad de los datos, la propiedad intelectual, el secreto comercial, el fraude y los derechos de reproducción de música, en el país o en el territorio en el que se utilice el producto de Avaya.

Prevención del fraude telefónico

El fraude telefónico se refiere al uso no autorizado de su sistema de telecomunicaciones por parte de un participante sin autorización (por ejemplo, una persona que no es un empleado, agente ni subcontratista corporativo o no trabaja en nombre de su compañía). Tenga en cuenta que pueden existir riesgos de Fraude telefónico asociados con su sistema y que, en tal caso, esto puede generar cargos adicionales considerables para sus servicios de telecomunicaciones.

Intervención en fraude telefónico de Avaya

Si sospecha que es víctima de fraude telefónico y necesita asistencia o soporte técnico, llame a la línea directa de Intervención de Fraude Telefónico del Centro de servicio técnico al +1-800-643-2353 para Estados Unidos y Canadá. Para obtener números de teléfono de soporte técnico adicionales, visite el sitio web de soporte técnico de Avaya: https://support.avaya.com o el sitio web posterior a este designado por Avaya.

Vulnerabilidades de seguridad

En la sección Security Policies and Support (Políticas de seguridad y soporte técnico) de https://support.avaya.com/security podrá encontrar información acerca de las políticas de soporte técnico de seguridad de Avaya.

Las vulnerabilidades de seguridad de los productos de Avaya se gestionan según el Avaya Product Security Support Flow (Flujo de soporte técnico de seguridad de productos de Avaya) (https://support.avaya.com/css/P8/documents/100161515).

Descarga de documentación

Para obtener las versiones más actualizadas de la documentación, visite el sitio web del soporte técnico de Avaya: https://support.avaya.com o el sitio web posterior a este designado por Avaya.

Contacto con el soporte técnico de Avaya

Visite el sitio web de soporte técnico de Avaya: https://support.avaya.com para obtener avisos y artículos sobre productos o servicios alojados o para informar acerca de algún problema con su producto o servicio alojado Avaya. Para obtener una lista de los números de teléfono y las direcciones de contacto del soporte técnico, visite el sitio web de soporte técnico de Avaya: https://support.avaya.com (o el sitio posterior designado por Avaya); desplácese hasta la parte inferior de la página y seleccione Contact Avaya Support (Contacto con el soporte técnico de Avaya).

Marcas comerciales

Las marcas comerciales, los logotipos y las marcas de servicio (“Marcas”) que aparecen en este sitio, la Documentación, los Servicios alojados y los productos proporcionados por Avaya son Marcas registradas o no registradas de Avaya, sus afiliados, sus licenciantes, sus proveedores u otros terceros. Los usuarios no tienen permiso de usar dichas Marcas sin previo consentimiento por escrito de Avaya o dichos terceros que puedan ser propietarios de la Marca. Ningún contenido de este sitio, la documentación, los servicios alojados ni los productos deben considerarse como otorgamiento, por implicación, impedimento o de alguna otra forma, una licencia o derecho para usar las Marcas sin la autorización expresa por escrito de Avaya o del tercero correspondiente.

Avaya es una marca registrada de Avaya Inc.

Todas las demás marcas son propiedad de sus respectivos dueños. Linux® es una marca comercial registrada de Linus Torvalds en EE. UU. y en otros países.

Contenido

Capítulo 1: Introducción 8
Propósito 8
Change history 8
Capítulo 2: Avaya IP Office™ Platform overview 10
Ediciones IP Office 10
New in this release 11
Capítulo 3: Funciones 14
Funciones de administración de llamadas 14
Administración básica de llamadas 14
Advanced call handling 18
Funciones de administración de llamadas 25
Cobertura para operador 25
Marcar emergencia 25
Plan de marcación 25
Marcación directa interna 26
Duración máxima de llamada 26
Anuncio 26
Relé activado/desactivado/pulso 26
Privilegio de llamada saliente transferible 27
Funciones del centro de contactos 27
Códigos de cuenta 27
Adquirir llamada 28
Música de espera 28
Inicio de sesión del agente 28
Supervisar llamadas 29
Llamadas salientes 29
Llamadas entrantes 30
Funciones de telefonía IP 33
Extensiones de creación automática 33
Ruta directa de medios 33
Soporte técnico para medios iniciales y mensajes PRACK 33
Comienzo rápido 34
Transporte fax 34
Pantalla para nombre de directorio de llamada entrante 35
DTMF fuera de banda 35
Encabezados de privacidad y PAI 35
Supresión de silencio 35
SIP features 36
Compresión de voz 39
Telefonía de IP Office Branch 40
Funciones de mensajería 42
Comparación de las funciones de mensajería 43
Mensajería de IP Office Branch 46

Mobility features..... 47
Uso compartido de escritorio..... 47
Funciones de acceso remoto..... 47
Uso compartido de escritorio remoto..... 48
Remote Worker..... 49
Modo teletrabajador..... 50
Hermanamiento..... 50
Fallback Twinning..... 51
Acceso móvil simplificado..... 52
Teléfono VPN..... 52
Funciones de red..... 53
Selección de ruta alternativa..... 53
Conexión automática..... 53
Devolución de llamada..... 53
Firewall..... 54
Acceso a Internet..... 54
Esquemas de numeración de redes..... 55
Cuotas del servicio..... 55
Perfiles de horario..... 55
Red multisitio..... 56
Servicios de red..... 58
Funciones del teléfono..... 61
Tono de alerta/timbre para llamadas cubiertas..... 61
Botones, teclas y luces..... 61
Historial de llamadas..... 65
Identificador de llamada..... 66
Directorio personal centralizado..... 66
Idioma..... 67
Marcación con teléfono colgado..... 67
Autoadministración..... 67
Correo de voz visual..... 67
Capítulo 4: Aplicaciones..... 69
Aplicaciones de usuario..... 69
Avaya one-X® Mobile..... 69
Avaya one-X® Portal for IP Office..... 70
Avaya Equinox™ for IP Office..... 71
Avaya IP Office Web Client..... 72
Avaya Communicator..... 73
SoftConsole..... 76
Embedded Voicemail..... 78
Voicemail Pro..... 78
Conferencia..... 79
Aplicaciones de instalación y administración..... 83
IP Office Manager..... 83
Server Edition Manager..... 84
Web Manager..... 85
IP Office Media Manager..... 86

Aplicación para administración de soluciones..... 88
Modo administrador de SoftConsole..... 88
Consola de administración de SNMP..... 88
System Status Application (SSA)..... 89
SysMonitor..... 90
Cloud Operations Manager..... 90
Administrador de migración de datos (DMM)..... 91
Aplicaciones IP Office Branch..... 91
Administración centralizada..... 91
Licencias centralizadas..... 92
Sistemas de correo de voz..... 92
Avaya Aura® System Manager..... 92
Avaya Aura® Session Manager..... 94
Avaya Aura® Communication Manager..... 94
Aplicaciones de centro de contactos..... 95
Descripción general de IP Office Contact Center..... 95
Descripción general sobre Avaya Contact Center Select..... 96
Capítulo 5: Recursos..... 98
Documentación..... 98
Búsqueda de documentos en el sitio web de soporte técnico de Avaya..... 98
Capacitación..... 99
Visualización de videos de orientación de Avaya..... 100
Recursos adicionales de IP Office..... 100
Soporte técnico..... 101
Uso de la Base de conocimiento de Avaya InSite..... 101
Acceso a las notas de la aplicación Avaya DevConnect..... 102
Capítulo 6: Estándares..... 103
Estándares regulativos..... 103
Estándares de protocolo de red..... 105
Glosario..... 111

Capítulo 1: Introducción

Propósito

Este documento contiene descripciones detalladas de IP Office y brinda detalles sobre las características de la función, las capacidades y las interacciones.

Change history

Issue	Release date	Summary of changes
Release 11.0 FP4	February 2019	• Updated the What's new topic with the Release 11.0 FP4 features. • Updated Media Manager section to add new features supported in IP Office Release 11.0 FP4. • Added content on Fallback Twinning feature. • Updated the SIP features topic to add information on optional header P-Called-Party Id. • Updated the SIP features topic to add information on security enhancements for registration of SIP devices. • Added content on SIP and H.323 Registrars being disabled by default. • Updated Avaya Equinox™ topic to add content on Shared Control and Avaya Vantage™ support. • Updated Avaya one-X® Portal topic to add serviceability enhancements. • Added content on Conference Join feature.

La tabla continúa…

Issue	Release date	Summary of changes
Release 11.0	May 2018	• Updated the What's new topic with the Release 11.0 features. • Removed references to IP Office Integrated Contact Reporter. • Removed references to IP Office Video SoftPhone as it is not supported in Release 11.0. • Added content about the following applications: - Cloud Operations Manager - Avaya Equinox™ client for IP Office - Avaya IP Office Web Client • Updated the Web Manager section to add content about Configuration Dashboard. • Updated Media Manager section to add new features supported in IP Office Release 11.0. • Updated the IP Office branch telephony section to add J169 and J179 phones. • Update the SIP Features section to add SIP Line Appearances.
Release 10.1	June 2017	• Updated relevant sections with R10.1 features. • Updated the What's new topic with the R10.1 features included in this book. • Removed the What's new chapter created for R10.
Release 10.0	July 2016	• Se movió el contenido de Recursos a un capítulo separado al final de este documento. • Updated Avaya Contact Center Select overview content. • Updated "New in this release" content and minor updates to feature information.

Capítulo 2: Avaya IP Office™ Platform overview

The Avaya IP Office™ Platform is a cost-effective telephony system that supports a mobile, distributed workforce with voice and video on virtually any device. IP Office is an integrated, modular communications solution that scales up to 3000 extensions and 150 sites in a multisite network with resiliency. Match a deployment model to infrastructure needs from simple appliances to virtualized software in a data center with options in between. Improve customer experience and contact center agent efficiency with powerful, affordable multichannel functionality for voice, email and web chat. The solution combines collaboration software plus multichannel contact centers, networking, security and video.

IP Office provides a hybrid PBX with both Time Division Multiplexing (TDM) and IP telephony with trunk support, used in either mode or both concurrently. IP Office has data capabilities built-in, providing IP routing, switching and firewall protection, between LAN and WAN (LAN2).

In addition to basic telephony services and voicemail, IP Office offers both hard phone and soft phone options. Soft phone applications are designed to provide flexibility for remote workers and to allow workers to access telephony services, such as making and receiving calls, voicemail, and call forwarding from their computer or mobile device.

Ediciones IP Office

IP Office también ofrece funciones avanzadas como audio y videoconferencia y voz a través del protocolo de Internet (VoIP) para satisfacer las cambiantes necesidades de pequeñas, medianas y grandes empresas.

IP Office está disponible en muchos modelos de implementación según el tamaño de la empresa y las funciones requeridas, con uno de los siguientes elementos o todos:

- Software IP Office virtualizado que se ejecuta en una máquina virtual
- El servidor dedicado
- Unidad de control de IP Office 500 versión 2 (IP500 V2)

Edición	Plataforma	Tamaño de la empresa (usuarios)	Satisfacción de necesidades empresariales
Basic Edition	IP500 V2	Menos de 25	Solo capacidades simples de telefonía y mensajería

La tabla continúa…

Edición	Plataforma	Tamaño de la empresa (usuarios)	Satisfacción de necesidades empresariales
Essential Edition	IP500 V2	20–99	Funciones simples de telefonía y mensajería más telefonía IP con movilidad básica
Preferred Edition	IP500 V2	21–250	Funciones de Essential Edition más comunicaciones unificadas con movilidad especial
Server Edition	Linux Server, IP500 V2 y Linux Expansion	100 — 2000	Preferred Edition en una solución basada en software.
IP Office Select	Linux Server, IP500 V2 y Linux Expansion	100 — 3000	Preferred Edition en una solución basada en software aumento de su escala y resistencia.
Server Edition o IP Office Select con software virtualizado	Virtualizado	100 — 2000 (o bien) 100 — 3000	Funciones de Essential Edition más comunicaciones unificadas con movilidad especial
Server Edition o IP Office Select hospedado en la nube	Nube	100–2000 (o bien) 100-3000	Funciones de Essential Edition más comunicaciones unificadas con movilidad especial

También se hace referencia a IP Office Essential Edition y Preferred Edition como IP Office Standard Mode. Cada edición suma funcionalidad a las versiones anteriores.

New in this release

IP Office™ Platform Release 11.0 Feature Pack 4 offers the following new features and capabilities:

Nota:

Features are available worldwide unless otherwise specified. Not all features are supported on all platforms and phones. See the descriptions for details.

Fallback twinning

With this feature, IP Office redirects calls to the users twinned mobile number when the primary extensions are unreachable even if mobile twinning is disabled. The following two short codes are available for disabling and enabling mobile Fallback twinning:

- **Set Fallback Twinning Off**: To disable Fallback twinning
- **Set Fallback Twinning On**: To enable Fallback twinning

IP Office Media Manager enhancements

The following features have been added to IP Office Media Manager:

- Delete recordings

- Audit trail: Administrators can keep track of the usage of recording files in IP Office Media Manager. The following type of usage of a recording can be tracked using this feature:
  - Delete
  - Download
  - Replay
  - Search

Security enhancements for registration of SIP devices

The new security enhancements enable administrators to allow or disallow registration of SIP devices in IP Office based on their User Agent strings. Administrators can use the configuration settings to add, modify, or remove SIP User Agent strings to SIP UA Blacklist, SIP UA Whitelist, and IP Whitelist. Subsequently, the **Allowed SIP User Agents** setting can be used to select which SIP User Agents are allowed for registering with IP Office.

Automatic user synchronization with Avaya Spaces

IP Office R 11.0 FP4 system users and user details created for Avaya Equinox™ can be automatically synchronized with Avaya Spaces server. To use and receive additional Avaya Spaces features, the details of users configured for Avaya Equinox™ need matching users configured on the Avaya Spaces server. The synchronization can be done manually or automatically.

Default extension password

The default extension password or PIN is different than the user password and is much stronger with a minimum of nine digits. IP Office R11.0 FP4 deployments provide for an auto-generated default extension PIN of 10 digits, which can be viewed and modified later. An eye icon next to the **Default Extension Password** field in the user interface can be used to view the existing default extension password.

Avaya Equinox™ support on Avaya Vantage™

Avaya Equinox™ is supported on Avaya Vantage™ phones in IP Office R 11.0 FP4 deployments.

Route incoming SIP trunk calls based on an optional SIP header

This feature enables IP Office to route incoming SIP trunk calls based on optional SIP header **P-Called-Party**. IP Office reads the `P-Called-Party ID` header in the SIP message and routes the incoming SIP calls based on it.

SIP and H.323 Registrars disabled by default

To secure IP Office R 11.0 FP4 from vulnerabilities, the **H.323 Gatekeeper Enable** and **SIP Registrar Enable** fields are disabled by default. Whenever a new H,323 or SIP extension is added and the corresponding registrar is not enabled, IP Office system displays an error message and prompts to enable the fields. When resiliency support is enabled on an IP Office Line in systems having IP extensions and the systems do not have the corresponding registrars enabled, IP Office system displays an error message and prompts administrators to enable the corresponding registrars.

Avaya Equinox™ shared control

Avaya Equinox™ can now be used in shared control mode with desk phones. The shared control feature is available even when the Avaya Equinox™ client and desk phones are registered on different systems within the same network.

Conference Join

Conference Join feature allows two separate conferences to be joined into one single conference that contains all the previous participants of both the earlier conferences. Once the conferences have been joined it is not possible to revert to the two separate conferences again.

JEM 24 button module support on Avaya J169/J179 IP Phone

Avaya J169/J179 IP Phone can support up to three JEM24 button modules. Each JEM24 has 24 dual-LED buttons with adjacent button label display. The button LEDs are used to indicate the status of the button feature whilst pressing the button is used to access the feature. A single JEM24 supports 72 programmable button slots. These are arranged in 3-pages, with pages accessed using the module's page scroll button. When multiple modules are connected to a phone, each module only supports a single page of 24 programmable button slots.

The modules automatically match the display settings of the phone to which they are connected - color with Avaya J179 IP Phone or greyscale with Avaya J169 IP Phone, font size, background image, screen saver. The button modules are powered though the phone. For more information, see the *IP Office Platform R11.0 J100 Series Telephone User Guide*.

Avaya J139 IP Phone

IP Office support for Avaya J139 IP Phone. Avaya J139 IP Phone is an advanced SIP desk phone that supports IP Office interactive menus and button programming. For more information, see the *IP Office Platform R11.0 J100 Series Telephone User Guide*.

Serviceability enhancements in Avaya one-X® Portal

Avaya one-X® Portal supports a number of serviceability features such as displaying count of logged-in sessions, user avatar, option to block client versions, option to track repeated failed login attempts, and option to clear all sessions of a user.

Simplified Web Self-Administration

The enhanced interface is focused on simplifying the configuration and make it easier for non-technical users and provides a three step self-guided wizard for setting up the basic account. By default the new capability, that is running the wizard, is enabled for all users but the administrator can disable the capability or modify as required.

Capítulo 3: Funciones

Funciones de administración de llamadas

IP Office ofrece un conjunto integral de funciones de telefonía para permitir respuestas rápidas y eficientes a las llamadas. A través de algunas funciones, como Visualización de ID de llamada y Etiquetar llamadas, los usuarios pueden ver quién llama y a quién llaman antes de atender las llamadas. La información del cliente puede aparecer en el equipo del usuario.

Los auriculares inalámbricos y twinning brindan movilidad a los usuarios dentro de la oficina. Para los trabajadores que se encuentran fuera de la oficina, las funciones integrales y fáciles de usar para reenviar llamadas, Softphone y el servicio de acceso remoto les permiten estar en contacto y acceder a los recursos centralizados en todo momento.

Los usuarios pueden administrar las llamadas entrantes de manera eficaz mediante marcado directo (DDI/DID) u operadores dedicados. Para las llamadas que se realizan fuera del horario de oficina, IP Office ofrece servicios de correo de voz y de operadora automática opcional. Las funciones específicas TDM y las funciones específicas de teléfono TDM no son compatibles con Linux.

Administración básica de llamadas

Devolución automática de llamada

El usuario puede configurar la devolución de llamadas de dos formas:

- Cuando llame a una extensión que esté ocupada, solicita una llamada cuando se libere la extensión.
- Cuando llame a una extensión que sólo suene, solicita una llamada cuando la siguiente vez que se utilice la extensión.

En función del tipo de teléfono del usuario, se puede solicitar una devolución de llamada cuando se esté libre mediante el marcado de un código abreviado si se escucha un tono de ocupación interna, seleccionando una opción del menú interactivo o presionando una tecla DSS/BLF programada. También es posible configurar la devolución de llamada cuando se esté libre o la siguiente vez que se utilice con un código abreviado sin realizar la llamada.

Esta función está disponible en redes comunitarias pequeñas y redes multisitio.

Registrar timbrado con Avaya one-X® Portal

A partir de la versión 10.1, el cliente web de Avaya one-X® Portal ofrece el control “Registrar timbrado” en el gadget de Llamadas en los casos en los que un usuario está ocupado con otra llamada y la llamada no se envía al correo de voz. Al presionar este control, se registra un timbrado en IP Office para el usuario que recibió la llamada. Cuando el usuario que recibió la llamada está disponible, se realiza un timbrado de la manera habitual. El gadget Directorio

también ofrece un control similar para permitir la realización de un timbrado a cualquier usuario cuyo estado de presencia sea “Ocupado con llamada”. También es posible cancelar un timbrado usando el mismo control. El gadget Directorio está limitado a los usuarios del sistema solamente y no se aplica a los contactos personales ni a los contactos de los grupos de búsqueda.

Timbre característico

El sistema utiliza diferentes secuencias de timbre para indicar tipos de llamada. Por ejemplo, las llamadas internas y externas pueden tener diferentes timbres; esta función se llama timbre característico.

En los teléfonos analógicos, es posible ajustar las secuencias del timbre característico. En los teléfonos digitales e IP, las secuencias del timbre característico son fijas, a saber:

- Llamada interna: Un único timbre repetido.
- Llamada externa: Un timbre doble repetido.
- Llamada de timbrado: Un único timbre seguido de dos timbres cortos.

Las secuencias de timbrado funcionan con los siguientes tipos de llamada:

- Llamadas que se quitan del estacionamiento
- Llamadas que salen de la espera
- Llamadas que se transfieren
- Devolución de llamadas cuando esté libre
- Llamadas de timbre de correo de voz

Esta función está disponible en redes comunitarias pequeñas y redes multisitio.

Filtrado de llamadas

El usuario puede filtrar llamadas importantes y decidir si contestar o dejar que pase al correo de voz.

El usuario puede filtrar llamadas entrantes mientras el teléfono esté en un estado inactivo y puede escuchar las llamadas entrantes transferidas al correo de voz. Cuando llega una llamada entrante a su teléfono y se desvía al sistema de correo de voz y este la responde, es posible escuchar automáticamente a la persona que llama en el altavoz del teléfono, pero dicha persona no podrá escucharlo. El usuario puede decidir si desea responder o desconectar la llamada y permitir que el sistema de correo de voz siga administrando la llamada. El usuario no puede filtrar una llamada mientras está atendiendo otra llamada.

Reenvío

El usuario puede reenviar llamadas a otra extensión o a un número externo, incluso a dispositivos móviles.

El usuario puede reenviar llamadas de diferentes maneras, y si la llamada no se responde en el destino de reenvío llega al correo de voz si está habilitado para el usuario y la supervisión de llamada está disponible. Una vez que se ingresan los números, el usuario puede alternar el reenvío para que esté o no activo cuando se requiera sin tener que volver a ingresar los números.

Si el usuario es miembro de un grupo de búsqueda, algunos tipos de llamadas de grupo de búsqueda también se pueden reenviar de forma incondicional. El usuario puede seleccionar si

el reenvío se aplica solo a las llamadas externas o a todas las llamadas. El reenvío de llamadas se procesa después de probar las condiciones de no molestar y sígueme.

Cobertura para operador

Los administradores pueden configurar un operador o un grupo de operadores para ofrecer cobertura para las llamadas externas que, de lo contrario, irían al correo de voz.

Las llamadas no respondidas se pueden enrutar a un operador o a un grupo de operadores. Por ejemplo, las oficinas de los gobiernos locales prefieren ofrecer un servicio personal en lugar de correo de voz.

Sígueme

Sígueme permite que todas las funciones que un usuario configuró en el teléfono lo sigan a otro teléfono. La función de reenvío de llamadas no reenvía configuraciones, sólo llamadas.

Cuando el usuario no se encuentra en su puesto de trabajo, puede enviar la configuración de llamada del teléfono principal en el caso de llamadas que siguen al usuario, incluso reenviar si da ocupado y sin respuesta.

Sígueme se puede configurar desde el teléfono principal del usuario (Sígueme a) o desde el teléfono en el que desea recibir las llamadas (Sígueme aquí). Varias personas pueden reenviar las llamadas de sus teléfonos a un destino y, si el teléfono tiene pantalla, indicará para quién es la llamada.

Reenviar grupo de búsqueda

El usuario puede reenviar un grupo de búsqueda y reenviar llamadas a un grupo. Por ejemplo, en un entorno de ventas o soporte técnico donde es posible que ciertas personas estén fuera de la oficina pero disponibles en sus teléfonos móviles, esta función les permite participar de un grupo de búsqueda como si estuviesen en la oficina.

Las llamadas para un grupo de búsqueda al que pertenezca el usuario también pueden seguir reenviar incondicionalmente. El grupo de búsqueda se debe configurar para un tipo de timbre secuencial o rotatorio y, si la llamada no se responde en el destino del reenvío, seguirá la administración de llamadas del grupo de búsqueda en lugar de ir al correo de voz.

Reenviar si da ocupado

Si está habilitado, este reenvío se activará cuando el usuario esté ocupado y reciba otra llamada desviada, pero no incluye las llamadas para un grupo de búsqueda al que pertenezca.

Se considera que un usuario está ocupado cuando está en una llamada pero, en función de la configuración de las llamadas en espera y de las funciones de las teclas y las luces, este podría no ser el caso.

Reenviar si no responde

Si suena una llamada para un usuario pero este no responde dentro del período configurado, el sistema reenvía la llamada que se ha indicado como en espera, siempre que se haya activado la función.

Reenvío incondicional

El sistema reenvía todas las llamadas del usuario a un número, pero si la llamada no tiene respuesta dentro del período configurado, el sistema la envía al correo de voz, siempre que esta función esté activada.

Reenvío incondicional al correo de voz

El usuario puede desviar todas las llamadas al correo de voz incluso cuando el correo de voz del usuario no está activado.

En espera

El usuario puede colocar llamadas en espera y activar la música de llamada en especial, si así lo desea. Una llamada en espera regresa a la extensión luego de un período de espera, configurado por el administrador del sistema, para que las llamadas en espera no sean olvidadas.

Alternar llamadas

El sistema hace circular todas las llamadas que el usuario tiene retenidas en su extensión local dentro del sistema y las presenta una a la vez.

Mantener llamada en espera

Combina espera y respuesta para mantener en espera una llamada existente y responder una llamada en espera con presionar un botón.

Estacionar

Como alternativa para poner una llamada en espera, una llamada se puede estacionar en el sistema y ser atendida por otro usuario.

La función de estacionamiento está disponible en el teléfono del usuario, Avaya one-X® Portal for IP Office, Phone Manager y SoftConsole.

El sistema estaciona una llamada mediante un número de posición de estacionamiento que se puede anunciar mediante el sistema de anuncios. El usuario designado se puede dirigir a cualquier teléfono y tomar la llamada con la marcación del número de posición de estacionamiento.

Phone Manager posee 4 botones de estacionamiento predeterminados. En los teléfonos digitales con las teclas DSS/BLF, es posible programar la teclas de estacionamiento que indicarán cuando hay una llamada en una posición particular y permitirán que las llamadas se estacionen o recuperen.

Los administradores pueden determinar el período en el que la llamada se mantendrá estacionada antes de que se la presente a la extensión que originalmente estacionó la llamada.

Timbre personalizado

El usuario puede modificar el sonido o el tono del timbre de un teléfono.

En muchos teléfonos digitales, el usuario puede personalizar el sonido del timbre. Cambiar el sonido del timbre no altera la secuencia del timbre usada para el timbre característico. Esta función es local para el teléfono y no es compatible con todos los tipos de teléfonos.

Tonos

El sistema genera los tonos de usuario correctos según la región geográfica. Estos tonos se generan para todos los tipos de extensiones: analógicas, digitales e IP.

Los tonos admitidos son:

- Normal, alternativo y secundario
- Ocupado
- No obtenible
- Congestión
- Conferencia

Transferencia

El usuario puede transferir una llamada en curso a una extensión interna o a un número público externo. El sistema coloca la llamada en espeta mientras realiza la transferencia.

Si el usuario que transfiere la llamada cuelga el teléfono antes de que el usuario de destino responda, el sistema transfiere la llamada en forma automática; se denomina transferencia ciega o sin supervisión. De forma alternativa, un usuario también puede esperar a que el destino responda y anunciar la transferencia antes de colgar y completar el proceso; se denomina una transferencia con supervisión.

A menos que exista una restricción por parte del administrador, el sistema no hace diferencia entre transferencias de llamadas internas y externas.

Timbre al transferir

Las llamadas de solicitud de transferencia se presentan al destinatario con un timbre interno. Si el usuario que hace la transferencia de llamada finaliza la llamada durante el timbrado, el timbre cambia según la llamada que se está transfiriendo. Los clientes pueden elegir no usar esta opción configurable y continuar trabajando de la misma manera que con la versión 10 y anteriores.

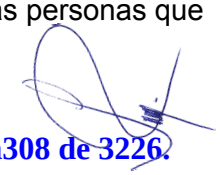
Advanced call handling

Texto de ausencia

El usuario puede configurar un texto de ausencia en su teléfono para informarles a otros usuarios internos de su estado actual y de la disponibilidad probable.

El texto de ausencia también se encuentra disponible para usuarios de teléfonos analógicos estándar; sin embargo, sólo se puede mostrar en algunos teléfonos con pantalla, Phone Manager y SoftConsole. La mayoría de los teléfonos con funciones admitidas brindan la opción de agregar un texto.

Cuando un usuario ha definido un mensaje de texto de ausencia, el procesamiento de llamadas no está afectado al usuario y aún tiene la opción de configurar funciones como no molestar o reenviar. Los teléfonos compatibles con la configuración interactiva de texto de ausencia también lo mostrarán en el teléfono del usuario para comodidad de las personas que



se acerquen a sus escritorios. Existen 10 cadenas predeterminadas y 1 cadena personalizada para configurar el texto de ausencia:

1. De vacaciones hasta
2. Vuelvo enseguida
3. En hora de almuerzo hasta
4. En reunión hasta
5. Por favor, llamar
6. No molestar hasta
7. Con visitas hasta
8. Con clientes hasta
9. Volveré pronto
10. Volveré mañana
11. Personalizada

Todos los textos poseen la opción de agregar un horario, por ejemplo, el mensaje 4 más `10:00` muestra **En reunión hasta las 10:00**. Las cadenas de texto se localizan al idioma del sistema.

Esta función está disponible en redes comunitarias pequeñas y redes multisitio.

Grabación de llamada

El usuario puede grabar un mensaje y guardar la grabación en un buzón de correo de voz, un buzón de correo de grupo o la biblioteca de grabación de voz.

Cuando una persona que llama va a indicar información detallada, como una dirección o un número de teléfono, y escucha un mensaje o un tono de advertencia que indica que la llamada se va a grabar en algunos países. Cuando la garantía de calidad requiere la grabación de llamadas, es posible configurar el sistema IP Office para grabar automáticamente un porcentaje de las llamadas para su posterior revisión.

Es posible grabar cualquier llamada en cualquier tipo de teléfono. Si es necesario reproducir un aviso de grabación, el sistema ignora la licencia del puerto del correo de voz si se tiene un número insuficiente de licencias de canales de correo de voz.

Nota:

En los teléfonos IP, se requiere un canal VCM para la duración de la grabación.

Etiquetado de llamadas

El etiquetado de llamadas muestra un mensaje de texto que proporciona información adicional sobre la llamada en el teléfono del usuario o Phone Manager cuando la llamada se presenta.

El usuario etiqueta llamadas cuando las transfiere desde Phone Manager o SoftConsole para brindar la información de que no pueden anunciar la llamada.

El usuario puede etiquetar una llamada en forma automática mediante CTI y Voicemail Pro según la ruta de la llamada entrante.

Nota:

En algunos teléfonos, mostrar la etiqueta puede significar que no se puede mostrar la información habitual de origen y destino de la llamada.

Llamada en espera

El usuario puede no querer que las llamadas reciban el tono de ocupado si están atendiendo otra llamada. En lugar del tono de ocupado, la llamada recibe un tono de timbre normal. EL usuario oye una alerta de que hay una llamada en espera.

El usuario puede decidir entre finalizar la llamada actual o ponerla en espera y responder la que está en espera. La cantidad de información que está disponible sobre la llamada en espera depende del tipo de teléfono que tenga el usuario o de si utiliza Avaya one-X® Portal for IP Office o Phone Manager.

Debido a que el tono de llamada en espera puede ser perturbante, por ejemplo durante una llamada en conferencia. El usuario puede activar o desactivar la función e incluso suspenderla durante una única llamada.

Intrusión de supervisión

Los usuarios designados se pueden unir a la conversación existente de una llamada interna o externa. Esta función también le permite al usuario interrumpir una llamada sin que escuche la persona que llama.

Los administradores y supervisores designan usuarios mediante la configuración Intrusión posible. Los usuarios pueden unirse a llamadas de cualquier extensión del sistema; sin embargo, los administradores también pueden designar usuarios mediante la función Intrusión no es posible, que evita intrusiones de otros en sus llamadas.

En los sistemas Essential y Preferred Edition, la Intrusión silenciosa o el Anuncio discreto pueden resultar efectivos en una situación en la que un usuario hace una intrusión en una llamada para anunciar en forma discreta que un cliente muy importante está en espera. El jefe escucha a su secretaria mientras habla con la persona que realiza la llamada, pero este no podrá escuchar a la secretaria.

Se utiliza en el escenario de un centro de atención telefónica y con otras aplicaciones entre empleados. Admite la interrupción o inclusión de un supervisor en una llamada en vivo para hablar con un agente sin que la persona que llama de forma externa escuche la conversación. Esto es útil cuando el agente necesita compatibilidad de supervisión/capacitación o cuando el supervisor necesita inmiscuirse para dar instrucciones a un agente. La persona que llama puede seguir hablando con el agente, pero dicha persona no escuchará lo que dice el supervisor. El agente podrá escuchar a la persona que llama y al supervisor.

La función permite que los usuarios en una llamada se “inmiscuyan” y escuchen, según la configuración de los usuarios finales si se usa la Intrusión de supervisión o el Anuncio discreto. No es posible realizar la Intrusión de supervisión y el Anuncio discreto en un usuario inactivo. Sí se puede realizar para llamadas internas o externas. Esta función se activa mediante IP Office Managerpara cada usuario. Sólo los usuarios autorizados pueden usar la función de supervisión/discreción. La configuración predeterminada es Desactivado.

Conferencia

Los usuarios pueden colocar las llamadas en espera y crear una conferencia con el teléfono o aplicaciones del escritorio. Se pueden agregar miembros adicionales a la conferencia; no obstante, una sola conferencia no puede tener más de 64 miembros (con IP500 V2 solamente y más con Server Edition).

En el caso de conferencias ad hoc, el sistema requiere la misma cantidad de canales VoIP/ líneas troncales y participantes externos (así como sucede con Preferred Edition para conferencias Meet-Me). El sistema admite 128 canales de conferencia en e IP500 V2, lo que permite realizar varias conferencias de cualquier tamaño de entre 3 y 64 participantes. Así, el sistema admite 42 conferencias de 3 participantes, 2 conferencias de 64 participantes o cualquier combinación entre estas. La capacidad Meet-Me requiere Preferred Edition para marcación directa hacia un puente de conferencia con un código PIN de seguridad. En una SCN, sólo se requiere una licencia Preferred Edition centralizada para alojar conferencias Meet-Me en cualquiera de los sitios. Los identificadores de conferencia también se comparten a través de los sitios SCN.

Las siguientes capacidades de canal de conferencia están disponibles:

Tabla 1: Capacidades de canal de conferencia

Plataforma	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
HP DL120 Dell R210	128	128	414	414
HP DL360	256	256	825	825
Dell R620	256	512	825	825
OVA	256	512	825	825
IP500V2	128	128	128	128

Para iniciar una conferencia, los usuarios marcan el número directo asignado al puente de conferencia e ingresan el PIN (requiere Preferred Edition y Voicemail Pro), en caso que sea necesario. Para las conferencias ad hoc con pocos participantes, los usuarios pueden configurar fácilmente conferencias inmediatas: se llama a todos los participantes y se los coloca en el puente de conferencia. Con Avaya one-X® Portal for IP Office, aquel que origina la conferencia posee el control: se muestra el número de identificador de cada participante (y el nombre asociado en caso de que se conozca). Si es necesario, es posible desconectar a participantes específicos. El sistema reproduce un único bip al ingresar y un bip doble al salir. El propietario de la conferencia puede utilizar su número de extensión como el identificador de conferencia. El propietario de la conferencia posee el control y tiene la posibilidad de silenciar y desconectar llamadas de otros participantes. Todos los participantes escucharán el sistema de música de espera (MOH) hasta que el propietario se una y escucharán MOH cuando el propietario se desconecte. Tenga en cuenta que el participante interno tiene la opción de ver y desconectar a los participantes (no solo el propietario de la conferencia).

Los usuarios pueden grabar un saludo personalizado para reproducir en una conferencia (requiere Preferred Edition y Voicemail Pro).

Los usuarios pueden grabar la conferencia mediante Avaya one-X® Portal for IP Office, teléfono digital o IP con pantalla o un código abreviado (requiere Preferred Edition y Voicemail Pro). Para impedir el acceso no autorizado al puente de conferencia, es posible configurar

códigos PIN, filtrado de números de identificador de llamadas entrantes y perfiles de hora y fecha con Voicemail Pro. Una sola persona puede administrar el puente de conferencia desde cualquier ubicación.

La realización de conferencias tiene las siguientes restricciones:

- Sólo se permiten dos llamadas en conexión a través de líneas troncales analógicas en una sola conferencia.
- Cada llamada externa requiere un canal de VoIP/línea troncal digital (por ejemplo, 1 T1 permite 23/24 participantes externos, 1 E1 permite 30 participantes y un VCM-64 con licencia completa permite 64 participantes).
- No existen límites en cuanto a la combinación de llamadas en conferencia internas y externas, pero si todos los participantes internos se desconectan del puente de conferencia, el sistema puede desconectar automáticamente a los participantes externos para ofrecer una seguridad adicional (parámetros configurables del sistema).
- Las funciones del sistema, como la intrusión de llamada, el registro de llamada y la supervisión silenciosa utilizan recursos de conferencia, al igual que la grabación automática si está habilitada. Cuando cualquiera de estas funciones está activa, se reduce el número de posiciones disponibles para los participantes de la conferencia. Por ejemplo, una llamada en conferencia entre 3 participantes y que se está grabando usará 4 posiciones de conferencia.

Conference Join

Conference Join feature allows two separate conferences to be joined into one single conference that contains all the previous participants of both the earlier conferences. Once the conferences have been joined it is not possible to revert to the two separate conferences again.

Marcar al capturar

Cuando se toma el auricular del teléfono, el usuario pueden marcar de manera automática una extensión específica.

Utilice esta función en áreas de recepción sin personal o para sistemas de entrada de puertas para que los visitantes obtengan asistencia de forma sencilla. Este tono también se conoce como “línea directa”.

Timbre demorado al capturar

Si un teléfono está descolgado o se activa el altavoz del teléfono pero no se marca durante un período configurado en segundos, se marca automáticamente una extensión definida.

Use esta función en áreas de recepción sin personal o en sistemas de puerta de ingreso para permitir que los visitantes obtengan asistencia fácilmente; los visitantes que conocen el número deseado tienen la opción de marcarlo, mientras que los demás visitantes se pueden derivar para recibir asistencia después de un breve tiempo de espera. Esta función también se puede usar como alerta de emergencia en entornos médicos; por ejemplo, cuando se levanta el auricular pero no se marca ningún dígito.

No molestar

El usuario puede suspender temporariamente las llamadas que suenan en sus teléfonos.

Esta función evita que el usuario reciba llamadas de grupos de búsqueda y enviará a la persona que llama un correo de voz (si está activado) o una señal de ocupado. El usuario puede activar y desactivar la función no molestar (DND) de sus teléfonos, Avaya one-X® Portal for IP Office o Phone Manager.

Puede derivar algunas llamadas de la configuración DND para que suenen en el teléfono. Por ejemplo, es posible que un director tenga el número de extensión de su secretario en la lista de excepciones de DND. EL usuario puede administrar la lista de excepciones con Avaya one-X® Portal for IP Office y Phone Manager. Tanto los números internos como los externos pueden estar en la lista de excepciones.

Emergency 911 call

When an emergency call is dialed, the system overrides any call barring that would otherwise apply to the user making the call.

Activar/Desactivar grupo de búsqueda

Un usuario puede ingresar o dejar un grupo de búsqueda en forma temporaria, por ejemplo, para ayudar durante el horario pico de llamadas.

Los supervisores o administradores generalmente no aceptan llamadas pero en los momentos de tráfico elevado se pueden unir al grupo para aceptar llamadas y cuando el pico se haya reducido abandonar el grupo para continuar con sus tareas habituales. Los administradores asigna a un usuario un grupo de búsqueda. Un usuario no puede ingresar en un grupo de búsqueda en forma arbitraria, salvo que haya sido identificado como miembro de tal grupo.

Inclusión

Los usuarios seleccionados pueden realizar intrusiones en llamadas en curso.

Cuando el usuario que realiza la intrusión se une a una llamada, todos los participantes de esa llamada oyen un tono. La ruta de voz se activa entre la persona que se une a la llamada y el usuario que ha recibido la llamada; la otra persona se mantiene en espera y no escuchará la conversación. Al finalizar la intrusión, se vuelve a conectar la ruta de voz de la persona que recibió la llamada con la persona conectada originalmente. Los administradores activan o desactivan la inclusión según el usuario mediante Manager.

Estación descolgada

La estación de teléfono descolgado está diseñada para los usuarios que desean que su teléfono analógico funcione como un teléfono digital o IP, para aislar el estado de inactividad del teléfono del usuario del estado de teléfono colgado. Esta es una función útil cuando se utiliza Avaya one-X® Mobile, Phone Manager o SoftConsole para supervisar el estado del teléfono al usar un auricular en un teléfono analógico y con la supervisión de llamada y el marcado desde Avaya one-X® Mobile o SoftConsole.

Captura

El usuario puede responder una llamada presentada a otra extensión.

La capturar de llamadas incluyen:

- Capturar cualquier llamada timbrando en otra extensión.

- Capturar una llamada del grupo de búsqueda timbrando en otra extensión, donde el usuario debe ser un miembro de ese grupo de búsqueda.
- Capturar una llamada timbrando en una extensión especificada.
- Capturar cualquier llamada timbrando en otra extensión que sea un miembro del grupo de búsqueda especificado.

Esta función está disponible en redes comunitarias pequeñas y redes multisitio.

Privacidad del usuario

Es necesario asegurar a ciertos usuarios la confidencialidad de la comunicación. Se debe proteger a estos usuarios de manera que los demás usuarios no puedan ver quién los está llamando y de que puedan impedir que otros contesten sus llamadas. Si se lo habilita, el campo Grupo de invalidación de la privacidad en los registros del usuario, impide que otros usuarios vean detalles de las llamadas o que las contesten.

Privacidad del botón Usuario

Cuando se presiona un botón Usuario para saber quién está conectado con el usuario o responder una llamada de alerta, el sistema comprueba la configuración del ajuste Grupo de invalidación de la privacidad del usuario. Si el grupo no está configurado o si el usuario se encuentra en la lista (el estado Habilitado/Deshabilitado no está seleccionado), se mostrará el estado DSS.

Protección contra contestación

Cuando un usuario intenta contestar la llamada de otro usuario, se comprueba la configuración del Grupo de invalidación de la privacidad del usuario de destino. Si el grupo no está configurado o si el usuario se encuentra en la lista, se permite contestarla. No se comprueba el estado Habilitado/Deshabilitado en el grupo.

Recuperación de llamada

La función recuperar, o reclamar, se aplica a la última llamada de su teléfono que esté timbrando o conectado en cualquier otro lugar.

Si el usuario perdió una llamada que va al correo de voz o a la cobertura de llamada, puede recuperar la llamada mientras se presenta o conecta mediante el sistema. Esta es una versión de la función adquirir llamada que sólo se aplica a la última llamada de una extensión.

Relé activado/desactivado/pulso

El sistema cuenta con dos salidas de conmutadores independientes para controlar el equipo externo como sistema de entrada de puertas.

Controla los conmutadores mediante auriculares designados para abrir, cerrar o pulsar los conmutadores según fuera necesario. Los usuarios también pueden controlar los conmutadores con Receptionist, SoftConsole y Voicemail Pro.

Restringir interconexión de redes

La función Restringir interconexión de red impide la conexión de llamadas entre grupos de interfaz de líneas troncales privadas y públicas.

Prevención de desvío de tráfico de llamadas de India

La regulación de telecomunicaciones de la India establece que la llamada VoIP no debe combinarse con una llamada PSTN si la ubicación de origen de llamada y la ubicación de destino de llamada se encuentran en áreas cuyos códigos son diferentes.

La función de Prevención de desvío de tráfico de llamadas de India garantiza que el sistema cumpla con la regulación y permite que las llamadas a teléfonos IP y desde ellos se conecten a líneas troncales públicas PSTN locales sólo si la ubicación del teléfono IP es igual a la ubicación del sistema. La función está habilitada de manera predeterminada para la configuración regional de India y deshabilitada de manera predeterminada para las demás configuraciones regionales. Esta función está disponible para las implementaciones de Branch y SCN en IP500 V2 en las ediciones Essential, Preferred y Select. No es necesario adquirir otras licencias.

Control de calidad de voz

Funciones de administración de llamadas

Cobertura para operador

Los administradores pueden configurar un operador o un grupo de operadores para ofrecer cobertura para las llamadas externas que, de lo contrario, irían al correo de voz.

Las llamadas no respondidas se pueden enrutar a un operador o a un grupo de operadores. Por ejemplo, las oficinas de los gobiernos locales prefieren ofrecer un servicio personal en lugar de correo de voz.

Marcar emergencia

Marcar emergencia es un código abreviado y permite marcar números específicos independientemente de la restricción de llamadas o de que el teléfono esté desconectado.

Plan de marcación

IP Office tiene un programa de numeración muy flexible para comandos de extensiones, grupos de búsqueda y funciones. Si bien el sistema tiene una numeración predeterminada para los códigos de función y las extensiones, se pueden redefinir. Las extensiones y los grupos de búsqueda predeterminados tienen números de 3 dígitos que comienzan en el 200, pero se pueden cambiar a entre 2 y 9 dígitos con IP Office Manager. Existe un conjunto predeterminado de códigos abreviados de acceso a las funciones, pero se puede cambiar según las necesidades del usuario, dentro de ciertos límites. Esto es útil, por ejemplo, si IP Office sustituye a un sistema donde se accede a DND al marcar *21, se puede cambiar el código abreviado para que imite al código del sistema sustituido.

En ciertos países, IP Office puede admitir un tono de marcación secundario cuando se marca un dígito de acceso, si bien esto limita cierta funcionalidad, como la Selección de ruta alternativa (ARS). IP Office también se puede configurar para funcionar sin dígitos de acceso de línea, al analizar los dígitos a medida que se marcan y al determinar si son para un número interno o si se deberían enviar en una línea (esto es útil en instalaciones SOHO donde los usuarios no se utilizarán necesariamente para marcar un dígito de acceso para una línea exterior).

Marcación directa interna

Marcación directa interna (DID/DDI) se basa en el intercambio de teléfono local para transmitir todo o parte del número marcado a IP Office.

El software para enrutamiento de llamadas dirige la llamada a un teléfono individual o a un grupo de teléfonos. Utilice esta función para reducir la carga de trabajo de un recepcionista mediante la concesión de números individuales de llamadas directas a los miembros del personal o de los departamentos. Por razones prácticas, es común que el número de la extensión o del grupo sea el mismo que los dígitos suministrados desde la red, pero IP Office puede convertir el número en otro si la empresa lo requiere, dentro de unos límites.

En Norteamérica, se requieren circuitos T1 para DID.

Duración máxima de llamada

Esta función permite que el sistema controle la duración máxima de cualquier llamada basada en el número marcado. Esto se puede usar para controlar las llamadas a redes celulares o las llamadas de datos hechas mediante la red pública hacia ISP.

Anuncio

Los supervisores y administradores pueden difundir mensajes de audio a teléfonos IP y digitales con altavoces sin tener que instalar un sistema de localización independiente. La localización puede ser a teléfonos individuales o grupos de teléfonos.

Los ingenieros de implementación pueden configurar los puertos de extensión analógica para la conexión a sistemas de localización de sobrecarga externa, generalmente mediante un adaptador, ese puerto se puede incluir en un grupo de localización para permitir el teléfono combinado y la localización de sobrecarga.

Algunos teléfonos IP y digitales pueden responder a un anuncio al presionar una tecla mientras el anuncio está activado; esto finaliza el anuncio y lo convierte en una llamada local.

Relé activado/desactivado/pulso

El sistema cuenta con dos salidas de conmutadores independientes para controlar el equipo externo como sistema de entrada de puertas.

Controla los conmutadores mediante auriculares designados para abrir, cerrar o pulsar los conmutadores según fuera necesario. Los usuarios también pueden controlar los conmutadores con Receptionist, SoftConsole y Voicemail Pro.

Privilegio de llamada saliente transferible

Los administradores y supervisores pueden conceder acceso a la línea externa a teléfonos restringidos; por ejemplo, los teléfonos en áreas públicas o en salas de conferencias, para controlas las llamadas externas.

Un usuario con privilegios, como un supervisor, puede transferir una línea externa (tono de marcado secundario) a un usuario que no tiene privilegios de llamada saliente.

Funciones del centro de contactos

Códigos de cuenta

A través de los registros de llamadas, los supervisores y administradores puede agrupar las llamadas por códigos de cuenta a fin de conocer el costo de la llamada y realizar un seguimiento. Los supervisores y administradores también pueden restringir las llamadas salientes si solicitan a los usuarios que ingresen códigos de cuenta válidos.

El sistema almacena una lista de números de código de cuenta válidos. Al realizar una llamada o durante la misma, el usuario puede ingresar el código de cuenta que desea asociar a esa llamada. El sistema comprueba el código de cuenta en su lista de códigos válidos y pide al usuario que vuelva a ingresar el código si no es válido. Para las llamadas entrantes, el ID de la persona que llama se puede usar para hacerlo coincidir con un código de cuenta de la lista de códigos válidos y comunicar al código de cuenta la llamada para fines de facturación.

Los supervisores y administradores pueden designar usuarios para que utilicen un código de cuenta forzado y deberán ingresar un código de cuenta válido antes de hacer llamadas externas. Al usar códigos abreviados se pueden identificar ciertos números o tipos de llamadas que requieren un código de cuenta válido antes de realizar la llamada, por ejemplo, números internacionales o de larga distancia. Los usuarios de teléfonos analógicos solo pueden ingresar códigos de cuenta antes de realizar una llamada o para responder a una petición del sistema audible de ingreso del código para realizar una llamada.

Los códigos de cuenta también se pueden ingresar con Avaya one-X™ Portal for IP Office y Phone Manager. Una configuración del sistema determina si Phone Manager mostrará una lista de códigos de cuenta en la que el usuario puede seleccionar el código que necesita u ocultará la lista de códigos de cuenta.

En todos los casos anteriores, el código de cuenta ingresado se incluye en los detalles de las llamadas en el informe de registro de llamadas de IP Office (SMDR).

Adquirir llamada

La función Adquirir llamada permite a los usuarios tomar una llamada conectada a otra extensión. Esta función también se llama Robar llamada.

Los administradores pueden configurar la opción Adquirir llamada como un código abreviado o asignarle un botón en un teléfono IP o digital con botones programables. Esta función está sujeta a la configuración de control de intrusión: el usuario que adquiere la llamada se debe configurar para que pueda inmiscuirse y el usuario cuya llamada se adquiere se debe configurar para que pueda ser inmiscuido.

Adquirir llamada funciona de dos formas:

Sin un número	Permite al usuario recuperar una llamada que estaba sonando en su teléfono pero que ahora está sonando en otro teléfono, por ejemplo, en un destino de Correo de voz o Reenviar sin respuesta. No se verifica la configuración de intrusión. El usuario puede reclamar la llamada aunque se la haya respondido. Si la última llamada a este usuario ya no está sonando o está conectada al sistema, se producirá un error en la función.
Con un número	Donde el número es el número de teléfono de un usuario que tiene actualmente la llamada a adquirir. Si el usuario tiene una llamada entrante o en espera, Adquirir llamada actuará como el código abreviado Extensión de captura de llamada y el usuario que está ejecutando Adquirir llamada se conectará a la llamada entrante/en espera más antigua. Si el usuario tiene una llamada conectada sin ninguna llamada en espera y la configuración de Intrusión de los dos usuarios lo permite, la llamada se conectará al usuario que está ejecutando Adquirir llamada y se desconectará del otro usuario. Si el usuario no tiene llamadas, se producirá un error en la función.

Música de espera

Los administradores pueden acceder a hasta 32 fuentes de música de espera. En los sistemas Linux, se admiten hasta cuatro fuentes USB.

Una fuente de música puede ser un archivo WAV (predeterminado) individual almacenado localmente o un directorio de archivos WAV local. Puede configurar la reproducción para que comience cada vez desde el principio del archivo o directorio, o para que comience desde donde se detuvo la última vez.

Las fuentes de música alternativas pueden encontrarse en los sistemas Server Edition principales, secundarios y de expansión. Server Edition también admite música de espera centralizada, donde el servidor principal transmite música al servidor secundario y a todos los servidores de expansión.

Inicio de sesión del agente

Los agentes del Centro de contactos deben iniciar sesión antes de realizar o recibir llamadas.

Los administradores y supervisores puedes especificar un período de inactividad en inicio de sesión para indicar por cuánto tiempo una extensión puede estar inactiva antes de que se cierre automáticamente la sesión del usuario, asegurando que una extensión no quede con la sesión iniciada y que las llamadas no queden sin responderse.

Supervisar llamadas

Los usuarios pueden supervisar las llamadas de otros usuarios mediante la escucha.

Esta función no está disponible de forma predeterminada; los ingenieros de implementación debe activarla durante la configuración del sistema. Incluye una opción para que un tono indique cuando está en uso la supervisión. El usuario solamente puede escuchar, no puede hablar en la conversión.

Llamadas salientes

Según el tipo de empresa, las llamadas deben tratarse de una forma específica, como grabarse en un proyecto o cliente mediante el uso de códigos de cuenta.

Una empresa puede tener varios sitios vinculados a través de una red privada, pero ciertos usuarios, como los agentes de servicio al cliente, puede necesitar llamar a los colegas en otras oficina cuando la red está ocupada, mientras que otros usuarios esperan a que una línea se libere. Las rutas de menor costo pueden traducir automáticamente el número interno a una llamada de marcación directa en la red pública mientras otros usuarios están en espera.

Códigos de autorización

Los códigos de autorización permiten al usuario ir a otra extensión del sistema y realizar llamadas con sus restricciones personales de tarifa; esto puede proporcionar al usuario más o menos privilegios que los del propietario normal de la extensión que usan.

Dado que los códigos de autorización no dependen de los códigos de cuenta, el usuario tiene que ingresar ambos si así lo requiere la configuración del sistema. Todos los códigos ingresados se registran en SMDR.

Restricción de llamadas

Los supervisores y administradores pueden rechazar o permitir las llamadas a ciertos números, como los números internacionales o los números de tarifas elevadas para los usuarios individuales o para todo el sistema.

El sistema admite la restricción de llamadas en muchos niveles. Se pueden usar códigos abreviados en el nivel del sistema o de los usuarios individuales para bloquear el enrutamiento externo de números o tipos de números específicos. Normalmente, los códigos abreviados de restricción se configuran para que reciban un tono de ocupado; sin embargo, se pueden desviar las llamadas a números alternativos o al servicio de correo de voz, que devuelve un "mensaje de marcación restringida".

Los usuarios puede asignar códigos abreviados a una plantilla de derechos de usuario. Luego, los usuarios pueden aplicar la plantilla a los usuarios cuyas llamadas requieren restricción. Los

administradores también pueden restringir el reenvío de llamadas a números externos según el usuario.

Preferencia de línea inactiva

Preferencia de línea inactiva permite al usuario seleccionar una línea externa específica para empresas que prefieren trabajar en modo de sistema clave.

Al descolgar se selecciona la primera línea inactiva y el usuario se conecta a una línea exterior.

Invalidar restricción de llamadas

Invalidar restricción permite marcar números desde el directorio, con remarcar, registro de llamadas, programación de botón, códigos abreviados y números ingresados de forma manual hacia números externos presentes en el directorio público (Directorio de sistema, LDAP, HTTP) aunque un código abreviado restringido coincida con los dígitos marcados.

Llamada privada

Los usuarios podrán configurar el estado de llamada privada mediante los códigos abreviado o un botón predeterminado.

Las llamadas privadas no se pueden grabar, supervisar, interrumpir ni puentear.

Llamadas entrantes

Grupos de búsqueda

Un grupo de búsqueda es un conjunto de usuarios, por lo general usuarios que manejan tipos de llamadas similares, por ejemplo, un departamento de ventas. Una persona que llama para hablar con un miembro de un grupo puede marcar un número, pero su llamada la responde cualquier extensión miembro del grupo de búsqueda.

Existen cuatro formas en la que un grupo de búsqueda procesa las llamadas:

Secuencial	Una extensión a la vez en forma secuencial; siempre se comienza por la parte superior de la lista.
Colectiva	Todas las extensiones del grupo de búsqueda en forma simultánea.
Rotativa	Se inicia con la extensión de la lista que sigue inmediatamente a la extensión que respondió la última llamada del grupo de búsqueda.
Espera más larga	Se inicia con la extensión que ha estado libre durante más tiempo.

Avisos

Utilice el correo de voz junto con los grupos de búsqueda para:

- Grabar todos los mensajes relacionados con el grupo.
- Pasar un anuncio con el grupo de búsqueda está en modo servicio nocturno o fuera de servicio.

- Pasar anuncios cuando una llamada queda en cola.

Existe una opción de difusión para el correo de voz interno. Esta función modificará el funcionamiento del buzón de correo de voz para que la notificación del mensaje solo se desactive para cada miembro del grupo de búsqueda cuando recuperen su propia copia del mensaje. Los anuncios de grupos de búsqueda están separados de la cola del grupo de búsqueda y es posible usarlos incluso si la cola está desactivada. Los avisos de grupos de búsqueda se admiten al utilizar Embedded Voicemail y Voicemail Pro. Los administradores y supervisores pueden configurar el horario del primer y segundo anuncio, y entre los siguientes anuncios.

Los grupos de búsqueda de una red comunitaria pequeña pueden incluir miembros ubicados en otros sistemas dentro de la red.

Asignar llamada ante respuesta del agente

Los supervisores pueden configurar la opción asignar llamada ante respuesta del agente para un grupo de búsqueda con el fin de activar las aplicaciones CTI para que informe correctamente los detalles de la llamada que se advierte y asegurar de que la primer llamada de la cola siempre se atienda en primer lugar.

Modos de servicio nocturno y fuera de servicio

Fuera de la operación normal, un grupo de búsqueda se puede poner en dos modos especiales: servicio nocturno y fuera de servicio.

Modo de servicio nocturno

Los usuarios pueden activar o desactivar el modo de servicio nocturno mediante el uso del código abreviado correcto. En este modo, las llamadas se derivan a un grupo de servicio nocturno. Es posible controlar automáticamente esta situación mediante la configuración de un perfil de horario que define las horas de operación del grupo principal, o manualmente mediante un código de función de teléfono. Cuando el modo de servicio nocturno está activo, el grupo de búsqueda original se desactiva en forma temporal. Es posible determinar que las llamadas al grupo de búsqueda:

- Se transfieran a un grupo de reserva de servicio nocturno que a su vez transfiere las llamadas a una extensión de atención personalizada o a un número externo.
- Reciban el mensaje de fuera de horario si el correo de voz está activo.
- Reciban el tono de ocupado.

Modo fuera de servicio

Los usuarios controlan el modo fuera de servicio de forma manual desde un teléfono. Mientras este modo esté activo, las llamadas se transfieren al grupo fuera de servicio. El servicio nocturno de reserva que utiliza un perfil de horario no se aplica al grupo de búsqueda ya configurado en fuera de servicio.

Grupos de desbordamiento

Los supervisores pueden diseñar un grupo de desbordamiento que tomará las llamadas si todas las extensiones del grupo de búsqueda están ocupadas o no responden.

Los supervisores también pueden configurar la extensión del tiempo de espera antes de que una llamada se transfiera al grupo de desbordamiento. Es posible configurar el tiempo de desbordamiento para llamadas individuales y para todas las llamadas en el grupo. El sistema puede modificar el estado de los usuarios que no responden una llamada del grupo de búsqueda que se les presente. Es posible configurar el estado del usuario en ocupado en

recapitulación, ocupado no disponible o desconectado. Es posible configurar el cambio de estado para usuario y para grupo de búsqueda.

Llamada en cola

La espera en cola permite que las llamadas para un grupo de búsqueda esperen en la cola cuando todas las extensiones en la lista de extensiones del grupo están ocupadas. Cuando una extensión se libera, se trasfiere la llamada en cola. La definición de las llamadas en cola ahora incluye las llamadas que suenan y las llamadas que esperan para sonar. Es posible establecer el límite de espera en cola para controlar una cantidad máxima de llamadas que esperarán en un grupo de búsqueda.

Mientras están en cola, si el correo de voz está activo, la persona que llama escuchará los anuncios para este grupo de búsqueda.

Alerta de umbral de cola

Los supervisores y administradores pueden configurar una alerta que se produzca en el puerto de extensión análoga seleccionado cuando la cantidad de llamadas en cola para un grupo de búsqueda supera el umbral.

Generalmente, la alerta consiste en un timbre fuerte u otro dispositivo de alerta. La alerta no presenta una llamada.

Enrutamiento de llamadas entrantes

El enrutamiento inteligente de llamadas toma decisiones sobre enrutamiento según uno de los siguientes criterios o todos los siguientes criterios:

- Los dígitos desde el intercambio, como DDI/DID o ISDN MSN
- El número de teléfono o el ID de la llamada entrante o parte del número recibido, como un código de área
- Subdirecciones ISDN
- Tipo de servicio ISDN/PRI, es decir, llamada de voz o llamada de datos

Por ejemplo, una llamada DDI/DID a un grupo de ventas se trata de forma diferente según en qué parte del país se origina la llamada.

Cada ruta para llamada entrante admite un segundo destino de servicio nocturno que puede brindar una ruta alternativa para las llamadas entrantes según la hora del día y el día de la semana, así como el desvío según el calendario para fechas específicas.

Las llamadas que no se pueden desviar al destino configurado se vuelven a desviar a un destino de reserva definido por el usuario. Esto tiene una utilidad especial si normalmente se responden llamadas mediante un operador automático y se produce un fallo de red.

Si hay varios desvíos de llamada configurados con el mismo destino, es posible asignar un nivel de prioridad a las llamadas. El nivel de prioridad determina la posición de una llamada en la cola según el orden de llegada.

Nota:

las llamadas que ya están sonando en una extensión libre no se consideran en cola y no se ven afectadas por una llamada que ingresa a la cola con mayor prioridad (a menos que

se seleccione la opción asignar llamada según respuesta de agente para ese grupo de búsqueda).

Los supervisores pueden configurar un temporizador de promoción de prioridad para aumentar la prioridad de las llamadas que han estado en la cola más tiempo del definido y agrega una etiqueta opcional a las llamadas en la ruta de llamadas entrantes, que se puede mostrar en el teléfono de alerta.

Perfiles de horario

Los perfiles de horario establecen el horario de operación del servicio. Por ejemplo, es posible establecer un perfil de horario para que el personal tenga acceso a Internet sólo durante el horario de almuerzo.

Mediante el uso de los perfiles de horario, es posible definir un servicio alternativo que funcione fuera del horario de operación del servicio principal. Esto se puede utilizar para aprovechar las tarifas alternativas fuera de los horarios pico. El cambio a este servicio de reserva también se puede controlar manualmente mediante el marcado de un código abreviado de seguridad desde un auricular. Esto tiene una particular utilidad dado que permite la restauración rápida del servicio en caso de producirse una falla en el proveedor de servicios de Internet (ISP). Esta función también se aplica a los días de la semana o a fechas específicas del calendario.

Funciones de telefonía IP

Extensiones de creación automática

Los ingenieros de implementación pueden configurar IP Office con el fin de crear entradas de extensión para teléfonos IP nuevos agregados a la red de área local.

En los casos donde la red de área local no sea segura, es posible desactivar esta función, pero simplifica la instalación.

Ruta directa de medios

La ruta directa de medios permite desviar la ruta de voz entre dos extensiones IP (configuración después de llamada) directamente entre sí. Esto permite al sistema liberar los recursos de compresión de voz después de establecer la conexión extremo a extremo, lo que permite usar los recursos de la forma más eficiente.

Soporte técnico para medios iniciales y mensajes PRACK

IP Officeadmite anuncios en banda, por ejemplo:

- Personalización desde proveedores de larga distancia o con descuento

- Indicaciones de progreso cuando los tiempos de espera extraordinarios son inherentes al escenario de la llamada, por ejemplo cuanto se intenta localizar un teléfono celular
- Devolución de llamadas específica para país y otros tonos de progreso
- Conferencia en el dominio IP antes de responder llamada, por ejemplo en el caso de grabaciones de llamadas o conferencias con marcadores automáticos

Los ingenieros de implementación pueden configurar las líneas troncales SIP, con el fin de admitir medios iniciales, mediante la adición de un encabezado **100rel to Supported** en el parámetro **INVITE**.

Comienzo rápido

Los ingenieros de implementación pueden configurar el inicio rápido en una extensión IP para reducir la sobrecarga de protocolo que permite que una ruta de audio se establezca más rápidamente.

Transporte fax

IP Office admite protocolos de transporte fax T.38 y pertenecientes a Avaya.

Protocolo de transporte fax perteneciente a Avaya

La llamada de fax se desvía hacia líneas troncales VoIP entre sistemas IP Office de una red IP que utiliza un protocolo de transporte que pertenece a Avaya.

Protocolo de transporte fax T.38

IP Office admite el protocolo T.38 para la transmisión de mensajes de fax entre IP Office y líneas troncales SIP y extensiones SIP.

Nota:

El protocolo T.38 no se admite en los sistemas Server Edition. Se utiliza el transporte fax G.711.

Plataformas	IP500 V2 con módulo VCM32 o VCM64
Tipos de línea troncal	SIP
Extensiones	SIP
Capas de transporte	UDPTL con corrección opcional de errores de redundancia
Versiones	0–3
Tipos de llamadas	Llamadas de voz con transición a transmisión por fax al detectar el tono de fax y llamadas que se negocian como solo fax.
Reserva de fax	Las líneas troncales SIP y las extensiones SIP pueden configurar ahora la compatibilidad de transporte fax a reserva T38, de modo que

las llamadas de fax salientes usen fax T38, pero cuando el destino de la llamada no admite T38 y rechaza la llamada, se envía una nueva invitación para el transporte de fax en G.711. Las llamadas de audio entrante que detectan tonos de fax también inician el transporte fax mediante la reserva T.38. Esto permite que IP Office admita implementaciones adicionales donde es posible que el fax T.38 no esté disponible universalmente.

Pantalla para nombre de directorio de llamada entrante

Los administradores pueden seleccionar el CLID o el nombre de directorio como pantalla predeterminada para las llamadas entradas.

DTMF fuera de banda

Los ingenieros de implementación pueden configurar una multifrecuencia de doble tono (DTMF) fuera de banda en una extensión IP para que se envíe una señal al otro extremo de la conexión con los dígitos que un generador local DTMF tiene que volver a generar en nombre de la extensión IP que envía la señal. Esto es útil cuando se navega por sistemas de correo de voz externos y de operadores automáticos.

Encabezados de privacidad y PAI

Los valores predeterminados para encabezados de privacidad y PAI permiten el anonimato de las personas o los terceros que llaman a pesar de proporcionar información necesaria para facturación y rastreo, e información de 911 de emergencia a la red. Esta característica alinea la funcionalidad con las pautas de implementación descritas en la recomendación técnica SIPconnect 1.1.

Supresión de silencio

La supresión de silencio brinda un aprovechamiento máximo del ancho de banda disponible, como la conexión por la que escucha la persona que llama, sin hablar. La supresión de silencio funciona al enviar descripciones del ruido de fondo en lugar del ruido real, durante intervalos en la conversación; esto reduce el número y la frecuencia de paquetes de voz enviados por la red. El ruido de fondo es muy importante durante una llamada telefónica. Sin ruido, la llamada se escucharía poco natural y daría una percepción de poca calidad.
Asegúrese de que la configuración de supresión de silencio coincida en ambos extremos de la línea troncal de la SCN para que funcione correctamente y también para una mejor calidad de sonido.

SIP features

SIP endpoints are supported on IP Office audio (voice) and T.38 fax communication using SIP terminal adapters. Users can use standards-compliant IP phones using the open SIP standard, offering a choice of endpoints including special purpose devices such as conference phones, hotel phones and terminal adapters.

IP Office supports Avaya 1100 and 1200 series phones using the SIP protocol. The phone user interface can vary when used on BCM with UNIStim. For example, with SIP, the 1100 and 1200 series IP phones only support a single call appearance although multiple calls are supported by the 1100 and 1200 series phones.

Nota:

These phones are only supported on IP500 V2 control units.

In pure SIP systems, IP Office expands the feature set beyond the SIP standard offering features on SIP endpoints delivering features consistently between SIP and Avaya digital and IP endpoints.

Nota:

In order to use a non-Avaya SIP endpoint with IP Office, obtain a Third-party IP Endpoint license from Avaya. This license supports endpoints based on the H.323 standard and is required for generic SIP endpoints on IP Office. Avaya IP Office SIP phones use the IP Endpoint license.

PSTN toll bypass

Toll bypass allows each system to leverage the trunk connections of the other system in the network to avoid international and long distance charges.

Standard call features

- Basic Call Completion
- Handling of busy called party
- DTMF and ring-back tone
- Hold and Retrieve
- Transfer
- Call Waiting presentation
- Called Number display
- Calling number and name display
- Abandoned call
- Single call appearance

Advanced call features

SIP endpoints support a number of extended features according to the SIP service samples, also referred to as “Sipping-19”. Features include:

- Calling line identification
- Hold/Consultation Hold

- Attended/Unattended Transfer
- Message waiting
- Do not disturb
- Conference Add
- From in Clear when privacy is requested
- User agent header (configurable) included to identify call in SIP trunks for troubleshooting
- Busy lamp keys with speed-dial, status indication, and pickup
- Self-labeling feature keys for softkey support including a Special feature key. The supported features are also available pressing a feature key plus the appropriate feature code. The feature codes are identical to the features codes from BCM

Feature activation key features

A large number of additional features are supported on IP Office using feature activation keys. These features include but are not limited to:

- Call forward: Unconditional/Busy/no Answer
- Follow me
- Park/Unpark
- Music on Hold
- Meet me conferencing
- Conference join
- Ring back when free
- Multiple call appearances

Nota:

Does not include bridged appearances or outside-line appearances.

CTI features

The new centralized CTI web service API provides a more open platform to allow third parties add value and build solutions. Support is provided for distributed (IP Office Server Edition and SCN) environment – not limited to nodal as per current TAPI. Centralized CTI web service API is dependent on Avaya one-X® Portal access for the users. Creating a new user in IP Office with the new API does not require a reboot. SIP endpoints support the following CTI-based features using the TAPI interface:

- Outgoing call (without remote activation of speakerphone/headset)
- Hang up
- Hold
- Attended/Unattended transfer
- Conferencing
- Voicemail collect
- Set forwarding/DND (IP Office based)
- Park/Ride (IP Office based)

Nota:

Avaya Phone Manager and Phone Manager Pro and SoftConsole are currently not supported in combination with SIP endpoints.

Video conferencing

Video conferencing is supported in the following configurations:

- Local system
- Small community network
- Video-ready SIP trunk such as Avaya Aura®

All video communication is end-to-end; IP Office does not natively manage or perform video conferencing.

The softphone application handles video conferencing. IP Office video conference supports the following features using feature access codes:

- Make calls to all phones and trunk lines as audio only
- Receive audio calls
- Call forwarding
- Forward to voicemail recording audio streams, not video.
- Application sharing
- Accept several video calls in parallel to leverage the Multi-Conference Unit (MCU) functionality, for example, the Avaya 1040 system

Video requires high network bandwidth, depending on codec video quality it can be up to 1 Mbit/sec. IP Office supports with H.263 and H.264 codecs. During planning, a network assessment identifies the bandwidth requirements. Refer to product details for video requirements. Typical bandwidth requirements for HD video are:

- 1010: 1 Mbps for 720p/30fps
- 1040:
  - 768 Kbps for 720p 30fps
  - 1.1 Mbps for 720p 60fps
  - 1.7 Mbps for 1080p 30fps

Parameters for passing User to User Information (UUI)

IP Office passes on the received UUI information element back to the public network in case of a transit call. This feature is supported only on SIP trunks and the UUI information element is not passed internally to other elements in the solution such as IP Office Contact Center, , and so on. The UUI information is not mapped to any other trunks types such as ISDN or H.323. IP Office carries the UUI information using a proprietary IP Office field.

Two new parameters are added in the SIP Advanced tab, Identity group, called Add UUI header and Add UUI header to redirected calls. The Add UUI header to redirected calls field is dependent on the Add UUI header field and can be selected only when Add UUI header is selected. The default value for the field is false. These configuration items are a mergeable feature and applicable to Standard and Server Edition mode on all supported IP Office platforms.

SIP Line Appearances

Trunk line selection enables the familiar line appearance operation on Powered by Avaya (Release 3.0) or IP Office Essential Edition, Server Edition, and IP Office Select. The feature

provides easier migration from familiar analog line appearances to SIP line appearances. Line appearance buttons for SIP URIs looks and operates in the same way as the analog trunk appearances. SIP trunk appearances is supported on all phones that support line appearances.

Route incoming SIP trunk calls based on an optional SIP header

This feature enables IP Office to route incoming SIP trunk calls based on optional SIP header P-Called-Party. IP Office reads the P-Called-Party ID header in the SIP message and routes the incoming SIP calls based on it. As P-Called-Party-ID is an optional header it is not parsed by default and it has to be explicitly configured. IP Office uses it for call routing only when the configuration option is selected and the header is present in the incoming SIP call. If the configuration item is checked and the header is not present IP Office uses the header configured in Call Routing Method for Incoming Call Route. P-Called-Party-ID is not used for SM trunks and SIP phones and IP Office does include this header in any outgoing messages.

Security enhancements for registration of SIP devices

This security enhancements enable administrators to allow or disallow registration of SIP devices in IP Office based on their User Agent strings. Administrators can use the configuration settings to add, modify, or remove SIP User Agent strings to SIP UA Blacklist, SIP UA Whitelist, and IP Whitelist. Subsequently, the **Allowed SIP User Agents** setting can be used to select which SIP User Agents are allowed for registering with IP Office. A default blacklist comes preconfigured with some known malicious user agent strings and can be updated as required. The lists can be configured using Web Manager and Manager.

SIP and H.323 Registrars disabled by default

To secure IP Office R 11.0 FP4 from vulnerabilities, the H.323 and SIP Registrars are disabled by default. Whenever a new H,323 or SIP extension is added and the corresponding registrar is not enabled, IP Office system displays error messages and prompts administrators to enable the Registrars. When resiliency support is enabled on an IP Office Line in systems having IP extensions and the systems do not have the corresponding registrars enabled, IP Office system displays an error message and prompts administrators to enable the corresponding registrars.

Compresión de voz

IP Officeadmite una amplia gama de estándares de compresión de voz, incluida G.711, G. 729a y G.722. El método de compresión se puede establecer automáticamente para cada llamada o configurar para una extensión individual.

Compresión de voz

G.722 se admite en los siguientes tipos de teléfonos SIP:

- Serie 9600
- Serie 96x1
- Teléfonos de conferencia B179
- Teléfonos IP 1100/1200
- Teléfonos SIP de terceros

Nota:

G.722 no es compatible para los teléfonos de las series 5600 y 1600.

Telefonía de IP Office Branch

Servicios de telefonía

La solución Branch ofrece servicios de telefonía a usuarios centralizados y a usuarios IP Office.

Los usuarios IP Office obtienen servicios de telefonía desde IP Office local. La solución Branch admite todos los terminales IP Office de hardware y software. Para obtener una lista de terminales IP Office, consulte “Teléfonos” en *Instalación de IP500/IP500 V2* (15-601042).

Los usuarios centralizados se registran en Avaya Aura® Session Manager y obtienen servicios de telefonía de Communication Manager Feature Server o Evolution Server de Avaya Aura® en la empresa central. Los usuarios centralizados pueden usar uno de los siguientes terminales centralizados admitidos:

- SIP 9620
- SIP 9630
- SIP 9640
- SIP 9650
- SIP 9601
- SIP 9608
- SIP 9611G
- SIP 9621G
- SIP 9641G
- J169
- J179
- SIPAvaya one-X® Communicator (solo audio)

Supervivencia para usuarios centralizados

Si la conectividad WAN al Avaya Aura® Session Manager se pierde o si todos los servidores Avaya Aura® Session Manager implementados están caídos, los usuarios centralizados obtienen automáticamente los servicios de telefonía básica desde IP Office local con modo Supervivencia o Día lluvioso. Las funciones de telefonía provistas por IP Office en modo Día lluvioso son limitadas si se las compara con las funciones que se brindan normalmente a los teléfonos centralizados.

Las siguientes funciones se encuentran disponibles en los teléfonos SIP centralizados de la serie 9600 cuando están registrados en IP Office con el modo Día lluvioso:

- Realice o reciba llamadas a otros terminales o desde otros terminales de la sucursal y hacia cualquier tipo de línea troncal PSTN local o desde esta
- Identificador de llamada
- Varias apariencias de llamada, pero apariencias sin puentes
- Llamada en espera y llamada en espera por consulta

- Música de espera
- Transferencia de llamada asistida
- Transferencia de llamada no asistida
- Conferencia ad-hoc entre tres participantes realizada de manera local en el teléfono, así como capacidad para marcar en conferencia Meet-Me en IP Office con hasta 64 participantes
- Cobertura de correo de voz centralizado y acceso por PSTN, pero sin Indicación de mensaje en espera (MWI)
- Operadora automática
- Indicación de modo supervivencia en la pantalla del teléfono
- Funciones locales del teléfono: remarcado, silenciar, selección de audio (altavoz/auricular), Registro de llamadas, Control de volumen, contactos locales, marcaciones rápidas, marcaciones automáticas
- Registros detallados de mensajes en la estación (SMDR) almacenados en IP Office para recuperar después de la recuperación de WAN
- Grupos de búsqueda

  IP Office puede configurarse con grupos de búsqueda centralizados para los cuales el procesamiento de IP Office esté en funcionamiento solamente en el modo Día lluvioso. El administrador de IP Office debe configurar los grupos de búsqueda en IP Office de forma coherente con la configuración de Avaya Aura® Communication Manager central para el modo Día soleado.
- Administración de llamadas

  IP Office puede configurarse con códigos abreviados mediante la función Restringido para restringir, en modo Día lluvioso, qué llamadas puede realizar el usuario centralizado. El administrador de IP Office debe configurar esto en coherencia con la Clase de restricción (CoR) configurada en Communication Manager, la cual se aplica al mismo usuario en el modo Día soleado.
- Envío de llamada al teléfono móvil

  IP Office puede configurarse con Mobile Twinning para enviar llamadas para el usuario centralizado en modo Día lluvioso a un número de móvil. El administrador de IP Office debe configurar esto en IP Office de manera coherente con la configuración de EC500 en Communication Manager central para el mismo usuario centralizado.
- Reenvío de llamadas

  Es posible configurar el reenvío de llamadas locales en el teléfono si se encuentra en el modo Día lluvioso. El reenvío de llamadas establecido en Communication Manager en el modo Día soleado no afecta el comportamiento local del teléfono ni el comportamiento de IP Office en el modo Día lluvioso. Además, el reenvío de llamadas locales establecido en el teléfono funciona solamente en el modo Día lluvioso después de la conmutación por recuperación.
- Códigos de autorización

  IP Office puede configurarse para que sea compatible con códigos de autorización que los usuarios centralizados pueden usar en el modo Día lluvioso. El administrador de IP Office debe configurar los códigos de administración en coherencia con los códigos de

autorización configurados en Communication Manager, los cuales están disponibles para los mismos usuarios centralizados en el modo Día soleado. Los usuarios de teléfonos SIP centralizados en modo Día soleado oirán 3 pitidos que indican que se requiere un código de autorización. En el modo Día lluvioso, los usuarios de teléfonos SIP centralizados oirán 1 pitido que se repite, aproximadamente, cada 5 segundos.

Funciones de mensajería

El servicio de mensajería le permite a los usuarios administrar todos sus mensajes, es decir los mensajes de correo electrónico y de correo de voz, en un solo lugar. Dado que la plataforma principal de mensajería es típicamente el correo electrónico, IP Office le permite a los usuarios administrar los mensajes de correo de voz a través del sistema de correo electrónico con el fin de mantener todos los mensajes sincronizados a través de una interfaz de usuario. IP Office ofrece dos opciones para correo de voz: Embedded Voicemail y Voicemail Pro.

En general, el correo de voz ofrece un contestador automático telefónico con un saludo personalizado en el escritorio de cada empleado y permite que las personas que llaman dejen mensajes de voz cuando un usuario no puede responder la llamada. Es posible acceder a los mensajes de correo de voz de forma local o remota a través de cualquier teléfono (el sistema le solicitará a los usuarios ingresar un PIN si utilizan un teléfono diferente al de su extensión o ubicación asignada, por ejemplo un teléfono celular).

El servidor de correo de voz es multilingüe y puede ofrecer diferentes avisos según el idioma de preferencia del usuario e independientemente de la configuración predefinida del sistema. Del mismo modo, las personas externas que llaman pueden escuchar avisos en su propio idioma según la ruta de llamadas entrantes (por ejemplo, según el ID de llamada).

Las funciones disponibles del correo de voz son:

- IP Office Essential Edition Embedded Voicemail permite algunas funciones básicas de mensajería gracias a la capacidad de reenviar los mensajes de correo de voz a la bandeja de entrada del correo electrónico del usuario.
- IP OfficePreferred Edition
  - Voicemail Pro: para uso en un solo sitio, pero en una SCN de usuarios remotos
  - Voicemail Pro distribuido: para uso en multisitio dentro de una SCN
  - Mensajería modular centralizada: para uso con Avaya Aura® Communication Manager

IP Office Preferred Edition se encuentra disponible para los sistemas operativos Windows y Linux OS. Preferred Edition para Linux ofrece las mismas funcionalidades que se describirán en este capítulo, a excepción de:

- Web Voicemail está suministrado por la aplicación de productividad de usuario incluido en Office Worker, Teleworker y Power User.
- VPNM
- Acciones relacionadas con IVR (base de datos y secuencia de comandos de VB)
- Autentificación de la biblioteca de grabaciones de voz (VRLA)

Vínculos relacionados

Comparación de las funciones de mensajería en la página 43

Comparación de las funciones de mensajería

La siguiente tabla resume las diferencias funcionales y operativas entre las aplicaciones de mensajería que IP Office admite en la unidad de control IP500 V2.

Capacidades

Capacidad	Voicemail Pro	Embedded Voicemail
Cantidad de buzones de correo	Sin límite: sólo limitada por la configuración de IP Office.	Sólo limitada por la configuración de IP Office.
Llamadas concurrentes (puertos)	Hasta 40, según la licencia	6 llamadas simultáneas
Tiempo de grabación	Dependiente de la PC (requiere 1 MB por minuto)	2 puertos: hasta 15 horas 4 puertos: hasta 20 horas 6 puertos: hasta 25 horas

Funciones

Función	Voicemail Pro	Embedded Voicemail
Se ejecuta como un servicio	Sí	No
Compatibilidad multilingüe	Sí	Sí
Correo de voz para usuarios individuales	Sí	Sí
Correo de voz para usuarios virtuales	Sí	Sí
Correo de voz para grupos de búsqueda	Sí	Sí
Difusión de grupo	Sí	No
Servicio unificado de mensajes (UMS)	Opción	No
Integración con Microsoft Exchange Server	Opción	No
Capacidad de interactuar con una solución Blackberry	Opción[1]	No
Resistencia y copia de seguridad	Opción	No
Funcionamiento de Small Community Network	Sí	No
Servicios de correo de voz centralizado	Sí	No

La tabla continúa…

[1] Requiere el servicio UMS (habilitado mediante las licencias de Power User, Office Worker y Teleworker) y MS Exchange Server 2007/2010 con una solución de movilidad (por ejemplo, Blackberry) no suministrada por Avaya.

Página333 de 3226.

Función	Voicemail Pro	Embedded Voicemail
Servidores de correo de voz distribuido en una red comunitaria pequeña (SCN)	Sí	No
Timbre de correo de voz	Interno y externo	Sí
TUI de ayuda de correo de voz	Sí	No
Indicación de mensaje en espera	Sí	Sí
Correo de voz visual (menú interactivo en la pantalla del teléfono)	Sí	Sí
Integración con Phone Manager Pro	Sí	No
Saludos personalizados	Sí	Sí
Saludos personales extendidos	Sí[2]	No
Saludo de reproducción continua	Sí	No
Reenviar a correo electrónico	Sí	Sí
Copiar a correo electrónico	Sí	Sí
Escuchar correo electrónico (Texto a voz)	Sí[2]	No
Enviar notificaciones de correo electrónico.	Sí	Sí
Guardar mensaje	Sí	Sí
Eliminar mensaje	Sí	Sí
Reenviar mensaje a otro buzón	Sí	Sí
Reenviar a varios buzones	Sí	Sí
Reenviar con mensaje de encabezado	Sí	Sí
Repetir mensaje	Sí	Sí
Retroceder mensaje	Sí	Sí
Avanzar mensaje	Sí	Sí
Pausar mensaje	Sí	No
Saltar un mensaje	Sí	Sí
Opción de reproducir mensaje nuevo/antiguo primero	Sí	No
Definir prioridad de mensajes	Sí[2]	No
Configurar tiempos de eliminación automática de mensajes	Sí	No
Recopilación de datos alfanuméricos	Sí[2]	No

La tabla continúa…

[2] Sólo modo Intuity.

Función	Voicemail Pro	Embedded Voicemail
Anuncio de fecha, hora e identificador de llamada de interlocutores	Sí	Sí
Devolución de llamada al remitente (si el identificador de llamada está disponible)	Sí	Sí
Acceso remoto al buzón de correo	Sí	Sí
Código PIN definible por el usuario	Sí	Sí
Derivar código PIN de identificador de llamada conocido	Sí	Sí
Interrupción de la recepción	Interno y externo.	Interno y externo.

Anuncios en cola

Función	Voicemail Pro	Embedded Voicemail
Anuncio de entrada en cola	Sí	Sí
Anuncio de actualización de cola	Sí	Sí
Anuncio de posición en cola	Sí	No
Anuncio de tiempo en cola	Sí	No
Anuncio de tiempo en el sistema	Sí	No
Tiempo de espera estimado (ETA)	Sí	No
Salir de la cola hacia un punto de respuesta alternativo	Sí	No

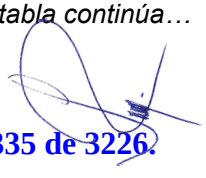
Operadora automática/Audiotex

Función	Voicemail Pro	Embedded Voicemail
Estructura de árbol multinivel	Sí	Sí
Anuncio de mensajes	Sí	No
Anuncio discreto	Sí	No
Llamadas de alarma	Sí	No
Transferencias asistidas	Sí	No
Marcado por nombre	Sí	Sí
Marcado directo por número	Sí	Sí

Otras funciones

Función	Voicemail Pro	Embedded Voicemail
Grabación de llamada	Sí	No
Alteración de grabación de llamada identificada/verificada	Sí	No

La tabla continúa…



Función	Voicemail Pro	Embedded Voicemail
Condiciones de prueba	Sí	No
Numeración personal	Sí	No
Servicio telefónico de información horaria	Sí	No
Campaign Manager	Sí	No
Voicemail Pro Manager	Sí	No
Correo de voz personalizado	Sí	No
Modo de emulación TUI Intuity	Sí	No
Reenviar mensajes de correo electrónico a sistemas externos (VPIM)	Sí	Sí
Acceso a bases de datos de terceros (IVR)	Sí	No
Texto a voz en flujos de llamadas	Sí	No
Compatibilidad con secuencias de comandos en Visual Basic	Sí	No

Vínculos relacionados

Funciones de mensajería en la página 42

Mensajería de IP Office Branch

Mensajería

La solución IP Office Branch admite los sistemas de correo de voz y los sistemas de correo de voz centralizados IP Office.

Se admiten los siguientes sistemas de correo de voz centralizados:

- Avaya Aura®Messaging
- Avaya Modular Messaging
- Avaya CallPilot®: solo se admite en entornos de sucursal distribuidos que están conectados a CS 1000.

Se admiten los siguientes sistemas de correo de voz de IP Office:

- Embedded Voicemail: sistema de correo de voz IP Office predeterminado
- Voicemail Pro: disponible con Preferred y Advanced Editions de IP Office

Para obtener más información sobre los requisitos de configuración para cada sistema de correo de voz, consulte *Configuración de referencia para Avaya IP Office en un entorno de sucursal* (15–604253).

En un entorno de sucursal independiente, la sucursal empresarial solo puede usar un sistema de correo de voz de IP Office.

En un entorno de sucursal distribuida, la sucursal empresarial puede optar por un sistema de correo de voz de IP Office o un sistema de correo de voz centralizados para usuarios. Si el

Página336 de 3226.

entorno distribuido está conectado a CS 1000, los usuarios también pueden usar Avaya CallPilot® como el sistema de correo de voz.

En un entorno de sucursal mixto o centralizado, la sucursal empresarial solo puede utilizar un sistema de correo de voz centralizado.

Vínculos relacionados

Funciones de mensajería en la página 42

Mobility features

Uso compartido de escritorio

El uso compartido de escritorio le permite a los usuarios el uso no exclusivo de una única extensión.

El usuario inicia sesión con su propia identidad, de modo que puede recibir las llamadas y acceder a su propio correo de voz y a otros servicios. Por ejemplo, el personal de ventas que no visita la oficina con frecuencia puede tener servicios de telefonía y correo de voz sin poseer una extensión física permanente. Cuando termina su visita, solo tienen que cerrar la sesión para que la extensión esté libre para otros usuarios, o si el usuario inicia sesión en otro teléfono, la extensión original se desconectan en forma automática.

El uso compartido de escritorio en teléfonos SIP como J129, H175 y demás no es compatible a partir de IP Office versión 10.1. Esto incluye el uso compartido de escritorio a través de CTI o los códigos abreviados estándar; los predeterminados son *35 y *36. Los teléfonos SIP de IP Office no admiten la eliminación de contactos de usuario ni del historial de llamadas cuando un nuevo usuario inicia sesión en esos teléfonos mediante el uso compartido de escritorio. Esto puede dar lugar a que un usuario tenga visibilidad de la información de contactos historial de llamadas de otro usuario.

Funciones de acceso remoto

El firewall integral de IP Office, las cuotas de servicio y las bandas de tiempo se aplican a las llamadas de acceso remoto. Es posible complementar la seguridad del acceso remoto mediante el uso de CHAP (contraseñas cifradas) para verificar los usuarios finales o PAP que no admiten el cifrado. Las bandas de tiempo pueden controlar las horas en las que el servicio de acceso remoto está disponible.

Es posible configurar una ubicación confiable para la marcación entrante. Se trata de ubicaciones a las que el sistema permitirá el acceso de datos; por ejemplo, un usuario que realiza una marcación entrante desde su casa, o un usuario que recupera sus mensajes de voz desde un teléfono móvil sin un código de correo de voz. La ubicación confiable es también la ubicación a la que el servidor de correo de voz llamará para informarle al usuario que hay un nuevo mensaje.

Por el contrario, una ubicación especificada puede establecer qué acción restringe el acceso remoto desde esa ubicación únicamente; esta ubicación especificada también se le puede designar un número para volver a marcar y por lo tanto se minimiza la amenaza del acceso remoto no autorizado.

IP Office también puede incorporar los servicios para volver a marcar el acceso remoto de manera que el usuario siempre pueda acceder en forma remota a la oficina desde una única ubicación, por ejemplo su casa; después de la verificación del inicio de sesión el sistema desconectará su llamada y la volverá a marcar. Además del nivel de seguridad que la acción de volver a marcar agrega, también se convierte en un excelente método para consolidar los cargos por acceso remoto en la factura de teléfono de la oficina central.

Además del acceso remoto desde los adaptadores del teléfono, todas las tarjetas de líneas troncales ATM4 (inclusive la tarjeta de combinación ATM IP500 V2) admiten la conmutación de la primera línea troncal analógica a un módem V.32 integral para el acceso remoto.

Uso compartido de escritorio remoto

El usuario puede realizar y recibir llamadas desde cualquier oficina como si usara el teléfono de su escritorio. Puede acceder al sistema centralizado y al directorio personal así como a sus registros de llamadas (sólo disponible en teléfonos IP, análogos y digitales).

Cuando un usuario se registra en un sistema remoto de IP Office, todas las configuraciones del usuario se transfieren a ese sistema.

- Las llamadas entrantes del usuario se vuelven a redirigen a través de la SCN.
- Las llamadas salientes del usuario utilizan la configuración del sistema remoto IP Office.
- Sin embargo, algunas configuraciones no se pueden utilizar o pueden operar de manera diferente. Por ejemplo si el usuario utiliza un perfil de horario para algunas funciones, esas funciones solamente funcionarán si también existe un perfil de horario del mismo nombre en el IP Office remoto.

IP Officeadmite el uso compartido de escritorio remoto entre sistemas IP Office dentro de una SCN. El sistema en el que el usuario realiza la configuración se denominaIP Office “local”; todos los otros sistemas son IP Office “remotos”. La única licencia que se requiere para admitir el uso compartido de escritorio remoto es la licencia Voice Networking en cada IP500 V2 dentro de la SCN. Un único número proporciona movilidad mejorada y acceso sencillo a las funciones familiares. Por ejemplo, los asesores, gerentes y abogados pueden utilizar el servicio telefónico en diferentes oficinas y diferentes días.

En algunos casos, un usuario de uso compartido de escritorio que inició sesión en un sistema remoto querrá marcar un número mediante los códigos abreviados de otro sistema. Esto es posible mediante los códigos abreviados con la función interrumpir o un botón programable definido como interrupción. Esta función puede ser usada por cualquier usuario dentro de la red comunitaria pequeña pero es de extrema importancia para los usuarios de uso compartido de escritorio remoto.

Nota:

El uso compartido de escritorio remoto no es compatible con el centro de contacto. Las funciones manejadas por el teléfono no son afectadas por el uso compartido de escritorio, por ejemplo el registro de llamadas y marcación rápida del teléfono.

Remote Worker

Remote Worker permite la conexión de teléfonos IP remotos de la serie 9600 con H.323 FW, que se ubica detrás de un enrutador NAT en IP Office. La configuración no requiere ningún equipo concentrador de VPN con IP Office.

Con la función Remote Worker activada, es posible conectar los teléfonos IP remotos 9600 H.323 a IP Office, incluso si se ubica detrás de un enrutador NAT. Los conjuntos se autentifican en IP Office de la misma manera en que lo hacen los conjuntos en la red privada. IP Office solamente determina que un conjunto está ubicado fuera de la red privada y retransmite el tráfico VOIP RTP para garantizar que atraviese el enrutador NAT.

Nota:

La señalización H.323 y el tráfico de medios no están cifrados; sin embargo, el formato binario exclusivo añade un nivel de cifrado básico.

Para llegar a IP Office desde la red privada remota, se necesita configurar el teléfono IP remoto H.323 para la dirección IP pública del enrutador NAT que hospeda IP Office. Los puertos configurables se deben reenviar a IP Office. IP Office requiere que se configure una dirección IP pública válida para que la función esté operativa. Es posible configurar estadísticamente la dirección IP pública o descubrirla dinámicamente mediante un servidor STUN.

Los administradores habilitan Remote Worker mediante IP Office Manager. Para utilizar la función Remote Worker, es necesario contar con la licencia Essential Edition que proporciona 4 puestos de trabajador remoto. Es posible aumentar la cantidad de puestos de trabajador remoto mediante el paquete Teleworker User y una licencia Preferred Edition.

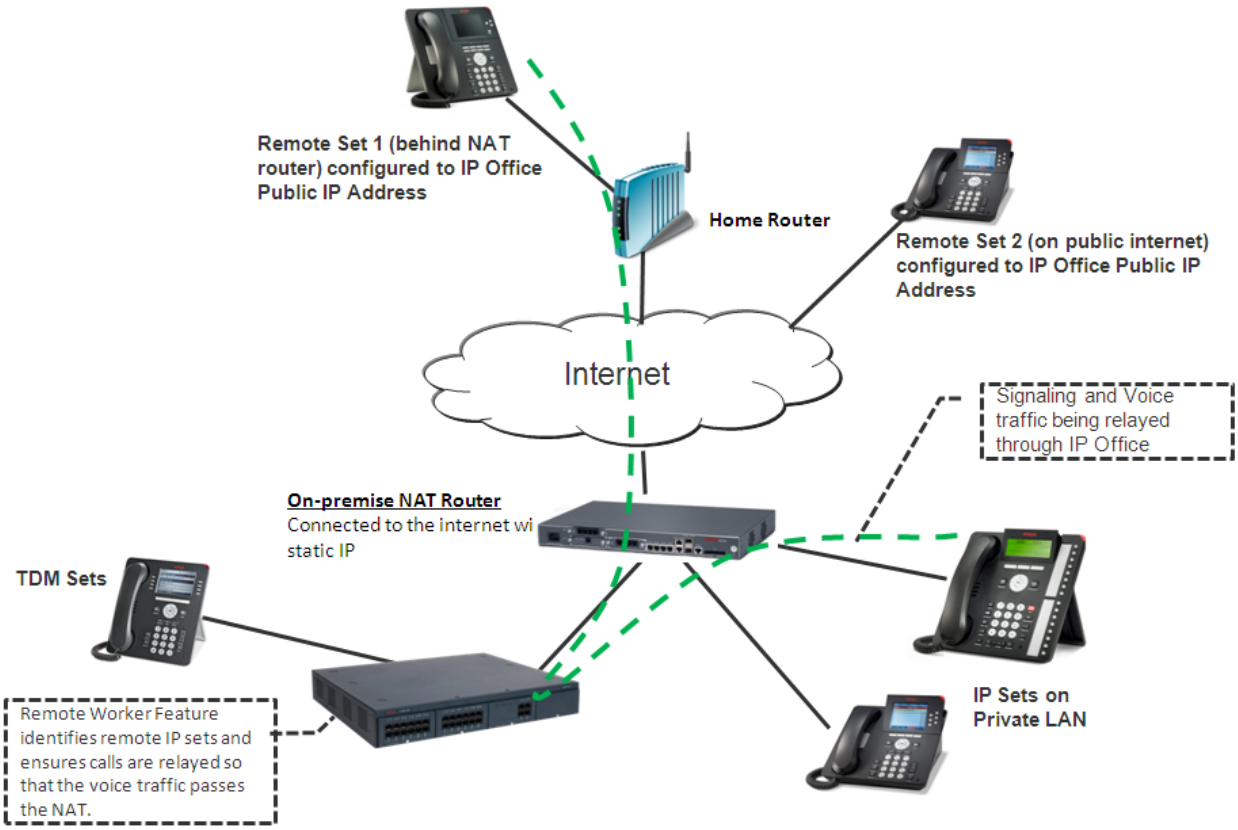


Figura 1: Interacciones de Remote Worker

Modo teletrabajador

El usuario puede realizar y recibir llamadas y recuperar mensajes de correo de voz desde un número de teléfono externo, como si estuviera en la oficina, dado que el servidor realiza el control de llamadas.

El escenario habitual muestra al trabajador remoto que en ocasiones trabaja desde su casa o desde una habitación de hotel. Esta función también representa una comodidad en la facturación y un potencial de ahorro en el costo de tener trabajadores remotos y personal móvil debido a que IP Office establece todas las llamadas. No es necesario verificar facturas ni pagar costosas llamadas de hotel.

Hermanamiento

La función de hermanamiento permite que una extensión primaria y un número secundario (extensión o externo) operen en conjunto como un solo teléfono.

La función permite que las llamadas que se realicen al número de extensión principal de un usuario emitan una alerta tanto en la extensión principal como en la secundaria. Esta función apunta principalmente a usuarios que utilizan un teléfono de escritorio y una extensión inalámbrica. Las llamadas de la segunda extensión hermanada se muestran como

provenientes de la extensión principal del usuario. La presentación de las funciones de llamada en espera y ocupado depende de si las extensiones hermanadas están en uso.

Cuando suena una llamada en el teléfono principal, el teléfono secundario también sonará. Si el teléfono principal no suena, por ejemplo en el modo no molestar, el teléfono secundario no sonará.

En general, este sistema se utiliza en escenarios como talleres o depósitos, donde los supervisores de equipos tienen un teléfono fijo en el escritorio y una extensión inalámbrica (por ejemplo, DECT). Cuando se realiza una llamada desde cualquiera de los teléfonos hermanados, la llamada se mostrará como si proviniera del teléfono principal. Otros usuarios del sistema deben saber que el supervisor cuenta con dos teléfonos diferentes. El temporizador de cobertura y el tiempo sin respuesta del supervisor se ejecutan para la llamada, y si no se responde la llamada en el período determinado, se derivará a los botones de cobertura disponibles y luego al correo de voz.

El hermanamiento admite las siguientes funciones:

- Seguirme a
- Seguirme hasta aquí
- Reenvío
- No molestar (excepciones incluidas)
- Acciones de grupo de búsqueda sin contexto: configuración del grupo de reserva/estado del servicio/membresía
- Acceso/Correo de voz activado/no activado
- Registro de llamadas (registro de llamadas central sólo para teléfonos T3 y 1600)
- Remarcación (registro de llamadas central sólo para teléfonos T3 y 1600)
- Entradas al directorio personal (sólo para teléfonos T3 y 1600)

Entre las Mobility Features, se incluyen:

- Hermanamiento móvil (externo)
- Control de llamadas móviles
- Devolución de llamadas desde teléfonos móviles
- Asistencia para el cliente Avaya one-X Mobile

Fallback Twinning

IP Office redirects calls to the users twinned external phone numbers when the primary extensions are unreachable even when the Mobile Twinning is disabled.

The following two short codes are available for disabling and enabling mobile Fallback Twinning:

- Set Fallback Twinning Off: To disable Fallback twinning
- Set Fallback Twinning On: To enable Fallback twinning

When Fallback Twinning feature is enabled:

- If Mobile Twinning is enabled – the only change will be to ignore the Mobile Dial Delay setting if the user's devices are unreachable.
- If Mobile Twinning is disabled – and if the user has no reachable devices, the normal evaluation of all Mobile Twinning conditions is performed, and if met, calls are redirected to the twinned mobile number immediately, that is, ignoring the Mobile Dial Delay setting.

Acceso móvil simplificado

El comportamiento estándar de la función de control de llamadas móviles consiste en emitir nuevamente el tono de marcado para el Mobile Worker si el destinatario de la llamada la desactiva. Este es el funcionamiento previsto, ya que impide que el Mobile Worker vuelva a marcar para seguir haciendo llamadas. El acceso móvil simplificado introduce un nuevo conjunto de FNE (FNE35, FNE36 y FNE 37) para desactivar la llamada al finalizarla; no se emite tono de marcado después de que la llamada finaliza.

Teléfono VPN

El teléfono VPN es una solución completa de telefonía IP que proporciona una comunicación segura a través de redes ISP públicas a un sistema IP Office en la sede central de la empresa. Los teléfonos VPN brindan una solución completa de telefonía disponible desde el escritorio del usuario hacia una ubicación remota, como una oficina en casa. No existe restricción en el uso del teléfono VPN.

El teléfono VPN es una solución sólo software según el teléfono IP 4610/21 o el teléfono estándar 5610/5620/5621. En combinación con uno de estos teléfonos y los productos de puerta de enlace de VPN más populares, el software extiende la telefonía empresarial a ubicaciones remotas. Los teléfonos IP 9600 admiten la funcionalidad de VPN y no es necesario instalar otro software.

El teléfono VPN funciona en las siguientes situaciones:

- Trabajadores de la oficina virtual
- Trabajadores remotos
- Centro de atención telefónica remoto
- Asistencia técnica para la continuidad del negocio
- Ubicaciones muy pequeñas que requieren un solo teléfono
- Instalaciones temporales, por ejemplo conferencias, reuniones fuera de la oficina y ferias comerciales

El teléfono VPN se ha probado con una variedad de puertas de enlace de VPN de importantes proveedores, como Cisco o Juniper, así como con dispositivos de acceso de VPN más pequeños de empresas como Adtran, Kentrox, Netgear y SonicWall. Consulte las páginas de asistencia técnica (support.avaya.com) para obtener una lista de las notas de la aplicación disponibles sobre puertas de enlace de VPN que se probaron con cada línea de teléfonos.

Funciones de red

Selección de ruta alternativa

Si una línea troncal principal está disponible, entonces la selección de ruta alternativa (ARS) proporciona la reserva automática a una línea troncal disponible, por ejemplo la reserva de la línea troncal análoga si falla la línea troncal SIP o T1, o uso de PSTN para la reserva de SCN.

Mediante la configuración de la función ARS, el sistema envía llamadas a través del portador más óptimo. También es posible utilizar los perfiles de horario para aprovechar tarifas más económicas o mejor calidad en momentos específicos del día.

Se admiten varios portadores. Por ejemplo, las llamadas locales atravesarán un portador entre las horas específicas; las llamadas internacionales, un portador alternativo. Es posible seleccionar el portador mediante la configuración de llamada de 2 etapas a través de DTMF en banda. Es posible asignar rutas específicas según el usuario, para permitir que el personal principal use las rutas costosas.

Conexión automática

Si un servicio está inactivo, es decir que nadie está usando Internet, la función conexión automática permite que el sistema se conecte periódicamente con un servicio. Esto es ideal para que el sondeo de correo electrónico recupere correos desde un proveedor de servicios de Internet. Un perfil de horario de conexión automática controla el período durante el que se realizan las llamadas automáticas, por ejemplo el perfil no funciona durante fines de semana o por la noche.

Devolución de llamada

Se admiten tres tipos de devolución de llamada:

Protocolo de control de enlace (LCP)	Después de la autenticación, se desconecta la llamada entrante y se realiza una llamada saliente a un número predefinido para reestablecer la conexión.
Protocolo de control de devolución de llamada de Microsoft (CP)	Después de la autenticación desde ambos extremos, se desconecta la llamada entrante y se realiza una llamada saliente a un número predefinido para reestablecer la conexión.
Protocolo extendido de control de devolución de llamada (CBCP)	Es similar al CP de devolución de llamada; sin embargo, la aplicación de Microsoft en el extremo remoto solicitará un número de teléfono. Luego, se realiza una llamada saliente a ese número para volver a establecer la conexión.

Firewall

El firewall integrado de IP Office ofrece la función de filtrado de paquetes de los protocolos IP más comunes, por ejemplo el protocolo de transferencia de archivos (FTP) y la exploración de Internet (HTTP). Es posible restringir/permitir todos los protocolos que pasan el firewall de cuatro formas diferentes:

Desconexión	No se permite ninguna sesión con este protocolo a través del firewall.
Fuera de sesión	Una sesión entrante puede atravesar el firewall para permitir el tráfico en ambas direcciones.
En sesión	Una sesión saliente puede atravesar el firewall para permitir el tráfico en ambas direcciones.
Ambos sentidos	Las sesiones entrantes y salientes pueden atravesar el firewall para permitir el tráfico en ambas direcciones.

Cuando no se admite el protocolo de forma predeterminada, es posible personalizar el firewall para controlar los paquetes según su contenido.

IP Office permite la configuración de la cantidad de firewalls necesarios mediante IP Office Manager. Esto permite aplicar diferentes normas de seguridad a los servicios de datos y los usuarios de marcación individuales.

Acceso a Internet

IP Officeofrece un acceso compartido, seguro y de alta velocidad a Internet mediante líneas de intercambio (oficina central), líneas digitales arrendadas o los servicios IP de VPN.

IP Office controla la seguridad de Internet mediante un firewall integrado sin necesitada de instalar un firewall independiente. Los administradores del sistema pueden configurar el firewall para acomodar una cantidad de situaciones y controlar quién tiene acceso a los recursos externos y cuándo.

El firewall aísla de Internet las redes privadas; esta situación garantiza que la red permanezca fuera del alcance de los piratas informáticos y se puedan configurar cuotas de servicio para los servicios de acceso remoto para asegurar que solo los usuarios autorizados tengan acceso. Las cuotas de servicio establecen un límite de tiempo en las llamadas salientes hacia un servicio IP en particular, por lo que se restringen los costos.

Los servicios se pueden configurar con un recurso alternativo, por ejemplo, para conectar su ISP durante las horas de trabajo y en otros horarios aprovechar las ventajas de los diferentes costos de las llamadas de un ISP alternativo. O bien, es posible configurar un servicio para conectarse durante el horario pico y otro para que actúe como reserva durante el período más económico.

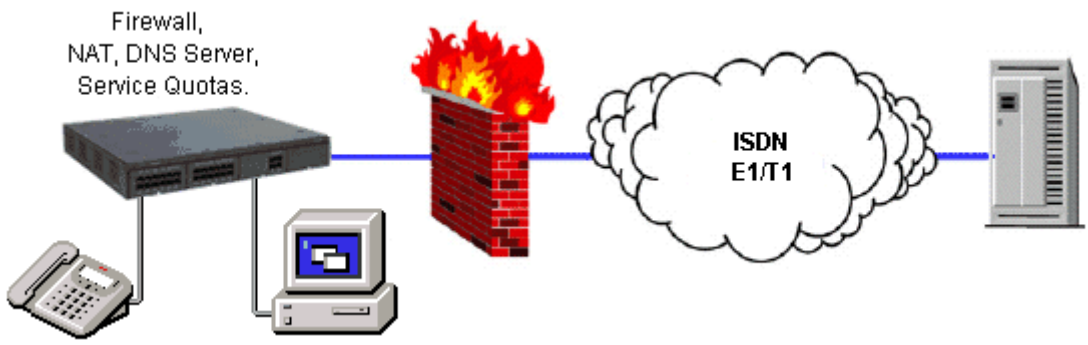


Figura 2: acceso a Internet

Esquemas de numeración de redes

IP Officebrinda flexibilidad en las opciones para numeración de redes. El sistema puede manipular dígitos marcados, mediante la adición o eliminación de dígitos y códigos de acceso, con el fin de acomodarlos al esquema de numeración. Normalmente se implementan dos tipos de esquemas de numeración: esquemas de numeración enlazada y numeración de nodo.

En los esquemas de numeración enlazada, cada sitio de la red tiene un rango único de números de extensión y los usuarios simplemente marcan el número de extensión del participante llamado. Con frecuencia, los esquemas de numeración enlazado se usan en redes muy pequeñas (menos de 5 sitios) con menos de 500 extensiones.

En los esquemas de numeración de nodo, cada sitio recibe un ID de nodo que es preestablecido por el usuario al marcar extensiones en otros sitios. De esta manera, los números de extensión se pueden replicar en los sitios mientras todavía se visualizan como únicos en la red. Los esquemas de numeración de nodo son comunes en redes más grandes.

En ocasiones, los esquemas de numeración enlazada y los esquemas de numeración de nodo se usan dentro de la misma red con la numeración de nodo utilizada en las grandes oficinas y la numeración enlazada empleada en clústeres de oficinas satélites.

Cuotas del servicio

Es posible configurar IP Office para restringir la cantidad máxima de minutos que un servicio, como el acceso a Internet, dispone para cada usuario. Esta es la suma total de llamadas realizadas y no incluye los períodos de inactividad. Cuando la cuota se usó, el servicio ya no está disponible. Es posible actualizar la cuota cada día, cada semana o cada mes en forma automática, o al marcar un código de función segura en un teléfono.

Perfiles de horario

Es posible utilizar los perfiles de horario para definir el horario de operación de un servicio, grupo de búsqueda, ruta de menor costo, puente de conferencia o del centro de marcado del usuario. Por ejemplo, es posible utilizar un perfil de horario para dirigir llamadas de grupos de búsqueda hacia una extensión personalizada o un correo de voz fuera de las horas operativas, o para aplicar diferentes rutas de menor costo durante diferentes horas del día

para aprovechar las tarifas de llamadas más económicas. Es posible crear entradas múltiples de horario para que el perfil de horario pueda definir un horario específico del día, por ejemplo 09:00 a 12:00 y 13:00 a 17:00. Fuera de ese perfil de horario definido, las llamadas de voz se redirigirán según la configuración; sin embargo, las llamadas que están cursando durante el cambio del perfil de horario no se desconectarán, dado que el cambio solamente afecta su redirección. Cuando se produzca el cambio de perfil de horario, se interrumpirán las llamadas de datos, pero se iniciará de inmediato una nueva llamada si así se especifica. Los perfiles de horario se pueden basar en fechas específicas del calendario para tener en cuenta días festivos y otros eventos.

Red multisitio

Cuando se conectan sistemas IP Office mediante redes basadas en paquetes o IP, las redes comunitarias pequeñas (SCN) aumenta la transparencia de la función. Estas redes pueden admitir hasta un máximo de 1000 usuarios en 32 sitios.

IP Office admite las siguientes funciones en un entorno de SCN:

Configuración de llamada básica (voz)	Admitido por H.323 y SIP en líneas troncales IP
Llamada retenida (local)	Admitido por H.323 y SIP en líneas troncales IP
Transferencia de llamada (local)	Admitido por H.323 y SIP en líneas troncales IP
Nombre que realiza/recibe la llamada	Admitido por H.323 y SIP en líneas troncales IP
Número que realiza/recibe la llamada	Admitido por H.323 y SIP en líneas troncales IP
Luz de ocupado (BLF)	
Espera	
Devolver llamada cuando esté libre	
Anuncio	
Captura	
Ubicación según zonas horarias	Diferentes zonas horarias para un grupo de extensiones según ubicaciones. Para teléfonos 96xx, 16xx, 11xx/12xx, D100 y E129
Directorio personal centralizado	Para teléfonos 1400, 1600, 9600 y T3 y Avaya one-X® Portal for IP Office

Directorio de sistema centralizado	Para teléfonos 1400, 1600, 9600 y T3 y Avaya one-X® Portal for IP Office
Registro de llamadas centralizado	Para teléfonos 1400, 1600, 9600 y T3 y Avaya one-X® Portal for IP Office
Correo de voz centralizado	Preferred Edition. Compatibilidad con buzones de correo, grabación de llamada, marcado por nombre y operadora automática. También se admite la puesta en cola remota en sistemas remotos.
Mensajería de voz distribuida/de respaldo	
Directorio interno	
Texto de ausencia	
Anti-trombonamiento	
Grupos de búsqueda distribuidos	Los grupos de búsqueda pueden incluir usuarios ubicados en otros sistemas IP Office de la red.
Uso compartido de escritorio remoto	Los usuarios pueden utilizar escritorios compartidos entre sistemas IP Office de la red. El sistema en el que el usuario realiza la configuración se denomina IP Office regular; todos los otros sistemas son sistemas IP Office remotos.
Marcación de interrupción	Esta función permite que el usuario seleccione un sistema IP Office de la red a partir de una lista desplegada y que luego marque un número subsiguiente como si marcara en forma local en el sistema seleccionado. La función se activa mediante un botón programable o código abreviado.

Resistencia

Por ejemplo, en la configuración de una SCN del sistema A y el sistema B donde el correo de voz centralizado se conecta al sistema B, y una cantidad de teléfonos IP se conectan a un sistema A o sistema B. Si el sistema B falla, entonces:

- El sistema A automáticamente tomará el control del sistema B y será compatible con los teléfonos IP, grupos de búsqueda y DHCP si es necesario.
- Voicemail Pro se volverá a registrar en el sistema A.
- Los usuarios en una SCN, cuando comparten el escritorio en otro sistema IP Office, conservan la configuración del perfil con licencia según se configuró en el sistema regular.
- Todos los contactos personales/registros de llamadas de los usuarios del sistema B continuarán disponibles (teléfonos 96x1, 9600 y 1600).

En el caso de las redes multisitio, se requieren módulos VCM en todos los sistemas que se conecten. Las líneas IP se pueden configurar en una configuración de inicio o de malla. Una de las ventajas de la configuración en malla es que elimina el riesgo de un solo punto de falla

en la red. También, los nombres y los números (grupos, línea, servicios, etc.) en los sistemas IP Office separados deben ser únicos para reducir la posible confusión de mantenimiento.

Todo sistema IP Office transmite mensajes UDP mediante el puerto 50795. Estas transmisiones en general se repiten cada 30 segundos, pero las actualizaciones de la BLF se pueden producir con mayor frecuencia. No se realizan actualizaciones si no hay actividad y el nivel de tráfico general es muy bajo, por lo general menos de 1 kbps por sistema.

La red multisitio se admite entre los sistemas IP Office con diferentes niveles de software; sin embargo, las funciones de red se basarán en el menor nivel de software en de la red. Esta opción apunta a permitir la actualización de sitios por fases en la red multisitio y aún se recomienda que todos los sistemas dentro de la red se actualicen al mismo nivel donde sea posible.

Si se requieren redes más grandes, es posible utilizar Q.SIG para vincular varias SCN. La funcionalidad entre comunidades se rige mediante el conjunto de funciones de Q.SIG.

Licencias de red de voz

En los sistemas IP500 V2, la red multisitio (con SCN) requiere una o más licencias adicionales. Los sistemas de expansión Server Edition (V2) no requieren licencias de red de voz.

Las capacidades Q.SIG, H.323 y SCN no están activadas de forma predeterminada en IP500 V2. Se requiere una licencia adicional para activar esta funcionalidad con 4 canales de red simultáneos (no hay límite de canal para Q.SIG). Es posible obtener licencias para canales adicionales en incrementos de 4. Aún así, se requiere una licencia Voice Networking para activar TDM Q.SIG, aunque no haya límite para el número de llamadas TDM Q.SIG que se pueden realizar o recibir una vez que se obtiene la licencia.

Servicios de red

Soporte de circuito de marcación

Si la cantidad de tráfico no justifica el costo de una línea concedida y arrendada, el sistema puede proporcionar conectividad de datos a través de circuitos de marcación ISDN con enlaces E1/T1 o líneas troncales con índice básico. Si se requiere una velocidad de datos superior a la de un solo canal (64K/56K), es posible agregar canales adicionales a la llamada en el momento necesario, si así se requiere.

Servidor DHCP

IP Office puede administrar su red IP en su nombre a través del servidor DHCP integral. Es posible configurar IP Office para guardar un grupo de direcciones IP para los usuarios de la red de área local. Cuando un usuario enciende su PC, el sistema le asigna una dirección IP para la duración de su sesión. El servidor DHCP también proporciona a la PC del usuario la dirección del servidor del servicio de nombres de dominio (DNS) y del servidor del servicio de nombres de Windows (WINS). De forma alternativa, para los clientes que tienen un servidor DHCP independiente, es posible configurar IP Office para obtener direcciones de ese servidor DHCP o con su propia dirección IP estática. IP500 V2 tiene dos servidores DHCP independientes, cada uno dedicado a LAN conmutado de nivel 3.

Proxy del servicio de nombres de dominio (DNS)

Los servidores del servicio de nombre de dominio brindan la traducción de nombres, como www.avaya.com, a la dirección IP del dominio necesario para establecer una conexión. IP Office ofrece este servicio a las PC de la red mediante proxy.

Servicios LAN/WAN

IP500 V2 admite un conmutador Ethernet de nivel 3 y 2 puertos con firewall.

Cuando se comunican las computadoras en la LAN, no tienen en cuenta cuál es el destino, solo envían mensajes con la dirección del mismo. Es muy probable que estos mensajes se reciban en el resto de computadoras de la misma red, pero solo una (el destino objetivo) actuará sobre el mensaje. Cuando el destino está en otra red, se necesita el enrutador como "puerta de enlace" hacia el resto del mundo, para encontrar la ruta óptima por la que enviar el mensaje hasta su destino. El enrutador satisface la necesidad de establecer y mantener una llamada durante una sesión de comunicación (cuando los mensajes o los paquetes IP se envían entre origen y destino) mediante una conexión automática solo cuando se van a pasar los datos. Los enrutadores se pueden conectar juntos mediante enlaces WAN (red de área extensa) que podrían ser líneas punto a punto concedidas, redes IP administradas, redes de Frame Relay o líneas de intercambio (oficina central). El sistema IP Office admite todos estos tipos de conexiones de red.

IP Office posee un enrutador integral con compatibilidad para ancho de banda a demanda que permite la negociación de un ancho de banda adicional dinámicamente con el tiempo. Si la conexión es mediante ISDN, IP Office inicia conexiones de datos adicionales entre sitios solo si hay datos para enviar o datos suficientes para garantizar canales adicionales. Luego, desconecta los canales adicionales que no se necesitan. Las llamadas se realizan en forma automática, sin que los usuarios sepan cuándo comienzan o finalizan. Las normas para realizar llamadas, el tiempo de mantenimiento de las mismas, etc., se configuran en IP Office.

Se pueden tener varios destinos o rutas de desvío diferentes activos en cualquier momento que conectan la oficina con las otras oficinas e Internet simultáneamente.

Enrutamiento LAN a LAN

En la actualidad, todos los negocios necesitan enviar datos ya sea como requisito para compartir los recursos, como servidores de correo electrónico, servidores de archivo y puertas de enlace de Internet, o para transportar sin problemas los datos entre sitios o redes desde y hacia sus clientes y proveedores. Es por eso que todas las plataformas de IP Office ofrecen el enrutamiento IP como estándar.

Integrar un enrutador con IP Office elimina los costos, la complejidad y los puntos de falla adicionales de los multiplexores WAN externos y se permite que el tráfico de voz y los datos reúnan y compartan los recursos de la red de IP Office. Estos recursos de red pueden variar según las conexiones ISDN de marcado, los circuitos punto a punto concedidos, las redes IP administradas o Frame Relay, ya que IP Office admite todos estos tipos de conexiones de red.

Conmutador integral de Ethernet de nivel 3 y 10/100 Mbit

La conmutación de capa 3 es de particular utilidad en situaciones donde se desea una red "confiable" e "insegura", donde la red "insegura" no está controlada y lleva el tráfico público.

Es posible configurar un firewall entre dos segmentos LAN mediante el conmutador de capa 3 de IP Office. IP500 V2 admite un conmutador Ethernet de capa 3 y dos puertos con el firewall

entre ellos. Ambos puertos conmutados tienen sus propias direcciones IP (LAN1 y LAN2) y para que el tráfico pase de un puerto al otro, se configura una ruta en las tablas de enrutamiento del sistema.

Compatibilidad de línea concedida

IP Office se puede conectar con los servicios de línea concedidas.

Los servicios WAN de IP Office se admiten mediante las líneas troncales PRI E1/T1 y las líneas troncales BRI. Las líneas troncales E1/T1 se pueden configurar a fin de operar en un modo fraccional para las aplicaciones "de punto a multipunto"; es decir, una interfaz 2M simple puede ser tratada como 3 x 512K y 8 x 64K que va a 11 diferentes ubicaciones. Al usar T1 como línea concedida es posible usar el mismo circuito para los servicios de circuito conmutados. No todos los tipos de línea concedida están disponibles en todos los territorios, consulte por la disponibilidad.

Servidor de acceso remoto

IP Office brinda la funcionalidad servidor de acceso remoto (RAS) que permite a los usuarios externos realizar una marcación entrante en una red de área local desde módems, adaptadores de teléfonos y enrutadores.

Varias de las funciones y servicios descriptos anteriormente se pueden aplicar a los usuarios de marcación entrante para crear un poderoso servidor de acceso remoto. Los usuarios de marcación entrante se pueden autenticar mediante PAP o CHAP. Una vez autenticado, el servidor DHCP puede asignarle al usuario en forma automática una dirección IP para usar mientras está conectado a LAN. Los perfiles de horario individuales y firewalls se pueden aplicar al usuario para restringir a qué tiene acceso y cuándo tiene acceso. Para mayor seguridad y facilidad de contabilidad, IP Office puede volver a llamar a un usuario en forma automática. Esto mantiene el costo de la llamada telefónica en la factura de teléfono de la empresa y se elimina la necesidad de procesar reclamos de gastos individuales.

Acceso remoto de SSL/VPN

El acceso remoto de SSL/VPN brinda a Avaya y sus socios acceso remoto confiable que mejora la provisión de servicios y, a la vez, reduce el costo asociado con el despacho de unidades de servicio. La solución permite que los socios de cualquier tamaño creen una infraestructura que automatice la administración y el mantenimiento de los sistemas IP Office.

El software IP Office incluye un cliente SSL/VPN integrado. Por parte del servidor (si el socio decide alojar el servidor), el socio deberá instalar un servidor (VM) y el software Avaya VPN Gateway (AVG). El socio establecerá la configuración de puerta de enlace SSL/VPN en IP Office; de este modo IP Office desencadenará un túnel de seguridad de vuelta a la puerta de enlace.

Se configura nombre de usuario/contraseña durante el paso de configuración por cuestiones de seguridad. También se proporciona un segundo nivel de seguridad con un certificado de autenticación del servidor. Después, un servidor RADIUS validará el nombre de usuario/ contraseña ante la solicitud de conexión iniciada desde IP Office. Una vez validadas las credenciales, se establece el acceso remoto seguro.

Como mínimo, el socio debe asegurar que hay una conexión de ancho de banda disponible en el sitio del cliente. Un socio que decide alojar el servidor puede comprar (a la escala que le convenga) las licencias SSL/VPN según cuántas conexiones simultáneas se requieran. Se instala el software AVG en un software servidor VM (el socio puede elegir el servidor de su

preferencia) y configura un servidor RADIUS para la autenticación del nombre de usuario/contraseña. El mismo servidor VM puede también actuar como un servidor RADIUS o el socio puede utilizar un servidor RADIUS por separado o reutilizar un servidor RADIUS existente según las recomendaciones del departamento de TI y las políticas de seguridad.

Los socios que deseen alojar el servidor de la puerta de enlace se deben dirigir al portal para empresas de Avaya para obtener mayor información sobre la solución Avaya VPN Gateway (consulte https://enterpriseportal.avaya.com/ptlWeb/gs/products/P0623/AllCollateral).

El acceso remoto de SSL/VPN brinda la siguiente funcionalidad:

- Acceso remoto seguro a velocidades de banda ancha para soporte mejorado
- Implementación y configuración simples
- Escalamiento para ajustar futuros requisitos de crecimiento
- No se requiere un gran conocimiento sobre conexiones de red en el sitio del cliente (no se requiere administrador TI en el sitio del cliente)
- No es necesario abrir agujeros en el firewall (firewall agnóstico cuando se inicia la conexión desde el sitio de los clientes a la puerta de enlace)
- La conexión puede estar “siempre ENCENDIDA” o se puede iniciar mediante la marcación o mediante el teléfono.
- Facilitación de configuraciones, administración, monitoreo, diagnósticos y actualizaciones remotos.

Funciones del teléfono

Tono de alerta/timbre para llamadas cubiertas

Los usuarios pueden elegir la forma en la que sonará la llamada y configurar un sonido de alerta con volumen bajo en oficinas con diseño de espacio abierto.

Es posible configurar la señal de alerta (tono de timbre) para las llamadas entrantes de teléfonos cubiertos con los siguientes valores:

- Timbre (predeterminado)
- Timbre abreviado
- Sin timbre

Botones, teclas y luces

IP Officeadmite hasta 10 botones en cada teléfono y 10 teléfonos con la misma apariencia de línea.

Las funciones de teclas y luces requieren un teléfono con botones e indicadores y ciertos teléfonos IP digitales de Avaya. El funcionamiento de teclas y luces no es compatible con los teléfonos análogos. Es posible configurar una demora de timbre en cada botón de apariencia

para darle tiempo al número de destino que responda antes de otro timbre de extensiones o una alerta visual solamente sin timbre.

Botones programables

Los teléfonos IP y digitales poseen botones de función dedicada para silenciar, ajustar volumen, colocar llamada en espera, realizar conferencias y transferencias. En muchos teléfonos IP y digitales, los administradores pueden programar los botones y las teclas con diferentes funciones especiales.

Estos botones se utilizan para llamar a otras extensiones del sistema o para configurar otras opciones, como números de marcación rápida y función de no molestar. Muchas funciones usan un indicador para mostrar si la función está activada. Los ingenieros de implementación pueden programar botones en la configuración del sistema, aunque algunos teléfonos le permiten al usuario programar botones y funciones cuando los derechos de administración así lo permitan.

Para obtener más información, consulte *Referencia de acción de botones y código corto de Avaya IP Office™ Platform*.

Botones de apariencia

Muchos teléfonos IP y digitales de Avaya cuentan con botones programables. Es posible asignar funciones de apariencia a estos botones que permiten la administración de llamadas.

Utilice los botones programables disponibles en los teléfonos digitales e IP de Avaya para representar llamadas individuales. Responda e inicie llamadas, o únase a ellas, mediante los botones de apariencia adecuados. Los botones de apariencia del teléfono indican llamadas conectadas y llamadas en espera. Esta función le permite al usuario administrar varias llamadas desde un único teléfono.

Botones de apariencia de línea

La apariencia de línea muestra los usuarios que realizan y responden llamadas en una cierta línea troncal externa.

Los botones de apariencia de línea muestra el uso de una línea troncal del sistema y realiza un seguimiento de la actividad en la línea. Sólo las llamadas externas se pueden responder o hacer llamadas en las apariencias de líneas. Las apariencias de línea se pueden usar con las líneas troncales analógicas, E1 PRI, T1 PRI, BRI y PSTN. No se pueden usar con las líneas troncales E1R2, Q.SIG e IP.

Botones de apariencia de llamada

Los botones de apariencia de línea le permite a un usuario realizar, responder y alternar entre múltiples llamadas mediante el botón de apariencia de llamada adecuado para cada llamada.

En teléfonos IP y digitales que cuentan con botones programables, es posible configurarlos como botones de apariencia de llamada mediante IP Office Manager. El número de botones de apariencia de llamada configurados para un usuario determina el número de llamadas simultáneas que puede realizar o responder. Si se utilizan todos los botones de apariencia de llamada, se recomienda un mínimo de tres botones de apariencia de llamada cuando sea posible, si bien algunos teléfonos están limitados a dos botones de línea de llamada por el número o el diseño de sus botones programables. Cuando sea posible, el estado de las llamadas (entrantes, conectadas o en espera) se indica mediante el indicador del botón.

Nota:

Tenga en cuenta que el uso de botones de apariencia de llamada sustituye a las funciones de llamado en espera. Sólo cuando todas las apariencias de llamada están en uso las siguientes personas que llaman reciben un tono de ocupación, un correo de voz o siguen una acción de reenviar por ocupado.

Botones de apariencia en puente

Los botones de apariencia en puente le permiten al usuario tener un botón de apariencia que corresponda con el botón de apariencia de llamada de otro usuario.

El botón de apariencia en puente le permite a un usuario realizar y responder llamadas en nombre de otro usuario de la vista de llamada. Se presenta una indicación audible de las llamadas al usuario en puente, si está programada. El botón brinda una indicación visual de cuándo el otro usuario tiene llamadas presentes, en espera o conectadas. Unión e intercambio de llamadas con los botones emparejados de línea de llamada y de línea en puente.

Por ejemplo, cuando el botón de apariencia de llamada de un usuario muestra una llamada entrante, el botón de apariencia en puente también mostrará la llamada entrante y se puede usar para responder a la llamada. De forma similar, si un usuario utiliza el botón de apariencia en puente se usa para realizar una llamada, la actividad de la llamada se muestra en el botón de línea de llamada correspondiente. El usuario del botón de apariencia de llamada se puede unir a la llamada o responderla con su botón de apariencia de llamada.

Los botones de apariencia en puente permiten el funcionamiento emparejado estilo “jefe/secretario” entre dos usuarios y solo se admite para los usuarios que tienen botones de línea de llamada.

Botones de cobertura de llamada

Los botones de cobertura de llamada permiten la recepción de alertas de las llamadas no respondidas en las extensiones de otros usuarios para que sean respondidas antes de reenviarlas o de enviarlas al correo de voz.

Los botones de cobertura de llamada le permiten al usuario responder la llamada no respondida de un colega antes de enviarlas al correo de voz. Cuando un usuario tiene una llamada entrante no respondida, después de un retraso configurable, la llamada comienza a alertarse en los botones de cobertura de llamada asociados al usuario en otras extensiones. otro usuario puede responder la llamada mediante un botón de cobertura de llamada. Si la llamada queda sin responder, la llamada se reenvía o se envía al correo de voz.

Es posible ajustar el período que una llamada queda sin responder hasta que comienza a alertar en un botón de cobertura de llamada.

Botones de acceso múltiple a números del directorio

La tecla de acceso múltiple a números del directorio (MADN) es una tecla y una función de lámpara que permite al usuario contar con varias apariciones de un número del directorio. Los usuarios pueden tener hasta treinta apariciones del mismo número del directorio. Para usar las características de MADN en el entorno de IP Office, el número de MADN debe configurarse como uno de los números del usuario.

Disposición de llamada única (SCA) MADN

- Uno o más usuarios pueden tener el número del directorio.

- Las llamadas emiten una alerta para todos los botones configurados con el número del directorio, y cualquier usuario puede responder la llamada con ese botón.
- Un usuario puede hacer una llamada saliente cuando el número del directorio está inactivo. Los detalles de la persona que llama serán el nombre y el número del botón seleccionado.
- Cuando el número del directorio esté en uso, los demás usuarios con la aparición del botón verán que el número está ocupado.
- Los usuarios pueden unirse a llamadas con configuración de privacidad.

Disposición de llamadas múltiples (MCA) MADN

- Uno o más usuarios pueden tener el número del directorio.
- Las llamadas emiten una alerta para todos los botones configurados con ese número del directorio, y cualquier usuario puede responder la llamada con ese botón. Después de que se responde la llamada, todos los demás usuarios ven que el número queda inactivo.
- Cuando el número del directorio está inactivo, el usuario puede seleccionar el botón para hacer una llamada saliente. Los detalles de la persona que llama serán el nombre de usuario y el número de directorio del botón seleccionado.

Nota:

La función MADN es compatible solamente en equipos con botones, y no en teléfonos analógicos ni DECT.

Indicadores de campo de luz de ocupado

Los indicadores de campo de luz de ocupado (BLF) muestran cuando un botón o función asociada está activa.

Los teléfonos digitales e IP cuentan con botones programables que se pueden asignar a varias funciones. Cuando esos botones incluyen alguna forma de indicador BLF, también se pueden usar para indicar cuándo está activa la función. Por ejemplo, un botón asociado a otro usuario indicará cuándo ese usuario está activo en una llamada. Un botón asociado a un grupo indicará cuándo el grupo tiene llamadas en espera de respuesta.

Las entradas de directorio y los iconos de marcación rápida en las aplicaciones Phone Manager y SoftConsole también funcionan como BLF. Cuando los iconos se asocian con usuarios internos, los íconos se cambiarán para indicar el estado actual de los usuarios.

Avaya one-X® Portal for IP Officemuestra estas condiciones:

Texto o ícono	Estado	Descripción
`available`	Disponible	Está disponible y puede recibir llamadas.
	Ocupado	Tiene una llamada entrante.
	No molestar	Tiene activa la función no molestar en el sistema telefónico. Las llamadas que reciba se redirigirán al correo de voz, si está disponible. Si no lo está, las personas que llamen oirán un tono de ocupado. La excepción son las llamadas de números que haya agregado a la lista de excepciones de la función no molestar.

La tabla continúa…

Texto o ícono	Estado	Descripción
	Desconectado	No ha iniciado sesión en la extensión del sistema telefónico. Las llamadas que reciba se redirigirán al correo de voz, si está disponible. Si no lo está, las personas que llamen oirán un tono de ocupado. No puede realizar llamadas. Sin embargo, aún puede usar para modificar la configuración.
	Sonando	El teléfono está sonando y tiene una llamada entrante.
`unknown`	Desconocido	Se desconoce su presencia en el sistema telefónico. No es posible identificar la presencia debido ya que el número no es una extensión del sistema.

Luces de llamada externa

Los usuarios pueden determinar si las llamadas cubiertas son externas o internas en el patrón del indicador.

Los usuarios pueden seleccionar el patrón de luces para llamadas externas en botones de apariencia de cobertura y en puente.

Luces de espera de mensaje

IP Officeutiliza la indicación de mensaje en espera (MWI) para establecer una luz u otra indicación en los teléfonos cuando se dejó un nuevo mensaje para el usuario, ya sea en un buzón de correo de voz personal o en un buzón de correo de voz de grupo o un mensaje de devolución de llamada. Luego de que el sistema reproduce el mensaje, la luz se apaga.

Todos los teléfonos IP y digitales cuentan con indicadores de mensaje en espera incorporados. Avaya one-X® Portal for IP Office brinda una indicación de mensaje en espera en la pantalla.

En los teléfonos analógicos, IP Office admite diferentes métodos de indicación de mensaje en espera analógicos (MWI).

- 51 V escalonado
- 81 V
- 101 V
- Inversión de línea

El administrador o instalador del sistema selecciona el método de MWI mediante IP Office Manager durante su configuración para que coincidan las propiedades de los teléfonos analógicos.

Nota:

La señalización 101 V sólo se encuentra disponible en tarjetas de módulos de expansión y teléfonos IP500.

Historial de llamadas

IP Office guarda un registro de las llamadas realizadas y recibidas, incluidas aquellas que no fueron respondidas. Se guardan los detalles de ambos usuarios (30 entradas como máximo) y de los grupos de búsqueda (10 entradas como máximo). El método de operación varía según

el tipo de teléfono, pero en todos los casos, los registros de llamadas se pueden usar para devolver llamadas.

El historial de llamadas puede mostrar información sobre todas las llamadas: llamadas perdidas, entrantes y salientes. Las entradas del historial de llamadas se pueden usar para devolver llamadas; se pueden ordenar y agregar al directorio local o a los números de marcado rápido. La información del registro de llamadas se guarda incluso después de desconectar y reiniciar el sistema. Se admite un registro de llamadas centralizado en la SCN cuando se utiliza la función uso compartido de escritorio para mantener consistencia entre teléfonos de escritorio y aplicaciones de productividad para el usuario. Las entradas del registro de llamadas se pueden agregar al directorio personal.

Identificador de llamada

Si el proveedor de servicios brinda un identificador de llamada, IP Office envía la llamada a la aplicación o teléfono que conteste y la ingresa en el registro o historial de llamadas admitido. Si el identificador de llamada reconoce el número porque está en el directorio, IP Office muestra el nombre del directorio que corresponda.

Si el servicio de IP Office Phone Manager o TAPI se conecta con una base de datos, IP Office realiza una consulta automática en el identificador de llamada provisto y muestra el registro del participante que llama antes de que la llamada sea atendida.

Para las llamadas salientes, IP Office puede insertar un identificador de llamada en todo el sistema o configurar un indicador que retenga el identificador de llamada. Para usuarios que posean un número de marcación directa desviado a su extensión, IP Office utiliza ese número como identificador para las llamadas salientes. De forma alternativa, IP Office puede usar códigos abreviados para especificar el identificador del participante que llama que se debería enviar con las llamadas salientes.

Nota:

Tenga en cuenta que el envío y la recepción del identificador del participante que llama está sujeto al proveedor que brinda ese servicio. El proveedor del servicio también puede restringir los números que se pueden usar para el identificador de las llamadas salientes.

Directorio personal centralizado

El directorio personal es una lista de hasta 100 números y nombres asociados almacenados en el sistema central de un usuario específico. Se puede usar una entrada del directorio para etiquetar una llamada entrante en la pantalla del identificador de llamada del teléfono o en una aplicación de PC. El directorio también aporta una lista de los números marcados con más frecuencia en todo el sistema para agregarlos a la marcación rápida.

Por ejemplo, “Sr. Martínez” puede aparecer cuando se recibe el identificador de un participante conocido que llama. El usuario también puede seleccionar **Sr. Martínez** desde la lista del directorio de Phone Manager, o desde un teléfono con pantalla para marcar rápidamente este número. Mediante Manager, un teléfono o un servicio externo, es posible agregar, eliminar o modificar todas las entradas. Los datos del directorio personal se envían/actualizan siempre que el usuario está conectado en un SCN.

Idioma

Los menús y pantallas de los teléfonos digitales de Avaya y los teléfonos IP están disponibles en muchos idiomas y generalmente la configuración de valores predeterminados del sistema se aplicará a todos los teléfonos; sin embargo, pueden haber idiomas establecidos según la extensión, esto también cambiará el idioma de los menús para IP Office Voicemail.

Marcación con teléfono colgado

Los teléfonos IP y digitales de Avaya le permiten al usuario hacer llamadas con solo marcar el número en el teclado, sin tener que descolgar el teléfono o presionar el botón del altavoz. Generalmente, es posible supervisar el progreso de la llamada con el altavoz en el teléfono, en los teléfonos que admiten la función de manos libre se puede supervisar toda la conversación sin tener que descolgar el teléfono.

Autoadministración

El administrador de IP Office puede darles a los usuarios seleccionados la habilidad de cambiar algunas configuraciones del teléfono. El rango de cambios que el usuario puede hacer depende del tipo de teléfono en uso.

Correo de voz visual

Los usuarios pueden tener acceso y controlar los mensajes de voz mediante la pantalla del teléfono digital o IP. El correo de voz visual funciona con Preferred o Essential Edition, y sólo se puede utilizar con equipos con pantalla grandes de LCD de la serie 1400, 1600, 2400, 5400, 4600, 5600, 9500, 9600 y T3. (1403, 1603, 1603SW, 2402, 5402, 4601, 4602SW, 5601, 5602SW no son compatibles con correo de voz visual).

En teléfonos que tienen pantalla, pero que no son compatibles con la función de correo de voz visual, se admite el uso del botón para acceder al buzón del usuario con indicaciones habladas y para transferir la llamada directamente al correo de voz (no incluye teléfonos T3 ni IP T3).

El correo de voz visual permite a los usuarios realizar las siguientes tareas:

- acceder a mensajes nuevos, antiguos y grabados en buzones de correo personales y de grupo
- mensaje anterior y siguiente
- avanzar y retroceder
- Pausar mensaje
- guardar, eliminar y copiar los mensajes a otros usuarios del sistema
- cambiar el saludo predefinido

- cambiar contraseña
- cambiar la configuración de correo electrónico (sólo en Preferred Edition).

Capítulo 4: Aplicaciones

Aplicaciones de usuario

Las siguientes secciones brindan descripción general sobre las aplicaciones destinadas a usuarios finales.

Avaya one-X® Mobile

Avaya one-X® Mobilees una aplicación que utilizan los usuarios móviles para conectarse a IP Office.

Avaya one-X® Mobilefunciona en el modo de telefonía de devolución de llamadas. Por ejemplo, cuando un usuario inicia una llamada del cliente, IP Office inicia una llamada al dispositivo móvil del participante y luego marca el destino. Este modo ofrece un ahorro en el costo para los usuarios de países en los que las llamadas de voz entrantes son gratis o para usuarios que gozan de un plan de voz ilimitado más económico en comparación con un plan de datos.

El cliente de movilidad one-X Mobile Preferred también funciona en el modo voz a través de IP (VoIP). En el modo VoIP, el cliente de movilidad puede realizar llamadas en redes de datos Wi-Fi/3G/4G. El cliente, mediante la pila IP subyacente, se registra con IP Office mediante la red de datos y funciones como la extensión de oficina.

Los usuarios que se encuentran en países en los que se cobran las llamadas entrantes notarán un ahorro significativo en el modo VoIP especialmente en redes Wi-Fi. La disponibilidad de los modos de devolución de llamada y VoIP del cliente de movilidad les permite a los usuarios alternar entre estos modos en función de sus conexiones de red. Esto les da la posibilidad a los usuarios finales de elegir el modo conveniente según su plan de voz o datos así como la disponibilidad y la calidad de la conexión de datos (WiFi/3G/4G). Por ejemplo,

- El usuario puede seleccionar el modo de devolución de llamada cuando no tenga acceso Wi-Fi y la conexión de datos 3G no brinde la calidad suficiente para voz.
- El usuario puede seleccionar el modo VoIP cuando tenga acceso a un punto de acceso móvil en donde haya disponible una conexión de datos Wi-Fi o cuando la conexión de datos 3G o 4G sea buena.

Un cliente de movilidad one-X Mobile Preferred admite el modo VoIP en dispositivos iOS y Android. El modo VoIP está disponible con el perfil Power User. Los usuarios con perfiles Mobile Worker sólo pueden utilizar el modo de devolución de llamada. El modo VoIP no requiere una licencia de terminales IP. Se encuentran disponibles los siguientes funciones:

- Selección de tono de timbre

Página359 de 3226.

- Selección de códec de ancho de banda o banda estrecha elevada según la disponibilidad de la conexión de red
- Control de audio con auricular con Bluetooth para llamadas VoIP
- Pantalla de conferencia
- Selección de número telefónico de contacto
- Indicador de prioridad del correo de voz
- Soporte de arrastre para mensajería instantánea en la pantalla principal
- Admite acción en grupo
- Emoticones
- Consultar CLID entre los contactos para llamadas
- Enviar correo de voz como archivo WAV en correo electrónico
- Activar o desactivar hermanamiento móvil (timbre simultáneo)
- Activar o desactivar DND (enviar todas las llamadas)
- Registro de llamadas combinado con correos de voz en el historial de eventos
- Supervisión de llamadas para observar e interactuar con todas las llamadas
- Plan de marcación en modo VoIP
- Transferir llamadas como controlador de llamadas externo (3PCC)

Avaya one-X® Portal for IP Office

Avaya one-X® Portal for IP Office provides users control of their telephone from a networked PC. Use this application with any extension; analog, digital or any IP telephone, wired or wireless, that is available as part of the Office Worker, Power User or Teleworker user licenses.

Avaya one-X® Portal for IP Office is a server-based application that the user accesses via web browser.

For Telecommuter mode, One-X applications require answer supervision and disconnect detection for proper functioning. As a result, the one-X applications will not work with trunks that do not support answer supervision and disconnect detection.

Nota:

one-X applications function on trunk types such as PRI, BRI, and SIP, however, they will not function on E1R2, T1 RBS and analog loop start trunks.

System administrators can control if Avaya one-X® Portal for IP Office can be accessed over a secure protocol only, recommended for hosted deployments to provide “secure only” access. The other option is to allow users to access the client over a secure and unsecure protocol (HTTP/HTTPS). The client application forces users to change their passwords and voicemail passcodes to meet the complexity settings configured by the administrator.

Through gadgets, Avaya one-X® Portal for IP Office provides the following features:

- Call information

- Call and conference control
- Presence and instant messaging notifications, monitoring and archiving
- Contact import and export
- XMPP groups displayed in the **System Directory** tab
- Support for User Avatar on Avaya one-X® Portal web client **System Directory** tab
- Dial to user's own bridge and invite other users to join
- Conference call and other meeting scheduling including port reservations, email support and automatic report creation — available within the Outlook interface
- One-click web conferencing hosting and single sign-on joining web conferences as a participant
- Display number of **Logged in Sessions** on Avaya one-X® Portal administrator dashboard under User Details section. This shows the number of clients a user is currently logged in. Detailed information on the Logged in sessions is displayed on the Avaya one-X® Portal under Health/Active sessions tab.
- Option to block client versions under configuration.
- Option to clear all sessions for a user.
- Option to track repeated failed login attempts.

Avaya Equinox™ for IP Office

Avaya Equinox™ for IP Office is a SIP-based Unified Communications (UC) client that provides users with real time collaboration capabilities and enables business users to easily manage their day-to-day communications from a single interface. IP Office supports the following operating systems:

- Desktop:
  - Windows
  - macOS
- Mobile phone:
  - Android
  - iOS

Avaya Equinox™ is a common cross-platform client. The client capabilities vary depending on the platform it is registered with. The supported features in Avaya Equinox™ for IP Office in Release 11.0 FP4 are:

- Top of Mind Home Screen
  - Next meetings showing local calendar schedule or Exchange Web Service/Office 365
  - Local Call History
  - Messages
  - Start Meetings/Launch Spaces dashboard
- Top of Mind Lite Option for Mobile phones

- IP Office directory and local contacts
- Messaging through Avaya Spaces
- Presence through IP Office server
- Local call history
- Dialpad with Redial
- Desktop integration with Microsoft Outlook and Browsers
- Softphone client audio and video calls

Avaya Equinox™ registers with IP Office server as a SIP softphone for audio and video calling, and telephony features. However, the client cannot control an associated IP Office deskphone. The following features are supported:

- Point to point audio and video calls (make, receive, and end)
- Multiple call handling (incoming and outgoing)
- Hold and retrieve (audio and video calls)
- Transfer (blind and consultative)
- Consult conferencing
- Escalate audio to video call
- Shared control
- Avaya Equinox™ on Avaya Vantage™
- Presence and directory integration with Avaya Equinox™ on Avaya Vantage™
- Enter DTMFs during a call

Avaya IP Office Web Client

Avaya IP Office Web Client es una aplicación WebRTC que brinda varias capacidades de comunicación. El cliente aprovecha las mejoras de resistencia de la Puerta de enlace WebRTC que se ofrecen en la versión R11.0 y es compatible tanto con Server Edition como con IP500 V2. Los usuarios deben tener licencia Office Worker o Power User para utilizar las funciones de Avaya IP Office Web Client. El cliente se admite en los siguientes entornos:

- Navegadores de Google Chrome en sistema operativo Windows
- Navegadores de Google Chrome en macOS
- Cliente autónomo en sistema operativo Windows

Avaya IP Office Web Client proporciona las siguientes funciones:

- Lamadas de audio y video de punto a punto
- Acceso a Acceso a correo de voz
- Registros de llamadas
- Conferencias:
  - Conferencia Ad-hoc uniendo llamadas
  - Iniciar o unirse a una Conferencia Meet Me de IP Office
  - Cómo acceder a IP Office Web Collaboration

- Presencia y mensajería instantánea punto a punto integrándose con Avaya one-X® Portal for IP Office
- Clic-para-llamar usando la extensión de Google Chrome
- Compatibilidad de Single-Sign-On (SSO) en Avaya one-X® Portal for IP Office y IP Office Web Collaboration
- Favoritos y directorio de sistema (Directorio personal)

Avaya Communicator

Avaya Communicatores un cliente de software en colaboración que proporciona una innovadora interfaz para comunicaciones en tiempo real para Windows y en el iPad. Permite que el usuario administre llamadas telefónicas, mensajes instantáneos, conferencias, colaboración web, presencia, contactos de la empresa y correo electrónico, todo desde una interfaz única. Avaya Communicator brinda un diseño gráfico intuitivo con novedades, menú de medios, barra de notificación y tarjetas de contacto.

Avaya Communicatorpara IP Office se comunica con IP Office y Avaya one-X® Portal para proporcionar funciones de comunicación y colaboración. Las funciones de telefonía, tal como hacer/recibir llamadas, retener/liberar, silenciar/desactivar silencio, DTMF, MWI, etc., las proporciona IP500 V2, y las funciones UC, por ejemplo mensajería instantánea (MI), presencia y contactos de la empresa las proporciona el servidor Avaya one-X® Portal.

Si el servidor Avaya one-X® Portal no está disponible, debido a una restricción de licencia o por problemas de conectividad, el cliente Avaya Communicator trabajará en un modo sólo telefonía que proporciona únicamente funciones de telefonía. La interoperabilidad con Avaya Session Border Controller for Enterprise le permite a los usuarios con el perfil Remote Worker utilizar el cliente Flare Communicator y registrarse con IP Office sin necesidad de contar con una conexión VPN.

Avaya Communicator proporciona las siguientes funciones:

- Agregar participantes mediante un panel de marcación o la función arrastrar y colocar
- Silenciar y desactivar el silencio todos los participantes o un subconjunto de ellos
- Bloquear o desbloquear la conferencia
- Colocar la conferencia en modo lectura
- Activar y desactivar los tonos de entrada y salida de audio
- Excluir a todos o algunos de los participantes de una conferencia
- Finalizar la conferencia
- Activar y desactivar la continuación para permitir que la conferencia continúe después que se desconecte el moderador.
- Promover participantes a moderador
- Crear conferencias ad hoc mediante la fusión de llamadas P2P
- Códigos de cuenta y autorización (sólo Windows)
- Recordatorio de tiempo de espera (sólo Windows)
- Experiencia del usuario compacto

- Compatibilidad con TSL/SRTP
- Filtrado de contactos
- Integración de conferencia web
- Transferencia sin supervisión
- Respuesta automática
- Modo simultáneo
- Cambio de contraseña
- Códigos de cuenta
- Auto configuración (sólo iOS)
- Selección y compatibilidad de dispositivo auricular con Bluetooth (sólo iOS)
- Interoperabilidad con Scopia (Radvision XT5000)

Nota:

Avaya Communicatorno admite indicador de parlante activo y grabación.

Avaya Communicatorpara iPad

Avaya Communicator para iPad integra voz, video, presencia, mensajería instantánea y directorios en una interfaz unificada mediante conexiones VPN, 3G o Wi-Fi.

Avaya Communicatores una solución sólo software que se puede descargar muy fácilmente desde Apple iTunes Store y es compatible con iPad2, iPad3, iPad4, iPad Mini (con o sin pantalla retina), iPad Air modelos Wi-Fi y 3G y las siguientes versiones de iOS: 6.1.x, 7.0.x, 7.1.x y 8.0.x.

Nota:

Avaya Communicator no es compatible con iOS 6.0.x.

Con Avaya Communicator, los usuarios de IP Office pueden utilizar los dispositivos iPad para:

- Tener un acceso simple a herramientas de comunicación en tiempo real en las que confían día a día (teléfono, presencia, IM, etc.)
- Mezclar comunicaciones en tiempo real y procesos comerciales, por ejemplo las ventas móviles
- Aprovechar la conectividad de Wi-Fi y 3G para el ahorro en VoIP
- Señalización segura mediante TLS e intercambio seguro de medios mediante SRTP en entornos en la nube
- Como moderador de conferencias web, la posibilidad de compartir pizarras y documentos
- Cambio de contraseña
- Soporte para respuesta automática de llamadas
- Transferencia sin supervisión
- Servicio de autoconfiguración con un perfil de configuración alojado en un servidor web mediante correo electrónico o URL
- Selección y compatibilidad de dispositivo auricular con Bluetooth

- Búsqueda en el directorio del sistema
- Agregar/eliminar miembros de un equipo (Grupo XMPP)
- Buscar en el directorio del sistema y agregar a un equipo o a un contacto personal
- Compatibilidad con Radvision XT5000 para llamadas punto a punto

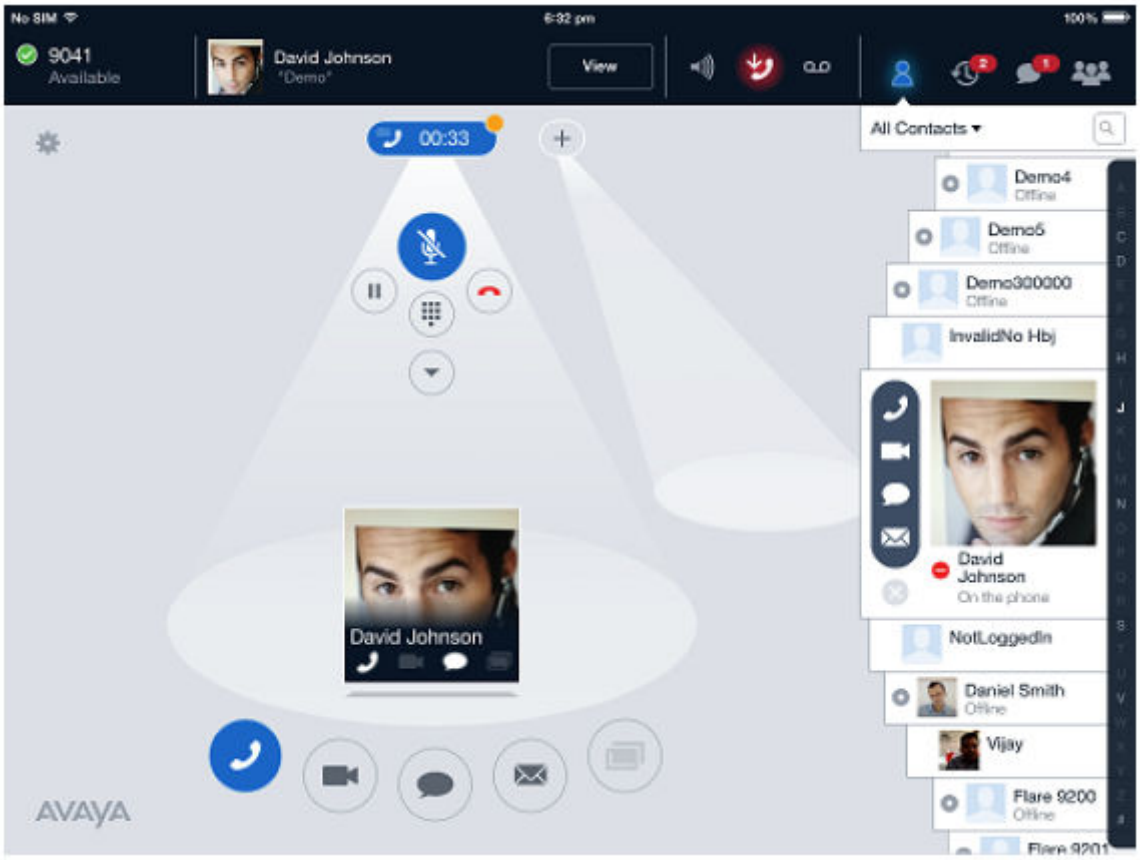


Figura 3: Avaya Communicatorpara iPad

Avaya Communicatorpara Windows

Avaya Communicator para Windows integra voz, presencia, MI y directorios en una oferta unificada para computadoras de escritorio y portátiles de Windows mediante una conexión LAN.

Avaya Communicator proporciona las siguientes funciones:

- Modo compacto que ocupa menos pantalla

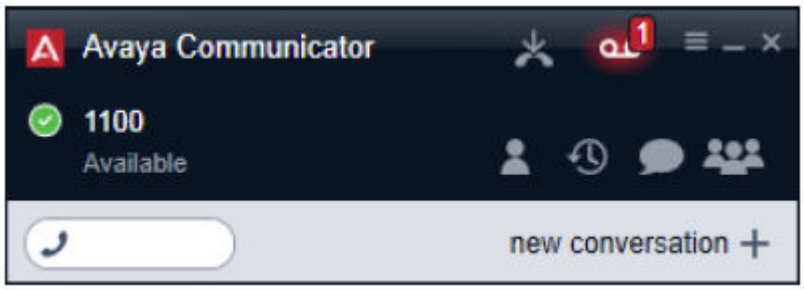


Figura 4: Vista compacta de Avaya Communicator para Windows

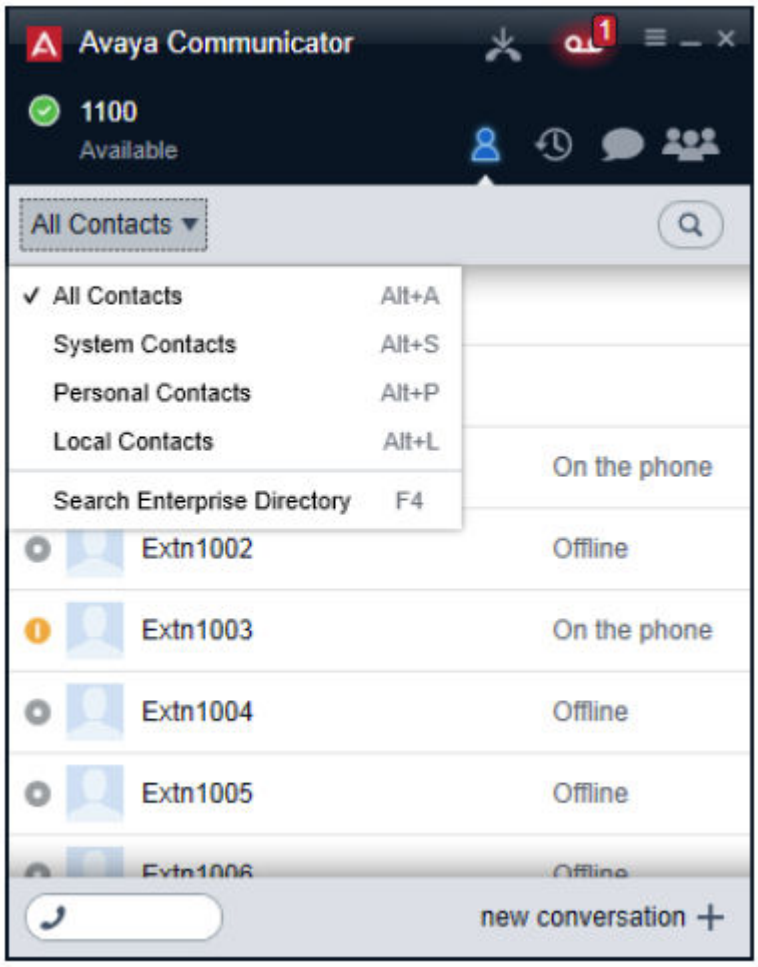


Figura 5: Vista completa de Avaya Communicator para Windows

- Señalización segura mediante TLS e intercambio seguro de medios mediante SRTP en entornos en la nube
- Filtrado de contactos según criterios y posibilidad de visualizar sólo contactos personales, locales o del sistema
- Integración de conferencia web
- Transferencia sin supervisión
- Respuesta automática
- Modo simultáneo para interfaces para one-X Portal, Outlook y Salesforce
- Cambio de contraseña.
- Códigos de cuenta

SoftConsole

SoftConsole es una aplicación basada en PC de Windows destinada a recepcionistas para IP Office. Puede adquirirla mediante una licencia de usuario Receptionist.

SoftConsole brinda a los recepcionistas y operadores empresariales información de llamadas y acciones de llamadas para simplificar la gestión de llamadas y la mensajería instantánea.

Con SoftConsole, los usuarios pueden ver el estado del resto de los usuarios y ajustar la configuración básica de telefonía del resto de los usuarios, por ejemplo los números de reenvío. Avaya recomienda utilizar teléfonos que admitan la función Respuesta automática. Los usuarios pueden utilizar la función de mensajería instantánea que proporciona Avaya one-X® Portal, si está disponible.

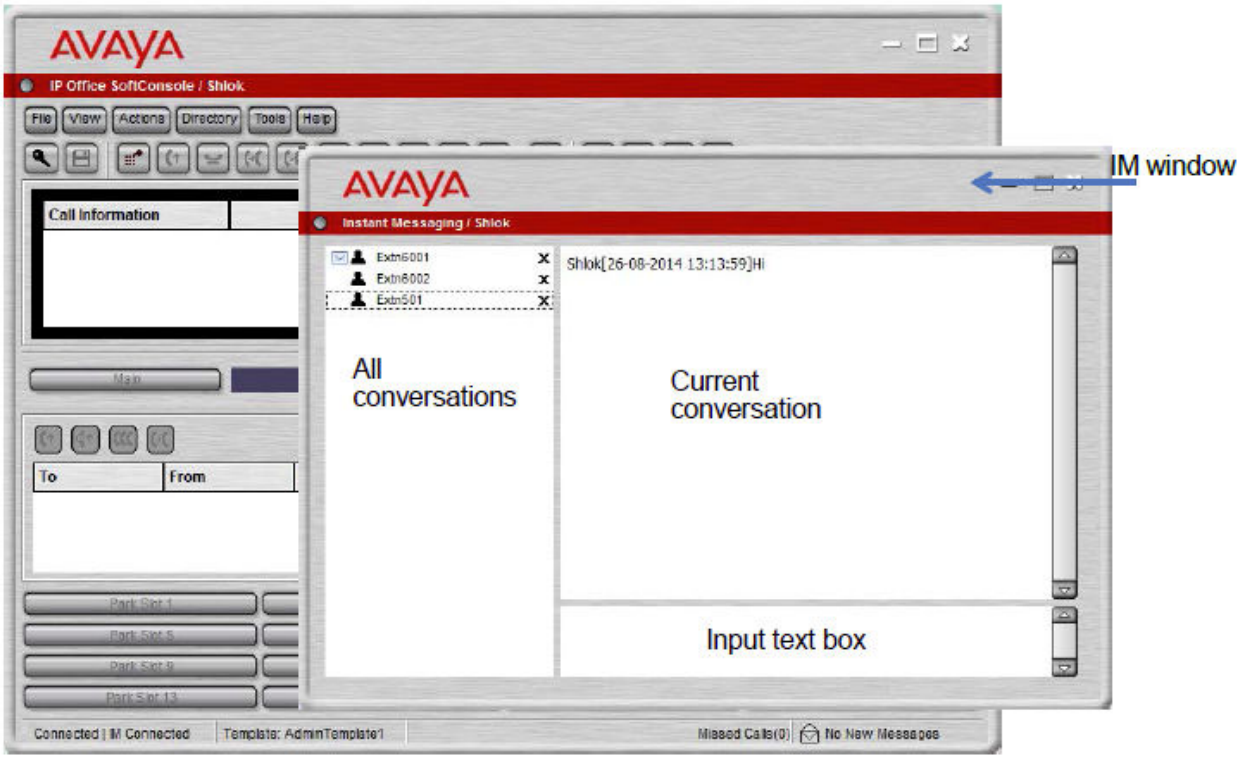


Figura 6: Venta de mensajería instantánea de SoftConsole

La comunicación WebSocket permite que los clientes SoftConsole se comuniquen con IP Office y Avaya one-X® Portal. El protocolo de WebSocket es bidireccional entre el cliente y el servidor. Dado que la comunicación se realiza mediante el puerto 80 o 443 (el mismo que se utiliza para HTTP), no se presentan inconvenientes con el cruce seguro de firewall. En un entorno hospedado, la comunicación mediante WebSocket brinda seguridad.

Es posible minimizar SoftConsole en la bandeja del sistema de Windows cuando no se utiliza, pero volverá a aparecer como ventana emergente cuando se reciba una llamada. Es posible asociar con las llamadas archivos de medios y de audio. Si se utiliza esta función, la PC requiere una tarjeta de sonido y parlantes.

SoftConsole admite las siguientes funciones:

- Contestar llamadas
- Realizar llamadas salientes
- Realizar transferencias con y sin supervisión
- Transferir llamadas al correo de voz
- Poner en espera y estacionar llamadas
- Supervisar colas y llamadas en cola
- Utilizar y observar salas de conferencia

- Poner en conferencia llamadas en espera
- Agregar usuarios a una conferencia
- Agregar texto a una llamada
- Abrir la puerta
- Intrusión
- Enviar de mensajes de texto
- Anuncio
- Grabar llamadas
- Enviar correos electrónicos
- Usar del teclado de marcación
- Seleccionar varios idiomas

Embedded Voicemail

En entornos como comercios u oficinas caseras,en donde el espacio, el ruido o los costos no permiten utilizar una PC para correos de voz, Embedded Voicemail brinda servicios básicos de correo de voz. Embedded Voicemail se ubica en la unidad de control IP500 V2 y no requiere un servidor aparte para correo de voz.

Embedded Voicemailes compatible con IP Office Essential Edition. No es necesario adquirir otras licencias.

Voicemail Pro

Voicemail Pro se proporciona con IP Office Preferred Edition y es una aplicación avanzada para administrar flujos de llamadas y mensajes en los sistemas IP Office. Voicemail Pro puede gestionar hasta 40 llamadas simultáneas (hasta 250/500 en Server Edition/Server Edition Select) según la licencia y la configuración del sistema. Los usuarios tienen la opción de activar o desactivar el correo de voz. Cuando está activado, el sistema responde el teléfono de forma automática cuando el usuario no puede contestar una llamada, reproduce un saludo personal y graba un mensaje.

Cuando se deja un mensaje, el usuario verá un indicador de mensaje en espera encendido en el teléfono y podrá presionar un botón de recuperación para reproducir los mensajes.

Voicemail Pro también puede llamar al usuario para brindarle mensajes nuevos. Los mensajes de correo de voz tienen la marca de fecha y hora, y el número de la persona que llamó queda registrado. Voicemail Pro se puede configurar para eliminar o leer mensajes automáticamente, a menos que el usuario elija guardarlos de forma permanente.

Es posible recopilar los correos de voz de forma remota al marcar en el servidor Voicemail Pro. Si se reconoce el número desde el que el usuario está llamando (por ejemplo, un número particular o teléfono móvil/celular), el usuario oirá los mensajes de correo de voz inmediatamente. Si el número que llama es desconocido, se solicitará al usuario que proporcione un número de buzón y un código PIN para ese buzón antes de oír los mensajes de correo de voz. Los usuarios pueden definir y modificar sus propios códigos PIN.

Cuando un correo de voz se debe reenviar a otros usuarios, Voicemail Pro proporciona una variedad de opciones:

- Los mensajes de correo de voz se pueden reenviar a otro buzón o a un grupo de buzones
- Los destinatarios pueden agregar sus comentarios al mensaje de correo de voz antes de reenviarlo a otro buzón o buzones.
- Los mensajes de correo de voz se pueden reenviar como archivo adjunto en formato .WAV.

Todas las opciones están disponibles en varios idiomas, tanto las indicaciones habladas como las interfaces de programación gráfica, e incluyen las opciones de IP Office TUI y emulación INTUITY TUI.

Conferencia

Los usuarios pueden colocar las llamadas en espera y crear una conferencia con el teléfono o aplicaciones del escritorio. Se pueden agregar miembros adicionales a la conferencia; no obstante, una sola conferencia no puede tener más de 64 miembros (con IP500 V2 solamente y más con Server Edition).

En el caso de conferencias ad hoc, el sistema requiere la misma cantidad de canales VoIP/ líneas troncales y participantes externos (así como sucede con Preferred Edition para conferencias Meet-Me). El sistema admite 128 canales de conferencia en e IP500 V2, lo que permite realizar varias conferencias de cualquier tamaño de entre 3 y 64 participantes. Así, el sistema admite 42 conferencias de 3 participantes, 2 conferencias de 64 participantes o cualquier combinación entre estas. La capacidad Meet-Me requiere Preferred Edition para marcación directa hacia un puente de conferencia con un código PIN de seguridad. En una SCN, sólo se requiere una licencia Preferred Edition centralizada para alojar conferencias Meet-Me en cualquiera de los sitios. Los identificadores de conferencia también se comparten a través de los sitios SCN.

Las siguientes capacidades de canal de conferencia están disponibles:

Tabla 2: Capacidades de canal de conferencia

Plataforma	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
HP DL120 Dell R210	128	128	414	414
HP DL360	256	256	825	825
Dell R620	256	512	825	825
OVA	256	512	825	825
IP500V2	128	128	128	128

Para iniciar una conferencia, los usuarios marcan el número directo asignado al puente de conferencia e ingresan el PIN (requiere Preferred Edition y Voicemail Pro), en caso que sea necesario. Para las conferencias ad hoc con pocos participantes, los usuarios pueden configurar fácilmente conferencias inmediatas: se llama a todos los participantes y se los coloca en el puente de conferencia. Con Avaya one-X® Portal for IP Office, aquel que origina

la conferencia posee el control: se muestra el número de identificador de cada participante (y el nombre asociado en caso de que se conozca). Si es necesario, es posible desconectar a participantes específicos. El sistema reproduce un único bip al ingresar y un bip doble al salir. El propietario de la conferencia puede utilizar su número de extensión como el identificador de conferencia. El propietario de la conferencia posee el control y tiene la posibilidad de silenciar y desconectar llamadas de otros participantes. Todos los participantes escucharán el sistema de música de espera (MOH) hasta que el propietario se una y escucharán MOH cuando el propietario se desconecte. Tenga en cuenta que el participante interno tiene la opción de ver y desconectar a los participantes (no solo el propietario de la conferencia).

Los usuarios pueden grabar un saludo personalizado para reproducir en una conferencia (requiere Preferred Edition y Voicemail Pro).

Los usuarios pueden grabar la conferencia mediante Avaya one-X® Portal for IP Office, teléfono digital o IP con pantalla o un código abreviado (requiere Preferred Edition y Voicemail Pro). Para impedir el acceso no autorizado al puente de conferencia, es posible configurar códigos PIN, filtrado de números de identificador de llamadas entrantes y perfiles de hora y fecha con Voicemail Pro. Una sola persona puede administrar el puente de conferencia desde cualquier ubicación.

La realización de conferencias tiene las siguientes restricciones:

- Sólo se permiten dos llamadas en conexión a través de líneas troncales analógicas en una sola conferencia.
- Cada llamada externa requiere un canal de VoIP/línea troncal digital (por ejemplo, 1 T1 permite 23/24 participantes externos, 1 E1 permite 30 participantes y un VCM-64 con licencia completa permite 64 participantes).
- No existen límites en cuanto a la combinación de llamadas en conferencia internas y externas, pero si todos los participantes internos se desconectan del puente de conferencia, el sistema puede desconectar automáticamente a los participantes externos para ofrecer una seguridad adicional (parámetros configurables del sistema).
- Las funciones del sistema, como la intrusión de llamada, el registro de llamada y la supervisión silenciosa utilizan recursos de conferencia, al igual que la grabación automática si está habilitada. Cuando cualquiera de estas funciones está activa, se reduce el número de posiciones disponibles para los participantes de la conferencia. Por ejemplo, una llamada en conferencia entre 3 participantes y que se está grabando usará 4 posiciones de conferencia.

Conferencia Meet-Me

Las conferencias Meet-Me permite que varias llamadas interactúen en una conferencia de audio. Los participantes pueden ser personal interno, así como participantes externos, ya sean ingenieros de campo, personal de ventas en desplazamiento, clientes o proveedores. Las llamadas en conferencia se pueden planificar por adelantado o establecerse ad hoc de la forma y en el momento que se requiera.

Colaboración de video

IP Office brinda la función traiga su propio dispositivo (BYOD) y sala HD para la colaboración de video.

IP Office admite colaboración de video con sesión para compartir datos mediante aplicaciones móviles y de escritorio Avaya Scopia® cuando se utiliza Radvision MCU o colaboración de video para IP Office. Los clientes Avaya Communicator también pueden participar en

videoconferencias con varios participantes. Avaya Scopia® se conecta a IP Office como terminal SIP mediante una licencia IP de Avaya.

Avaya Video Collaboration para IP Office ofrece las siguientes funciones clave:

- Integración directa con plan de marcación común con IP Office
- “Sala de conferencia virtual” para ocho participantes como máximo con funciones clic para ingresar desde cualquier sistema de sala que cumpla con los estándares o dispositivo móvil o de escritorio
- Clientes de video móvil o de escritorio se distribuyen en forma gratuita para PC, Mac y los dispositivos iOS y Android más populares; esta características le permite a participantes internos y externos ingresar fácilmente a la videoconferencia
- Videoconferencia HD de varios participantes con ancho de banda bajo con colaboración mediante SIP/H.323 nativo
- Cruce seguro de firewall automático para interactuar con los participantes que se ubican fuera de la red

El siguiente diagrama muestra la topología de IP Office implementada con terminales de video.

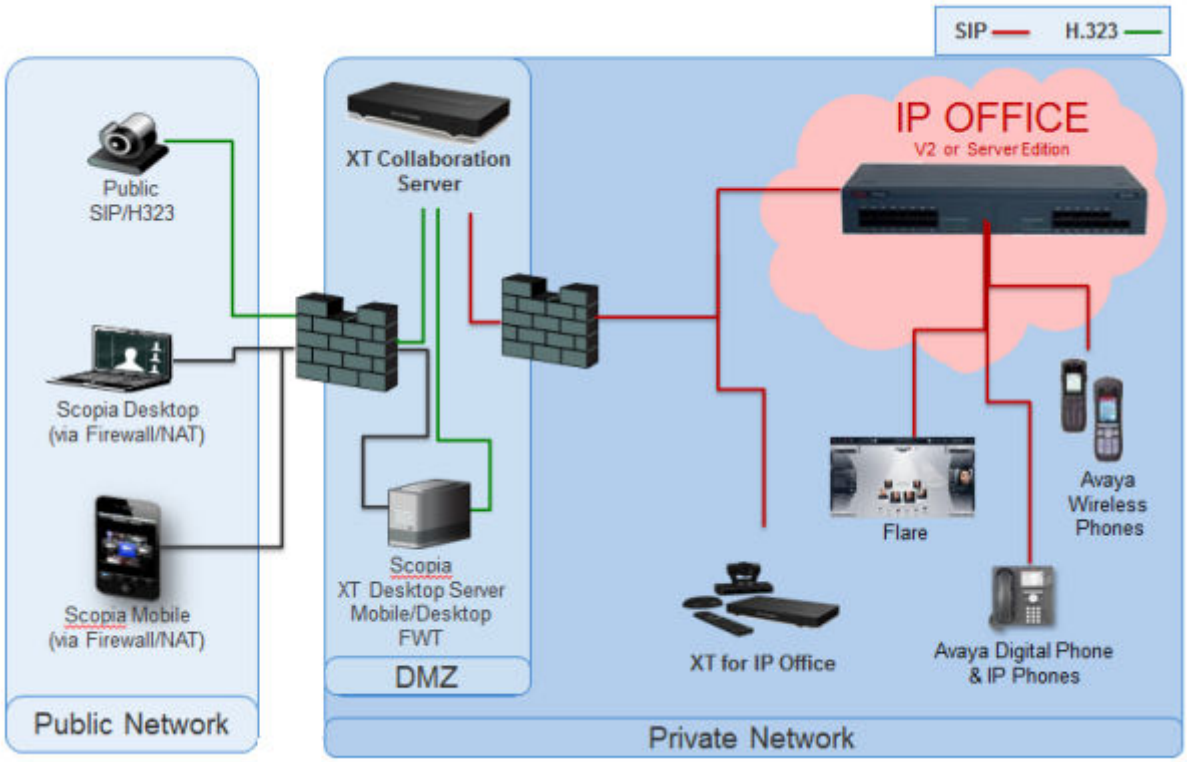


Figura 7: Terminales de video

Collaboration Agent

Collaboration Agent es una aplicación que ofrece herramientas de conferencias y colaboración web. Los usuarios con cuentas de Avaya Aura® Conferencing y los invitados pueden usar las herramientas para administrar conferencias y participar y colaborar en estas.

Los participantes de la conferencia pueden unirse a las conferencias al iniciar sesión en Collaboration Agent y marcar el número del puente de audio asignado a la conferencia. Los participantes también pueden usar la función de audio y video integrados de Collaboration

Agent. Los participantes pueden usar las herramientas de Collaboration Agent para impulsar la productividad y hacer un seguimiento de las acciones incluso después de que la conferencia finalice. Los moderadores de la conferencia pueden:

- Grabar todos los aspectos de las conferencias
- Registrar y editar actas de reunión
- Crear y distribuir informes de reunión en función de las actas de reunión

Funciones de Collaboration Agent

En Collaboration Agent, los participantes y los moderadores pueden realizar varias tareas como, por ejemplo:

- Ver una lista de los demás participantes
- Levantar la mano virtualmente y solicitar permiso para hablar
- Enviar mensajes
- Anotar el contenido compartido
- Grabar o editar actas
- Configurar los tonos de entrada y salida
- Realizar una llamada saliente a otros usuarios y los usuarios realizar una llamada saliente a la conferencia
- Desconectar a participantes
- Promover a los participantes al rol de moderador
- Invitar a más participantes a unirse a una conferencia activa

Durante la conferencia, los participantes pueden ver la siguiente información en Collaboration Agent:

- Los participantes que solo se unieron en el puente de audio
- Los participantes activos en la colaboración web
- El participante que habla actualmente.
- El presentador actual.

Funciones opcionales

Las siguientes funciones son opcionales y el administrador del sistema las debe activar:

- Iniciar conferencias antes de que se unan los moderadores
- Video integrado
- Promover a todos los participantes al rol de presentador, de modo que todos los participantes puedan compartir contenidos
- Realizar una marcación saliente desde Collaboration Agent para conectar a usuarios a las conferencias
- Grabar conferencia

Aplicaciones de instalación y administración

Las siguientes secciones brindan descripción general sobre las aplicaciones relacionadas con la instalación y administración.

IP Office Manager

Use Manager para administrar sistemas IP Office independientes o los sistemas de una red de comunidad pequeña (SCN). Manager realiza un seguimiento de los cambios en la configuración del sistema, administra las actualizaciones y gestiona la importación y exportación de configuraciones.

IP Office tiene un seguimiento de auditoría integrado que efectúa el seguimiento de los cambios en la configuración del sistema e indica quién los ha realizado. Manager puede mostrar el seguimiento de auditoría para ayudar en la resolución de problemas. El seguimiento de auditoría registra los últimos 15 cambios realizados en la configuración y los siguientes elementos:

- Configuración modificada: para cambios de configuración, el registro notifica un nivel alto en todas las categorías de configuración (usuarios, grupos de búsqueda...) que se han modificado.
- Configuración eliminada
- Configuración fusionada
- Reinicio: reinicio instigado por el usuario
- Actualización
- Inicio en frío
- Inicio en caliente
- Escribir a las HH:MM: cuando el administrador guardó la configuración con la opción de programación
- Escritura con reinicio inmediato
- Escritura con reinicio cuando esté libre

IP Office Manager también se usa para funciones de mantenimiento, por ejemplo:

- Actualizar al software del sistema IP Office
- Posibilidad de enviar software a través de un enlace de red IP a un sistema y tenerlo validado antes de realizar la actualización
- Compatibilidad con versiones anteriores de sistemas de la versión 2.1 en adelante para habilitar una aplicación de administración sencilla
- Importación y exportación de información de configuración de IP Office en archivos ACSII-CSV.

Server Edition Manager

Server Edition Manager admite una administración centralizada completa para Primario de Server Edition, Secundario de Server Edition y Sistema de expansión Server Edition. Manager también proporciona funciones de telefonía de IP Office y Unified Communications.

Manager permite la administración de todos los componentes dentro de la solución para actividades tales como:

- Único punto de configuración para IP Office y correo de voz
- Sencillo asistente de instalación inicial
- Visión general del sistema con inventario y estado
- Configuraciones comunes consolidadas en el Primario de Server Edition
- Acceso a la configuración del cliente integrado de Voicemail Pro, System Status Application y la plataforma Linux
- Es compatible con administración en línea, fuera de línea y configuración de una solución completa
- Operaciones de plantilla
- Configuración y almacenamiento de plantilla centralizados
- Utilidad de gestión de cuentas de administrador
- Mantiene la experiencia de IP Office actual
- Ayuda sensible al contexto

Si bien Manager es una aplicación para Windows, se puede instalar directamente desde el portal de administración web del servidor Primario de Server Edition. Esto le permite utilizar inmediatamente cualquier computadora personal con Windows que posea cualquier IP Office Manager pre-instalado.

Al utilizar Manager, el administrador puede crear plantillas para muchos elementos de administración como usuarios, extensiones, grupos de búsqueda y líneas. Luego, el administrador puede crear cualquier elemento nuevo utilizando la configuración predeterminada o la plantilla. Puede crear varios usuarios y extensiones utilizando una plantilla.

Soporte para el enrutamiento de llamadas:

- Total soporte para el plan de discado e IP Office ARS
- El enrutamiento predeterminado simplifica la configuración
- Numeración automática de los grupos de líneas en toda la solución
- Las rutas de llamadas entrantes comunes proporcionan resistencia
- Grupos de búsqueda resistentes

Funcionamiento fuera de línea:

- Se puede crear o administrar una solución completa fuera de línea, si se requiere
- Aún así, se puede administrar cuando algunos dispositivos están desconectados
- Opciones de sincronización en línea/fuera de línea para la configuración que permiten generar una armonía según se requiera

Administración de solución:

- Visión completa de la solución con estado e inventario
- Los usuarios y grupos de búsqueda se aplican a toda la solución
- Derechos de usuarios centralizados, códigos cortos de características, perfiles horarios, rutas de llamadas entrantes y códigos de cuentas
- Si se desea, permite una configuración avanzada dispositivo a dispositivo
- Todas las configuraciones almacenadas en el servidor primario
- Directorio de sistema en toda la solución
- Fácil administración de licencias centrales y por dispositivo

Administración de la resistencia:

- Puede administrar cada dispositivo de manera local para eventos "de día lluvioso"
- Puede administrar la solución mediante un servidor secundario cuando el primario falla o en una configuración WAN dividida
- Opciones de sincronización en línea/fuera de línea para la configuración que permiten generar una armonía según se requiera

Añadir o eliminar dispositivos:

- Proceso individual para añadir o eliminar un dispositivo
- Utilidad de configuración inicial (ICU) incorporada para simplificar la adición de un nuevo dispositivo
- Los elementos de configuraciones comunes del servidor primario se completan automáticamente
- Se puede configurar antes de instalar un nuevo dispositivo

Validación :

- Validación de la configuración durante la lectura y cualquier cambio.
- Validaciones en toda la solución

Plantilla:

- Crea una plantilla centralizada y local de una línea existente, extensión, usuario, grupo de búsqueda, perfil horario, perfil de firewall, ruta IP y entradas de servicio
- Recrea múltiples extensiones y usuarios en base a una plantilla

Acceso remoto:

- Es compatible con acceso al servicio mediante SSL VPN

Seguridad:

- Inicio de sesión único para todo, salvo para la administración de one-X Portal

Web Manager

Web Manager es una herramienta de administración basada en un navegador que se diseñó para simplificar el proceso de instalación y mantenimiento y proporcionar acceso a la mayoría de las opciones de configuración de IP Office. Web Manager elimina la necesidad de tener un

sistema operativo Windows, ya que se ejecuta en cualquier dispositivo que admite navegadores comunes.

Acceso granular:

Web Manager ofrece a los usuarios del servicio acceso a la totalidad de los objetos de configuración si dicho usuario cuenta con acceso a la configuración. Sin embargo, los grandes clientes que tienen varios roles de usuario de servicio o los clientes con implementaciones en el entorno de la nube deben contar con acceso granular a la configuracion para los distintos usuarios del servicio. Los socios de hosting podrán crear una cuenta para el cliente o el revendedor con permisos limitados. Estos permisos impedirán que el cliente o el revendedor realicen actividades que comprometan el servicio del sistema.

Panel de configuración:

El Panel es una versión simplificada de IP Office Web Manager existente y se presenta a los administradores cuando se instala un nuevo sistema IP Office de un solo nodo. El Panel consta de un conjunto mínimo requerido de campos de configuración para ajustar el sistema. La configuración completa puede llevarse a cabo en cualquier momento posterior.

IP Office Media Manager

IP Office Media Manager is a native IP Office application to archive, store, search, playback, download, audit, and delete IP Office call recordings. The Operation, Administration, and Management of (OAM) of the application is integrated within the IP Office solution, for example, IP Office Web Manager.

Media Manager obtains the recordings from the IP Office Voicemail Pro application through a pre-configured hand-off directory. Media Manager moves the recordings from the hand-off directory to an additional hard disk partition on the Primario de Server Edition or Application Server and then archives the recordings to a storage location configured by the administrator. The archiving location can be a Network-Attached Storage (NAS), a local DVD drive, or cloud storage. For cloud storage, Media Manager supports only Google Drive in this release.

Media Manager is licensed on a system basis. Apart from a new IP Office Release 11.0 and later Media Manager license, the application also works with an earlier Contact Recorder license, for customers upgrading from an earlier IP Office version. Media Manager allows a 90–day trial period before licensing is enforced.

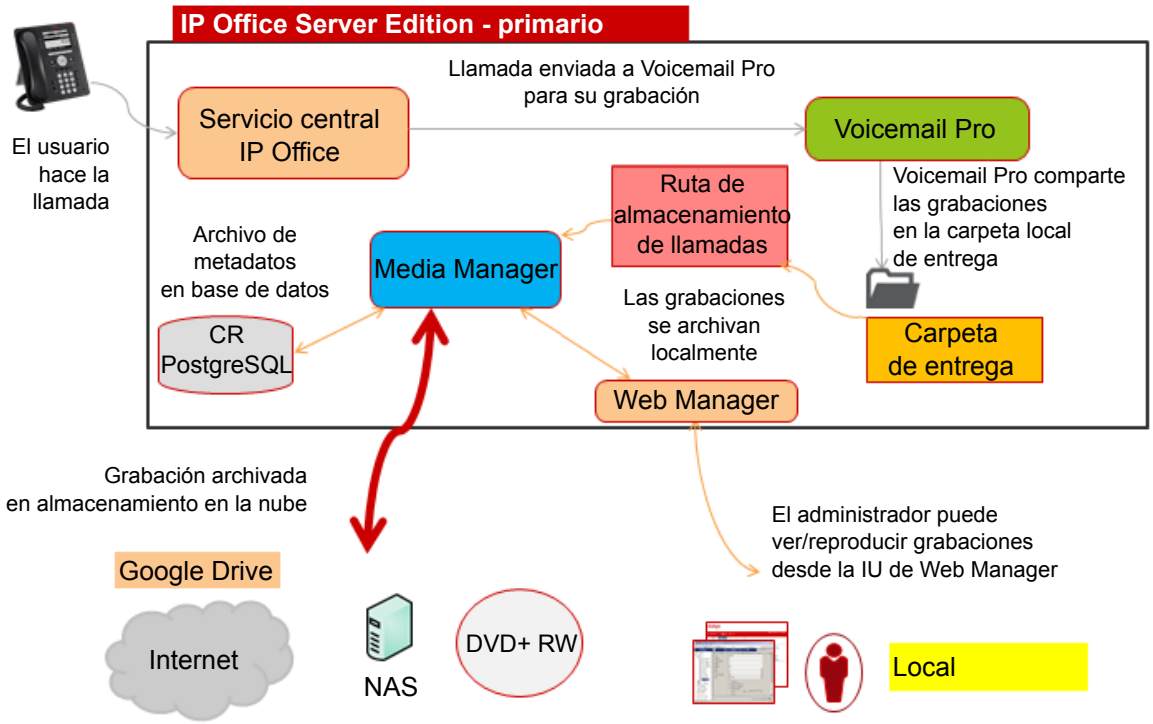
Contact Recorder is not supported in IP Office Release 11.0 and later and is not part of IP Office Release 11.0 and later software. However, Media Manager supports migration of Contact Recorder data to IP Office Release 11.0 and later.

Media Manager is available as part of the IP Office Server Edition and Application Server software image. The application runs on the standard Linux distribution supported by IP Office Server Edition and Application Server platforms. The software is installed as a standard Linux RPM only on the Primario de Server Edition server or the Application Server in case of IP500 V2 deployments. The application is not supported on UCM or Windows platforms. The management interface is web-based and all popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Internet Explorer are supported.

Media Manager is available as part of the IP Office Server Edition and Application Server software image. The application runs on the standard Linux distribution supported by IP Office Server Edition and Application Server platforms. The software is installed as a standard Linux

RPM only on the Primario de Server Edition server or the Application Server in case of IP500 V2 deployments. The application is not supported on UCM or Windows platforms. The management interface is web-based and all popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Internet Explorer are supported.

A standard IP Office Server Edition deployment:



Availability of Contact Recorder features in Media Manager

The search capabilities in Media Manager has been enhanced for the administrators and the users.

Functionality	Description	Availability in Contact Recorder	Availability in Media Manager
Search by administrator	Search by administrators using Target Number, Skills, Agent, and Call ID	Yes	Yes
Search through Web Self-Admin	Search by users using the search filters Target Number, Skills, Agent, and Call ID	Yes	Yes
Web Self-Admin search results	A maximum of 100 results are displayed.	Yes	Yes
Call sets	Facility to save search results for retrieving in the future.	Yes	No

La tabla continúa…

Functionality	Description	Availability in Contact Recorder	Availability in Media Manager
Email	Attaching recordings to emails.	Yes	No
Bulk Export	Exporting multiple recordings and the related details	Yes	Yes
Owner	Available as a search option.	No	Yes
Audit Trail	Audit can be performed to track the use of call recordings.	Yes	Yes
Windows Domain Authentication	-	Yes	No

Aplicación para administración de soluciones

IP Office Managery Web Manager utilizan la aplicación para administración de soluciones (SMA) para tener acceso a la configuración del sistema.

SMA se ubica en el servidor principal o secundario. La configuración se encuentra disponible desde un acceso remoto y desde un acceso central mediante Server Edition. La función acceso central se comunica con el servidor principal o secundario en lugar de con cada nodo en particular. Avaya requiere acceso central para un entorno hospedado y lo recomienda para entornos no hospedados con 32 nodos como mínimo.

Modo administrador de SoftConsole

Los administradores del sistema pueden iniciar SoftConsole en modo administrador. Cuando se ejecuta en este modo, no hay acceso a las funciones de telefonía.

El modo administrador de SoftConsole le permite al usuario configurar las siguientes funciones:

- Crear y editar perfiles de usuario
- Modificar la longitud de las notas de llamadas
- Crear y editar plantillas
- Eliminar o mostrar paneles de interfaz

Consola de administración de SNMP

El protocolo de administración de redes simples (SNMP) es un estándar de industria diseñado para permitir la gestión de equipos de datos de diferentes proveedores mediante una sola aplicación Network Manager. Network Manager realizará sondeos periódicos de los equipos para solicitar una respuesta. De no recibirla, se emitirá una alarma. Además de emitir respuestas, IP Office supervisa el estado de las extensiones, tarjetas troncales, módulos de

Página378 de 3226.

expansión y tarjetas de medios para que, en caso de detectarse un problema, IP Office notifique a Network Manager.

Como la plataforma de IP Office reúne varias aplicaciones, el software principal notifica los eventos SNMP de Voicemail Pro y de Embedded Voicemail para advertir sobre los límites de capacidad de almacenamiento a punto de excederse.

IP Office envía notificaciones de correo electrónico directamente al servidor de correo. No se requiere un cliente de PC adicional.

En los sitios de clientes donde la administración SNMP no se encuentre disponible, IP Office puede enviar eventos por correo electrónico a un máximo de 3 direcciones, cada una con un conjunto diferente de alarmas.

Las siguientes categorías de eventos del sistema pueden seleccionarse para notificaciones de correo electrónico si están instaladas en el sistema:

- Genérico
- Líneas troncales
- Tarjeta de Embedded Voicemail
- VCM
- Módulos de expansión
- Aplicaciones
- Licencia
- Cambio de teléfono
- Bucle de retorno de CSU

IP Office se ha probado con SNMPc-EE™ de CastleRock y la aplicación Network Node Manager de HP (parte del paquete de software OpenView).

System Status Application (SSA)

System Status Application (SSA) es una herramienta de diagnóstico para administradores de sistemas que permite supervisar y verificar el estado de sistemas IP Office de forma local o remota. SSA visualiza tanto el estado actual de un sistema IP Office como detalles de problemas producidos. La información informada es una combinación de eventos históricos y en tiempo real así como datos de estado y de configuración para la identificación de fallas y la realización de diagnósticos. SSA proporciona estados en tiempo real, historial de utilización e información de alarmas para puertos, módulos y tarjetas de expansión del sistema. SSA se conecta con todas las unidades IP Office mediante una conexión IP remota o local. Admite el diagnóstico remoto en conexiones con módem con velocidades de 14.4 kbps o más.

SSA proporciona la siguiente información:

Alarmas SSA muestra todas las alarmas registradas dentro de IP Office para cada dispositivo con error. Se registra la cantidad, y la fecha y hora de las instancias. Para evitar la necesidad de utilizar una computadora local, se almacenan las últimas 50 alarmas en IP Office.

Detalles de la llamada	Información acerca de llamadas entrantes y salientes; incluye información de duración, identificador de llamada y enrutamiento.
Extensiones	SSA detalla todas las extensiones (con tipo de dispositivo y ubicación de puerto) del sistema IP Office. También muestra información sobre el estado actual de un dispositivo. SSA muestra extensiones IP registradas que ya no están disponibles y extensiones IP configuradas que no se han registrado después del último reinicio. Esto permite identificar teléfonos inactivos, desconectados o mal configurados. SSA también muestra los teléfonos en cuarentena y las extensiones y direcciones IP agregados a listas negras.
Líneas troncales	Muestra las conexiones y líneas troncales de IP Office (VoIP, analógicas y digitales) y su estado actual. Para líneas troncales VoIP, se muestra información acerca de la calidad del servicio (QoS), como el retardo de viaje ida y vuelta, la fluctuación y la pérdida de paquetes.
Recursos de sistema	IP Office cuenta con recursos centrales que se utilizan para realizar diversas funciones. El diagnóstico de estos recursos es a menudo crítico para la operación satisfactoria del sistema. Incluye detalles sobre módulos de comprensión de voz (VCM), correos de voz y conferencias.
Control de calidad de servicio (QoS)	El sistema controla los parámetros QoS de las llamadas conectadas, como la fluctuación y el retardo de viaje ida y vuelta.

Es posible iniciar SSA de forma independiente o a través de la aplicación IP Office Manager, y puede haber hasta dos (2) clientes SSA conectados simultáneamente a una unidad IP Office.

SSA no es una herramienta de configuración para sistemas IP Office.

SysMonitor

Utilice SysMonitor para solucionar problemas con IP Office desde una ubicación remota (WAN) o local (LAN).

Seleccione los protocolos e interfaces para supervisar y diagnosticar mediante una interfaz gráfica. Capture los seguimientos directamente en la pantalla o como un archivo de registro para un análisis posterior. Asigne un código de color para los diferentes seguimientos para maximizar la claridad en archivos de mayor tamaño. Esta utilidad también captura alarmas del sistema y muestra el registro de actividad de las últimas 20 alarmas disparadas.

Cloud Operations Manager

Cloud Operations Manager es una herramienta de administración que permite una manera simplificada de administración de múltiples clientes. La herramienta permite la administración de sistemas IP Office Server Edition y proporciona las siguientes capacidades.

- Unified Management Portal único capaz de administrar hasta 3000 sistemas IP Office.

- Panel que muestra las condiciones de los errores, las actividades en curso del sistema y el estado del sistema.
- Agrupamiento de sistemas en función de versiones y etiquetas para acceder a sistemas similares con un clic.
- Muestra todos los sistemas conectados como Primario, Secundario, Expansiones y aplicaciones abiertas.
- Capacidad para administrar centralmente actualizaciones del software de IP Office y crear parches en diferentes sistemas y versiones.
- Administración basada en roles: Cloud Operations Manager tiene sus propios usuarios de servicio con acceso a todos los clientes o a algunos clientes de IP Office. La versión 11.0 no es compatible con el acceso a nivel de función granular.
- Ofrece facilidad para iniciar aplicaciones de Native IP Office Management. Los usuarios deben iniciar sesión en las aplicaciones de forma separada después de que se inicia la aplicación. La versión 11.0 no admite el inicio de IP Office Contact Center, Avaya Contact Center Select y Avaya Workforce Optimization Select.
- Alarmas para Configuración, Servicios, Líneas troncales, Enlace, y Seguridad por tipo de seguridad
- Alarmas para el estado de los sistemas IP Office que indican si están conectados o desconectados
- Alarmas que indican el estado de diferentes aplicaciones

Administrador de migración de datos (DMM)

El administrador de migración de datos (DMM) facilita la migración de datos desde sistemas Norstar y BCM hacia IP Office. Existen tres pasos en la migración de datos: extracción, conversión y aplicación.

DMM migra:

- Anuncios y saludos
- Mensajes de correo de voz
- Extraer la configuración del piloto de llamadas

Aplicaciones IP Office Branch

Administración centralizada

Con los modelos de implementación centralizada, distribuida o mixta puede usar Avaya Aura® System Manager para administrar de forma central todos los componentes de la solución. System Manager administra las aplicaciones y servicios centralizados que se incluyen en la solución, los sistemas IP Office en la sucursal, los usuarios centralizados y los usuarios de IP Office. Para aquellas capacidades que no se pueden administrar de forma central, System

Manager lanza IP Office Manager en el modo adecuado donde puede administrar los sistemas IP Office individuales de forma remota.

La administración centralizada de los componentes a través de Avaya Aura® System Manager es opcional. Por ejemplo, puede optar por administrar los sistemas IP Office directamente a través de IP Office Manager.

Con la opción de IP Office de sucursal independiente, no está disponible la opción de administración centralizada. Debe administrar todos los sistemas IP Office directamente a través de IP Office Manager.

Licencias centralizadas

Con una implementación distribuida, mixta o centralizada conectada a la red Avaya Aura®, puede acceder a las funcionalidades de licencias centralizadas mediante el servidor System Manager Avaya WebLM. Con las licencias centralizadas, un archivo de licencia único se genera en el sistema de licencia y entrega de productos (PLDS) para varias sucursales.

Para usar las licencias centralizadas, la empresa debe obtener una licencia WebLM de PLDS para cada sucursal de IP Office. Las licencias centralizadas no están disponibles en los entornos de sucursales IP Office independientes.

Sistemas de correo de voz

La solución IP Office Branch admite los sistemas de correo de voz y los sistemas de correo de voz centralizados IP Office.

El sistema IP Office Embedded Voicemail se incluye en IP Office Essential Edition, y el sistema IP Office Voicemail Pro se incluye en IP Office Preferred y Advanced.

La solución Branch admite los siguientes tres sistemas de correo de voz centralizados como componentes adicionales con la solución:

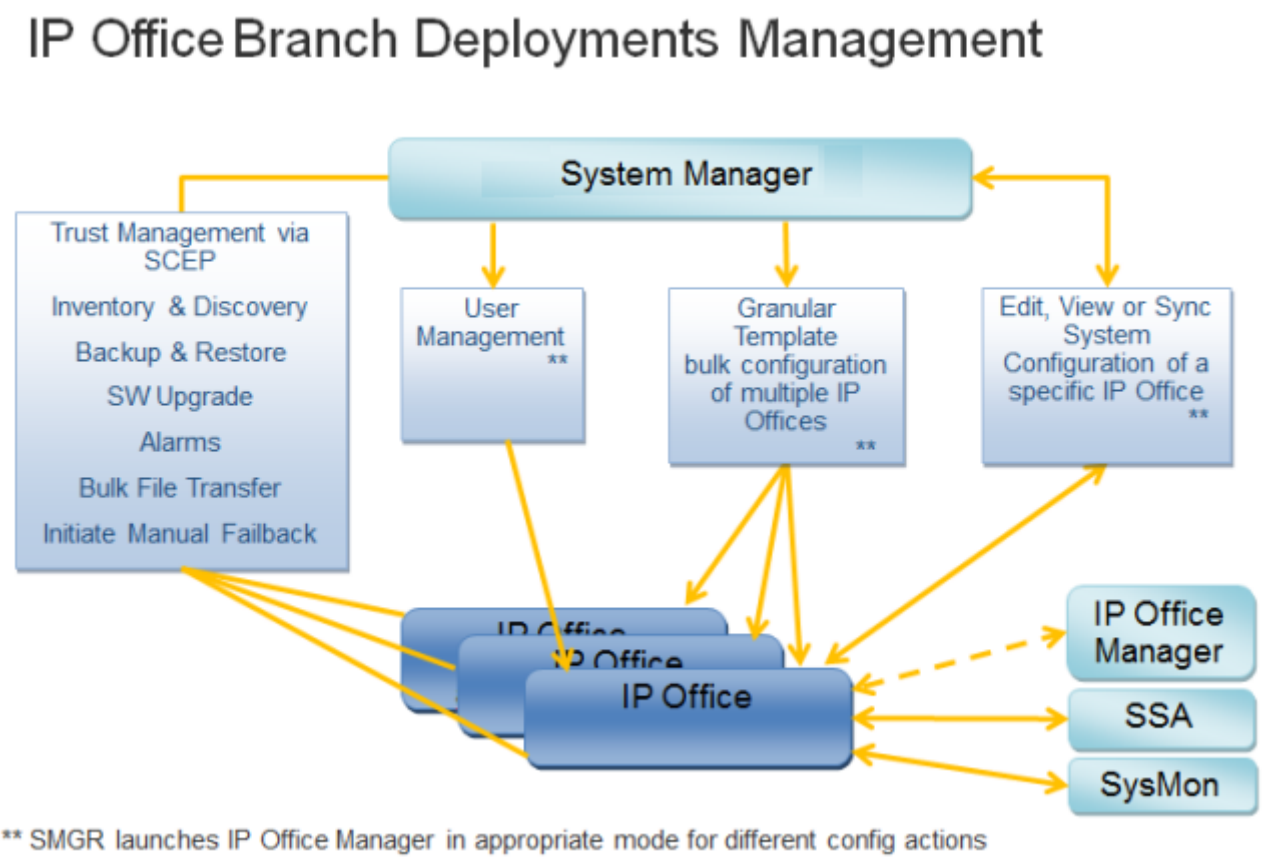
- Avaya Aura®Messaging
- Avaya Modular Messaging
- Avaya CallPilot®: solo se admite en entornos de sucursal distribuidos que están conectados a CS 1000.

Avaya Aura® System Manager

Avaya Aura® System Managerpermite administradores en Distribuido. Los entornos de implementación Mixtos y Centralizados conectados a Avaya Aura® para centralizar la administración de todos los usuarios y sistemas IP Office en la sucursal de la empresa. En un entorno de sucursal Distribuido conectado a CS 1000, también puede configurar Avaya Aura® System Manager para centralizar la administración de CS 1000.

System Manager proporciona la siguiente administración Centralizada y funcionalidad de administración.

- Actualizar los sistemas IP Office.
- Agregar dispositivos de IP Office desde la red a System Manager.
- Crear plantillas de terminal de IP Office que se utilizan para crear usuarios IP Office y usuarios centralizados. Estas plantillas se pueden editar, duplicar o eliminar.
- Crear plantillas de configuración de sistema IP Office que pueden aplicarse a los sistemas IP Office seleccionados. Estas plantillas se utilizan para el aprovisionamiento inicial de dispositivos. Estas plantillas se pueden editar, duplicar o eliminar.
- Cargar y convertir archivos de sonido a System Manager para utilizar en la función de Configuración de operadora automática del sistema IP Office.
- Administrar las configuraciones del sistema IP Office. Desde System Manager, puede iniciar IP Office Manager para ver o editar una configuración de sistema. Con esta función, puede hacer cambios directamente en el dispositivo IP Office. Puede aplicar los cambios de inmediato o programar la ejecución de esos en un período determinado.
- Administrar la configuración de seguridad de IP Office. Desde System Manager, puede iniciar IP Office Manager para ver o editar una configuración de seguridad del sistema. Con esta función, puede hacer cambios directamente en el dispositivo IP Office.
- Crear plantillas de usuario. Estas plantillas se pueden editar o eliminar. Las plantillas pueden crearse para usuarios centralizados o de IP Office.
- Realizar un respaldo de IP Office con la opción de almacenar el resultado del respaldo en System Manager o de crear un respaldo local donde el sistema almacene los resultados del respaldo en el almacenamiento local adjunto al dispositivo IP Office.
- Realizar una restauración de IP Office. Esta función le permite restaurar:
  - una configuración de sistema IP Office guardada en IP Office desde System Manager.
  - un respaldo de una configuración de sistema IP Office en IP Office desde el dispositivo de tarjeta SD.
  - usuarios desde System Manager en IP Office.
  - una configuración de sistema IP Office y un usuario guardados desde System Manager en IP Office.
- Ver eventos y alarmas respecto de las distintas operaciones que tienen lugar en IP Office.



Avaya Aura® Session Manager

Avaya Aura® Session Manageradministra el control de admisión de llamadas, la redirección de llamada, el análisis de dígito, la administración del plan de marcación, las fuentes de contabilidad de llamada de red interna, el envío de cuota, el enrutamiento entre oficinas y el enrutamiento menos costoso internacional. Este dispositivo de comunicaciones maneja toda la administración y gestión de la red del plan de marcación global privado en toda la empresa como una sola empresa con Avaya Aura® System Manager.

Session Manager tiene un rol diferente para los usuarios centralizados y IP Office para los usuarios de entornos implementados que están conectados a Avaya Aura®. Para los usuarios de IP Office, Avaya Aura® Session Manager funciona como un SIP proxy para enrutar las sesiones SIP hacia y desde las conexiones SIP a IP Office. Para los usuarios centralizados, Avaya Aura® Session Manager también es la interfaz principal que administra el registro del usuario y el enrutamiento de llamadas.

Avaya Aura® Communication Manager

Los usuarios centralizados se registran en Avaya Aura® Session Manager y obtienen servicios de telefonía de Avaya Aura® Communication Manager Feature Server o Evolution Server en la

empresa central. Avaya Aura® Communication Manager no brinda ninguna función a los usuarios de IP Office.

Aplicaciones de centro de contactos

Las siguientes secciones brindan descripción general sobre las aplicaciones de centro de contactos.

Para obtener información general sobre:

- IP Office Contact Center, consulte *Descripción de la función Avaya IP Office Contact Center*.
- Avaya Contact Center Select, consulte *Descripción de la solución Avaya Contact Center Select*.

Descripción general de IP Office Contact Center

Avaya lidera el mercado de la tecnología para centros de llamadas y IP Office Contact Center puede llevar su negocio al próximo nivel. IP Office Contact Center brinda capacidades integradas de centro de contactos diseñadas específicamente para empresas que poseen entre 5 y 250 agentes y supervisores en el centro de contactos.

IP Office Contact Center brinda las siguientes funciones y características:

- Solución de servicio al cliente todo en uno que brinda un servicio al cliente consistente en una variedad de ubicaciones y canales de medios. IP Office Contact Center incluye una interfaz de usuario (IU) para Microsoft Windows, una IU de Chrome para dispositivos con Chrome OS, y una interfaz web compatible con varios navegadores de Windows y Mac.

  IP Office Contact Center User Interface for Chrome Devices y Interfaz de usuario web de IP Office Contact Center ofrecen funcionalidades similares.
- Rápida implementación con disrupción mínima del servicio. IP Office Contact Center también incluye una función de sincronización automática para la configuración. Esta función puede activarse y desactivarse según sea necesario durante la implementación.
- Acceso a la funcionalidad Agent UI, que incluye control de llamadas, desde un complemento de SalesForce (SFDC) o un conector SAP CRM.
- Acceso a opciones de control de llamadas con un auricular Plantronics cuando se usa IP Office Contact Center User Interface for Chrome Devices.
- Capacidades de correo electrónico y chat en todas las IU.
- Llamadas de voz entrantes y salientes con capacidad de telefonía y marcado.
- Enrutamiento según habilidades.
- Acceso a la libreta de direcciones para que los agentes puedan encontrar rápidamente la información del contacto que necesitan para realizar la llamada y enviar correos electrónicos.
- Informes históricos y en tiempo real para todos los canales de medios.

- Script de respuesta de voz interactiva (IVR) y editor de flujo de tareas.
- Configuración de privilegio de grupo de agentes y perfil de usuario para determinar qué funciones están disponibles para loso usuarios de la interfaz. Los administradores deben asignar los privilegios y crear los grupos de agentes.
- Acceso a un portal de administración web. Puede utilizar el portal de administración para realizar tareas de configuración, mantenimiento, supervisión y administración. También puede cargar certificados, recopilar registros y descargar archivos de correo electrónico y la aplicación IP Office Contact Center User Interface for Windows. Las tareas avanzadas de administración deben realizarse en IP Office Contact Center User Interface for Windows. No es posible ejecutar tareas de administración con las interfaces IP Office Contact Center User Interface for Chrome Devices y Interfaz de usuario web de IP Office Contact Center.
- Acceso a un tablero en el que se muestran las estadísticas de IP Office Contact Center. Para obtener más información sobre Tablero, consulte *Uso del Tablero Avaya IP Office Contact Center*.
- Opción de fácil integración de funcionalidades de chat en una página web. Para obtener más información, consulte *Guía basada en tareas de servicios de chat y correo electrónico Avaya IP Office Contact Center*.
- Integración opcional con aplicaciones de grabación de llamadas, como Avaya Contact Recorder. Las llamadas se graban con Voicemail Pro y los detalles de la grabación completa se almacenan en la base de datos de la aplicación de grabación de llamadas. Es posible buscar y administrar grabaciones mediante un navegador web.
- Interoperabilidad opcional con Avaya Workforce Optimization Select, que es un producto independiente que actualmente no se integra con aplicaciones o IU de IP Office Contact Center.

Descripción general sobre Avaya Contact Center Select

Avaya Contact Center Select es una solución de centro de contactos multimedia, de voz, sensible al contexto y de colaboración que le permite a pequeñas y medianas empresas anticipar, acelerar y mejorar las interacciones con los clientes. Avaya Contact Center Select utiliza el sistema de telefonía Avaya IP Office para brindar una plataforma de telefonía en tiempo real.

Avaya Contact Center Select utiliza interfaces SIP y CTI estándares de la industria para integrarse con IP Office. Esta integración le brinda a Avaya Contact Center Select acceso y control de una amplia variedad de teléfonos y funciones de IP Office. Los clientes que integran Avaya Contact Center Select con IP Office obtienen enrutamiento basado en habilidades, tratamientos de llamadas, informes, administración de agentes unificada y la utilidad gráfica de Orchestration Designer.

Avaya Agent Desktop es una aplicación cliente de una sola interfaz utilizada por agentes de Avaya Contact Center Select para ayudar a los clientes.Los agentes de Avaya Contact Center Select utilizan el software Agent Desktop para responder a los contactos multimedia y de voz de los clientes. Agent Desktop admite diversos teléfonos IP Office y una amplia variedad de tipos de contactos multimedia.

De manera predeterminada, los servicios web y las conexiones de Avaya Contact Center Select utilizan una comunicación TLS segura. La herramienta de Administración de

certificados de Avaya Contact Center Select facilita la administración de certificados de seguridad.

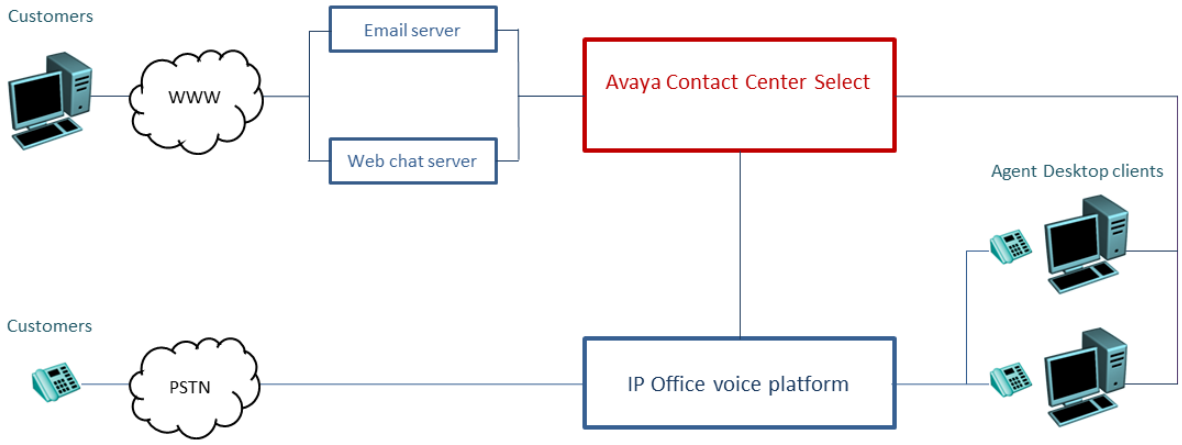


Figura 8: Solución de centro de contactos típica que usa Avaya Contact Center Select de voz y multimedia y el sistema de telefonía de voz de Avaya IP Office

Avaya Contact Center Select brinda una solución de voz y multimedia con diversas funciones que cuenta con informes y enrutamiento integrados para pequeñas y medianas empresas. Avaya Contact Center Select brinda un centro de contactos unificado y administración de cuenta de usuario de teléfonos IP Office para agentes y supervisores. Los agentes y supervisores con función de voz habilitada creados en Avaya Contact Center Select se agregan automáticamente a IP Office. Avaya Contact Center Select sincroniza información de usuario (agente y supervisor) entre Avaya Contact Center Select y IP Office.

Capítulo 5: Recursos

Documentación

Consulte los siguientes documentos relacionados en el sitio web de Soporte técnico de Avaya en support.avaya.com y en la IP Office Base de conocimiento en marketingtools.avaya.com/knowledgebase.

Número de documento	Título	Utilice este documento para:	Audiencia
Descripción general			
16-604278	*Primeras instrucciones para Avaya IP Office™ Platform*	Consulte una lista de todos los documentos relacionados con la solución.	Todos
No está numerado	*Descripción de la solución Avaya IP Office™ Platform*	Comprensión detallada de la solución.	Todos
Referencia			
No está numerado	*Referencia de acción de botones y código corto de Avaya IP Office™ Platform*	Comprensión de los detalles de los códigos abreviados y la acción de botones.	Administradores
No está numerado	*Pautas de seguridad de Avaya IP Office™ Platform*	Comprensión de los detalles de seguridad de la Plataforma Avaya IP Office™.	Ingenieros de implementación Administradores

Búsqueda de documentos en el sitio web de soporte técnico de Avaya

Acerca de esta tarea

Utilice este procedimiento para encontrar la documentación del producto en el sitio web de soporte técnico de Avaya.

Procedimiento

1. Use un navegador para navegar al sitio web de soporte técnico de Avaya en http://support.avaya.com/.
2. En la parte superior de la pantalla, introduzca su nombre de usuario y contraseña y haga clic en **Login**.
3. Coloque el cursor sobre **Support by Product**.
4. Haga clic en **Documents**

5. En el cuadro de búsqueda **Enter your Product Here**, escriba el nombre del producto y, luego, seleccione el producto de la lista desplegable.
6. Si existe más de una versión, seleccione el número de versión correspondiente en la lista desplegable de **Choose Release**.
7. Utilice el filtro **Content Type** a la izquierda para seleccionar el tipo de documento que busca o haga clic en **Select All** para ver una lista de todos los documentos disponibles.

   Por ejemplo si busca guías de usuario, seleccione **User Guides** en el filtro **Content Type**. La lista de documentos solo mostrará documentos de la categoría seleccionada.
8. Haga clic en **Enter**

Capacitación

Las credenciales y capacitación de Avaya están diseñadas para garantizar que todos nuestros socios comerciales tengan las capacidades y habilidades para vender, implementar y brindar soporte técnico con éxito para las soluciones Avaya y superar las expectativas de los clientes. Se encuentran disponibles las siguientes credenciales:

- Avaya Certified Sales Specialist (APSS) (Especialista en ventas certificado por Avaya)
- Avaya Implementation Professional Specialist (AIPS) (Especialista profesional en implementación de Avaya)
- Avaya Certified Support Specialist (ACSS) (Especialista en soporte técnico certificado por Avaya)

Los siguientes trayectos de credenciales están disponibles en el sitio web de aprendizaje Avaya en http://avaya-learning.com/.

Los siguientes cursos también están disponibles en el sitio web de aprendizaje Avaya. Después de iniciar sesión en el sitio web, introduzca el código del curso o el título del curso en el campo de **búsqueda**.

Código del curso	Título del curso
2S00012W	APSS – Small and MidMarket Communications – IP Office™ Platform and Select Overview (APPS: Comunicaciones para pequeñas y medianas empresas: Descripción general de la plataforma IP Office™ y Select)
4601W	Avaya IP Office™ Platform — Components (Plataforma Avaya IP Office™: Componentes)
4602W	Avaya IP Office™ Platform — Editions (Plataforma Avaya IP Office™: Ediciones)
2S00015O	Small and Midmarket Communications — IP Office — Endpoints (Comunicaciones para pequeñas y medianas empresas: IP Office: Terminales)
10S00005E	Knowledge Access: Avaya IP Office™ Platform Implementation (Acceso al conocimiento: Implementación de la plataforma Avaya IP Office™)
5S00004E	Knowledge Access: Avaya IP Office™ Platform Support (Acceso al conocimiento: Soporte técnico de la plataforma Avaya IP Office™)

En todas las ofertas de Knowledge Collection Access (Acceso a colección de conocimiento) se incluye un área aparte llamada IP Office Supplemental Knowledge (Conocimiento complementario sobre IP Office). Este piso en el Campus virtual contiene objetos de aprendizaje autodirigido, que abarcan la información delta sobre IP Office. Este material está dirigido a técnicos con experiencia en IP Office.

Visualización de videos de orientación de Avaya

Los videos de orientación de Avaya proporcionan contenido técnico sobre cómo instalar, configurar y resolver problemas en los productos Avaya.

Acerca de esta tarea

Los videos están disponibles en el sitio web de soporte de Avaya, ubicados bajo el tipo de documentos de video, y en el canal de YouTube administrado por Avaya.

Procedimiento

- Para encontrar videos en el sitio web de soporte de Avaya, vaya a http://support.avaya.com y realice una de las siguientes acciones:
  - En **Search**, ingrese `Avaya Mentor Videos` para ver una lista de los videos disponibles.
  - En **Search**, ingrese el nombre del producto. En la página **Search Results**, seleccione **Video** en la columna **Content Type** de la izquierda.
- Para buscar los videos de orientación de Avaya en YouTube, vaya a www.youtube.com/AvayaMentor y realice una de las siguientes acciones:
  - Ingrese una palabra o palabras clave en **Buscar en el canal** para buscar un producto o tema en particular.
  - Desplácese hacia abajo en **Listas de reproducción** y haga clic en el nombre del tema para ver la lista de videos disponibles publicados en el sitio web.

Nota:

No todos los productos tienen videos disponibles.

Recursos adicionales de IP Office

Puede encontrar información en los siguientes sitios web de recursos adicionales.

Avaya

http://www.avaya.com es el sitio web oficial de Avaya. La página principal proporciona acceso a sitios web individuales de Avaya para los distintos países.

Ventas de Avaya y portal para socios

http://sales.avaya.com es el sitio web oficial para todos los socios comerciales de Avaya. Este sitio requiere del registro de un nombre y contraseña de usuario. Una vez que ha obtenido acceso, puede personalizar el portal para los productos específicos y tipos de información que desea ver y sobre los que desea recibir notificaciones por correo electrónico.

Base de conocimientos Avaya IP Office

http://marketingtools.avaya.com/knowledgebase proporciona acceso a una versión en línea y con actualizaciones regulares de la Base de conocimientos IP Office.

Información sobre el mantenimiento, el ciclo de vida y la garantía de Avaya

Los servicios de soporte técnico de Avaya complementan los estándares de las políticas de garantía, ciclo de vida y mantenimiento de Avaya, las cuales están publicadas en http://support.avaya.com. Para obtener más información, envíe un correo electrónico a support@avaya.com.

Grupo de usuarios internacionales de Avaya

http://www.iaug.org es el foro de discusión oficial para los usuarios de productos Avaya.

Soporte técnico

Consulte el sitio web de soporte de Avaya en http://support.avaya.com para obtener la documentación más actualizada, avisos sobre productos y artículos de conocimiento. También puede buscar notas de publicación, descargas y soluciones a problemas. Utilice el servicio web de solicitud de servicios para crear una solicitud de servicio. Realice consultas a los agentes en directo o solicite que un agente lo comunique con el equipo de soporte técnico si un problema requiere conocimientos específicos adicionales.

Uso de la Base de conocimiento de Avaya InSite

La Base de conocimientos de Avaya InSite es un motor de búsqueda web que provee:

- Procedimientos actualizados para solución de problemas y consejos técnicos
- Información sobre los service packs
- Acceso a documentación del cliente y técnica
- Información sobre programas de capacitación y certificación
- Vínculos a otra información pertinente

Si es un socio de Avaya autorizado o un cliente actual de Avaya con un contrato de soporte, puede acceder a la Base de conocimiento sin costo adicional. Debe tener una cuenta de inicio de sesión y un número Sold-To válido.

Use la Base de conocimiento Avaya InSite para buscar posibles soluciones para los problemas.

1. Vaya a http://www.avaya.com/support.
2. Inicie sesión en el sitio web de Avaya con un usuario y contraseña válidos.

   Aparece la página de **Support** (soporte).
3. En **Support by Product** (Soporte por producto), haga clic en **Product-specific support** (Soporte de producto específico).
4. Escriba el producto en el cuadro de texto **Enter Product Name** (Escriba el nombre del producto) y presione Intro.

5. Seleccione el producto de la lista desplegable y elija la versión relevante.
6. Seleccione la ficha **Technical Solutions** (Soluciones técnicas) para ver artículos.
7. Seleccione los artículos relevantes.

Acceso a las notas de la aplicación Avaya DevConnect

El programa Avaya DevConnect realiza pruebas con los proveedores de servicio para establecer compatibilidad con los productos Avaya.

Procedimiento

1. Vaya a http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp.
2. Inicie sesión o regístrese.
3. Haga clic en un tiempo para buscar allí.

   Aparece una lista de todas las notas de la aplicación para ese tiempo.
4. En el campo **Búsqueda**, escriba `IP Office` y pulse **Intro**.

   Aparece una lista de las Notas de la aplicación relevantes.

Capítulo 6: Estándares

Estándares regulativos

Calidad de los estándares de servicio

Cada cliente tendrá diferentes expectativas y diferentes presupuestos con los que deberán trabajar. Algunos estarán dispuestos a actualizar sus redes para utilizar los mejores equipos y prácticas posibles. Para otros, el gasto adicional puede resultar innecesario. Los ejemplos de estándares basados en los protocolos de Calidad de servicio se basan en:

- 802.1Q (Nivel 2)
- DiffServ (Nivel 3)
- Rango de puerto (Nivel 4)
- 802.1X (MD-5)

Códecs de compresión de voz

La banda ancha usada varía en función del método de compresión elegido. IP Office admite las normas de la siguiente lista. Ocuparán aproximadamente 10K y 13K de banda ancha respectivamente. Use el siguiente gráfico para elegir el algoritmo de compresión más adecuado para su banda ancha disponible.

Códec de audio	Carga de datos de voz RTP (bytes)	Paquetes por segundo	LAN (bps)	% de LAN general	WAN (bps)	% de WAN general	Demora algorítmica (ms)
G.723.1 (6,3K)	24	33,33	20.800	225%	9.867	54%	80
G.729a	20	50	29.600	270%	13.200	65%	40
G.711 (64K)	160	50	85.600	34%	69.200	8%	20
G.722 (64K)	160	50	85.600	34%	69.200	8%	20

Estándares de VoIP

IP Office admite los siguientes protocolos y estándares:

H.323 V2 (1998) Sistemas de comunicaciones multimedia basados en paquetes.

Q.931 Especificación de capa 3 de interfaz de red de usuario ISDN para el control básico de llamadas.

H.225.0 (1998) Protocolos de señalización de llamadas y paquetización de secuencia de medios para sistemas de comunicaciones multimedia basados en paquetes.

H.245 (1998) Protocolo de control para comunicación multimedia.

SIP Protocolo de Inicio de Sesiones

T.38 Estándar de fax

Estándares de Internet (Además de TCP/UDP/IP.)

Estándar	Descripción
RFC 1889	Protocolo en tiempo real (RTP) y Protocolo de control en tiempo real (RTCP)
RFC 2507, 2508, 2509	Compresión de encabezado
RFC 2474	DiffServ, Tipo de servicio configurable in situ
RFC 1990	Fragmentación PPP
RFC 1490	Encapsulación de Frame Relay
RFC 2686	Extensiones multiclases para PPP multivínculo
RFC 3261	SIP
RFC 3489	STUN

Estándares de línea troncal analógica

Las tarjetas de línea troncal analógicas de IP Office cumplen con los estándares:

TIA/EIA-646-B Inicio de bucle

GR-188-CORE y GR-31-CORE Identificación de línea de interlocutor entrante (ICLID)

ANSI T1.401 y TIA/EIA-646-B Inicio básico (no disponible en todas las localidades)

Estándares de interfaz de base de datos

IP Office admite el estándar de interfaz ActiveX Data Object (ADO).

Estándares del consejo estándar de seguridad PCI

Las empresas de tarjeta de crédito líder definen los estándares en el consejo estándar de seguridad PCI y una de estas normas no graba los números de tarjeta de crédito que entrega el cliente.

Estándares WiFi inalámbrico

Sobre la base de los estándares globales para redes LAN inalámbricas, la solución de teléfonos IP inalámbricos de Avaya simplifica la infraestructura de redes y permite que el tráfico de voz se transporte junto con el tráfico de datos a través de la misma red inalámbrica. Los teléfonos 3641 y 3645 admiten varios estándares WiFi (802.11 a/b/g). Con estos auriculares los clientes tienen una opción que se ajusta sus necesidades e infraestructura. El 3641 y el 3645 también funcionarán en redes 802.11a y 802.11g. Estos teléfonos también son actualizables in situ a través de clientes TFTP externos (no incluidos), por lo que los teléfonos pueden actualizarse con nuevos protocolos, funciones y capacidades a medida que estén disponibles.

Estándares de protocolo de red

Protocolo	RFC	Descripción
Protocolo Punto a punto (PPP)	RFC1661	Protocolo WAN que permite el interfuncionamiento con una amplia variedad de enrutadores de terceros. PPP se utiliza en circuitos de línea dedicada donde se usa un solo canal para conectar las dos ubicaciones juntas. Por ejemplo, un solo canal puede ser un canal de 64K en un circuito de marcado o una línea dedicada de 256K.
Protocolo de control de enlace (LCP)	RFC1570	En PPP, LCP establece, configura y prueba las conexiones a Internet por enlace de datos.
Protocolo multienlace punto a punto (ML-PPP)	RFC1990	Permite la realización de llamadas adicionales donde se requiere un ancho de banda superior a un solo canal. La cantidad máxima de canales disponibles para los datos se puede fijar según el servicio. Cuando el ancho de banda disponible alcanza un límite definido por el usuario, se pueden agregar automáticamente canales adicionales. De la misma forma, cuando el tráfico cae entonces la cantidad de canales en uso se puede reducir automáticamente. Si no hay tráfico de datos en ninguno de los canales en uso, entonces se pueden borrar todas las líneas. Como la mayoría de las transportadoras tienen un costo mínimo para las llamadas, se puede configurar el período en que un canal debe estar inactivo antes de borrarlo. Mediante estos mecanismos los costos de la llamada se pueden controlar eficazmente mientras se asegura que el ancho de banda esté disponible cuando sea necesario.
Protocolo de control de protocolo de Internet (IPCP)	RFC1332	Un protocolo de control de red (NCP) para establecer y configurar un IP en un PPP.
Compresión de encabezado de protocolo de Internet (IPHC)	-	Reduce el tamaño del encabezado del paquete de datos para ganar eficiencia del ancho de banda en WAN, pero agrega latencia de transmisión.
Protocolo de autenticación de contraseñas (PAP)	RFC1334	Un método de autenticación del fin remoto de una conexión usando las contraseñas no cifradas.
Protocolo de transporte de tiempo real (RTP) Protocolo de control de transporte de tiempo real (RTCP)	RFC1889	RTP define a un formato de paquete estandarizado para entregar audio y video en redes IP. RTCP funciona con RTP para enviar paquetes de control a los participantes en la llamada que proporcionan comentarios sobre la calidad del servicio.
Protocolo de autenticación por desafío mutuo (CHAP)	RFC1994	Permite que las llamadas de datos entrantes se puedan autenticar con contraseñas no cifradas. El sistema también ofrece la opción de reafirmar periódicamente la autenticidad de la persona que llama durante la llamada de datos.

La tabla continúa…

Protocolo	RFC	Descripción
Protocolo de control de compresión (CCP)	RFC1962	Configura, habilita y deshabilita los algoritmos de compresión de datos en ambos extremos del vínculo PPP. También se utiliza para indicar una falla.
Protocolo ligero de acceso a directorios (LDAP)	RFC4510	Permite que el directorio de números telefónicos (nombres y números de teléfono) que se guarda en IP Office se sincronice con la información en un servidor de LDAP (limitado a 5000 entradas). Aunque está diseñado para la interoperación con el Directorio activo del servidor de Windows 2000, la función se puede configurar para interoperar con cualquier servidor que admita la versión 2 o posterior de LDAP.
Compresión Punto a punto Microsoft (MPPC)	RFC2118	Método de compresión de datos para lograr una mayor rendimiento en los vínculos WAN de baja velocidad.
Protocolo de control de asignación de banda ancha (BACP)	RFC2125	Permite la negociación con el extremo remoto de la llamada de datos para solicitar la realización de llamadas adicionales y mejorar así el rendimiento de los datos agregados.
Protocolo de datagrama del usuario (UDP)	RFC768	Un modelo de transmisión sin conexiones simple con un mecanismo de protocolo mínimo que se utiliza para permitir que las aplicaciones envíen mensajes (datagramas) a otros host en una red IP son comunicaciones previas para configurar canales de transmisión especiales o rutas de datos.
Protocolo de Internet (IP)	RFC791	Un conjunto de reglas que rigen el formato de los datos enviados por Internet u otra red.
Protocolo de control de transmisión (TCP)	RFC793	Una conexión se establece y mantiene hasta que la aplicación en cada extremo haya terminado de ocupar mensajes.
Protocolo de configuración dinámica de host (DHCP)	RFC1533	Distribuye dinámicamente parámetros de configuración de red en una red IP, como las direcciones IP para interfaces y servicios.

La tabla continúa…

Protocolo	RFC	Descripción
Traducción de direcciones de red (NAT)	RFC1631	Un mecanismo que permite usar diferentes direcciones IP en una red privada detrás de un enrutador con una dirección IP pública. Cuando se conecta a Internet, ISP desea típicamente que un cliente use una dirección IP que asignaron. Con NAT esto se puede asignar fácilmente, erradicando la necesidad de que el cliente cambie el esquema de numeración de la red y proporcionando seguridad adicional a los usuarios internos ya que sus direcciones están ocultas para el público. Generalmente, una empresa asigna sus direcciones de red internas a una dirección IP externa global y elimina la asignación de la dirección IP global en los paquetes entrantes en las dirección IP internas. Esto ayuda a garantizar la seguridad ya que cada solicitud saliente y entrante debe pasar por un proceso de traducción. Esto también hace referencia a la oportunidad de calificar o autenticar el pedido o hacerlo coincidir con un pedido anterior. NAT también conserva la cantidad de direcciones IP globales que necesita una empresa.
Protocolo de arranque (BOOTP)	RFC951	Asigna automáticamente una dirección IP a los dispositivos de red desde un servidor de configuración en una red IP.
Protocolo trivial de transferencia de archivos (TFTP)	RFC1350	Un protocolo simple para transferir archivos implementado en la parte superior de UDP mediante el puerto número 69.
Protocolo de tiempo de redes (NTP)	RFC868	Proporciona sincronización del reloj entre los sistemas de computación en conmutación de paquetes, redes de datos de latencia variable.
Protocolo proxy de resolución de direcciones (ARP)	-	La compatibilidad con el Protocolo proxy de resolución de direcciones permite a IP Office responder en nombre de la dirección IP de un dispositivo conectado a él al recibir una petición de ARP.
Protocolo simple de administración de red (SNMPv1)	RFC1157 RFC1155 RFC1212 RFC1215	Protocolo simple de administración de red. (STD15) Estructura e identificación de la información de administración para internets basadas en TCP/IP. (STD16) Definiciones concisas de MIB. (STD16) Una convención para capturas de definición a usar con SNMP.
Base de información de administración (MIB-II)	RFC1213	Base de información de administración para la administración de red de internet basadas en TCP/IP: MIB-II. (STD17)
ENTITY MIB	RFC2737	Entity MIB (Versión 2)

La tabla continúa…

Protocolo	RFC	Descripción
Protocolo de información de enrutamiento (RIP)	RFC1058 RFC2453 RFC1722	Un protocolo de vector de distancia que permite a los enrutadores determinar la ruta más corta hacia una red de destino. Hace esto al medir la cantidad de rutas intermediarias que se deben cruzar para alcanzar la red de destino. Si existe más de una ruta hacia el mismo destino se usa la ruta más corta. Si ocurre una falla en la ruta más corta se volverá a marcar como infinita y una ruta alternativa se convertirá en la nueva ruta más corta. Este comportamiento se puede usar para agregar resistencia a una red de datos. Donde un cliente tiene una red de datos existente que comprende los enrutadores de terceros, IP Office agregado a la red puede proporcionar una copia de seguridad usando su capacidad de enrutamiento y marcación. Los enrutadores habilitados con RIP comparten su conocimiento de la red al anunciar y escuchar los cambios de la tabla de enrutamiento. IP Office admite los estándares RIP I y RIP II.
Protocolo de seguridad de Internet (IPSec)	RFC2401 RFC2402 RFC2403 RFC2404 RFC2405 RFC2406 RFC2407 RFC2408 RFC2409 RFC2410 RFC2411	Arquitectura de seguridad para el protocolo de Internet Encabezado de autenticación de IP El uso de HMAC-MD5-96 en ESP y AH El uso de HMAC-SHA-1-96 en ESP y AH El algoritmo de cifrado ESP DES-CBC con Explicit IV Carga de seguridad de encapsulación IP. (ESP) El dominio de seguridad IP de Internet de interpolación para ISAKMP Asociación de seguridad de Internet y protocolo de administración clave Intercambio de clave de Internet El algoritmo de cifrado NULO y su uso con IPSec Mapa de ruta del documento de seguridad IP

La tabla continúa…

Protocolo	RFC	Descripción
Protocolo de túnel nivel 2 (L2TP)	RFC2661 RFC3193	La autenticación de PPP usando PAP o CHAP ocurre únicamente entre enrutadores conectados de forma directa. Cuando se usa una red IP pública para conectar los sitios, esta autenticación ocurre entre el enrutador del cliente y el enrutador del proveedor de servicios al que está conectado. En algunas circunstancias se recomienda autenticar entre los enrutadores del cliente y omitir todos los enrutadores intermediarios de la red del proveedor de servicios. El protocolo de túnel nivel 2 permite que esto ocurra al facilitar una autenticación de dos etapas, primero con el enrutador del proveedor de servicios y luego con el enrutador del cliente en la red remota. Los túneles de IPSec permiten a una empresa pasar datos entre ubicaciones por redes IP no seguras, como Internet público. La seguridad de los datos de la empresa se garantiza con cifrado 3DES, que los hace ininteligibles para las otras partes que podrían estar "escuchando a escondidas" en el tráfico. El protocolo de túnel se puede aplicar para unir oficinas o para ofrecer acceso a la oficina a los empleados por Internet. Todos los sistemas IP Office admiten un total de 256K de tráfico cifrado hacia múltiples ubicaciones. Inicialmente, el interfuncionamiento se admite solo entre IP Offices que estén conectados directamente en un puerto WAN o a través de la LAN con un enrutador de tercero. IPSec es opcional y se habilita en IP Office con una clave de licencia.
Servicios diferenciados (DiffServ)	RFC2474	Arquitectura de red que especifica un mecanismo simple, escalable y general para clasificar y administrar el tráfico de red y brinda calidad de servicio (QoS) en redes IP.
Encapsulación de Frame Relay	RFC 1490	Interconexión del protocolo múltiple en Frame Relay

Estándares de Protocolo de inicio de sesiones (SIP)

Rec. E.164 [2] Recomendación ITU-T E.164: el plan de numeración de telecomunicaciones públicas internacionales

RFC 2833 [7] Carga de RTP para los dígitos de DTMF, los tonos y las señales de telefonía

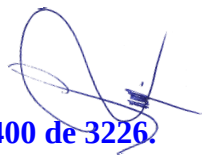
RFC 3261 [8] SIP: protocolo de inicio de sesión

RFC 3263 [10] Protocolo de inicio de sesión (SIP): localización de servidores SIP

RFC 3264 [11] Un modelo de oferta/respuesta con protocolo de descripción de sesión (SDP)

RFC 3323 [14] Un mecanismo de privacidad al protocolo de inicio de sesión (SIP)

RFC 3489 [18]	STUN: protocolo de datagrama de usuario de transversal simple (UDP) a través de los traductores de dirección de red (NAT)
RFC 3824 [24]	Uso de números E.164 con el protocolo de inicio de sesión (SIP)
RFC 1889	RTP
RFC 1890	Audio RTP
RFC 4566	SDP
RFC 3265	Notificación de eventos
RFC 3515	Refer SIP
RFC 3842	Mensaje en espera
RFC 3310	Autenticación
RFC 2976	INFORMACIÓN
RFC 3323	Privacidad para SIP (PAI) y draft-ietf-sip-privacy-04 (RPID)
RFC 3325	Extensiones de privacidad al protocolo de inicio de sesión (SIP) para la identidad afirmada dentro de redes confiables
RFC 3581	Una extensión al protocolo de inicio de sesión (SIP) para enrutamiento de respuesta simétrica
RFC 3311	Método de ACTUALIZACIÓN del protocolo de inicio de sesión (SIP)



Glosario

Aplicación de telecomunicaciones compatible con la computadora (CSTA)	Una interfaz estándar para las aplicaciones de Integración de telefonía e informática (CTI), tales como correo de voz y operadora automática, que permite interactuar con el equipo de telefonía.
Comisión Federal de Comunicaciones (FCC)	Un organismo federal de Estados Unidos que regula las comunicaciones, por ejemplo las comunicaciones por cable e Internet.
Communication Manager	Un componente clave de Avaya Aura®. Proporciona capacidades enriquecidas de voz y video y una red resistente y distribuida para puertas de enlaces de medios y dispositivos de comunicación analógicos, digitales y basados en IP. Incluye funciones de portabilidad avanzadas, aplicaciones incorporadas de llamada en conferencia, centro de contactos y capacidades de E911.
Conmutador de enrutamiento Ethernet (ERS)	El sistema de chásis apilable de Avaya que ofrece conectividad de conmutación Ethernet de alto rendimiento, convergente, segura y resistente.
Conversión de direcciones de red y puertos	Una técnica de enrutamiento de red. La traducción de puertos de direcciones de red (NAPT) se utiliza para acceder a sistemas en la misma subred que IP Office.
Directory Enabled Management	Una interfaz que utiliza Avaya Directory Server para simplificar la administración de Modular Messaging desde una ubicación centralizada.
Extensión a número de acceso de celular	El número de teléfono marcado para conectarse al servidor Avaya que está ejecutando Communication Manager. La extensión a número de acceso de celular inicia el proceso de activación o desactivación de la extensión a celular o cambia el código de seguridad de la estación.
Intercambio dinámico de datos (DDE)	Un método de comunicación entre procesos (IPC).
Interfaz de expansión	Un paquete de circuitos de puerto en una red de puertos (PN) que proporciona la interfaz entre un bus multiplexado de división de tiempo (TDM) o un paquete de bus en la PN y un vínculo de fibra óptica. La interfaz de expansión (EI) transporta datos con conmutación de circuitos, datos con conmutación de paquetes, control de red, control de tiempo y control de señal digital 1 (DS1). EI en una red de puerto

Página401 de 3226.

	de expansión (EPN) también se comunica con el paquete de circuito de mantenimiento principal para proporcionar el estado del entorno y el estado de alarma de EPN al elemento de procesamiento del conmutador (SPE).
Interfaz de programación de aplicaciones de telefonía (TAPI)	Una API de Microsoft® Windows que le permite utilizar servicios de telefonía a los equipos que ejecutan Windows. TAPI se utiliza para comunicaciones de datos, FAX y voz. Las aplicaciones pueden utilizar TAPI para controlar funciones de telefonía tales como marcar, atender y colgar.
Interfaz de proveedor de servicio de telefonía (TSPI)	Una interfaz definida por Microsoft para el proveedor de servicio de telefonía (TSP). Microsoft® Windows cuenta con un TSP H.323, un TSP de conferencia IP, un TSP controlador de dispositivo en modo Kernel y un TSP unimodem.
Llamadas completadas en hora pico	Es una medición de las llamadas de tráfico dinámico que se pueden completar en una hora pico promedio.
Novell® eDirectory™	Un producto de software para servicio de directorio compatible con X.500 que Novell® lanzó por primera vez en 1993 para administrar de forma central el acceso a los recursos en múltiples servidores y computadoras dentro de una red determinada. Novell® eDirectory™ se conocía anteriormente como Novell® Directory Services. Se le refiere en ocasiones como Servicios de directorio Netware. Novell® eDirectory™ es una base de datos jerárquica, orientada al objeto que se utiliza para representar ciertos activos en una organización en un árbol lógico, incluye las personas, las posiciones, los servidores, las estaciones de trabajo, las aplicaciones, las impresoras, los servicios y los grupos.
OFCOM	La oficina de comunicaciones del Reino Unido para la regulación de las telecomunicaciones.
PARTNER® Cierre de contacto adjunto	Un dispositivo que se conecta al chasis de una puerta de enlace de medios y proporciona cierres de contacto. Cierre de contacto adjunto (CCA) cierra un relé en respuesta a un comando de marcación entrante que proviene de la puerta de enlace de medio para operar una puerta o llevar a cabo una acción similar.
Política de enrutamiento de red	Una aplicación para administrar de forma central el enrutamiento SIP para las instancias Session Manager. Una política de enrutamiento que describe el modo en que se enruta una llamada: el origen, el destino, el patrón de marcación, la hora del día en que se enruta y el costo de un enrutamiento determinado.
Procesador de supervivencia local	Una configuración del servidor de medios S8300 en la que el servidor actúa como alternativo o como equipo selector para entidades IP, como los teléfonos IP y las puertas de enlace de medios G700. Estas entidades IP usan el procesador de supervivencia local (LSP) cuando pierden conectividad con el servidor primario.

Protocolo de comunicaciones digitales	Un protocolo exclusivo que se utiliza para transmitir datos y voz digitalizados por el mismo vínculo de comunicaciones. Un vínculo de protocolo de comunicaciones digitales (DCP) consta de dos canales de información de 64 kbps (I) y un canal de señalización de 8 kbps (S). El protocolo DCP admite dos canales que transmiten información y dos teléfonos o módulos de datos.
Protocolo de configuración dinámica de host (DHCP)	Un protocolo de Grupo de trabajo de ingeniería de Internet (IETF) que se utiliza para automatizar la asignación y administración de direcciones IP.
Protocolo de Internet	Un protocolo sin conexión que funciona en el Nivel 3 del modelo de interconexión de sistemas abiertos (OSI). El protocolo de Internet (IP) se utiliza para el direccionamiento en Internet y enrutamiento de paquetes en redes múltiples hacia un destino final. IP funciona junto con el protocolo de control de transmisión (TCP) y se identifican como TCP/IP.
Puerta de enlace de medios	Un elemento de hardware que permite aplicaciones y es parte de la familia de tales elementos. Esta familia incluye conectividad intraconmutadores, interfaces de control, interfaces de puerto y armario. Avaya: sus puertas de enlace de medio admiten tanto el tráfico de portador como el tráfico de señalización que se enruta entre las redes de conmutación de paquete y las redes de conmutación de circuito para entregar capacidades de datos, voz, fax y mensajería. Las puertas de enlace de medios ofrecen conversión de protocolo, como IP a ATM a TDM; conferencia; presencia, como activación o desactivación; conectividad a redes privadas y públicas, como IP, ATM, TDM y redes, como QSIG, DCS, ISDN. Las puertas de enlace de medio admiten factores de forma opcionales.
Red de puerto de expansión	En las configuraciones de Intuity Audix Server, una red de puerto (PN) que está conectada al bus multiplexado de división de tiempo (TDM) y al paquete de bus de una red de puerto de procesador (PPN). El control se logra con la conexión indirecta de EPN a PPN a través de un vínculo de red de puerto (PNL).
Red de teléfono pública conmutada (PSTN)	Una red de teléfono que incluye muchas tecnologías de comunicación, como transmisión por microonda, satélites y cables submarinos.
Remote Feature Activation	Una aplicación Avaya basada en la web para activar funciones de forma remota y aumentar las capacidades del sistema de un cliente mediante la entrega de un archivo de licencia nuevo.
Selección de ruta automática	Es una función que presentan algunos teléfonos y gracias a la cual el sistema selecciona automáticamente la forma más efectiva para enviar una llamada de pago.
Servicios técnicos globales	Un equipo de Avaya responde las llamadas de clientes sobre los productos en Administración integrada de Avaya.

Sistema de comunicaciones distribuido	Un protocolo entre redes exclusivo de Avaya con el que puede configurar dos o más redes de comunicación privadas basadas en Avaya para que funcionen como una sola gran red.
Sistema de licencia y entrega de productos (PLDS)	El sitio web de descarga y licencia de Avaya y el sistema de administración. Los socios comerciales y clientes de Avaya utilizan este sitio para obtener archivos de imágenes ISO y otras descargas de software.
Sistema de nombre de dominio (DNS)	Un estándar de Grupo de trabajo de ingeniería de Internet (IETF) que las cadenas ASCII utilizan para representar direcciones IP. El DNS es un servicio de directorio interno distribuido que se utiliza mayormente para traducir nombres de dominio y direcciones IP. Los teléfonos IP de la serie 9600 de Avaya pueden usar DNS para resolver los nombres en direcciones IP. En DHCP, TFTP y archivos HTTP, los nombres DNS pueden usarse donde sea que las direcciones IP estén disponibles, en tanto y en cuanto primero se identifique un servidor DNS válido.
Sistema de presentación de información de producto	El sistema de presentación de información de producto (PIPS) hace un reporte de los datos provistos por el Experto en información de productos (PIE), una herramienta para minería de datos que extrae información sobre configuración adjunta y conmutador del cliente Avaya y la almacena en una base de datos.
System Manager	Un marco de administración común de Avaya Aura® que proporciona funciones de administración centralizadas para el aprovisionamiento y la administración a fin de reducir la complejidad de la administración. System Manager también puede funcionar como autoridad de certificado (CA) raíz o como CA intermedia. System Manager permite la aplicación del protocolo simple de inscripción de certificado (SCEP) para la firma de certificados para teléfonos de escritorio Avaya.
System Status Application	Una aplicación IP Office que muestra el estado de los elementos, tales como las llamadas salientes.
Teletrabajo	Es la configuración donde Communication Manager establece la conexión de voz a un teléfono con conmutación de circuitos. Requiere dos conexiones: una conexión TCP/IP para el control de la señalización y una conexión con conmutación de circuitos para la voz.

Índice

A

acceso a Internet 54
Acceso a Internet 55
Acceso central 88
acceso móvil simplificado 52
acceso remoto 47
Acceso remoto 60
Activar/Desactivar grupo de búsqueda 23
administración 91
administración centralizada 91
administración de llamadas 14
    llamadas salientes 29
administración de llamadas de salida 30
Administración de SoftConsole 88
Administrador 67
Adquirir llamada 28
alerta 61
alerta de umbral de cola 32
alternar llamadas 17
anuncio 26
aplicaciones de usuario final 69
Aplicaciones IP Office
    aplicaciones de centro de contactos 95
    aplicaciones de instalación y administración 83
    aplicaciones de usuario 69
Aplicación para administración de soluciones 88
Archivo WAV 28
ARS 25, 53
asignados 58
asignar llamada ante respuesta del agente 31
asignar llamadas 31
auricular 23
Auricular 55, 67
Autoadministración 67
Avaya Communicator 73
    iPad 74
    Windows 75
Avaya Contact Center Select
    descripción general 96
avisos 30
Avisos 32

B

Base 60
Base de conocimiento InSite 101
BLF 64
Botón Altavoz 67
botones 62
botones de apariencia de línea 62
botones de apariencia de llamada 62
botones de apariencia en puente 62
Botones de apariencia en puente 63
botones de cobertura de llamada 62, 63
botones programables 62

C

CA 88
calidad de voz 25
call redirection 36
campo de luz de ocupado 64
capacitación 99
Capa integral de 10/100 Mbit 59
captura 23
CBCP 53
CDR 29
centro de contactos 95
CHAP 60
cliente web
    cliente web de IP Office
        webrtc 72
cobertura para operador 16, 25
códigos de autorización 29
códigos de cuenta 27, 29
códigos de cuenta forzados 27
colgado 23
Colgado 67
Comienzo rápido 34
Communication Manager 94
comparación de las funciones de mensajería 43
Compatibilidad de línea concedida 60
compresión 39
compresión de voz 39
Conexión automática 53
conference join 22
Conferencia Meet-Me 80
conferencing 36
con firewall 59
Conmutador de Ethernet 59
Consola de administración de SNMP 88
Control de protocolo 53
correo de voz 46
    reenvío a 17
Correo de voz 32, 55
correo de voz visual 67
Correo electrónico 59
costo de llamada 27
CP 53
Cuotas 55

D

DDI 26
descripción general 95
    Avaya Contact Center Select 96
Desvío de tráfico de llamadas de India 24
DevConnect 102
Devolución automática de llamada 14
devolución de llamada 14, 53
DHCP 58, 60
día lluvioso 40
DID 26

direccionamiento
Servicio de nombre de dominio 58
Directorio personal centralizado 66
Disponible 67
DMM 91
DND 22, 25
DNS 58, 59
document changes 8
documentos relacionados 98
Dominio 58, 59
DTMF 35
duración máxima de llamada 26

E

E1/T1 ..... 58, 60
ediciones de ip office 10
el enrutador satisface 59
Embedded Voicemail 78
emergency calling 23
Encabezados de privacidad y PAI 35
en espera 17, 23
En espera 58, 59
enlace de horario
oficina 59
Enlace WAN 59
enrutamiento de llamadas entrantes 32
enrutamiento menos costoso 53
Entradas de horario 55
Entradas múltiples de horario 55
Equinox for IP Office
Equinox
Avaya Equinox 71
especificaciones
protocolos 105
esquemas de numeración 55
estacionar 17
Estación de teléfono descolgado 23
Estándares regulativos 103
Ethernet 59
etiquetado de llamadas 19
extensiones
creación automática 33

F

Fallback Twinning 51
filtrado de llamadas 15
firewall
Ofertas de Small Office Edition 59
firewalls 54, 60
Frame Relay 59
FTP 54
fuera de servicio 30
funcionamiento de tecla y luz 61

G

gestor de operaciones en la nube 90
grabación de voz 19
grupos de búsqueda 30
grupos de búsqueda *(continuado)*
avisos 30
grupos de desbordamiento 31
Modo de servicio nocturno 31
grupos de desbordamiento 31

H

hermanamiento 50
historial de llamadas 65

I

Identificador de llamada 66
Idioma 67
indicadores
ocupado 64
información general de las funciones 81
inicio de sesión del agente 28
intrusión 20, 23
intrusión de llamada 20
IP412 ..... 58, 59
IP500 59
iPad 74
ISDN 58, 59

L

LCP 53
Licencias 92
licencias centralizadas 92
Línea concedida 58, 59
tipos 60
línea directa 22
lista de excepciones 22
Llamada de datos 55
llamada en espera 17, 20
llamadas
adquirir 28
enrutamiento entrante 32
Pantalla para nombre de directorio entrante 35
reenvío 15
restricción 29
supervisión 29
llamadas de conferencia 21, 79
llamadas de filtrado 15
Llamadas de grupos de búsqueda 55
llamadas entrantes
tonos de timbre 61
llamadas privadas 30
los servidores brindan 59
luces 61
luces de espera de mensaje 65
luces de llamada externa 65

M

madn
botones 63
Manager 83
Marcación con teléfono colgado 67

Marcación directa interna 26
marcación entrante 60
marcar emergencia 25
media manager
overview 86
medios iniciales 33
Menor costo 55
mensaje en espera 65
mensajería 42, 46
modo de sistema clave 30
Modo fuera de servicio 31
Monitor 67
Multiplexores WAN 59
Mundo 59
música de espera 28
MWI 65

N

new features 11
Nivel de firewall 59
Nombre en pantalla del nombre SIP 35
no molestar 22
no segura 59
notas de la aplicación 102
numeración de la red 55
numeración del nodo 55
numeración enlazada 55
numeración predeterminada 25

O

Oficina central (CO) 59
one-X Mobile Preferred 69
one-X Portal for IP Office 70
overview 10

P

PAP 60
Perfil de horario 55
perfiles de horario 33
plan de marcación 25
PPP 59
PRACK 33
preferencia de línea inactiva 30
privilegio de llamada saliente transferible 27
privilegios de llamada saliente 27
Protocolo de control de devolución de llamada 53
Protocolo de control de enlaces 53
Protocolo punto a punto\ 59
protocolos 105
protocolos de red 105
PSTN toll bypass 36
Público 55, 59
Puente de conferencia 55
Puerta de enlace 59
Puertos Ethernet 59
Punto a punto 59

R

Radvision 80
RAS 60
recuperación de llamadas 24
Red de área extensa 59
Red de área local 58–60
redes
multisitio 56
SCN 56
red multisitio 56
redundancia 40
reenviar grupo de búsqueda 16
Reenviar si da ocupado 16
Reenviar si no responde 16
Reenvío de llamadas 15
reenvío incondicional 17
Reenvío incondicional 17
registros de llamadas 27
relé activado/desactivado/pulso 24, 26
Reloj 60
remote worker 49
Resto del 59
restricción de llamadas 25, 29, 30
restricciones de acceso a Internet 33
Restringir interconexión de redes 24
ruta directa de medios 33
Rutas de menor costo 55

S

SCN 56
Scopia 80
Selección de ruta alternativa 25, 53
Server Edition Manager 84
Servicio de nombre de dominio 58, 59
servicio nocturno 30
Servidor de acceso remoto 60
Servidor DHCP 58
Session Manager 94
Sígueme 16
SIP 36
SIPconnect 1.1 35
SIP endpoints 36
sistemas de correo de voz 92
sitios web de recursos 100
SMA 88
Small Community Network 56
SMDR 27
SoftConsole 23, 76
SOHO 25
Solución de colaboración de video 80
Soporte de circuito de marcación 58
soporte técnico 101
SSA 89
SSL/VPN 60
standard call features 36
supervisar llamadas 29
supervisión
calidad de voz 25
supervivencia 40
supresión de silencio 35

Página407 de 3226.

SysMonitor 90
System Manager 92

T

T1 60
teclas 61
telefonía 40
telefonía centralizada 40
teléfonos
botones de apariencia 62
botones de apariencia de línea 62
botones de apariencia de llamada 62
Botones de apariencia en puente 63
botones de cobertura de llamada 63
botones de programación 62
funcionamiento de tecla y luz 61
luces de llamada externa 65
Teléfonos IP 67
teletrabajador 50
texto de ausencia 18
timbrado 14
timbre al transferir 18
timbre característico 15
timbre demorado al capturar 22
Timbre personalizado 17
Tomar llamada 28
tonos 18
tonos de timbre 61
tráfico de voz 59
tramado 59
transferencia ciega 18
transferencia con supervisión 18
transferencias 18
transferencia sin supervisión 18
Transporte fax 34

U

Unidad base 60
uso compartido de escritorio 47
uso compartido de escritorio remoto 48
usuario
privacidad 24

V

V.24 60
V.35 ..... 59, 60
V24 60
V35 60
Versión 4.1 ..... 55, 59
Videoconferencia 80
videos 100
Voicemail Pro 78
VPN 52

W

WAN 59, 60
Web Manager 85
WINS 58

X

X.21 ..... 59, 60

Traducido del inglés al español - www.onlinedoctranslator.com

Oficina IP de Avaya™Plataforma Solución Descripción

Versión 11.0.4
Mayo 2019

©2018-2019, Avaya Inc. Todos
los derechos reservados.

Aviso

Si bien se han realizado esfuerzos razonables para garantizar que la información de este documento sea completa y precisa en el momento de la impresión, Avaya no asume ninguna responsabilidad por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información de este documento sin la obligación de notificar a ninguna persona u organización sobre dichos cambios.

Descargo de responsabilidad de la documentación

"Documentación" se refiere a la información publicada en diversos medios que pueden incluir información sobre el producto, instrucciones de funcionamiento y especificaciones de rendimiento que generalmente se ponen a disposición de los usuarios de los productos. La documentación no incluye materiales de marketing. Avaya no será responsable de ninguna modificación, adición o eliminación de la versión original publicada de la Documentación, a menos que dichas modificaciones, adiciones o eliminaciones hayan sido realizadas por Avaya o en su nombre expreso. El usuario final acepta indemnizar y eximir de responsabilidad a Avaya, a los agentes, servidores y empleados de Avaya frente a todos los reclamos, juicios, demandas y juicios que surjan de, o en relación con, modificaciones, adiciones o eliminaciones posteriores a esta documentación, en la medida en que lo haga End Usuario.

Descargo de responsabilidad del enlace

Avaya no es responsable del contenido o la confiabilidad de los sitios web vinculados a los que se hace referencia en este sitio o la documentación proporcionada por Avaya. Avaya no es responsable de la precisión de la información, declaración o contenido proporcionado en estos sitios y no respalda necesariamente los productos, servicios o información descritos u ofrecidos en ellos. Avaya no garantiza que estos enlaces funcionen todo el tiempo y no tiene control sobre la disponibilidad de las páginas enlazadas.

Garantía

Avaya proporciona una garantía limitada para el hardware y el software de Avaya. Consulte su contrato de venta para establecer los términos de la garantía limitada. Además, el lenguaje de la garantía estándar de Avaya, así como la información sobre el soporte para este producto mientras está bajo garantía, está disponible para los clientes de Avaya y otras partes a través del sitio web de Soporte de Avaya:https://support.avaya.com/ helpcenter/ getGenericDetails?detailId=C20091120112456651010 bajo el enlace "Garantía y ciclo de vida del producto" o el sitio sucesor designado por Avaya. Tenga en cuenta que si adquirió los productos de un socio de canal autorizado de Avaya fuera de los Estados Unidos y Canadá, dicho socio de canal de Avaya le proporciona la garantía y no Avaya.

"Servicio alojado" hace referencia a una suscripción de servicio alojado de Avaya que adquiere de Avaya o de un socio de canal autorizado de Avaya (según corresponda) y que se describe con más detalle en SAS alojado u otra documentación de descripción del servicio con respecto al servicio alojado aplicable. Si compra una suscripción al Servicio alojado, es posible que la garantía limitada anterior no se aplique, pero puede tener derecho a servicios de soporte en relación con el Servicio alojado, como se describe más adelante en los documentos de descripción del servicio para el Servicio alojado correspondiente. Comuníquese con Avaya o con el socio de canal de Avaya (según corresponda) para obtener más información.

Servicio alojado

LO SIGUIENTE SE APLICA ÚNICAMENTE SI COMPRA UNA SUSCRIPCIÓN AL SERVICIO ALOJADO DE AVAYA DE AVAYA O DE UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA), LOS TÉRMINOS DE USO PARA LOS SERVICIOS ALOJADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA,HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO BAJO EL ENLACE "Términos de uso de Avaya para servicios alojados" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, Y SON APLICABLES A CUALQUIER PERSONA QUE ACCEDA O UTILICE EL SERVICIO ALOJADO. AL ACCEDER O UTILIZAR EL SERVICIO ALOJADO, O AL AUTORIZAR A OTROS A HACERLO, USTED, EN NOMBRE DE USTED Y DE LA ENTIDAD PARA LA QUE LO ESTÁ HACIENDO (EN ADELANTE DENOMINADO INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA LOS TÉRMINOS DE USO. SI USTED ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR DICHA ENTIDAD A ESTOS TÉRMINOS DE USO. SI USTED NO TIENE DICHA AUTORIDAD, O SI USTED NO DESEA ACEPTAR ESTOS TÉRMINOS DE USO, NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO.

Licencias

LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA,HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, BAJO EL ENLACE "TÉRMINOS DE LICENCIA DE SOFTWARE DE AVAYA (Productos de Avaya)" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, SON APLICABLES A CUALQUIER PERSONA QUE DESCARGUE, UTILICE Y/O INSTALE SOFTWARE DE AVAYA, COMPRADO DE AVAYA INC., CUALQUIER AFILIADO DE AVAYA O UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA) BAJO UN ACUERDO COMERCIAL CON AVAYA O UN SOCIO DE CANAL DE AVAYA. A MENOS QUE AVAYA ACORDE LO CONTRARIO POR ESCRITO, AVAYA NO EXTENDERÁ ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE CUALQUIER PERSONA QUE NO SEA AVAYA, UNA AFILIADA DE AVAYA O UN SOCIO DE CANAL DE AVAYA; AVAYA SE RESERVA EL DERECHO DE TOMAR ACCIONES LEGALES CONTRA USTED Y CUALQUIER OTRA PERSONA QUE UTILICE O VENDA EL SOFTWARE SIN LICENCIA. AL INSTALAR, DESCARGAR O UTILIZAR EL SOFTWARE, O AUTORIZAR A OTROS A HACERLO, USTED, EN SU NOMBRE Y EN EL DE LA ENTIDAD PARA LA QUE ESTÁ INSTALANDO, INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA ESTOS TÉRMINOS Y CONDICIONES Y CREA UN CONTRATO VINCULANTE ENTRE USTED Y AVAYA INC. O LA AFILIADA DE AVAYA CORRESPONDIENTE ("AVAYA").

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el cual el alcance de la licencia se detalla a continuación. Cuando la documentación del pedido no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de Sistema Designado como se establece a continuación en la sección Licencia de Sistema(s) Designado(s) (DS) según corresponda. El número aplicable de licencias y unidades de capacidad para las que se otorga la licencia será uno (1), a menos que se especifique un número diferente de licencias o unidades de capacidad en la documentación u otros materiales disponibles para Usted. "Software" hace referencia a los programas informáticos en código objeto, proporcionados por Avaya o un socio de canal de Avaya, ya sea como productos independientes, preinstalados en productos de hardware y cualquier mejora, actualización, parche, corrección de errores, o versiones modificadas de los mismos. "Procesador designado" significa un único dispositivo informático independiente. "Servidor" hace referencia a un conjunto de Procesadores designados que aloja (física o virtualmente) una aplicación de software a la que acceden varios usuarios. "Instancia" significa una única copia del Software que se ejecuta en un momento determinado: (i) en una máquina física; o (ii) en una máquina virtual de software implementada ("VM") o implementación similar.

Tipos de licencia

Licencia de sistema(s) designado(s) (DS). El Usuario final puede instalar y utilizar cada copia o una Instancia del Software únicamente: 1) en una cantidad de Procesadores designados hasta la cantidad indicada en el pedido; o 2) hasta el número de Instancias del Software que se indique en el pedido, la Documentación o que Avaya autorice por escrito. Avaya puede solicitar que los Procesadores designados se identifiquen en el pedido por tipo, número de serie, clave de función, Instancia, ubicación u otra designación específica, o que el Usuario final los proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este objetivo.

Licencia de Usuario Concurrente (CU). El Usuario final puede instalar y utilizar el Software en varios Procesadores designados o en uno o más Servidores, siempre que solo el número de Unidades con licencia acceda y utilice el Software en un momento dado. Una "Unidad" hace referencia a la unidad en la que Avaya, a su exclusivo criterio, basa el precio de sus licencias y puede ser, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o correo de voz a nombre de una persona. o función corporativa (por ejemplo, webmaster o servicio de asistencia), o una entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software. Las Unidades pueden vincularse a un Servidor específico e identificado oa una Instancia del Software.

Licencia de clúster (CL). El Usuario final puede instalar y usar cada copia o una Instancia del Software solo hasta la cantidad de Clústeres que se indica en el pedido con un valor predeterminado de un (1) Clúster si no se indica. "Cluster" significa un grupo de Servidores y otros recursos que actúan como un solo sistema.

Licencia de empresa (EN). El usuario final puede instalar y usar cada copia o una instancia del software solo para el uso de una cantidad ilimitada de instancias del software en toda la empresa, según se indica en el pedido o según lo autorice Avaya por escrito.

Licencia de usuario nominal (NU). Usted puede: (i) instalar y usar cada copia o Instancia del Software en un solo Procesador o Servidor Designado por Usuario Designado autorizado (definido a continuación); o (ii) instalar y usar cada copia o Instancia del Software en un Servidor, siempre que solo los Usuarios designados autorizados accedan y usen el Software. “Usuario designado” significa un usuario o dispositivo que ha sido expresamente autorizado por Avaya para acceder y utilizar el Software. A discreción exclusiva de Avaya, un "Usuario designado" puede ser, entre otros, designado por nombre, función corporativa (por ejemplo, webmaster o servicio de asistencia técnica), una cuenta de correo electrónico o correo de voz en nombre de una persona o función corporativa, o un entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software.

Licencia Shrinkwrap (SR). Usted puede instalar y usar el Software de acuerdo con los términos y condiciones de los acuerdos de licencia aplicables, como la licencia "shrinkwrap" o "clickthrough" que acompaña o se aplica al Software ("Licencia Shrinkwrap").

Software de la herencia de Nortel

“Software Heritage Nortel” significa el software que fue adquirido por Avaya como parte de su compra de Nortel Enterprise Solutions Business en diciembre de 2009. El software Heritage Nortel es el software incluido en la lista de productos Heritage Nortel ubicada enhttps://support.avaya.com/LicenseInfo bajo el enlace "Productos de Heritage Nortel" o el sitio sucesor designado por Avaya. Para el software Heritage Nortel, Avaya le otorga al Cliente una licencia para usar el software Heritage Nortel proporcionado en virtud del presente únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la Documentación, y únicamente como integrado, para ejecución en, o para comunicación con equipos Avaya. Los cargos por el software Heritage Nortel pueden basarse en el grado de activación o uso autorizado según se especifica en un pedido o factura.

Derechos de autor

Salvo que se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, la documentación, el software, el servicio alojado o el hardware proporcionado por Avaya. Todo el contenido de este sitio, la documentación, el Servicio alojado y el producto proporcionado por Avaya, incluida la selección, disposición y diseño del contenido, es propiedad de Avaya o de sus otorgantes de licencias y está protegido por derechos de autor y otras leyes de propiedad intelectual, incluida la ley sui generis. derechos relativos a la protección de las bases de datos. No puede modificar, copiar, reproducir, volver a publicar, cargar, publicar, transmitir o distribuir de ninguna manera ningún contenido, en su totalidad o en parte, incluido cualquier código y software, a menos que Avaya lo autorice expresamente. La reproducción, transmisión, difusión, almacenamiento o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede ser un delito,

virtualización

Lo siguiente se aplica si el producto se implementa en una máquina virtual. Cada producto tiene su propio código de pedido y tipos de licencia. A menos que se indique lo contrario, cada Instancia de un producto se debe licenciar y pedir por separado. Por ejemplo, si el cliente usuario final o el socio de canal de Avaya desea instalar dos instancias del mismo tipo de productos, entonces se deben pedir dos productos de ese tipo.

Componentes de terceros

"Componentes de terceros" significa que ciertos programas de software o partes de los mismos incluidos en el Software o el Servicio alojado pueden contener software (incluido el software de código abierto) distribuido bajo acuerdos de terceros ("Componentes de terceros"), que contienen términos relacionados con los derechos de uso de ciertos partes del Software ("Términos de terceros"). Según sea necesario, la información sobre el código fuente del sistema operativo Linux distribuido (para aquellos productos que tienen el código fuente del sistema operativo Linux distribuido) y la identificación de los titulares de derechos de autor de los componentes de terceros y los términos de terceros que se aplican está disponible en los productos, la documentación o en el sitio web de Avaya. a:https://support.avaya.com/Copyright o el sitio sucesor designado por Avaya. Los términos de licencia de software de código abierto proporcionados como Términos de terceros son consistentes con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del código abierto.

software. Los Términos de terceros prevalecerán sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables en la medida en que estos Términos de licencia de software le impongan mayores restricciones que los Términos de terceros aplicables.

Lo siguiente se aplica solo si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO TIENE LICENCIA BAJO LA LICENCIA DE CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS POR LOS QUE NO RECIBE REMUNERACIÓN PARA (i) CODIFICAR VÍDEO EN CUMPLIMIENTO CON EL ESTÁNDAR AVC (“AVC VIDEO”) Y/O (ii) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL DE MPEG LA, LLC VERHTTP://WWW.MPEGLA.COM .

Proveedor de servicio

LO SIGUIENTE SE APLICA AL ALOJAMIENTO DE PRODUCTOS O SERVICIOS DE AVAYA POR PARTE DEL SOCIOS DE CANAL DE AVAYA. EL PRODUCTO O EL SERVICIO ALOJADO PUEDE UTILIZAR COMPONENTES DE TERCEROS SUJETOS A TÉRMINOS DE TERCEROS Y REQUIERE QUE UN PROVEEDOR DE SERVICIOS TENGA UNA LICENCIA INDEPENDIENTE DIRECTAMENTE DEL PROVEEDOR DE TERCEROS. EL ALOJAMIENTO DE PRODUCTOS DE AVAYA POR PARTE DE UN SOCIO DE CANAL DE AVAYA DEBE SER AUTORIZADO POR ESCRITO POR AVAYA Y SI DICHOS PRODUCTOS ALOJADOS UTILIZAN O INTEGRAN DETERMINADO SOFTWARE DE TERCEROS, INCLUYENDO, ENTRE OTROS, SOFTWARE O CÓDECS DE MICROSOFT, EL SOCIO DE CANAL DE AVAYA DEBE
OBTENGA DE FORMA INDEPENDIENTE CUALQUIER ACUERDO DE LICENCIA CORRESPONDIENTE, POR CUENTA DEL SOCIO DE CANAL DE AVAYA, DIRECTAMENTE DEL PROVEEDOR TERCERO CORRESPONDIENTE.

CON RESPECTO A LOS CÓDECS, SI EL SOCIO DE CANAL DE AVAYA ALOJA CUALQUIER PRODUCTO QUE UTILICE O INTEGRA EL CÓDEC H.264 O EL CÓDEC H.265, EL SOCIO DE CANAL DE AVAYA RECONOCE Y ACEPTA QUE EL SOCIO DE CANAL DE AVAYA ES RESPONSABLE DE TODAS LAS TARIFAS RELACIONADAS Y/O O REGALÍAS. EL CÓDEC H.264 (AVC) TIENE LICENCIA BAJO LA LICENCIA DE LA CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS EN LOS QUE NO RECIBE REMUNERACIÓN PARA: (I) CODIFICAR VÍDEO DE CONFORMIDAD CON EL ESTÁNDAR AVC (“AVC VIDEO ”) Y/O (II) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO CON LICENCIA PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL PARA LOS CÓDECS H.264 (AVC) Y H.265 (HEVC) DE MPEG LA, LLC VERHTTP://WWW.MPEGLA.COM .

De acuerdo con las leyes

Usted reconoce y acepta que es su responsabilidad cumplir con las leyes y reglamentaciones aplicables, incluidas, entre otras, las leyes y reglamentaciones relacionadas con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude y los derechos de interpretación musical, en el país o territorio donde se utiliza el producto Avaya.

Prevención del fraude de llamadas

El "fraude interurbano" es el uso no autorizado de su sistema de telecomunicaciones por parte de una parte no autorizada (por ejemplo, una persona que no es un empleado corporativo, agente, subcontratista o que no trabaja en nombre de su empresa). Tenga en cuenta que puede haber un riesgo de fraude de llamadas asociado con su sistema y que, si ocurre, puede resultar en cargos adicionales sustanciales para sus servicios de telecomunicaciones.

Intervención de fraude de llamadas de Avaya

Si sospecha que está siendo víctima de fraude de llamadas y necesita asistencia o soporte técnico, llame a la línea directa de intervención de fraude de llamadas del Centro de Servicio Técnico al +1-800-643-2353 para los Estados Unidos y Canadá. Para obtener números de teléfono de soporte adicionales, consulte el sitio web de soporte de Avaya:https://soporte.avaya.com o el sitio sucesor designado por Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de soporte de seguridad de Avaya en la sección Políticas de seguridad y soporte dehttps://support.avaya.com/security .

Las sospechas de vulnerabilidades de seguridad de productos de Avaya se manejan según el Flujo de soporte de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Descarga de documentación

Para obtener las versiones más recientes de la documentación, consulte el sitio web de soporte de Avaya:https://soporte.avaya.com , o el sitio sucesor designado por Avaya.

Comuníquese con el soporte de Avaya

Consulte el sitio web de soporte de Avaya:https://soporte.avaya.com para avisos y artículos sobre productos o Servicios alojados, o para informar un problema con su producto o Servicio alojado de Avaya. Para obtener una lista de números de teléfono y direcciones de contacto de soporte, vaya al sitio web de Soporte de Avaya:https://soporte.avaya.com (o el sitio sucesor designado por Avaya), desplácese hasta la parte inferior de la página y seleccione Contactar con el soporte de Avaya.

Marcas registradas

Las marcas comerciales, los logotipos y las marcas de servicio ("Marcas") que se muestran en este sitio, la Documentación, los Servicios alojados y los productos proporcionados por Avaya son Marcas registradas o no registradas de Avaya, sus afiliados, sus licenciantes, sus proveedores u otros terceros. Los usuarios no pueden usar dichas Marcas sin el consentimiento previo por escrito de Avaya o de un tercero que pueda ser propietario de la Marca. Nada de lo contenido en este sitio, la Documentación, los Servicios alojados y los productos debe interpretarse como una concesión, por implicación, impedimento legal o de otro modo, de cualquier licencia o derecho sobre las Marcas sin el permiso expreso por escrito de Avaya o el tercero aplicable.

Avaya es una marca registrada de Avaya Inc.

Todas las marcas comerciales que no son de Avaya son propiedad de sus respectivos dueños. linux®es la marca registrada de Linus Torvalds en los EE. UU. y otros países.

Contenido

Capítulo 1 Introducción..... 7
Objetivo..... 7
Cambia la historia..... 7
Capítulo 2: Oficina IP de Avaya™Descripción general de la plataforma..... 10
Ediciones de IP Office..... 10
Nuevo en esta versión..... 11
Características..... 13
Topología..... 14
Redes..... 14
Redes de voz conmutadas por circuito privado..... 14
Redes de voz públicas..... 15
Redes de voz y datos basadas en paquetes..... 18
Telefonía con protocolo de Internet..... 19
Integración de telefonía informática..... 27
Componentes..... 29
Componentes de hardware..... 29
Los telefonos..... 38
Aplicaciones de IP Office..... 40
Capítulo 3: Especificaciones de la solución..... 67
Configuraciones de referencia..... 67
Ediciones de IP Office..... 67
Otras opciones de implementación..... 73
Opciones de hardware y software..... 84
Especificaciones del servidor..... 85
Compatibilidad con el sistema operativo y el navegador..... 87
Requisitos de PC proporcionados por el cliente..... 91
Requisitos del entorno virtual..... 93
Interoperabilidad..... 93
Interoperabilidad del teléfono..... 95
IP Office y Avaya Aura®Interoperabilidad de Communication Manager..... 99
Interoperabilidad de BCM e IP Office..... 100
Especificación de seguridad..... 101
Detalles de seguridad de la plataforma y la aplicación..... 102
Asignaciones de puertos..... 105
Rutas de actualización típicas..... 106
Migración de BCM con CS1000 a IP Office..... 107
Migración de sucursales de IP Office..... 108
Licencias..... 109
Licencias PLDS..... 109

Migración de licencias ADI..... 110
Licenciamiento centralizado y nodal de Server Edition..... 111
Licencia de edición básica para nuevos sistemas..... 118
Licencias Essential Edition y Preferred Edition..... 118
Licencias de la edición del servidor..... 119
Licencias de sucursal 120
Licencias de Redes Comunitarias Pequeñas 120
Licencias troncales..... 121
Licencias de usuario..... 122
Licencias de punto final de IP..... 126
Licencias de prueba..... 126
Licencias de actualización..... 127
Capítulo 4: Recursos..... 130
Documentación..... 130
Búsqueda de documentos en el sitio web de soporte de Avaya..... 131
Capacitación..... 131
Visualización de videos de orientación de Avaya..... 132
Recursos adicionales de IP Office 133
Compatibilidad del producto..... 133
Apoyo..... 133
Uso de la base de conocimientos de Avaya InSite..... 134
Acceso a las notas de la aplicación Avaya DevConnect 134
lista del glosario..... 136

Capítulo 1 Introducción

Objetivo

Este documento describe IP Office desde una perspectiva holística que se centra en las vistas estratégica, empresarial y funcional de la arquitectura. Este documento también incluye una descripción de alto nivel de las especificaciones de la solución y las configuraciones de referencia disponibles.

Cambia la historia

La siguiente tabla describe los principales cambios realizados en este documento para cada versión.

Tema	Fecha de lanzamiento	Resumen de Cambios
Versión 11.0 FP4	febrero 2019	• Se actualizó el tema Novedades con las funciones de la versión 11.0 FP4. • Avaya Equinox actualizado™tema para agregar contenido en Shared Control y Avaya Vantage™apoyo. • Avaya one-X actualizado®Tema del portal para agregar mejoras de capacidad de servicio. • Se actualizó la información de licencias. • Se actualizó la sección de navegadores compatibles. • Se actualizó la sección Media Manager para agregar nuevas funciones admitidas en la versión 11.0 FP4 de IP Office. • Incluyó VMWare ESXi 6.7 como hipervisor compatible.

La tabla continúa...

Tema	Fecha de lanzamiento	Resumen de Cambios
Versión 11.0	mayo 2018	• Se actualizó el tema Novedades con las funciones de la versión 11.0. • Se eliminaron las referencias a IP Office Integrated Contact Reporter. • Se eliminaron las referencias a IP Office Video SoftPhone, ya que no es compatible con la versión 11.0. • Contenido agregado sobre las siguientes aplicaciones: - Gerente de Operaciones en la Nube - Equinoccio de Avaya™cliente para IP Office - Cliente web Avaya IP Office • Se actualizó la sección Administrador web para agregar contenido sobre el Panel de configuración. • Se actualizó la sección Media Manager para agregar nuevas funciones compatibles con la versión 11.0 de IP Office. • Se agregaron los teléfonos J169 y J179 a las secciones de interoperabilidad y disponibilidad de teléfonos.
Versión 10.1, Número 1	junio 2017	• Se actualizó la sección "Novedades en esta versión". • Información agregada sobre dos nuevas aplicaciones: IP Office Integrated Contact Reporter e IP Office Media Manager • Se agregó información sobre la compatibilidad con hipervisores adicionales en la sección "Requisitos del entorno virtual". • Información agregada sobre dos nuevos teléfonos DECT: 3730 y 3735 • Se agregó información sobre una nueva API/SDK de administración y dos nuevas interfaces de CTI: API de servicio web de CTI centralizado y SSI sobre servicios web. • Información agregada sobre dos nuevos módulos de expansión: DS16B2 y DS30B2 • Se agregó información de acceso granular en la sección "Administrador web". • Información de extensión agregada en la sección "Solicitud de estado del sistema (SSA)" • Se actualizó la sección "Sistema operativo y compatibilidad con navegadores"

La tabla continúa...

Tema	Fecha de lanzamiento	Resumen de Cambios
Versión 10.0, Número 1	julio de 2016	• Se actualizó la sección "Novedades en esta versión". • Se reemplazaron las referencias del teléfono 3740 DECT con 3745 DECT. • Contenido actualizado de Avaya Contact Center Select. • Hizo las siguientes actualizaciones importantes de licencias: - Se agregó más información contextual. - Nombres de licencia actualizados y sus códigos asociados. - Contenido de licencias de Server Edition reorganizado. - Se agregaron licencias de la Edición Básica. - Soporte de licencia de usuario básico aclarado.
Versión 9.1, Problema 01.18	febrero 2016	Este documento fue creado para reemplazar el*Descripción del producto Avaya IP Office*.

Capítulo 2: Oficina IP de Avaya™Plataforma

visión general

La oficina IP de Avaya™Platform es un sistema de telefonía rentable que admite una fuerza de trabajo móvil y distribuida con voz y video en prácticamente cualquier dispositivo. IP Office es una solución de comunicaciones modular e integrada que se amplía hasta 3000 extensiones y 150 sitios en una red multisitio con resiliencia. Haga coincidir un modelo de implementación con las necesidades de infraestructura, desde dispositivos simples hasta software virtualizado en un centro de datos con opciones intermedias. Mejore la experiencia del cliente y la eficiencia de los agentes del centro de contacto con una potente y asequible funcionalidad multicanal para voz, correo electrónico y chat web. La solución combina software de colaboración más centros de contacto multicanal, redes, seguridad y video.

IP Office proporciona un PBX híbrido con multiplexación por división de tiempo (TDM) y telefonía IP con compatibilidad con troncales, que se usan en cualquiera de los dos modos o en ambos al mismo tiempo. IP Office tiene capacidades de datos integradas, que brindan enrutamiento IP, conmutación y protección de firewall, entre LAN y WAN (LAN2).

Además de los servicios básicos de telefonía y correo de voz, IP Office ofrece opciones de telefonía fija y virtual. Las aplicaciones de softphone están diseñadas para brindar flexibilidad a los trabajadores remotos y permitirles acceder a servicios de telefonía, como hacer y recibir llamadas, correo de voz y desvío de llamadas desde su computadora o dispositivo móvil.

Ediciones de IP Office

IP Office también ofrece funciones avanzadas como conferencias de audio y video y voz sobre IP para satisfacer las necesidades cambiantes de las pequeñas, medianas y grandes empresas.

IP Office está disponible en muchos modelos de implementación según el tamaño de la empresa y las funciones requeridas mediante uno o todos los siguientes elementos:

- Software IP Office virtualizado que se ejecuta en una máquina virtual
- Servidor dedicado
- Unidad de control IP Office 500 V2 (IP500 V2)

Edición	Plataforma	tamaño de la empresa (usuarios)	Aborda las necesidades comerciales
Edición básica	IP500 V2	menos de 25	Capacidades simples de telefonía y mensajería solamente
Edición esencial	IP500 V2	20–99	Capacidades simples de telefonía y mensajería más telefonía IP con movilidad esencial
Edición preferida	IP500 V2	21–250	Capacidades de Essential Edition más comunicaciones unificadas con movilidad preferida
Edición del servidor	servidor linux, IP500 V2 y Expansión Linux	100 — 2000	Preferred Edition en una solución basada en software.
Seleccionar IP Office	servidor linux, IP500 V2 y Expansión Linux	100 — 3000	Preferred Edition en una solución basada en software con mayor escala y resiliencia.
Server Edition o IP Office Select con Software virtualizado	virtualizado	100 — 2000 (o) 100 — 3000	Preferred Edition en una solución basada en software con mayor escala y resiliencia.
Server Edition o IP Office Select alojado en la nube	Potencializado por la nuve por Avaya)	100–2000 (o) 25–3000	Preferred Edition en una solución basada en software con mayor escala y resiliencia.

IP Office Essential Edition y Preferred Edition también se denominan Modo estándar de IP Office. Cada edición se basa en la siguiente para ofrecer funcionalidad adicional.

Nuevo en esta versión

Oficina de PI™Platform Release 11.0 Feature Pack 4 ofrece las siguientes características y capacidades nuevas:

Nota:

Las funciones están disponibles en todo el mundo a menos que se especifique lo contrario. No todas las funciones son compatibles con todas las plataformas y teléfonos. Vea las descripciones para más detalles.

Hermanamiento alternativo

Con esta función, IP Office redirige las llamadas al número de teléfono móvil hermanado de los usuarios cuando no se puede acceder a las extensiones principales, incluso si la hermanación móvil está deshabilitada. Esta función proporciona un mecanismo para la conmutación por error a un dispositivo externo, como un dispositivo móvil y PSTN, si el sitio de un cliente que admite teléfonos IP Office pierde la conectividad con el centro de datos en la nube. Los siguientes dos códigos cortos están disponibles para deshabilitar y habilitar el hermanamiento alternativo móvil:

- **Desactivar el hermanamiento alternativo**: para deshabilitar el hermanamiento alternativo

- **Activar el hermanamiento alternativo**: Para habilitar el hermanamiento alternativo

Mejoras de IP Office Media Manager

Se agregaron las siguientes funciones a IP Office Media Manager:

- Eliminar grabaciones
- Registro de auditoría: los administradores pueden realizar un seguimiento del uso de los archivos de grabación en IP Office Media Manager. El siguiente tipo de uso de una grabación se puede rastrear usando esta característica:
  - Borrar
  - Descargar
  - Repetir
  - Búsqueda

Mejoras de seguridad para el registro de dispositivos SIP

Las nuevas mejoras de seguridad permiten a los administradores permitir o rechazar el registro de dispositivos SIP en IP Office en función de sus cadenas de Agente de usuario. Los administradores pueden usar los ajustes de configuración para agregar, modificar o eliminar cadenas de SIP User Agent en la lista negra de SIP UA, la lista blanca de SIP UA y la lista blanca de IP. Posteriormente, el**Agentes de usuario SIP permitidos**La configuración se puede utilizar para seleccionar qué agentes de usuario SIP pueden registrarse en IP Office.

Sincronización automática de usuarios con Avaya Spaces

Usuarios del sistema IP Office R 11.0 FP4 y detalles de usuario creados para Avaya Equinox™se puede sincronizar automáticamente con el servidor de Avaya Spaces. Para usar y recibir funciones adicionales de Avaya Spaces, los detalles de los usuarios configurados para Avaya Equinox™necesita usuarios coincidentes configurados en el servidor de Avaya Spaces. La sincronización se puede realizar de forma manual o automática.

Contraseña de extensión predeterminada

La contraseña de extensión predeterminada o PIN es diferente a la contraseña de usuario y es mucho más segura con un mínimo de nueve dígitos. Las implementaciones de IP Office R11.0 FP4 proporcionan un PIN de extensión predeterminado generado automáticamente de 10 dígitos, que se puede ver y modificar más adelante. Un ícono de ojo al lado del **Contraseña de extensión predeterminada**El campo en la interfaz de usuario se puede usar para ver la contraseña de extensión predeterminada existente.

Equinoccio de Avaya™soporte en Avaya Vantage™

Equinoccio de Avaya™es compatible con Avaya Vantage™teléfonos K165 y K175 en implementaciones de IP Office R 11.0 FP4.

Enrute las llamadas de troncales SIP entrantes en función de un encabezado SIP opcional

IP Office se puede configurar para usar el opcional**P-persona-llamada**encabezado en el mensaje SIP entrante para el enrutamiento de llamadas. IP Office lee elID de la parte llamada Pencabezado en el mensaje SIP y enruta las llamadas SIP entrantes en función de él.

Registradores SIP y H.323 deshabilitados por defecto

Para proteger IP Office R 11.0 FP4 de vulnerabilidades, el**H.323 Gatekeeper Habilitar**y**Habilitar registrador SIP**Los campos están deshabilitados por defecto. Cada vez que se agrega una nueva extensión H.323 o SIP y el registrador correspondiente no está habilitado, el sistema IP Office muestra un mensaje de error y solicita habilitar los campos. Cuando el soporte de resiliencia está habilitado en una línea de IP Office en sistemas que tienen extensiones de IP y los sistemas no tienen habilitados los registradores correspondientes,

El sistema IP Office muestra un mensaje de error y solicita a los administradores que habiliten los registradores correspondientes.

Equinoccio de Avaya™control compartido

Equinoccio de Avaya™ahora se puede usar en modo de control compartido con teléfonos de escritorio. La función de control compartido está disponible incluso cuando Avaya Equinox™los teléfonos cliente y de escritorio están registrados en diferentes sistemas dentro de la misma red.

Unirse a la conferencia

La función Unirse a la conferencia permite unir dos conferencias separadas en una sola conferencia que contiene a todos los participantes anteriores de ambas conferencias anteriores. Una vez que se han unido las conferencias, no es posible volver a las dos conferencias separadas nuevamente.

Compatibilidad con el módulo de 24 botones JEM en el teléfono IP Avaya J169/J179

Avaya J169/J179 IP Phone puede admitir hasta tres módulos de botones JEM24. Cada JEM24 tiene 24 botones de doble LED con pantalla de etiqueta de botón adyacente. Los LED de los botones se usan para indicar el estado de la función del botón, mientras que presionar el botón se usa para acceder a la función. Un solo JEM24 admite 72 espacios para botones programables. Estos están organizados en 3 páginas, a las que se accede mediante el botón de desplazamiento de página del módulo. Cuando se conectan varios módulos a un teléfono, cada módulo solo admite una sola página de 24 ranuras de botones programables.

Los módulos coinciden automáticamente con la configuración de pantalla del teléfono al que están conectados: color con Avaya J179 IP Phone o escala de grises con Avaya J169 IP Phone, tamaño de fuente, imagen de fondo, protector de pantalla. Los módulos de botones se alimentan a través del teléfono. Para obtener más información, consulte el*IP Office Platform R11.0 Guía del usuario del teléfono de la serie J100*.

Teléfono IP Avaya J139

Compatibilidad con IP Office para el teléfono IP Avaya J139. Avaya J139 IP Phone es un teléfono de escritorio SIP avanzado que admite la programación de botones y los menús interactivos de IP Office. Avaya J139 IP Phone no es compatible con todas las funciones avanzadas de trabajadores del conocimiento y centros de contacto que están disponibles en los teléfonos Avaya J169 IP Phone y Avaya J179 IP Phone. Para obtener más información, consulte el*IP Office Platform R11.0 Guía del usuario del teléfono de la serie J100*.

Mejoras en la capacidad de servicio en Avaya one-X®Portal

Avaya one-X®Portal admite una serie de funciones de mantenimiento, como mostrar el recuento de sesiones iniciadas, el avatar del usuario, la opción para bloquear versiones de clientes, la opción para rastrear intentos de inicio de sesión fallidos repetidos y la opción para borrar todas las sesiones de un usuario.

Autoadministración web simplificada

La interfaz mejorada se enfoca en simplificar la configuración y hacerla más fácil para los usuarios no técnicos y proporciona un asistente autoguiado de tres pasos para configurar la cuenta básica. De manera predeterminada, la nueva capacidad, que ejecuta el asistente, está habilitada para todos los usuarios, pero el administrador puede deshabilitar la capacidad o modificarla según sea necesario.

Características

Ver*Oficina IP de Avaya™Característica de la plataforma Descripción*para obtener descripciones detalladas de las funciones.

Topología

Hay muchas opciones para la topología de IP Office. Para obtener información detallada sobre todos los escenarios de implementación, consulte el*Configuración de referencia*documentos para cada escenario de implementación.

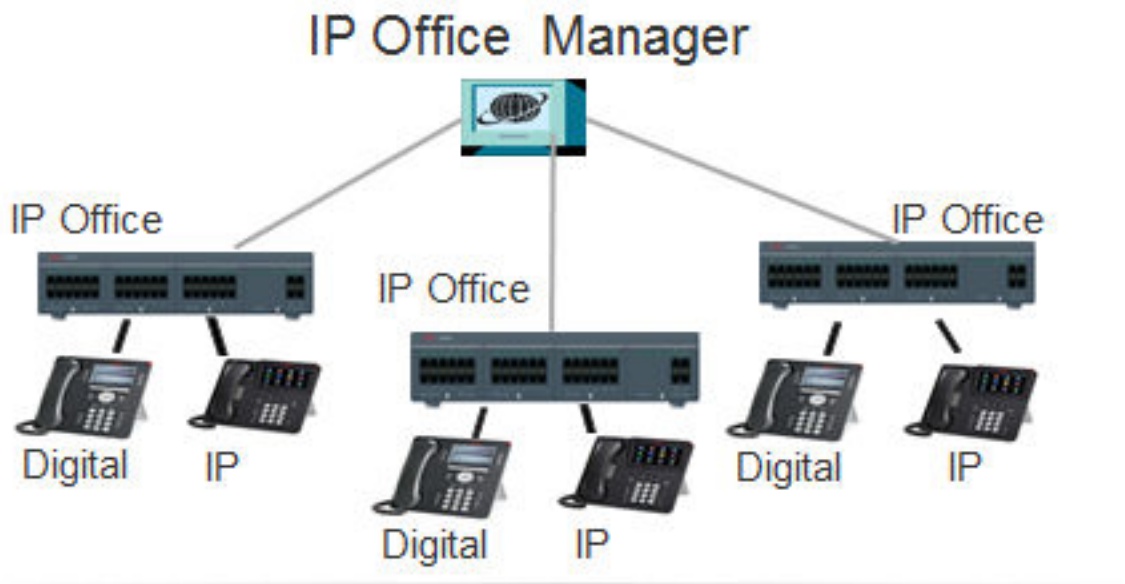


Figura 1: Sistemas IP Office conectados a un solo terminal de IP Office Manager

Redes

Redes de voz conmutadas por circuito privado

Cuando los circuitos de línea alquilada se usan en un escenario de red privada, estas interfaces E1 o T1 generalmente se configuran para usar señalización Q.SIG entre sitios.

Q.SIG proporciona un nivel de transparencia de funciones de voz entre PBX y es el estándar de señalización preferido dentro de múltiples proveedores y redes de voz internacionales. El módulo IP Office E1 o T1 termina una conexión QSIG con una interfaz RJ45 de 120 ohmios.

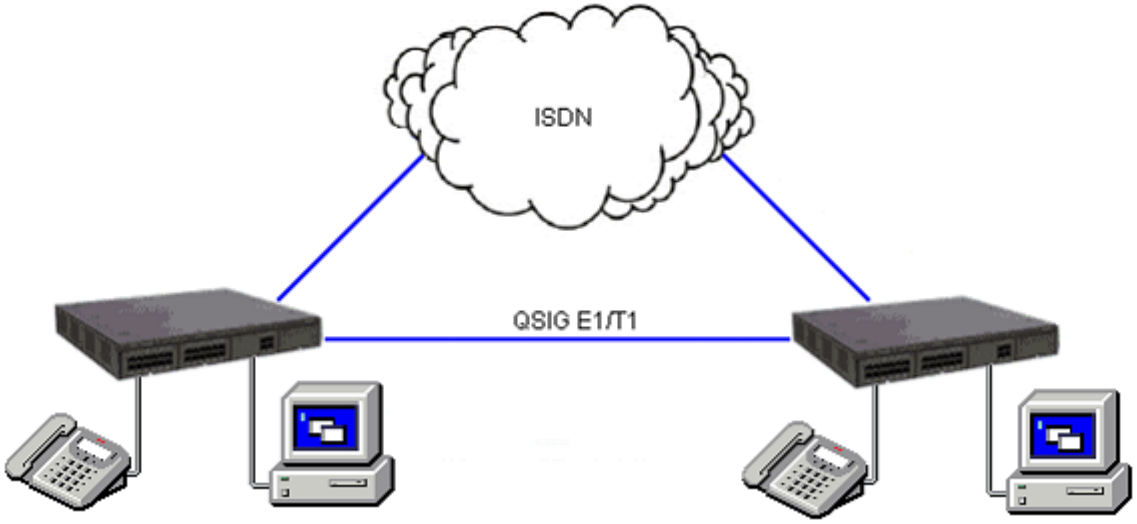


Figura 2: Redes de voz con conmutación de circuitos

IP Office admite los siguientes servicios Q.SIG en esta red: **Llamada de**

Telefonía Simple/Llamada Básica	ETS300 171/172
Llamada de datos con conmutación de circuitos/llamada básica	ETS300 171/172
Presentación de ID de línea llamada/llamante	ETS300 173
Presentación del llamado/nombre del llamante	(SS-CNIP, SS-CONP, SS-CNIR) ETS300 237/238
mensaje en espera	(SS-MWI) EN301 260/255
Transferir	(SS-CT) ETS 300 260/261

Redes de voz pública

IP Office admite una variedad de troncales y modos de señalización para la conexión a la red telefónica pública conmutada (oficina central). Algunas de estas líneas solo están disponibles en ciertos territorios; consulte con su distribuidor para conocer la disponibilidad local. Las troncales de tasa primaria están disponibles con una troncal simple (24/30 canales) o doble (48/60 canales).

Tarifa primaria ISDN (ETSI CTR4)

El servicio es provisto por tarjetas IP500V2 Universal PRI. ISDN Primary Rate proporciona 30 canales de voz PCM de 64K sobre un circuito E1 y un canal de señalización. Señalización Cumple con el estándar ETSI Q. 931 con verificación de errores de redundancia cíclica (CRC).

Se admiten los siguientes servicios complementarios:

línea de llamada Identificación Presentación (CLIP)	Proporciona el número de teléfono de la llamada entrante.
línea de llamada Identificación Restricción (CLIR)	Evita que se presente el número de teléfono de IP Office en una llamada saliente.
Marcación directa (DDI)	Donde el intercambio proporciona los últimos x dígitos del número marcado en una llamada entrante. Esto permite que IP Office enrute la llamada a diferentes usuarios o servicios.
subdireccionamiento	Permite la transmisión/recepción de hasta 20 dígitos, adicionales a cualquier información DDI/DID o CLIP, para fines de enrutamiento e identificación de llamadas.

IP Office admite las siguientes funciones en troncales PRI y BRI.

Nota:

La disponibilidad de funciones depende del proveedor de servicios ISDN por el cual puede haber cargos.

Llamada maliciosa Identificación (MCID)	(2400, 4600, 5400, 5600, T3, IP T3, 9500, 9600) Los códigos cortos y las funciones de programación de botones están disponibles para que los usuarios puedan activar esta actividad en el intercambio ISDN cuando sea necesario. Esta función NO está disponible en teléfonos ISDN DSS1 estándar.
Consejo de Cargo (COA)	(Solo teléfonos IP y digitales T3; Phone Manager) Se admite el aviso de cargo durante una llamada (AOC-D) y al final de una llamada (AOC-E) para llamadas ISDN salientes que no sean Q.SIG. El costo de la llamada se puede mostrar en los teléfonos T3 para fines de contabilidad de llamadas. IP Office permite la configuración de la moneda del costo de la llamada y un recargo del costo de la llamada para cada usuario.
Finalización de llamadas ocupado Abonado (CCBS)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, teléfonos DECT; Phone Manager) CCBS se puede utilizar cuando lo proporcione el proveedor de servicios ISDN. Permite establecer una devolución de llamada en llamadas RDSI externas que regresan ocupadas. También se puede utilizar para llamadas ISDN entrantes a un usuario ocupado. Esta función no está disponible en teléfonos ISDN DSS1 estándar.
Cambio de ruta parcial (PR)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, teléfonos DECT; Phone Manager) Al reenviar una llamada en un canal ISDN a un número externo mediante otro canal ISDN, el reenrutamiento parcial informa a la central ISDN que realice el reenvío, liberando así los canales a IP Office. Esta función no está disponible en teléfonos estándar ISDN DSS1 y no es compatible con Q.SIG.

Llamada explícita Transferencia (TEC)	(Usado normalmente por una aplicación de terceros) ECT es compatible con la interfaz S0. Una llamada a un terminal S0 se puede transferir a cualquier otro dispositivo, como un terminal analógico, digital o IP, o a cualquier troncal. El uso normal de esta función es por parte de una aplicación de terceros conectada a través de una o más interfaces S0 a IP Office. Un ejemplo es VoiceDirector, un asistente automático de llamadas.

Tarifa básica RDSI (ETSI CTR3)

El servicio es proporcionado por tarjetas IP500 V2 BRI. ISDN Basic Rate proporciona 2 canales de voz PCM de 64K y un canal de señalización mediante señalización Q.931 y comprobación de errores CRC. Se admite la operación punto a punto y punto a multipunto. Las líneas multipunto permiten que múltiples dispositivos compartan la misma línea; sin embargo, punto a punto es el modo preferido.

La tarifa básica admite todos los servicios que se admiten en la versión de tarifa principal con la adición de número de suscriptor múltiple. Este servicio suele ser mutuamente excluyente con el servicio DDI/DID y proporciona hasta 10 números para propósitos de enrutamiento, muy similar a DDI/DID.

Señalización asociada al canal E1R2

El servicio es proporcionado por tarjetas IP500 V2 Universal PRI.

La tarjeta IP500 Universal PRI configurada como PRI E1R2 admite una conexión de red RJ45 simple o doble. Cada tarjeta proporciona canales que se pueden configurar para marcación MFC, Pulse o DTMF según los requisitos de la red.

Tarifa primaria T1 norteamericana

El servicio es proporcionado por tarjetas IP500 V2 Universal PRI. T1 Primary Rate proporciona hasta 24 canales de 64K en un circuito de 1,54M. Cada canal del troncal T1 puede configurarse (canalizarse) de forma independiente para admitir las siguientes emulaciones de señalización con tipos de protocolo de enlace inmediato, retardado o parpadeante.

- Inicio de bucle
- Inicio en tierra
- Línea de enlace E&M
- E&M HIZO
- E&M conmutado 56K
- DID: los canales configurados para DID/DDI solo admiten llamadas entrantes. El operador o la oficina central proporcionará los últimos x dígitos que se marcaron para que se utilicen para el enrutamiento de llamadas.
- Guiño-Inicio

Las troncales T1 de IP Office admiten servicios DNIS y ANI, cuando estén disponibles en la oficina central.

Número marcado Cadena de identificación (DNIS)	Proporciona una cadena de dígitos a IP Office según el número marcado por la persona que llama. Esta cadena se puede usar para enrutar a las personas que llaman a extensiones, grupos o servicios individuales.
Número automático Identificación (ANI)	Proporciona a IP Office un número que identifica quién es la persona que llama. Esto puede usarse para enrutamiento o aplicaciones de telefonía informática.

Las tarjetas de troncales T1 incorporan una CSU/DSU integral, lo que elimina la necesidad de una unidad externa. La función CSU permite que la troncal se ponga en modo de bucle invertido para fines de prueba. Esto se puede configurar

manualmente, usando la aplicación de monitoreo, o automáticamente desde una Oficina Central enviando un patrón de Line Loop Back (LLB). La función DSU permite compartir el troncal T1 entre los servicios de datos y de voz.

Interfaz de velocidad primaria de América del Norte (PRI)

El servicio es proporcionado por las tarjetas IP500V2 Universal PRI. IP Office es compatible con troncales ISDN de tasa primaria en conmutadores de oficina central 5ESS o DMS100 proporcionados por AT&T, Sprint, WorldCom y otras empresas de telecomunicaciones locales. Los canales pueden configurarse previamente para los servicios admitidos o negociarse llamada por llamada.

Se pueden configurar servicios especiales para enrutar llamadas a operadores locales o proveedores pre-suscritos para llamadas nacionales e internacionales (SSS). También se pueden seleccionar operadores alternativos a través de la configuración de las tablas de selección de red de tránsito (TNS) de IP Office.

IP Office también es compatible con el servicio de nombre y número de llamada a través de troncales de velocidad primaria (NI2).

Troncales analógicos

Círculo comienzo

Las troncales de inicio de bucle están disponibles en las tarjetas de troncales analógicas de IP Office instaladas dentro de la unidad de control de IP Office o en los módulos de expansión de 16 puertos de troncales analógicas (ATM16). Los primeros dos troncales en el ATM16 se cambian automáticamente a enchufes de falla de energía en caso de que se interrumpa la energía. Powerfail también está disponible en la tarjeta de troncales cuando se instala en una tarjeta combinada o telefónica. Cumplen con el estándar TIA/EIA-646-B. Los troncales de inicio de bucle también admiten la identificación de línea de llamadas entrantes (ICLID) conforme a los estándares GR-188-CORE y GR-31-CORE. IP Office puede usar esta información para enrutar llamadas o proporcionarla a aplicaciones informáticas para mostrar información adicional sobre la persona que llama.

Terrestre comienzo

Las troncales Ground Start solo están disponibles en el ATM16, configurado a través de IP Office Manager. Los dos primeros troncales del módulo se cambian automáticamente a la toma de corriente en caso de que se interrumpa la alimentación. Cumplen con las normas ANSI T1.401 y TIA/EIA-646-B. No disponible en todos los territorios.

Redes de voz y datos basadas en paquetes

IP Office admite el uso de la red de datos para la comunicación de voz, llamada voz sobre IP (VoIP).

IP Office admite comunicaciones de voz y datos en red con los siguientes servicios:

- Enrutador IP incorporado
- Un enlace para redes de voz y datos
- Acceso común a Internet; compartir archivos y enviar correos electrónicos a otros sitios
- Compatibilidad con el protocolo RIP-2 para el enrutamiento dinámico de datos; IPSec VPN, cortafuegos y NAT (traducción de direcciones de red) y para seguridad; Gestión centralizada y gestión proactiva de fallos a través de SNMP.

IP Office admite redes de voz basadas en paquetes IP entre sitios a través de VoIP en la LAN del campus o VoIP en la red pública.

En un entorno de fábrica o campus, las llamadas de voz se pueden enviar a través de conexiones LAN de 10/100 Mbps en sistemas equipados con módulos de compresión de voz (VCM) opcionales. IP Office es compatible con Diffserve al marcar adecuadamente tanto los paquetes RTP como los paquetes de señalización para facilitar la administración del ancho de banda de la red.

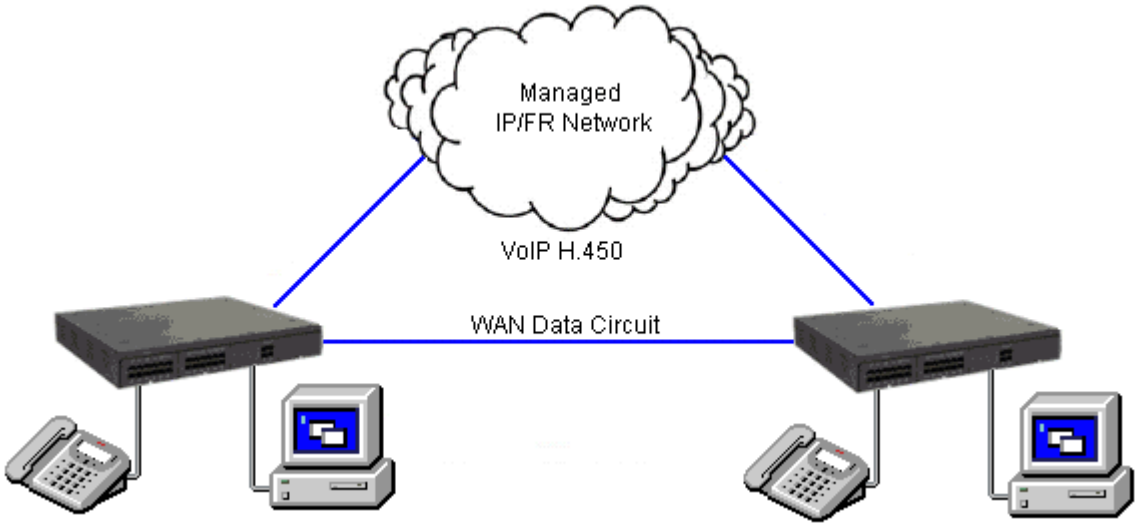


Figura 3: Red VoIP a través de una red IP o WAN

IP Office puede obtener los beneficios del soporte de servicios complementarios Q.931 y H.450 a través de una conexión pública donde se puede establecer una conexión QoS adecuada.

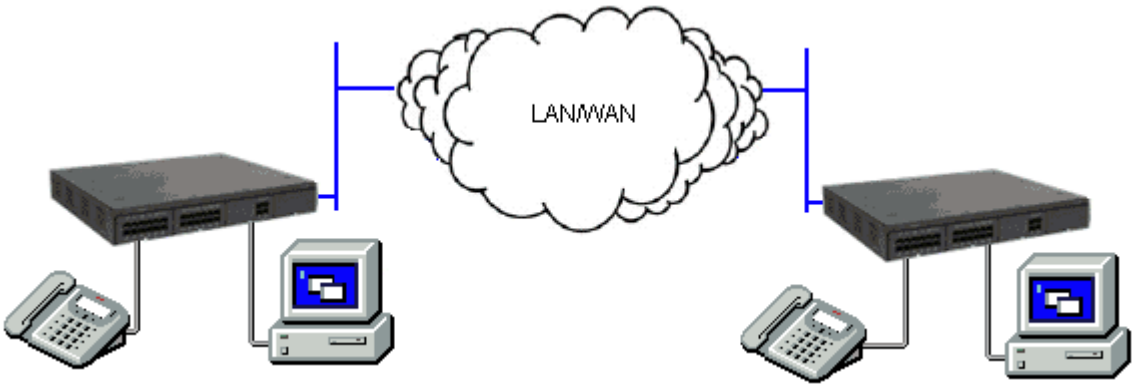


Figura 4: Red VoIP en la LAN

Telefonía con protocolo de Internet

El Protocolo de Internet (IP) se refiere al tipo de reglas que utiliza la red para enviar y recibir señales. La telefonía IP convierte las comunicaciones de voz en paquetes de datos. Convenientemente, funciona con tecnología Ethernet LAN (red de área local). La telefonía IP une las muchas ubicaciones de una empresa, incluidos los trabajadores móviles, en una única red de comunicaciones convergente.

IP Office es un sistema de telefonía convergente; combina aspectos de los sistemas de telefonía PABX tradicionales y los sistemas de telefonía y datos IP. IP Office es compatible con PSTN, SIP, POT, hora digital

Teléfonos multiplexados de división y teléfonos IP digitales todos en el mismo sistema. IP Office permite que todas las tecnologías coexistan.

IP Office se conecta a la PSTN ya los troncales IP proporcionando una función PABX "híbrida", donde las tecnologías heredadas y futuras se pueden usar juntas para minimizar los costos operativos y optimizar las comunicaciones comerciales a través de voz y datos. La funcionalidad convergente funciona en múltiples niveles:

- Los usuarios de teléfonos individuales pueden controlar el funcionamiento de su teléfono a través de aplicaciones que se ejecutan en su PC.
- El tráfico de datos se puede enrutar desde la interfaz LAN a una interfaz troncal de telefonía.
- El tráfico de voz se puede enrutar a través de enlaces de datos internos y externos. Esta opción se conoce como voz sobre IP (VoIP).

Voz sobre IP (VoIP) y evaluaciones de red

Voz sobre IP (VoIP) significa voz transmitida a través de una red de paquetes de datos. VoIP a menudo se denomina telefonía IP porque utiliza los protocolos de Internet para posibilitar comunicaciones de voz mejoradas dondequiera que existan conexiones IP.

El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas de clientes y/o teléfonos IP H.323 o SIP para usuarios. En cualquier caso, se deben considerar los siguientes factores:

- La unidad de control de IP Office debe estar equipada con canales de compresión de voz. Estos se utilizan cuando un dispositivo IP (troncal o extensión) necesita comunicarse con un dispositivo que no es IP (troncal o extensión) o con un dispositivo que utiliza un códec diferente.
- Una evaluación de la red es un requisito obligatorio para todos los sistemas que utilizan VoIP. Para problemas de soporte con VoIP, Avaya puede solicitar acceso a los resultados de la evaluación de la red y puede rechazar el soporte si no están disponibles o no son satisfactorios.

Una evaluación de la red incluiría una determinación de lo siguiente:

- Una auditoría de red para revisar el equipo existente y evaluar sus capacidades, incluida su capacidad para satisfacer las necesidades de voz y datos actuales y planificadas.
- Una determinación de los objetivos de la red, incluido el tipo de tráfico dominante, la elección de tecnologías y el establecimiento de objetivos de calidad de voz.
- La evaluación debe dejarle la confianza de que la red implementada tendrá la capacidad para el tráfico de voz y datos previsto, y puede admitir H.323, DHCP, TFTP y búferes de fluctuación en aplicaciones H.323.

Un resumen de los objetivos esperados de la evaluación de la red es:

Prueba	Objetivo mínimo de evaluación
Latencia	Menos de 150ms
Paquete perdido	Menos de 3%
Duración	Supervise las estadísticas una vez cada minuto durante una semana completa

Protocolos de señalización

Para hacer uso de VoIP, IP Office utiliza protocolos de señalización llamados H.323 y Protocolo de inicio de sesión (SIP), para establecer conexiones de extremo a extremo para la ruta de voz a través de una red IP. Este

La conexión garantiza que cada extremo pueda transmitir y recibir voz y proporciona el direccionamiento de red para la transmisión de paquetes de extremo a extremo. IP Office también conecta las diferentes tecnologías al traducir las señales que utilizan. Por ejemplo, un teléfono analógico puede conectarse a un destino de VoIP. Esta conexión requiere que se traduzcan tanto la señalización como la transmisión de voz. IP Office realiza esta traducción mediante puertas de enlace y guardianes.

Con la telefonía IP se conecta un teléfono IP a una IP PBX a través de una LAN. Hay dos tipos básicos de teléfonos IP:

- Un teléfono físico, que se parece mucho a un teléfono estándar, denominado "teléfono fijo"
- Una aplicación de software, denominada "softphone", que se ejecuta en la PC del usuario y le permite usar un auricular y un micrófono para realizar y recibir llamadas en cualquier lugar donde tenga una conexión IP.

Consideraciones de calidad de servicio

Al hacer uso de la telefonía IP, hay una serie de consideraciones centradas en los datos, como qué tipos de datos tienen prioridad en la red IP cuando hay contención. Esto se configura con calidad de servicio IP/TCP y no debe ignorarse. En situaciones en las que el ancho de banda de la LAN es limitado, se debe utilizar un conmutador de LAN con capacidad de calidad de servicio para garantizar que los paquetes de voz se transmitan con la prioridad requerida en la red. De lo contrario, la conversación transmitida a través de IP parece interrumpida debido a retrasos o se han introducido retrasos inaceptables en la conversación que causan latencia y fluctuación. Con los teléfonos fijos IP, existe la necesidad de alimentación a través de Ethernet (PoE), o suministros de energía telefónicos locales para los teléfonos, ya que los teléfonos IP no reciben alimentación de IP Office.

Canales de compresión de voz

Las llamadas hacia y desde dispositivos IP pueden requerir la conversión al formato de códec de audio que utiliza el dispositivo IP. Los sistemas IP Office utilizan canales de compresión de voz para realizar la conversión. Estos canales admiten los códecs de audio IP comunes G.711, G.723 y G.729a.

La aplicación de estado del sistema se puede usar para mostrar el uso del canal de compresión de voz. Dentro de**Recursos**sección muestra el número de canales en uso. También muestra con qué frecuencia ha habido canales insuficientes disponibles y la última vez que ocurrió tal evento.

Tabla 1: Canales de compresión de voz

Tipo de llamada	Uso del canal de compresión de voz
Dispositivo IP a dispositivo no IP	Requiere un canal de compresión de voz durante la duración de la llamada. Si no hay ningún canal disponible, la indicación de ocupado se devuelve a la persona que llama.

La tabla continúa...

Tipo de llamada	Uso del canal de compresión de voz
Dispositivo IP a dispositivo IP	Los tonos de progreso de llamada (por ejemplo, tono de marcado, tono de marcado secundario, etc.) no requieren canales de compresión de voz con las siguientes excepciones: • Los tonos de confirmación de código corto, activación de ARS y entrada de código de cuenta requieren un canal de compresión de voz. • Los dispositivos que utilizan G723 requieren un canal de compresión de voz para todos los tonos excepto para llamada en espera. Cuando se conecta una llamada: • Si los dispositivos IP utilizan el mismo códec de audio, no se utiliza ningún canal de compresión de voz. • Si los dispositivos usan diferentes códecs de audio, se requiere un canal de compresión de voz para cada uno.
Dispositivo no IP a dispositivo no IP	No se requieren canales de compresión de voz.
Música en espera reproducida en dispositivo IP	Se proporciona desde el bus TDM y, por lo tanto, requiere un canal de compresión de voz cuando se reproduce en un dispositivo IP.
Recursos de la conferencia y dispositivos IP	Gestionado por el chip de conferencia que está en el bus TDM. Por lo tanto, se requiere un canal de compresión de voz para cada dispositivo IP involucrado en una conferencia. Esto incluye servicios que usan recursos de conferencia como escucha de llamadas, intrusión, grabación de llamadas y monitoreo silencioso.
Llamada de buscapersonas a dispositivo IP	Utiliza G729a para llamadas de buscapersonas, por lo que solo requiere un canal, pero también solo admite búsquedas a dispositivos compatibles con G729a.
Servicios de correo de voz y dispositivos IP	Se tratan como llamadas de datos desde el bus TDM. Por lo tanto, las llamadas desde un dispositivo IP al correo de voz requieren un canal de compresión de voz.
Llamadas de fax	Estas son llamadas de voz pero con un rango de frecuencia ligeramente más amplio que las llamadas de voz habladas. IP Office solo admite fax a través de IP entre sistemas IP Office con la opción de transporte de fax seleccionada. Actualmente no es compatible con T38.
Llamadas de fax T38	IP Office admite fax T38 en troncales SIP y extensiones SIP. Cada llamada de fax T38 utiliza un canal VCM. Dentro de una red comunitaria pequeña, una llamada de fax T38 se puede convertir en una llamada a través de líneas SCN H323 utilizando el protocolo de soporte de transporte de fax de IP Office. Esta conversión utiliza 2 canales VCM. Para utilizar la conexión de fax T38, se puede configurar la Clasificación de equipo de una extensión analógica conectada a una máquina de fax. Además, está disponible una nueva función de código corto Marcar fax.

Nota:

Los dispositivos IP T3 deben configurarse con un tamaño de paquete de 20 ms para que se apliquen las condiciones anteriores. Si se deja configurado para un tamaño de paquete de 10 ms, se necesita un canal de compresión de voz para todos los tonos y para llamadas de medios no directos.

Protocolo de señalización H.323

Los sistemas de telefonía IP de IP Office utilizan estándares abiertos. Los teléfonos IP digitales, gateways y gatekeepers soportan el estándar H.323 y es este el que permite que dispositivos de diferentes

fabricantes a trabajar juntos. IP Office también es compatible con una puerta de enlace integral opcional, módulos de compresión de voz (VCM) y funcionalidad de controlador de acceso.

IP Office utiliza el protocolo de señalización H.323 mediante los siguientes componentes arquitectónicos:

telefonos ip	Dispositivos de extremo de servicio H.323 que admiten llamadas de audio. Otros tipos de dispositivos H.323 pueden admitir video como parte de H.323.
Pasarelas	Proporcione traducción de medios para permitir que se realicen llamadas a dispositivos que no sean H.323, por ejemplo, un teléfono analógico o la red pública para conectarse con un dispositivo H.323.
porteros	Controle el procesamiento de llamadas y la seguridad de los dispositivos H.323.
multipunto Unidades de conexión (MCU)	Controle las conferencias agregando flujos de medios.

Estos elementos forman una zona H.323 que es análoga a una PABX. Cada zona tiene un único gatekeeper para controlar la distribución de llamadas, el control de llamadas y la gestión de recursos. Al encenderse, los teléfonos IP, las puertas de enlace y las MCU realizan solicitudes de registro a un controlador de acceso que luego autentica (acepta o rechaza) la solicitud para convertirse en miembro de la zona. Una vez aceptado, un teléfono que desea realizar una llamada envía un mensaje de establecimiento de llamada al portero, que luego determina cómo enrutar la llamada y luego envía una alerta al teléfono llamado, o si la llamada es a un no-H. El teléfono 323 establece la llamada a través de un Gateway dentro de la zona.

Troncalización del protocolo de inicio de sesión

IP Office utiliza troncales del Protocolo de inicio de sesión (SIP) para permitir que los usuarios aprovechen los servicios de telefonía que ofrecen los proveedores de servicios de Internet (ISP). En muchos casos, los servicios de telefonía ofrecen ahorros sustanciales en comparación con las líneas de intercambio tradicionales. Para ayudar a habilitar el proveedor de servicios SIP, Avaya ofrece un programa de prueba de cumplimiento de SIP (GSSCP) que validará el funcionamiento de IP Office con la oferta de troncales SIP de los ISP. Para obtener más información sobre el Programa de prueba de cumplimiento de SIP (GSSCP) de Avaya, consulte https://www.devconnectprogram.com/site/global/compliance_testing/overview/index.gsp .

IP Office permite que todos los usuarios, independientemente de su tipo de teléfono, realicen y reciban llamadas SIP. Los troncales SIP se manejan como cualquier otra línea en IP Office, lo que brinda todo el enrutamiento de llamadas y el control de peaje necesarios para administrar las llamadas entrantes y salientes.

Los troncales SIP requieren el aprovisionamiento de canales de compresión de voz a través de la instalación de módulos VCM dentro de la unidad de control. También se necesita una licencia para el número máximo requerido de llamadas SIP simultáneas. Se admiten hasta 128 llamadas simultáneas.

IP Office también es compatible con el protocolo T38 que permite el envío de fax por IP.

Existen varias topologías de red posibles para los sistemas troncales SIP, como se muestra en los siguientes diagramas:

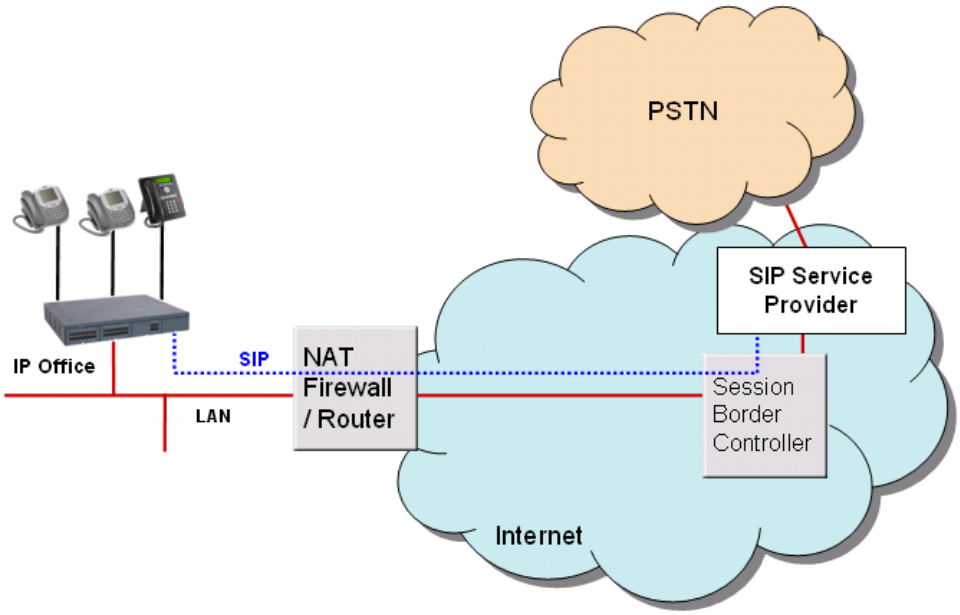


Figura 5: Proveedor de servicios con Avaya Session Border Controller for Enterprise (recomendado)

Para que esta configuración sea segura, el firewall de IP Office está configurado para descartar todos los paquetes excepto SIP.

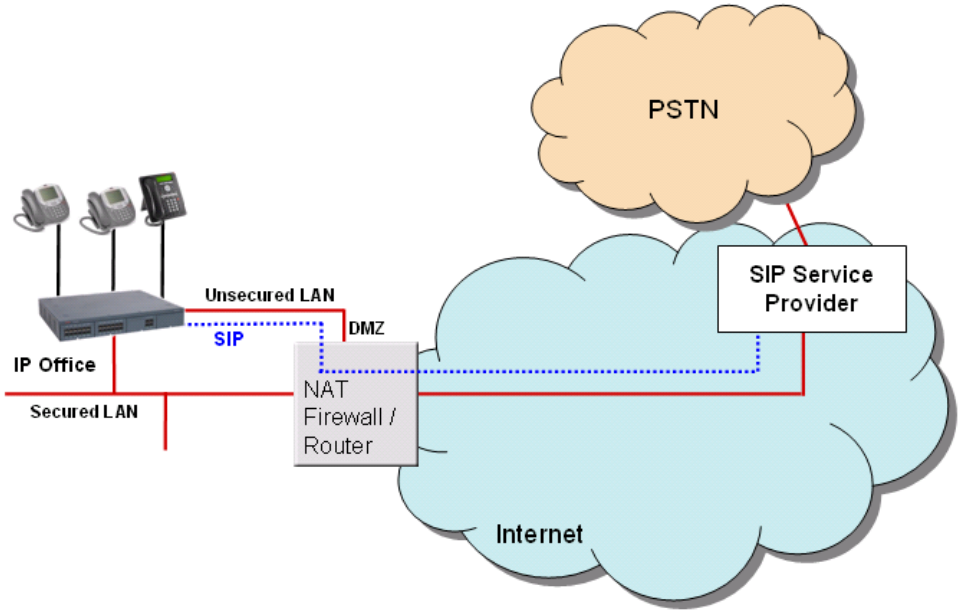


Figura 6: Conexión directa desde el segundo puerto Ethernet a Internet a través de un puerto DMZ en el enrutador

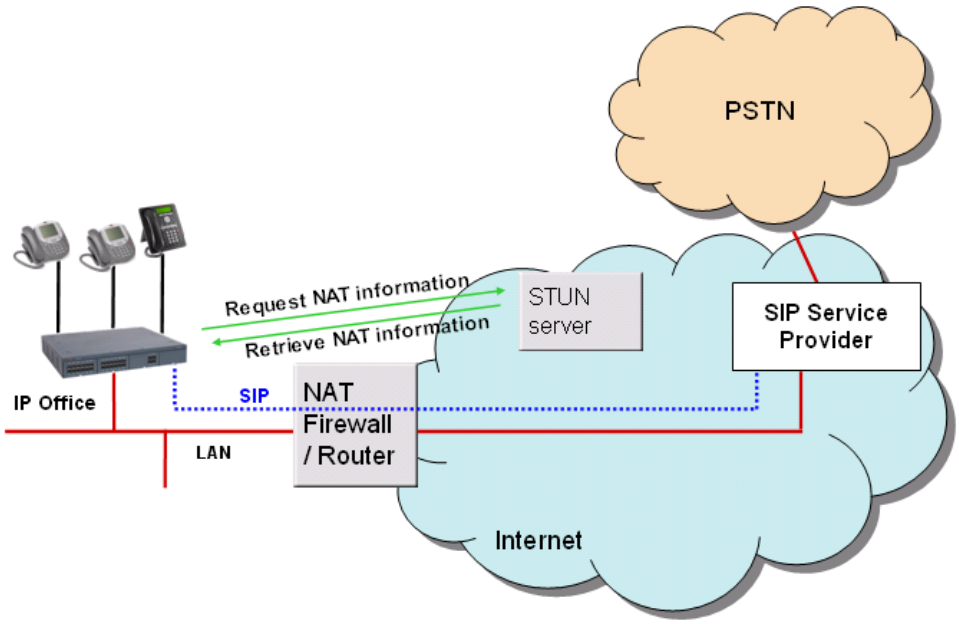


Figura 7: Conexión a ITSP sobre NAT utilizando servidores STUN de terceros

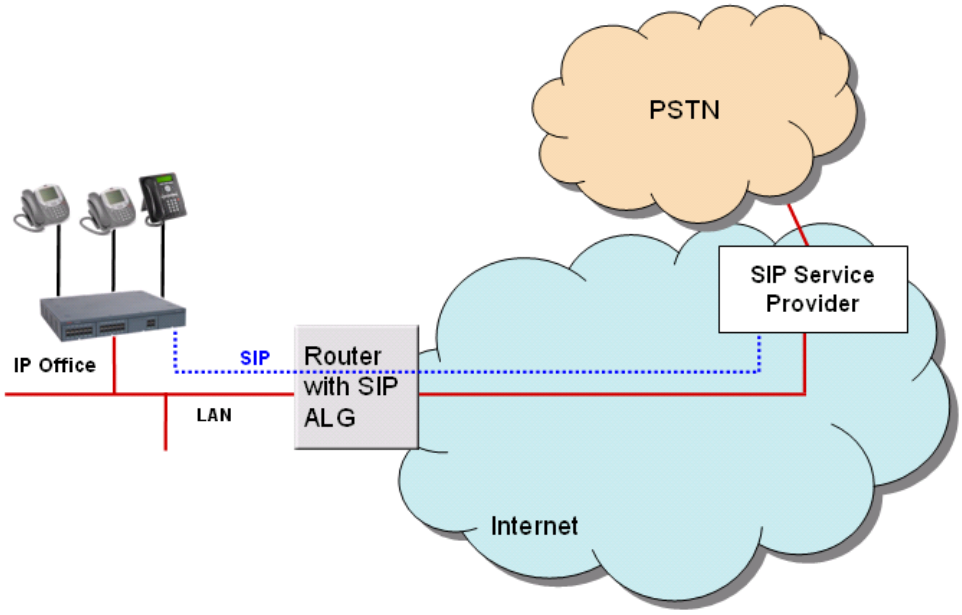


Figura 8: Conexión a ITSP a través del enrutador con ALG para resolver problemas de NAT

servidores SIP

La implementación del terminal SIP de IP Office se basa en dos componentes SIP principales: Componentes del servidor SIP Aplicaciones del agente de usuario del terminal SIP.

Los servidores SIP brindan compatibilidad con extremos SIP para permitir la interoperabilidad total entre extremos SIP, otros teléfonos IP basados en H.323, teléfonos digitales y analógicos, así como troncales de IP Office (analógicos, digitales o basados en SIP).

Los servidores SIP brindan información centralizada y servicios de habilitación en un ecosistema SIP. Los servidores SIP centrales y sus funciones se resumen aquí. IP Office proporciona las funciones de los siguientes dos servidores para comunicaciones de voz y fax.

- **servidor de registro**

  Cuando los teléfonos IP SIP se conectan, deben asegurarse de que los demás sepan que están disponibles para recibir y realizar llamadas. El registrador autentica y registra el teléfono IP (a menudo directamente relacionado con un usuario específico) cuando se conecta y luego almacena información sobre las identidades lógicas de los teléfonos.

- **Servidor proxy**

  Un servidor proxy toma las solicitudes SIP, las procesa y las pasa en sentido descendente mientras envía respuestas en sentido ascendente a otros servidores o dispositivos SIP. Un servidor proxy puede actuar como servidor y como cliente, y puede modificar una solicitud SIP antes de transmitirla. Un proxy solo participa en la configuración y finalización de una sesión de comunicación. Después de que los agentes de usuario establecen una sesión, las comunicaciones ocurren directamente entre las partes.

La funcionalidad de los siguientes dos servidores SIP generalmente está disponible para IP Office utilizando la funcionalidad existente de IP Office. Por lo tanto, si bien se proporciona la funcionalidad, por ejemplo, que permite compartir escritorios en una pequeña red comunitaria, se utiliza una metodología coherente entre los extremos SIP y no SIP para ofrecer esas funciones.

- **Servicio de localización**

  A medida que los usuarios se desplazan, la red debe estar continuamente al tanto de sus ubicaciones. El servicio de ubicación es una base de datos que realiza un seguimiento de los usuarios y sus ubicaciones. El servicio de ubicación obtiene su entrada del servidor de registro y proporciona información clave a los servidores proxy y de redirección. IP Office brinda soporte de escritorio compartido, brindando una funcionalidad similar pero trabajando consistentemente entre terminales SIP y no SIP.

- **servidor de redirección**

  Si los usuarios no están en sus dominios de origen, las sesiones vinculadas a ellos deben redirigirse a ellos.

  El servidor de redirección asigna una solicitud SIP destinada a un usuario al dispositivo más cercano al usuario. En IP Office, la función de desvío de llamadas y Sígueme se utiliza para brindar nuevamente una funcionalidad consistente entre todo tipo de terminales.

Agentes de usuario de punto final SIP

Los terminales SIP, como teléfonos SIP, teléfonos móviles, PDA o estaciones de trabajo, utilizan aplicaciones de agente de usuario (UA) para proporcionar la interfaz entre los usuarios y la red SIP.

La compatibilidad con terminales SIP está completamente integrada en IP Office. No se necesitan otros componentes. Los terminales SIP requieren la capacidad del módulo VCM como cualquier otro teléfono IP.

Las extensiones SIP funcionan como cualquier otra extensión de IP Office. IP Office proporciona la siguiente funcionalidad:

• Hacer y recibir llamadas a cualquier otra extensión, independientemente del tipo de extensión.

- Entregar medios de extremo a extremo. Durante las llamadas entre dos extensiones SIP o una extensión SIP y un teléfono IP de Avaya, IP Office transmite audio de extremo a extremo para llamadas telefónicas básicas. Las conferencias requieren un recurso de VCM.
- Utilice códigos cortos y códigos de autorización.
- Transmitir tonos de progreso de llamada en banda.
- Registrar punto final mediante autenticación con nombre de usuario y contraseña.
- Admite creación automática. El registro correcto de puntos finales utiliza una licencia de terceros.
- Varias extensiones pueden registrarse en una dirección IP, cada una usando una licencia. Esto permite la conexión de adaptadores de terminal SIP con más de un puerto analógico, dando un número de extensión diferente a cada puerto.

Integración de telefonía informática

Computer Telephony Integration (CTI) cierra la brecha entre el sistema telefónico y las aplicaciones comerciales. Con IP Office, esto se logra con IP Office CTI Link, un producto de middleware CTI y un kit para desarrolladores de software (SDK).

En IP Office, CTI se entrega mediante el cumplimiento de estándares abiertos. Esto brinda a las empresas acceso a una amplia gama de soluciones de terceros, dirigidas a mercados verticales y diseñadas para cumplir con sus requisitos. Para los desarrolladores, migrar su oferta desde otras plataformas a IP Office es rápido y fácil, y las funciones avanzadas de CTI que ofrece IP Office facilitan la demostración de la integración completa y más beneficios comerciales.

IP Office proporciona dos niveles de interoperabilidad de CTI:

Enlace CTI Lite	Gratis y proporciona toda la funcionalidad necesaria para admitir la gran mayoría de las aplicaciones, incluidas las pantallas emergentes y muchos productos de terceros.
Enlace CTI Pro	Brinda una funcionalidad mejorada, incluida la capacidad de controlar varios teléfonos y brinda acceso a la operación avanzada del centro de llamadas.

Debido a que las redes IP están integradas en el sistema IP Office, todo el CTI se realiza a través de la LAN. Esto introduce puntos adicionales de falla, además de depender de interfaces y teléfonos no estándar. En IP Office, todos los dispositivos se pueden usar con CTI.

Interfaces CTI compatibles

IP Office es compatible con las siguientes interfaces:

TAPI Link Lite	Proporciona compatibilidad con CTI de primera mano para Microsoft TAPI 2.1 y TAPI 3.0, por lo que cada PC puede controlar o monitorear un teléfono. Los componentes de software se suministran con el sistema IP Office en el CD del usuario y no requieren una clave de licencia para su uso. La especificación requiere que se implemente una cierta cantidad de funciones básicas y, además, define una serie de funciones opcionales que también pueden implementar los proveedores de conmutadores.

TAPI Link Pro

Proporciona compatibilidad con CTI de terceros para TAPI 2.1 y 3.0. Estos componentes son idénticos a su equivalente original; la presencia de la clave de licencia CTI Link Pro RFA (que se puede comprar de la forma habitual para los productos) habilita esta funcionalidad adicional. TAPILink Pro proporciona todas las características y funcionalidades de TAPILink Lite, pero además proporciona operación CTI de terceros. Esto significa que un solo servidor puede controlar y monitorear cualquier número de dispositivos telefónicos. Además, TAPILink Pro brinda la capacidad de monitorear y controlar grupos. Esto permite que una aplicación sea notificada cuando una llamada ingresa a una cola y también puede redirigirla a otra ubicación.

TAPI-WAV
conductor

Proporciona soporte basado en software para procesamiento de voz. El controlador TAPI-WAV solo se usa con TAPI 2.1; para TAPI 3.0, IP Office es compatible con la interfaz del proveedor de servicios multimedia (MSP), definida por Microsoft en TAPI 3.0. Esta funcionalidad solo funcionará junto con CTI Link Pro y también requiere licencias TAPI-WAV. Cada licencia habilita 4 puertos de procesamiento de voz.

DevLink Pro

Proporciona un flujo de eventos en tiempo real además de la interfaz SMDR proporcionada en IP Office SMDR. El flujo de eventos en tiempo real toma la forma de un registro de llamada, que se emite cada vez que cambia el estado de cualquier punto final de una llamada (normalmente hay dos puntos finales en una llamada, pero en algunas circunstancias, como llamadas en conferencia, llamadas intrusas puede haber más).

REDCE IP Office

Proporciona una interfaz para obtener eventos SMDR. Se emite un registro separado por comas para cada llamada, cuando se completa la llamada. Esta interfaz está diseñada para aplicaciones de contabilidad y facturación de llamadas. IP Office SMDR puede enviarse directamente desde la unidad de control de IP Office a una dirección IP y un puerto designados.

Oficina de PI
Software
Desarrollo
Equipo

Este kit de herramientas se entrega en un solo CD que contiene la documentación para desarrolladores de TAPILink Lite, TAPILink Pro, DevLink Lite y DevLink pro, así como programas precompilados para explorar TAPI 2.1 y 3.0. Además, se incluye código fuente de ejemplo, lo que facilita que los desarrolladores se familiaricen con las interfaces CTI de IP Office. El programa Developer Connection (DevConnect) es el programa de socios desarrolladores de Avaya y está diseñado para empresas de terceros que están creando un producto para la venta y que desean recibir soporte técnico. La membresía del programa queda a la sola discreción de Avaya. Los miembros de DevConnect pagan una tarifa anual, por la cual reciben soporte técnico directamente de Avaya. Además, Avaya realizará pruebas de interoperabilidad entre IP Office y el producto del miembro, y también puede crear oportunidades para el marketing conjunto, incluidas exhibiciones, el uso del logotipo de Avaya y otros beneficios. Puede encontrar más información sobre el programa DevConnect enhttp://www.devconnectprogram.com .

CTI centralizado
Servicio web
API

Proporciona una plataforma más abierta para permitir que terceros agreguen valor y desarrollen soluciones. Admite entornos distribuidos (SE/SCN) y, por lo tanto, no se limita a nodos como TAPI. Tiene una dependencia de Avaya one-X® Portal de acceso para los usuarios. Al crear un nuevo usuario en IP Office, no es necesario reiniciar.

SSI a través de la Web Servicios

Proporciona información de monitoreo del sistema de SSI a través de un servicio web REST de solo lectura disponible solo a través de https. Los datos de llamadas en tiempo real y el control de llamadas no están disponibles a través de esta interfaz, pero estarán disponibles a través del programa DevConnect.

Esta función ya tiene varias áreas instrumentadas, pero los datos son para SSA y se entregan a través de la interfaz SSI patentada, y hay un pequeño conjunto de datos disponible en SNMP.

No requiere licencia.

Abrir API/SDK

Con la versión 10.1, IP Office admite una nueva API/SDK de administración para abordar las necesidades de las configuraciones de "botón fácil". Mejoras para cubrir más áreas, específicamente lo que cubren los servicios web de configuración "XO" heredados para que la API heredada pueda llegar al final de su vida útil. La API de administración proporciona una interfaz API basada en REST a los desarrolladores de aplicaciones de terceros para consumir objetos de configuración de IP Office.

- Brinda todas las capacidades de los servicios de configuración de IP Office compatibles actualmente (servicios XO).
- La solicitud y la respuesta están en formato XML y JSON.
- Proporciona acceso de lectura/escritura únicamente a usuarios de servicios privilegiados.
- No se requiere una licencia por separado para acceder a las API.

Componentes

Componentes de hardware

unidad de control de IP Office

La unidad de control de IP Office (IP500 V2) es una unidad apilable con un kit de montaje en rack de 19" opcional y un kit de montaje en pared opcional para configuraciones más pequeñas.

La unidad de control IP500 V2 es compatible con todas las tarjetas de módulo de compresión de voz (VCM) y extensión base IP500, así como con todos los módulos de expansión IP500 externos.

La centralita IP500 V2 dispone de 4 slots para la inserción de tarjetas base IP500. Las ranuras están numeradas del 1 al 4 de izquierda a derecha. Normalmente se pueden usar en cualquier orden, sin embargo, si se excede la capacidad de un tipo de tarjeta en particular, la tarjeta en la ranura más a la derecha se desactivará. Cada tarjeta base incluye un panel frontal integral con puertos para conexiones de cable. Por lo general, los primeros 8 puertos de la izquierda son para la conexión de dispositivos de extensión. Los 4 puertos de la izquierda se utilizan para la conexión de troncales si se agrega una tarjeta secundaria de troncales a la tarjeta base.

La unidad de control proporciona la siguiente funcionalidad:

Máximo extensiones	Hasta 384 extensiones.
Conferencia fiestas	128 como estándar pero máximo 64 en cualquier conferencia individual. La supresión de silencio se aplica a conferencias con más de 10 participantes.
Tarjetas troncales	Hasta 4. Cualquier combinación de tarjetas secundarias de troncales.
Voz compresión canales	Hasta 148 canales usando hasta VCM y tarjetas combinadas.
Mensaje de voz canales	Se admiten hasta 250 canales de correo de voz/grabación en el servidor principal. Para implementaciones seleccionadas, el servidor secundario también puede admitir hasta 250 canales de correo de voz/grabación.
locales	Compatible en los siguientes países: Argentina, Australia, Baréin, Bélgica, Brasil, Canadá, Chile, China, Colombia, Personalizar, Dinamarca, Egipto, Finlandia, Francia, Alemania, Grecia, Hong Kong, Hungría, Islandia, India, Irlanda, Italia , Japón, Corea, Kuwait, Malasia, México, Marruecos, Países Bajos, Nueva Zelanda, Noruega, Omán, Pakistán, Perú, Polonia, Portugal, Qatar, Rusia, Arabia Saudita, Singapur, Sudáfrica, España, Suecia, Suiza, Taiwán, Turquía, Emiratos Árabes Unidos, Reino Unido, Estados Unidos, Venezuela.
Fuente de alimentación	Unidad de fuente de alimentación interna.
Montaje	Independiente, montado en bastidor o montado en la pared (requiere kits de montaje).
Memoria	Tamaño máximo del archivo de configuración: 2048 KB.

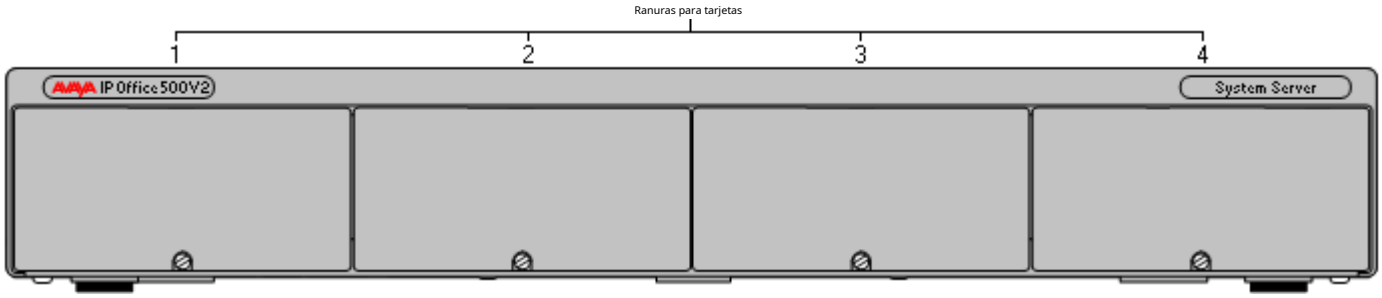


Figura 9: Vista frontal de IP500 V2

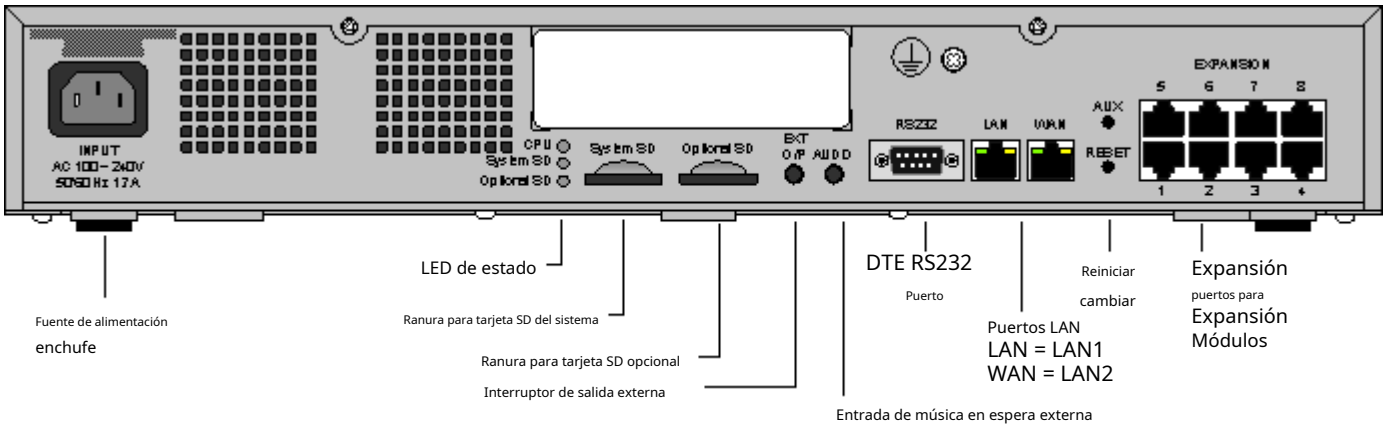


Figura 10: Vista trasera de IP500 V2

Teclas de función

El número de serie de la tarjeta SD de llave de función instalada en la unidad de control de IP Office se usa como base para todas las licencias emitidas para ese sistema IP Office y se usa para validar las licencias con regularidad. Si se extrae la tarjeta SD de la llave de funciones, en las próximas horas las funciones con licencia dejarán de funcionar.

Codificación de modulación de código de pulso

La modulación de código de pulso (PCM) es un método para codificar voz como datos. En telefonía, se utilizan ampliamente dos métodos de codificación PCM, a-law y μ-law (también llamado mu-law o u-law). Por lo general, la ley μ se usa en América del Norte y en algunos otros lugares, mientras que la ley a se usa en el resto del mundo. Además de configurar la codificación PCM correcta para la región, la configuración de ley a o ley μ de IP Office cuando se inicia por primera vez afecta una amplia gama de valores predeterminados regionales relacionados con la configuración de línea y otros valores.

Tarjetas base

Las siguientes tarjetas base están disponibles:

Tabla 2: Tarjetas base IP500 V2

Tarjeta básica	Máximo m por sistema	Puerto RJ45 asignación descripción	Teléfonos compatibles
Estación digital (DS8)	3	Puertos 1–8: digitales estaciones Con tarjeta de troncal: Puertos 9–12: Central Líneas de oficina	Teléfonos Avaya series 2400, 5400 y 9500 seleccionados Teléfonos T3 (solo EMEA) Teléfonos inalámbricos 3810 (solo en Norteamérica) **Nota:** Los teléfonos de la serie 4400 no son compatibles con esta tarjeta. Son compatibles con los puertos DS del módulo de expansión externo. Los teléfonos 4100, 7400, serie M y serie T utilizan la tarjeta de estación digital TCM8.

La tabla continúa...

Página439 de 3226.

Tarjeta básica	Máximo m por sistema	Puerto RJ45 asignación descripción	Teléfonos compatibles
Teléfono analógico 2	4	Puertos 1–2: Analógico estaciones Con tarjeta de troncal: Puertos 9–12: Troncal conexiones	Teléfonos analógicos
Teléfono analógico 8	4	Puertos 1–8: Analógico estaciones Con tarjeta de troncal: Puertos 9–12: Troncal conexiones	Teléfonos analógicos
Estación digital (TCM8)	4	Puertos 1–8: BST estaciones digitales Con tarjeta de troncal: Puertos 9–12: Central Líneas de oficina	Norstar®/teléfonos BCM Teléfonos de la serie BST Teléfonos globales de la serie M Controladores de movilidad digital (DMC) Teléfonos inalámbricos 7406e Unidad de audioconferencia digital
Voz Compresión Módulo (VCM V2)	2	Puertos 1–8: No presente Con tarjeta de troncal: Puertos 9–12: Central Líneas de oficina	Llamadas VoIP incluyendo extensiones IP o troncales IP. Hasta 128 canales de compresión de voz según el códec utilizado. La unidad de control IP500V2 admite hasta 148 canales de compresión de voz, usando la tarjeta más los puertos de compresión de voz en la tarjeta combinada.
Cajero automático Combinación (cajero automático V2)	2	Puertos 1–6: digitales estaciones Puertos 7–8: Analógico estaciones Puertos 9–12: Central Líneas de oficina 10 voz compresión canales códec el soporte es G.711, G729a y G.723 con eco de 64ms cancelación. G.722 Es apoyado por versión 8.0 y más alto.	Teléfonos digitales de Avaya excepto teléfonos de las series 3800 y 4400 Teléfonos analógicos Tarjetas de troncales preinstaladas

La tabla continúa...

Tarjeta básica	Máximo m por sistema	Puerto RJ45 asignación descripción	Teléfonos compatibles
BRI Combinación	2	Puertos 1–6: digitales estaciones Puertos 7–8: Analógico estaciones Puertos 9–10: BRI puertos troncales (4 canales BRI) 10 voz compresión canales códec el soporte es G.711, G729a y G.723 con eco de 64ms cancelación. G.722 es compatible con la versión 8.0 de IP Office y más alto.	Teléfonos digitales de Avaya, excepto teléfonos de las series 3800 y 4400 (tipo DS, no TCM) Teléfonos analógicos Tarjetas de troncales preinstaladas
unificado Comunicación Módulo ns (UCM V2)	1		Requiere una licencia Preferred Edition por separado. No compatible con Server Edition. Más de 200 usuarios cuando solo se ejecuta Voicemail Pro. Hasta 200 usuarios cuando se ejecuta Voicemail Pro y Avaya one-X®Portal de IP Office. 50 Avaya one-X simultáneos®Portal para usuarios de IP Office. Sin tarjetas troncales
ETR6	3	Puertos 1 a 6: ETR estaciones Con ATM4: Puertos 7–8: Alimentación Transferencia de fallas Puertos 9–12: Central Líneas de oficina	No compatible con Server Edition. Teléfono SOCIO ACS Tarjetas SD ATM4, PRI/T1 o PARTNER en modo µ-law (solo Norteamérica)

Tarjetas troncales

Las tarjetas de troncales se pueden instalar en tarjetas base existentes para brindar soporte a los puertos de troncales. La tarjeta troncal utiliza los puertos proporcionados en la tarjeta base para la conexión de cables. Cada tarjeta de troncal viene con clavijas espaciadoras para la instalación y etiquetas de identificación de puertos.

Nota:

Estas tarjetas se utilizan para puertas de enlace PSTN/FXS con IP Office para Linux.

Consejo:

En sistemas con tarjetas base de Analog Phone 8 y tarjetas de troncales analógicas, se recomienda combinar los dos tipos porque brinda soporte de falla de energía analógica para una troncal por extensión (no aplicable a la tarjeta base de Analog Phone 2).

Tabla 3: Tarjetas de troncales IP500 V2

Tarjeta de troncal	Máximo m por sistema	Funciona con estas tarjetas base.	Descripción
Analógico (V2)	4	ETR6 DS8 TCM8 Teléfono analógico 2/8	4 troncales de inicio de bucle analógico Módem V.32 para acceso remoto 1 extensión de falla de energía a conexión troncal en tarjetas Phone 8

La tabla continúa...

Tarjeta de troncal	Máximo m por sistema	Funciona con estas tarjetas base.	Descripción
PRI universal (PRI-U)	4	ETR6 DS8 TCM8 Teléfono analógico 2/8 VCM	Hasta 2 conexiones troncales PRI. La tarjeta está disponible en variantes de puerto único y doble. La tarjeta se puede configurar para troncales E1 PRI, T1 bit robado, T1 PRI o E1R2 PRI. Admite troncales digitales de tasa primaria. En cada tarjeta, 8 canales por interfaz están habilitados por defecto. Esto significa que el PRI simple tiene 8 canales habilitados, mientras que el PRI dual tiene 8 canales habilitados en cada uno de los dos circuitos. Se pueden habilitar más canales mediante la compra de licencias adicionales en incrementos de 2 u 8 canales. Disponible en versión simple y doble. La variante única puede admitir hasta 24 canales T1 o hasta 30 canales E1. La variante dual puede admitir hasta 48 canales T1 o 60 canales E1. Configurable para uso de MFC T1, E1, E1R2, según el territorio. Incluye una CSU/DSU integrada: • CSU permite que las troncales se pongan en modo de bucle invertido para fines de prueba. Esto se puede configurar manualmente, usando la aplicación de monitoreo, o automáticamente desde una oficina central enviando un patrón de bucle de línea (LLB). • DSU permite que el troncal T1 se comparta entre los servicios de datos y voz. Incluye capacidades de diagnóstico: indicadores visuales para mostrar el estado del servicio y puntos de prueba físicos para monitorear el tráfico. Admite funciones de movilidad: Mobile Call Control y clientes one-X Mobile
BRI (Euro RDSI)	4	DS8 TCM8 Teléfono analógico 2/8 VCM	Hasta 4 conexiones troncales BRI, cada troncal proporciona 2 canales digitales B+D. Disponible en 2 (4 canales) y 4 (8 canales) opciones. Admite funciones de movilidad: Mobile Call Control y clientes one-X Mobile.

Módulos de expansión externos

Los módulos de expansión externos se pueden utilizar con la unidad de control IP500 V2.

Módulos de expansión de teléfonos analógicos

En los puertos analógicos, la información de la llamada se envía mientras suena el teléfono y no se puede actualizar durante una llamada ni configurar en una llamada saliente (el teléfono puede hacer una coincidencia local, pero esto no está controlado por IP Office). El propósito principal de las pantallas es dar información sobre las llamadas entrantes. Cuando el estándar de visualización de la persona que llama elegido admite la entrega de texto (nombre de la extensión), así como el número, se entregan ambos.

Se puede configurar un puerto de extensión analógico para la operación de megafonía externa. No funciona como una extensión normal y se conecta a un equipo externo a través de un dispositivo de aislamiento (también se puede utilizar como fuente de MoH). El puerto siempre estará ocupado, por lo que no se puede llamar directamente y solo se puede acceder mediante una función de paginación. Cuando no reciba una página, el puerto permanecerá en silencio. Al ser buscado, el tono de buscapersonas se envía antes de que se abra la ruta de voz.

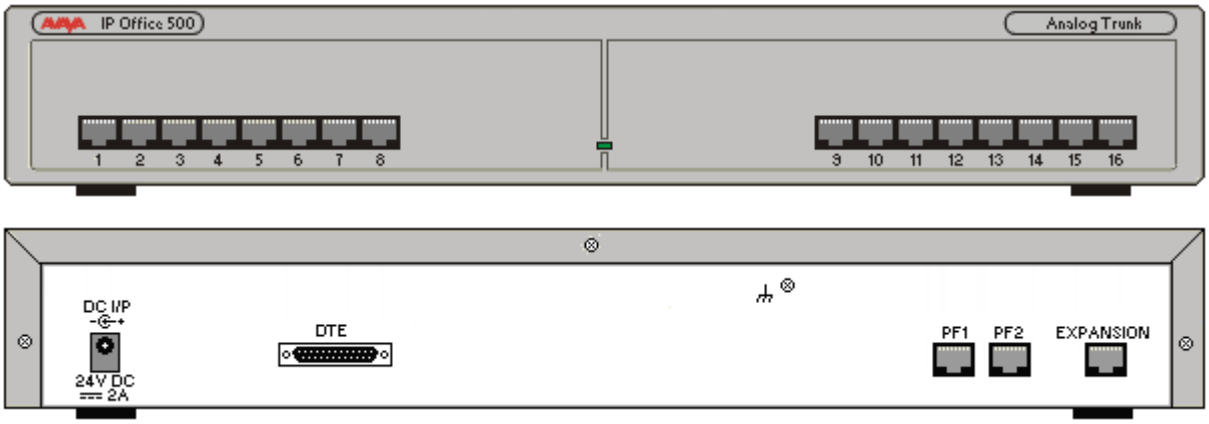
Para instalaciones en rack, este módulo requiere el kit de montaje en rack IP500 V2.

Expansión módulo	Teléfonos compatibles	Interfaces compatibles
Teléfono analógico 16	16 estaciones analógicas con presentación de línea de llamada	Señalización DTMF (sin desconexión rotativa ni de bucle) Recuperación de tiempo de descanso (sin recuperación de tierra) Indicación de mensaje en espera (MWI): 51 V escalonado, 81 V, 101 V e inversión de línea y Bellcore FSK
Teléfono analógico 30	30 estaciones analógicas con presentación de línea de llamada	

Módulos troncales analógicos

Este tipo de módulo se puede usar para agregar 16 troncales analógicas adicionales a un sistema IP500 V2. El módulo admite troncales de inicio por bucle y de inicio por tierra. El módulo también proporciona dos puertos de falla de energía para la conexión directa de teléfonos analógicos a los dos primeros troncales analógicos.

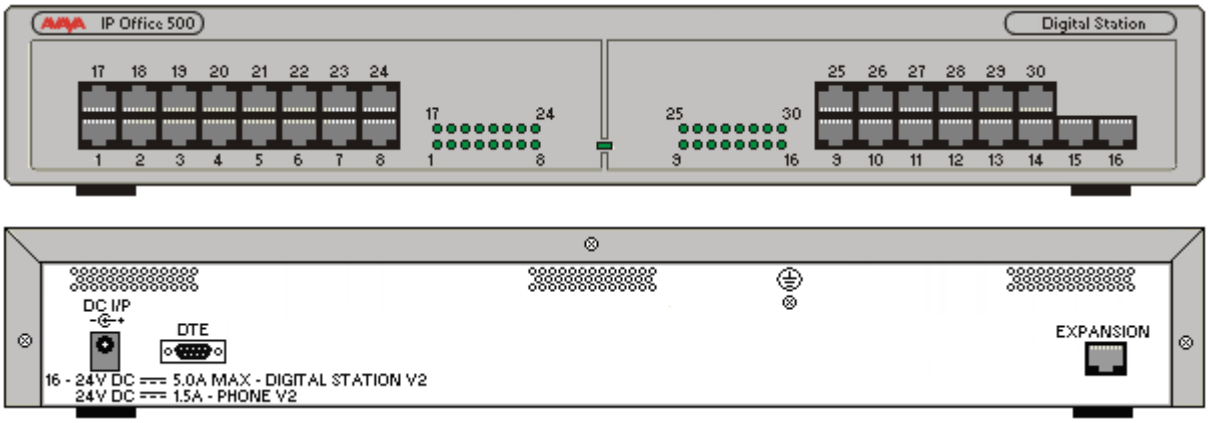
Los sistemas Basic Edition solo admiten un único módulo de expansión ATM16. Para instalaciones en rack, este módulo requiere el kit de montaje en rack IP500 V2.



Expansión módulo	Descripción	Interfaces compatibles
cajero automático16	16 troncales analógicas	Inicio de bucle Comienzo de tierra

Módulos de expansión de estaciones digitales

Para instalaciones en rack, este módulo requiere el kit de montaje en rack IP500 V2.



Expansión módulo	Teléfonos compatibles	Descripción
DS16A	Norstar®/Teléfonos BCM	16 puertos de estación digital
DS30A	Teléfonos de la serie BST Teléfonos de la serie Global M Controladores de movilidad digital (DMC) Teléfonos inalámbricos 7406e Unidad de audioconferencia digital	30 puertos de estación digital
DS16B, DS16B2[1]	Teléfonos Avaya	16 puertos de estación digital
DS30B, DS30B2[1]	Modo DS o TCM compatible con los teléfonos conectados a las tarjetas DS8 o TCM8.	30 puertos de estación digital

Servidor de aplicaciones

El servidor de aplicaciones de IP Office brinda confiabilidad, escalabilidad y potencia de procesamiento para implementaciones de IP Office a mayor escala. Es un servidor externo montado en rack que brinda escalabilidad para instalaciones más grandes e implementaciones en múltiples sitios que actualmente no son compatibles con Unified Communications Module (UCM V2).

El servidor de aplicaciones de IP Office es una instalación única de IP Office seleccionado™Aplicaciones de la plataforma que se ejecutan en Linux. El sistema operativo Linux se incluye como parte de la instalación. Sin embargo, la instalación requiere un conocimiento mínimo de Linux debido a la inclusión de una interfaz de administración basada en web para permitir que el servidor se administre de forma remota a través del navegador web.

[1]DS16B2 y DS30B2 son compatibles con 10.1, 9.1 SP 12 y 10.0 SP5 en adelante.

El servidor de aplicaciones de IP Office alberga las siguientes aplicaciones:

- Servicios de gestión
- Portal one-X para IP Office
- Correo de voz Pro
- Administrador de licencias web (WebLM)
- Administrador web
- Servicios opcionales
  - Administrador de medios
  - Colaboración web
  - Puerta de enlace WebRTC

Pautas de configuración de la puerta de enlace WebRTC

Use las siguientes pautas al configurar una puerta de enlace WebRTC:

- Definir extensiones SIP de WebRTC en:
  - Servidor SIP que forma parte de la configuración de la puerta de enlace WebRTC.
  - Servidor principal si forma parte de la topología de implementación.
- Con las implementaciones de IP500 V2, WebRTC debe estar habilitado en el servidor de aplicaciones.

Limitaciones de la puerta de enlace

La puerta de enlace WebRTC no es compatible con la resiliencia.

Controlador de borde de sesión de Avaya para empresas

Un controlador de borde de sesión actúa como un enrutador entre la empresa y el servicio del operador, lo que permite que solo las sesiones autorizadas pasen por el punto de conexión (borde). El controlador de borde de sesión para empresas (SBCE) de Avaya brinda seguridad a una red de comunicaciones unificadas basada en SIP.

Para obtener información sobre la SBCE, consulte*Resumen y especificaciones de Avaya Session Border Controller para empresas*.

Para obtener información sobre la implementación de SBCE con IP Office, consulte "Configuración de Avaya Session Border Controller para trabajadores remotos de IP Office" en

- *Administración de IP Office de Avaya™Plataforma con Web Manager*
- *Administración de IP Office de Avaya™Plataforma con Gerente*

Los telefonos

IP Office es compatible con varias soluciones telefónicas:

- Teléfonos IP

- Teléfonos digitales
- Teléfonos ETR
- Teléfonos analógicos
- Teléfonos inalámbricos
- Terminales SIP de terceros, como teléfonos de escritorio, softphones y teléfonos con altavoz para conferencias

Para obtener especificaciones detalladas, consulte la información telefónica específica en el sitio de soporte de Avaya en http://soporte.avaya.com .

Enlaces relacionados

Soporte telefónico remoto en la página 39
Acceso a las notas de la aplicación Avaya DevConnect en la página 134 Uso de la base de conocimientos de Avaya InSite en la página 134 Interoperabilidad telefónica en la página 95

Soporte telefónico remoto

Teléfonos IP que usan enrutador NAT

IP Office admite teléfonos IP remotos de la serie 9600 con el FW H.323 que reside detrás de un enrutador NAT para IP Office. La configuración no requiere ningún equipo concentrador VPN. Los teléfonos IP 9600 H.323 remotos pueden conectarse a IP Office incluso si está ubicado detrás de un enrutador NAT. Los teléfonos se autentican del mismo modo que los teléfonos de la red privada. IP Office determina que un teléfono está ubicado fuera de la red privada y retransmite el tráfico RTP de VOIP para garantizar que atraviese el enrutador NAT.

Nota:

La señalización H.323 y el tráfico de medios no están encriptados.

Para acceder a IP Office desde la red privada remota, los teléfonos IP H.323 remotos deben configurarse con la dirección IP pública del enrutador NAT que aloja IP Office. Los puertos configurables deben reenviarse a IP Office. IP Office requiere que se configure una dirección IP pública válida y la dirección IP pública puede configurarse estáticamente o descubrirse dinámicamente a través de un servidor STUN. La función de trabajador remoto requiere la licencia de Essential Edition, que proporciona 4 puestos de trabajo remoto. Habilite la función de trabajador remoto mediante IP Office Manager. La capacidad de trabajo remoto adicional está disponible con las licencias de usuario de teletrabajador o usuario avanzado y una licencia de edición preferida.

Teléfonos VPN

Los teléfonos VPN brindan comunicación segura a través de redes ISP públicas con IP Office en la sede de la empresa. Es un producto de solo software que se ejecuta en teléfonos IP 5610/5620/5621 o 4610/21. En combinación con uno de estos teléfonos y los productos de puerta de enlace VPN más populares, el software extiende la telefonía empresarial a ubicaciones remotas. La funcionalidad VPN es compatible con los teléfonos IP 9600 y no requiere una carga de software independiente. El teléfono VPN ha sido probado con varias puertas de enlace VPN de proveedores importantes como Cisco o Juniper, así como con dispositivos de acceso VPN más pequeños de compañías como Adtran, Kentrox, Netgear y SonicWall. Consulte el sitio web de soporte de Avaya para obtener una lista de las notas de aplicación disponibles en las puertas de enlace VPN probadas con cada línea de teléfonos.

Página447 de 3226.

Teléfonos SIP que utilizan Avaya SBCE

El controlador de borde de sesión de Avaya para empresas (Avaya SBCE) se encuentra en el borde de la red del cliente con interfaces IP internas y externas. Con estas interfaces IP, Avaya SBCE funciona como puerta de enlace para el tráfico SIP hacia y desde la red. Cuando se usan internamente, los clientes SIP se registran directamente en IP Office. Cuando se usan externamente, los clientes SIP se conectan a Avaya SBCE. Esto se logra mediante DNS dividido, que resuelve automáticamente los FQDN en la dirección IP interna de IP Office o la dirección IP pública de Avaya SBCE, según la ubicación actual de los clientes. Además de actuar como puerta de enlace, Avaya SBCE también brinda protección contra cualquier ataque externo basado en SIP. Para la privacidad en la Internet pública,

---

aplicaciones de IP Office

Aplicaciones de usuario

Las siguientes secciones proporcionan una descripción general de las aplicaciones destinadas a los usuarios finales.

Avaya one-X®Móvil

Avaya one-X®Mobile es una aplicación que los usuarios móviles utilizan para conectarse a IP Office.

Avaya one-X®El móvil funciona en modo de devolución de llamada telefónica. Por ejemplo, cuando un usuario inicia una llamada desde el cliente, IP Office inicia una llamada al dispositivo móvil de la persona que llama y luego marca el destino. Este modo ofrece ahorros de costos a los usuarios en países donde las llamadas de voz entrantes son gratuitas o para usuarios que tienen un plan de voz ilimitado más económico en comparación con un plan de datos.

El cliente de movilidad preferido de one-X Mobile también funciona en el modo Voz sobre IP (VoIP). En el modo VoIP, el cliente realiza llamadas a través de redes de datos Wi-Fi/3G/4G. El cliente, utilizando su pila SIP subyacente, se registra en IP Office a través de la red de datos y funciona como una extensión de la oficina.

Los usuarios de países en los que se cobran las llamadas entrantes verán un importante ahorro de costes en el modo VoIP, especialmente en redes Wi-Fi. La disponibilidad de los modos de devolución de llamada y VoIP en el cliente de movilidad permitirá a los usuarios alternar entre los modos en función de sus conexiones de red. Esto permitirá a los usuarios finales elegir el modo apropiado según su plan de voz y datos, así como la disponibilidad y calidad de su conexión de datos (WiFi/3G/4G). Por ejemplo,

- El usuario puede elegir el modo de devolución de llamada cuando no tiene acceso a Wi-Fi y la conexión de datos 3G no proporciona una buena calidad para la voz.
- El usuario puede elegir el modo VoIP cuando tiene acceso a un punto de acceso móvil donde hay disponible una conexión de datos Wi-Fi o cuando la conexión de datos 3G o 4G es buena.

Un cliente de movilidad preferente de one-X Mobile es compatible con el modo VoIP en dispositivos iOS y Android. El modo VoIP está disponible con el perfil de usuario avanzado. Los usuarios con perfiles de trabajador móvil solo pueden

usar el modo de devolución de llamada. El modo VoIP no requiere una licencia de terminal IP. Las siguientes características están disponibles:

- Selección de tono de llamada
- Selección de códec de ancho de banda alto o de banda estrecha según la conexión de red disponible
- Control de audio de auriculares Bluetooth en llamadas VoIP
- Pantalla de conferencia
- Selección de número de teléfono de contacto
- Indicador de prioridad de correo de voz
- Soporte de deslizamiento para mensajería instantánea en la pantalla de inicio
- Apoyo a la acción de grupo
- Emoticones
- Búsqueda CLID en contactos para llamadas
- Enviar correo de voz como WAV en el correo electrónico
- Habilitar o deshabilitar el hermanamiento móvil (anillo simultáneo)
- Activar o desactivar DND (enviar todas las llamadas)
- Registro de llamadas combinado con correos de voz en el historial de eventos
- Monitoreo de llamadas para ver e interactuar con todas las llamadas
- Plan de marcación del modo VoIP
- Transferir llamadas como un controlador de llamadas de terceros (3PCC)

Avaya one-X®Portal para IP Office

Avaya one-X®Portal for IP Office proporciona a los usuarios el control de su teléfono desde una PC en red. Utilice esta aplicación con cualquier extensión; analógico, digital o cualquier teléfono IP, alámbrico o inalámbrico, que esté disponible como parte de las licencias de usuario de Office Worker, Power User o Teleworker.

Avaya one-X®Portal for IP Office es una aplicación basada en servidor a la que el usuario accede a través de un navegador web.

Para el modo Teletrabajador, las aplicaciones One-X requieren supervisión de respuesta y detección de desconexión para un funcionamiento adecuado. Como resultado, las aplicaciones one-X no funcionarán con troncales que no admitan supervisión de respuesta y detección de desconexión.

Nota:

Las aplicaciones one-X funcionan en tipos de troncales como PRI, BRI y SIP; sin embargo, no funcionarán en E1R2, T1 RBS y troncales de inicio de bucle analógico.

Los administradores del sistema pueden controlar si Avaya one-X®Se puede acceder a Portal for IP Office solo a través de un protocolo seguro, recomendado para implementaciones alojadas para proporcionar acceso "solo seguro". La otra opción es permitir que los usuarios accedan al cliente a través de un protocolo seguro y no seguro (HTTP/ HTTPS). La aplicación cliente obliga a los usuarios a cambiar sus contraseñas y códigos de correo de voz para cumplir con la configuración de complejidad configurada por el administrador.

A través de dispositivos, Avaya one-X®Portal para IP Office ofrece las siguientes funciones:

- Información de llamadas
- Control de llamadas y conferencias
- Notificaciones de presencia y mensajería instantánea, monitoreo y archivo
- Importación y exportación de contactos
- Grupos XMPP mostrados en la**Directorio del sistema**pestaña
- Marcar al propio puente del usuario e invitar a otros usuarios a unirse
- Programación de conferencias telefónicas y otras reuniones, incluidas reservas de puertos, asistencia por correo electrónico y creación automática de informes, disponibles en la interfaz de Outlook
- Alojamiento de conferencias web con un solo clic e inicio de sesión único para unirse a conferencias web como participante

Equinoccio de Avaya™para IP Office

Equinoccio de Avaya™para IP Office es un cliente de comunicaciones unificadas (UC) basado en SIP que brinda a los usuarios capacidades de colaboración en tiempo real y permite a los usuarios comerciales administrar fácilmente sus comunicaciones diarias desde una única interfaz. IP Office es compatible con los siguientes sistemas operativos:

- Escritorio:
  - Ventanas
  - Mac OS
- Teléfono móvil:
  - Android: Desde un teléfono móvil, tableta o un Avaya Vantage™dispositivo
  - iOS

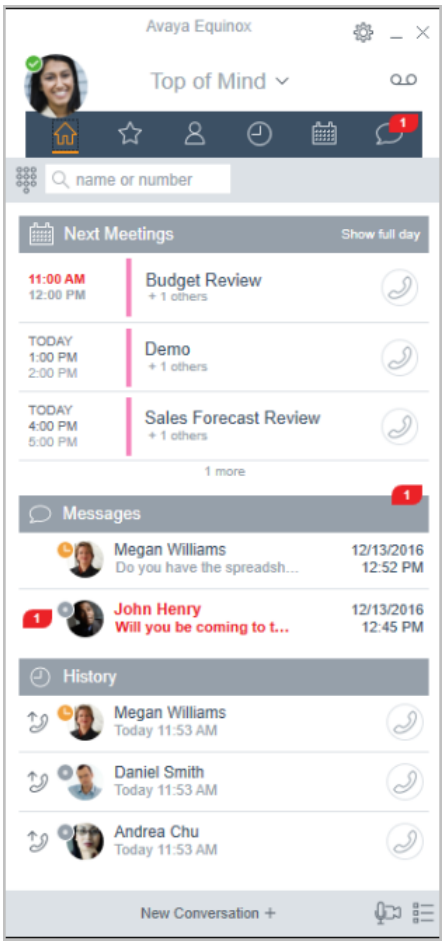
Nota:

En Avaya Vantage™Versión 2.0.1, los dispositivos K165 y K175 son compatibles con Avaya Equinox™cliente. El dispositivo K155 no es compatible con Avaya Equinox™cliente.

Equinoccio de Avaya™es un cliente multiplataforma común. Las capacidades del cliente varían según la plataforma en la que esté registrado. Las funciones admitidas en Avaya Equinox™para IP Office son:

- Pantalla de inicio de elementos destacados
  - Próximas reuniones que muestran el horario del calendario local o el servicio web de Exchange/Office 365
  - Historial de llamadas locales
  - Mensajes
  - Panel de inicio de reuniones/lanzamiento de espacios
- Opción Top of Mind Lite para teléfonos móviles
- Directorio de IP Office y contactos locales
- Mensajería a través de Avaya Spaces

- Presencia a través del servidor de IP Office
- Historial de llamadas locales
- Teclado con rellamada
- Integración de escritorio con Microsoft Outlook y navegadores
- Llamadas de audio y video del cliente Softphone
- Control compartido de un teléfono de escritorio de IP Office asociado.



Equinoccio de Avaya™se registra con el servidor de IP Office como un softphone SIP para llamadas de audio y video, y funciones de telefonía. Se admiten las siguientes características:

- Llamadas de audio y video punto a punto (realizar, recibir y finalizar)
- Manejo de múltiples llamadas (entrantes y salientes)
- Retener y recuperar (llamadas de audio y video)
- Transferencia (ciega y consultiva)
- Conferencia de consulta
- Escalar audio a videollamada
- Comparta el control con teléfonos de escritorio compatibles en Avaya Equinox™cliente de escritorio

- Equinoccio de Avaya™en Avaya Vantage™
- Integración de presencia y directorio con Avaya Equinox™en Avaya Vantage™
- Introducir DTMF durante una llamada

Equinoccio de Avaya™cliente en Avaya Vantage™admite las siguientes características:

- Realización de llamadas salientes.
- Manejo de llamadas entrantes.
- Poner una llamada en espera y reanudarla.
- Silenciar y reactivar una llamada.
- Transferir una llamada.
- Escalar una llamada de audio a una videollamada y desescalar una videollamada a una llamada de audio.
- Introducir dígitos DTMF mediante el teclado.
- Accede a tus contactos locales
- Acceda a sus contactos de IP Office mediante el directorio de IP Office.
- Administrar su estado de presencia y mensajes de estado de presencia.

Equinoccio de Avaya™para las limitaciones de IP Office:

- Control CTI: Avaya Equinox™para IP Office no se puede controlar a través de otras aplicaciones, como Avaya Contact Center Select, IP Office Contact Center o IP Office SoftConsole.
- Trabajador de sucursal: Avaya Equinox™para IP Office no admite conmutación por error entre Avaya Aura®Núcleo y sucursal de IP Office.
- Para mensajería instantánea, Avaya Equinox™para IP Office depende de la disponibilidad de la cuenta de Avaya Spacesbasic en la nube.
- El equinoccio de Avaya™el cliente accede a Avaya Equinox®Reuniones en línea mediante HTTPS, desde la pestaña Reuniones de Equinox del cliente. El equinoccio de Avaya™El cliente puede acceder a Equinox Conferencing local local de la misma manera mediante HTTPS, es decir, si la URL de acceso está configurada en Equinox Meetings. Sin embargo, si Avaya Equinox™el cliente accede a Equinox Conferencing local en las instalaciones a través de troncales SIP, el audio y el video estarán disponibles pero no se compartirán ni la lista de conferencias. Lo mismo se aplica para acceder a Scopia a través de troncales SIP. Incluso cuando Avaya Equinox™el cliente accede a IP Office Meet Me Conferencing local en las instalaciones, el audio estará disponible pero no se compartirá ni la lista de conferencias.

Cliente web Avaya IP Office

Avaya IP Office Web Client es una aplicación WebRTC que brinda varias capacidades de comunicación. El cliente aprovecha las mejoras de resiliencia de WebRTC Gateway proporcionadas en R11.0 y es compatible con Server Edition e IP500 V2. Los usuarios deben tener una licencia de Office Worker o Power User para usar las funciones de Avaya IP Office Web Client. El cliente es compatible con los siguientes entornos:

- Navegadores Google Chrome en el sistema operativo Windows
- Navegadores Google Chrome en macOS
- Cliente independiente en el sistema operativo Windows

Avaya IP Office Web Client ofrece las siguientes funciones:

- Llamadas de audio y video punto a punto
- Acceso al correo de voz
- Registros de llamadas
- Conferencias:
  - Conferencia ad-hoc mediante la fusión de llamadas
  - Iniciar o unirse a una conferencia Meet Me de IP Office
  - Acceder a la colaboración web de IP Office
- Presencia y mensajería instantánea punto a punto al integrarse con Avaya one-X®Portal para IP Office
- Hacer clic para llamar con la extensión de Google Chrome
- Compatibilidad con inicio de sesión único (SSO) para Avaya one-X®Portal para IP Office y colaboración web de IP Office
- Directorio del sistema y favoritos (Directorio personal)

Comunicador de Avaya

Avaya Communicator es un cliente de software de colaboración que ofrece una interfaz innovadora para comunicaciones en tiempo real para Windows y iPad. Permite a los usuarios manejar llamadas telefónicas, mensajes instantáneos, conferencias, colaboración web, presencia, contactos empresariales y correo electrónico, todo desde una única interfaz. Avaya Communicator ofrece el diseño gráfico intuitivo de focos, menú de medios, barra de notificaciones y tarjetas de contacto.

Avaya Communicator for IP Office se comunica tanto con IP Office como con Avaya one-X®Portal para proporcionar funciones de comunicación y colaboración. IP500 V2 proporciona funciones de telefonía como hacer/recibir llamadas, poner en espera/retirar, silenciar/activar, DTMF, MWI, etc. y Avaya one-X proporciona funciones de UC como mensajería instantánea, presencia y contactos empresariales.®Servidor de portales.

Si Avaya one-X®El servidor del portal no está disponible, ya sea debido a restricciones de licencia o problemas de conectividad, el cliente de Avaya Communicator funcionará en un modo de solo telefonía y brindará solo funciones de telefonía. La interoperabilidad con Avaya Session Border Controller for Enterprise permite que los usuarios con el perfil de trabajador remoto utilicen el cliente Flare Communicator y se registren en IP Office sin necesidad de una conexión VPN.

Avaya Communicator ofrece las siguientes funciones:

- Agregue participantes usando el teclado de marcación o arrastrando y soltando
- Silenciar y cancelar el silencio de todos o un subconjunto de participantes
- Bloquear y desbloquear la conferencia
- Colocar la conferencia en modo conferencia
- Habilitar y deshabilitar los tonos de entrada y salida
- Eliminar a todos o algunos participantes de la conferencia
- Terminar la conferencia

- Habilite y deshabilite la continuación para permitir que la conferencia continúe después de que el moderador se retire.
- Ascender a los participantes a moderadores
- Cree conferencias ad-hoc fusionando llamadas P2P
- Autorización y códigos de cuenta (solo Windows)
- Recordatorio de tiempo de espera en espera (solo Windows)
- Experiencia de usuario compacta
- Compatibilidad con TSL/SRTP
- Filtrado de contactos
- Integración de conferencias web
- Transferencia sin supervisión
- Respuesta automática
- Modo simultáneo
- Cambio de contraseña
- Códigos de cuenta
- Configuración automática (solo iOS)
- Compatibilidad y selección de dispositivos Bluetooth y auriculares (solo iOS)
- Interoperabilidad con Scopia (Radvision XT5000)

Nota:

Avaya Communicator no admite la grabación ni el indicador de altavoz activo.

Avaya Communicator para iPad

Avaya Communicator para iPad integra voz, video, presencia, mensajería instantánea, directorios en una interfaz unificada a través de conexiones Wi-Fi o celular 3G y VPN.

Avaya Communicator es una solución solo de software que se puede descargar fácilmente desde Apple iTunes Store y es compatible con iPad2, iPad3, iPad4, iPad Mini (con y sin pantalla retina), iPad Air, modelos Wi-Fi y 3G y las siguientes versiones de iOS: 6.1.x, 7.0.x, 7.1.x y 8.0.x.

Nota:

Avaya Communicator no es compatible con iOS 6.0.x.

Con Avaya Communicator, los usuarios de IP Office pueden usar dispositivos iPad para:

- Fácil acceso a las herramientas de comunicación en tiempo real en las que confían todos los días (teléfono, presencia, mensajería instantánea, etc.)
- Combinar las comunicaciones en tiempo real y los procesos comerciales, como las ventas móviles
- Aprovechar la conectividad Wi-Fi y 3G para VoIP económico
- Señalización segura sobre TLS e intercambio seguro de medios sobre SRTP en entornos de nube

- Como moderador de conferencias web, la capacidad de compartir pizarras y documentos
- Cambio de contraseñas
- Soporte de respuesta automática
- Transferencias no supervisadas
- Servicios de configuración automática utilizando un perfil de configuración alojado en un servidor web por dirección de correo electrónico o URL
- Compatibilidad y selección de dispositivos Bluetooth y auriculares
- Búsqueda en el directorio del sistema
- Agregar/eliminar miembros de un equipo (Grupo XMPP)
- Buscar en el directorio del sistema y agregar a un equipo o contacto personal
- Compatibilidad con Radvision XT5000 para videollamadas punto a punto

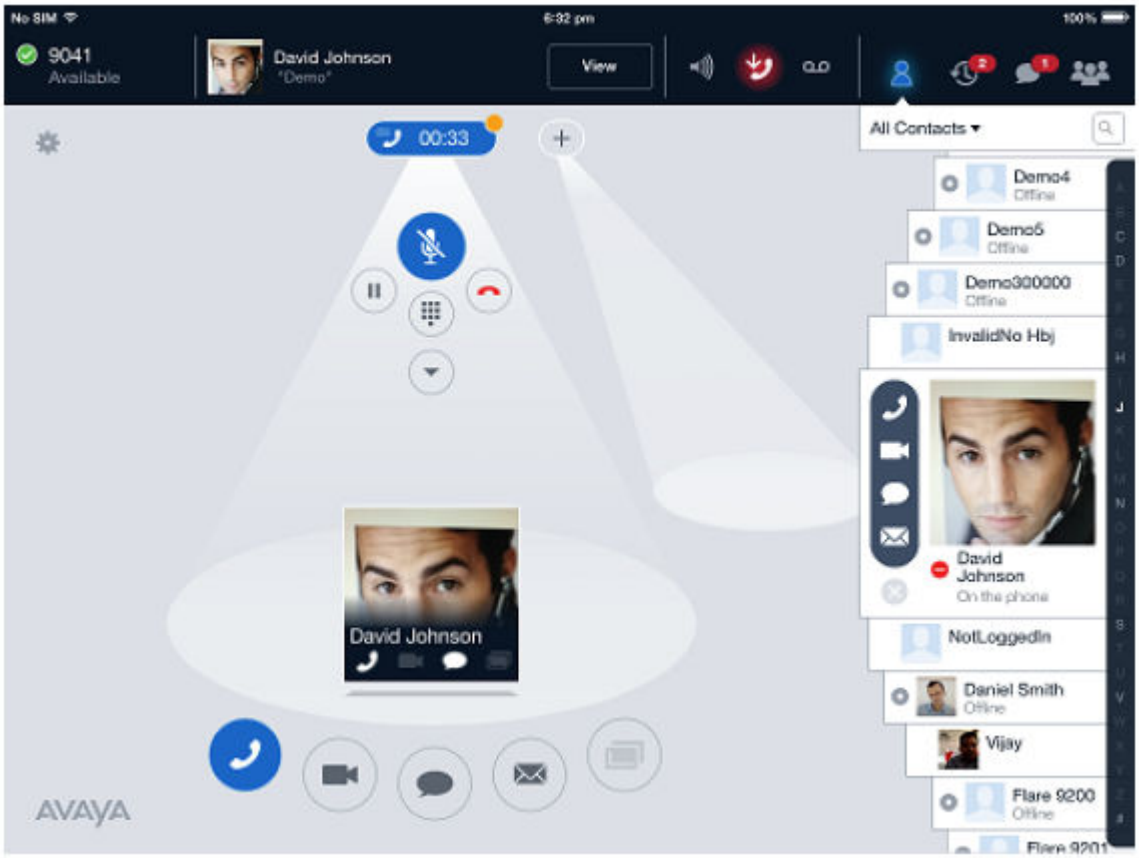


Figura 11: Avaya Communicator para iPad

Avaya Communicator para Windows

Avaya Communicator for Windows integra voz, presencia, mensajería instantánea y directorios en una oferta unificada para computadoras portátiles y de escritorio con Windows a través de una conexión LAN.

Avaya Communicator ofrece las siguientes funciones:

• Modo compacto que ocupa menos espacio en la pantalla

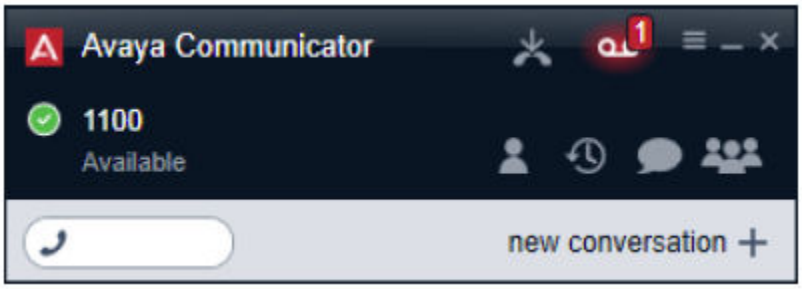


Figura 12: Vista compacta de Avaya Communicator for Windows

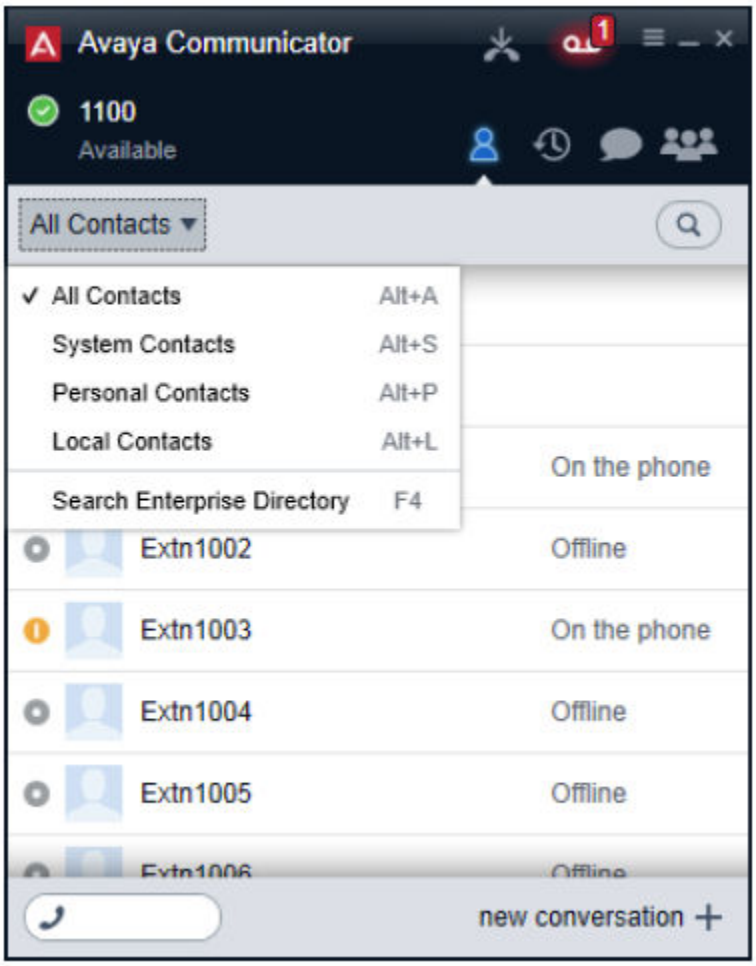


Figura 13: Vista completa de Avaya Communicator para Windows

• Señalización segura sobre TLS e intercambio seguro de medios sobre SRTP para entornos de nube

• Filtrado de contactos según criterios y opción de ver solo contactos del sistema, locales o personales

- Integración de conferencias web
- Transferencias no supervisadas
- Respuesta automática
- Modo simultáneo para interfaces con one-X Portal, Outlook y Salesforce
- Cambio de contraseña
- Códigos de cuenta

SoftConsole

SoftConsole es la aplicación de recepcionista de Windows basada en PC para IP Office. Se puede adquirir con la licencia de usuario Recepcionista.

SoftConsole proporciona a los recepcionistas y operadores empresariales información de llamadas y acciones de llamadas para simplificar el manejo de llamadas y la mensajería instantánea. Con SoftConsole, los usuarios ven el estado de otros usuarios y ajustan la configuración básica de telefonía de otros usuarios, como los números de desvío. Avaya recomienda usar teléfonos que admitan Respuesta automática. Los usuarios pueden usar las funciones de mensajería instantánea proporcionadas por Avaya one-X®Portal, si está disponible.

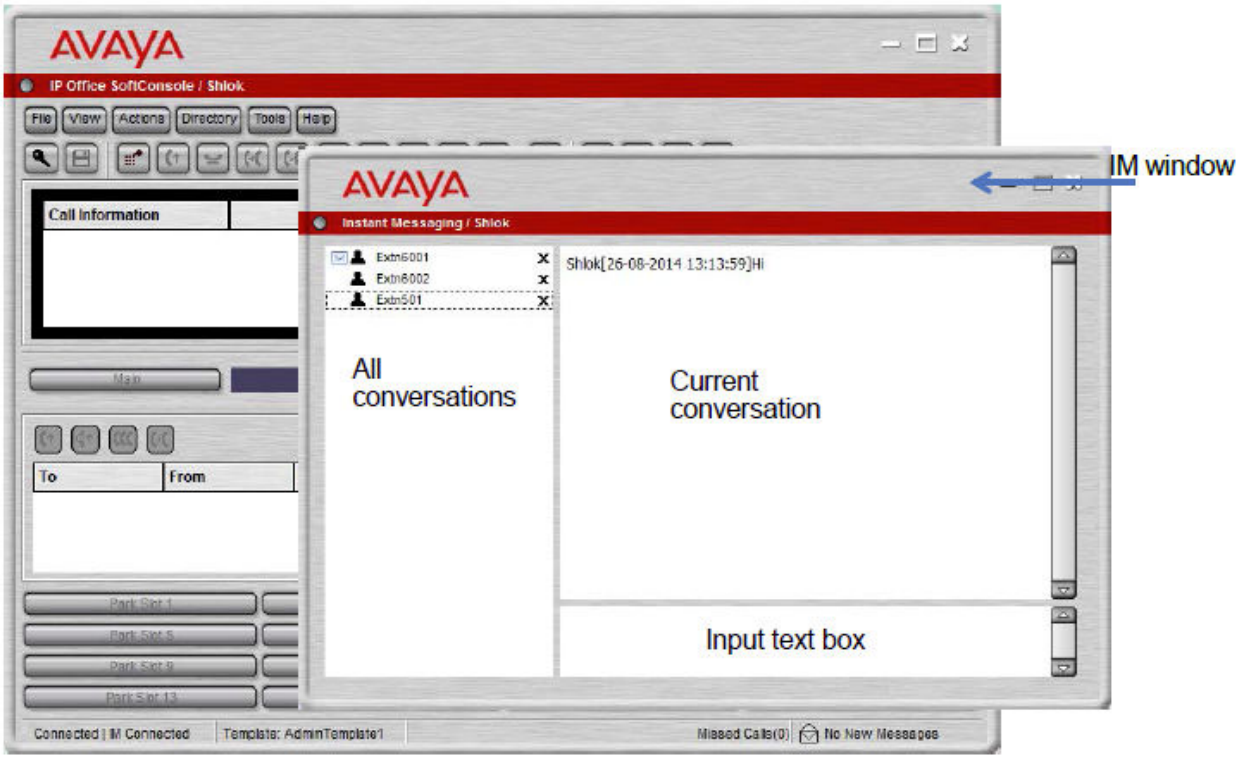


Figura 14: ventana de mensajería instantánea de SoftConsole

La comunicación WebSocket permite a los clientes de SoftConsole comunicarse con IP Office y Avaya one-X® Portal. El protocolo WebSocket es bidireccional entre el cliente y el servidor. Como la comunicación se realiza a través del puerto 80 o 443 (el mismo puerto utilizado para HTTP), no hay problemas con el cruce del cortafuegos. En un entorno alojado, la comunicación WebSocket proporciona seguridad.

SoftConsole se puede minimizar en la bandeja del sistema de Windows cuando no está en uso, pero aparecerá en la pantalla cuando se reciba una llamada. Los archivos de sonido y multimedia se pueden asociar con llamadas. Si se utiliza esta característica, la PC requiere una tarjeta de sonido y parlantes.

SoftConsole admite las siguientes características:

- Contestar llamadas
- Realización de llamadas salientes
- Transferencias supervisadas y no supervisadas
- Transferir llamadas al correo de voz
- Retener y estacionar llamadas
- Supervisión de colas y respuesta de llamadas en cola
- Uso y visualización de salas de conferencias
- Conferencia de llamadas retenidas
- Adición de usuarios a una conferencia
- Agregar texto a una llamada
- Liberación de la puerta
- entrometerse
- Envío de mensajes de texto
- Paginación
- Grabación de llamadas
- Envío de correo electrónico
- Uso del teclado de marcación
- Soporte de múltiples idiomas, los usuarios pueden seleccionar el idioma

Correo de voz integrado

En entornos como el comercio minorista o la oficina en el hogar, donde las consideraciones de espacio, ruido o costo descartan el uso de una PC para el correo de voz, Embedded Voicemail brinda servicios básicos de correo de voz. Embedded Voicemail está en la unidad de control IP500 V2 y no requiere un servidor de correo de voz separado.

Embedded Voicemail está disponible con IP Office Essential Edition. No se requieren licencias adicionales.

Buzón de voz profesional

Voicemail Pro se proporciona con IP Office Preferred Edition y es una aplicación avanzada de mensajería y flujo de llamadas para sistemas IP Office. Voicemail Pro puede manejar 40 (hasta 250/500 en Server Edition/ Server Edition Select) llamadas simultáneas según la licencia y la configuración del sistema. Cada usuario tiene la opción de activar o desactivar su correo de voz. Cuando está activado, el sistema contesta automáticamente su teléfono cuando no están disponibles para atender una llamada, reproduce un saludo personal y graba un mensaje.

Cuando se ha dejado un mensaje, el usuario verá una luz de mensaje en espera encendida en su teléfono y podrá presionar un botón de recuperación para recoger sus mensajes.

Voicemail Pro también puede llamar al usuario para entregar cualquier mensaje nuevo. Los mensajes de correo de voz se marcan con la fecha y la hora y se registra el número de la persona que llama. Voicemail Pro se puede configurar para eliminar los mensajes leídos automáticamente, a menos que el usuario elija guardar el mensaje de forma permanente.

Los correos de voz se pueden recopilar de forma remota llamando al servidor de Voicemail Pro. Si se reconoce el número desde el que está marcando el usuario (número de casa o teléfono móvil/celular, por ejemplo), el usuario escuchará su correo de voz de inmediato. Si no se reconoce el número de origen, se le solicitará al usuario un número de buzón y un código PIN para ese buzón, antes de que pueda escuchar su correo de voz. Los usuarios tienen la capacidad de establecer y cambiar sus propios códigos PIN.

Cuando es necesario reenviar un correo de voz a otros usuarios, Voicemail Pro ofrece muchas opciones:

- Los correos de voz se pueden reenviar a otro buzón o grupo de buzones
- Los destinatarios pueden agregar sus comentarios al correo de voz antes de reenviarlos a otro buzón o buzones.
- Los correos de voz se pueden reenviar como archivos adjuntos WAV de correo electrónico.

Todas las opciones están disponibles en varios idiomas; tanto indicaciones de voz habladas como interfaces de programación gráfica y tiene la opción de TUI de IP Office y TUI de emulación INTUITY.

conferencias

Los usuarios pueden poner llamadas en espera y crear una conferencia usando el teléfono o las aplicaciones de escritorio. Se pueden agregar miembros adicionales a la conferencia; sin embargo, una sola conferencia no puede tener más de 64 miembros (solo con IP500 V2 y más en Server Edition).

Para conferencias ad-hoc, el sistema requiere tantos troncales digitales/canales VoIP como participantes externos (así como Preferred Edition para conferencias Meet-Me). El sistema admite 128 canales de conferencia en el IP500 V2, lo que permite múltiples conferencias de cualquier tamaño de 3 a 64 participantes. El sistema admite 42 conferencias de 3 participantes, 2 conferencias de 64 participantes o cualquier combinación intermedia. Las capacidades Meet-Me requieren Preferred Edition para marcación directa en un puente de conferencia con seguridad de código PIN. En una red SCN, solo se requiere una licencia Preferred Edition centralizada para organizar conferencias Meet-Me en cualquiera de los sitios. Los ID de conferencia también se comparten en los sitios de SCN.

Están disponibles las siguientes capacidades de canal de conferencia:

Tabla 4: Capacidades del canal de conferencia

Plataforma	no seleccionado	Seleccione	Contacto Avaya Seleccionar centro	Contacto de la oficina de PI Centro
HP DL120 dell r210	128	128	414	414
HP DL360	256	256	825	825
dell r620	256	512	825	825

La tabla continúa...

Plataforma	no seleccionado	Seleccione	Contacto Avaya Seleccionar centro	Contacto de la oficina de PI Centro
ÓVULO	256	512	825	825
IP500V2	128	128	128	128

Para iniciar una conferencia, los usuarios marcan el número directo asignado al puente de la conferencia, ingresan el PIN (se requiere Preferred Edition y Voicemail Pro) si es necesario. Para conferencias ad-hoc con pocos participantes, los usuarios pueden configurar fácilmente conferencias inmediatas llamando a todas las partes y llevándolas al puente de conferencia. Con Avaya one-X®Portal para IP Office, el originador de la conferencia puede mantener el control: se muestra el número de identificación de llamadas (y el nombre asociado si se reconoce) de cada participante. Si es necesario, pueden colgar selectivamente a un participante específico. El sistema emite un solo pitido al entrar y un doble pitido a la salida. El propietario de la conferencia puede usar su número de extensión como ID de la conferencia. El propietario de la conferencia tiene el control de la conferencia con la capacidad de silenciar y desconectar las llamadas de los participantes. Todos los participantes escucharán la música en espera (MOH) del sistema hasta que el propietario se una, y escucharán MOH cuando el propietario se retire. Tenga en cuenta que cualquier parte interna tiene la opción de ver y eliminar participantes (no solo el originador de la conferencia).

Los usuarios pueden grabar un saludo personalizado para una conferencia (requiere Preferred Edition y Voicemail Pro).

Los usuarios pueden grabar la conferencia usando Avaya one-X®Portal para IP Office, teléfono con pantalla IP o digital o un código corto (requiere Preferred Edition y Voicemail Pro). Para evitar el acceso no autorizado al puente de conferencia, se pueden configurar códigos PIN, filtrado de números de identificación de llamadas y perfiles de fecha y hora mediante Voicemail Pro. Un usuario puede administrar la instalación del puente de conferencias desde cualquier ubicación.

Las conferencias tienen las siguientes restricciones:

- Solo se permiten dos llamadas conectadas a través de troncales analógicas en una sola conferencia.
- Cada llamante externo requiere un canal troncal/VoIP digital (por ejemplo, 1 T1 permite 23/24 interlocutores externos, 1 E1 permite 30 interlocutores y un VCM-64 con licencia completa permite 64 interlocutores).
- No hay límites en la combinación de llamadas internas y externas en la conferencia, pero si todos los participantes internos se desconectan del puente de conferencia, el sistema puede desconectar automáticamente a los participantes externos para mayor seguridad (configuración configurable del sistema).
- Las funciones del sistema, como la intrusión de llamadas, la grabación de llamadas y la supervisión silenciosa, utilizan recursos de conferencia, al igual que la grabación automática si está habilitada. Cuando alguna de estas funciones está activa, se reduce el número de espacios disponibles para los participantes en la conferencia. Por ejemplo, una llamada de conferencia entre 3 participantes y que se está grabando utilizará 4 espacios de conferencia.

Conferencia Meet-Me

La conferencia Meet-Me permite que varias personas que llaman hablen en una audioconferencia. Las personas que llaman pueden ser personal en el sitio, así como partes externas, ya sean ingenieros de campo, personal de ventas en el camino, clientes o proveedores. Las conferencias telefónicas se pueden planificar con anticipación o establecer ad-hoc cuando sea necesario.

Colaboración de vídeo

IP Office brinda compatibilidad con Bring Your Own Device (BYOD) y sistema de sala HD para la colaboración de video.

IP Office admite la colaboración de video con el intercambio de datos a través de Avaya Scopia®aplicaciones móviles y de escritorio al usar Radvision MCU o Video Collaboration para IP Office. Los clientes de Flare también pueden participar en videoconferencias multipartitas. Avaya Scopia®se conecta a IP Office como punto final SIP mediante una licencia IP de Avaya.

Avaya Video Collaboration for IP Office ofrece las siguientes funciones:

- Integración directa que incluye un plan de marcación común con IP Office
- "Sala de conferencias virtual" para hasta ocho participantes con capacidades de hacer clic para unirse desde cualquier sistema de sala basado en estándares, computadora de escritorio o dispositivo móvil
- Clientes de video móviles y de escritorio de distribución gratuita para PC, Mac y los dispositivos iOS y Android más populares, lo que permite a las personas dentro y fuera de una organización unirse fácilmente a una reunión de video
- Videoconferencia multipartita HD de bajo ancho de banda con colaboración de datos usando SIP/H nativo. 323
- Cortafuegos transversal automático para interactuar con participantes fuera de la red

El siguiente diagrama muestra la topología de IP Office implementada con terminales de video.

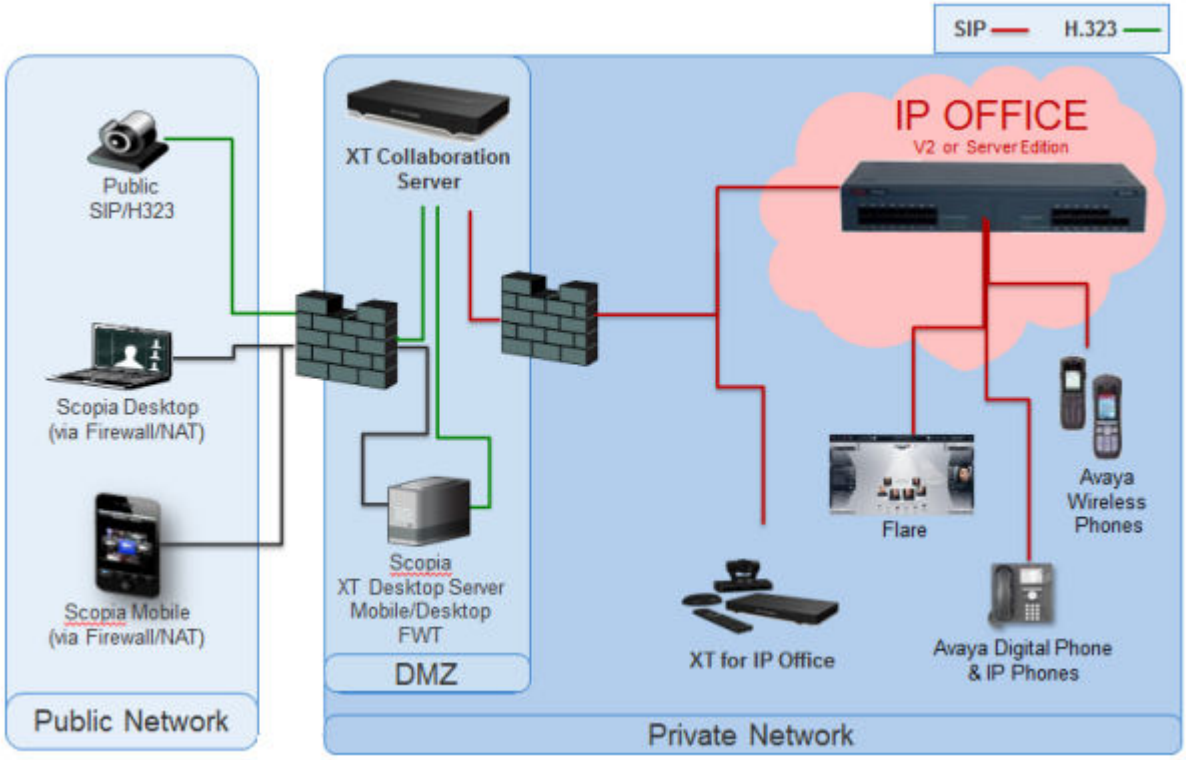


Figura 15: Puntos finales de video

Agente de colaboración

Collaboration Agent es una aplicación que proporciona herramientas de conferencia y colaboración web. Usuarios con Avaya Aura®Las cuentas de conferencias y los invitados pueden usar las herramientas para administrar conferencias y participar y colaborar en conferencias.

Los participantes de la conferencia pueden unirse a conferencias iniciando sesión en Collaboration Agent y llamando al puente de audio asignado a la conferencia. Los participantes también pueden usar la función integrada de audio y video de Collaboration Agent. Los participantes pueden usar las herramientas de Collaboration Agent para aumentar la productividad y realizar un seguimiento de los elementos de acción incluso después de que finaliza la conferencia. Los moderadores de la conferencia pueden:

- Grabar todos los aspectos de las conferencias.
- Grabar y editar actas de reuniones.
- Crear y distribuir informes de reuniones basados en las actas de las reuniones.

Características del Agente de colaboración

En Collaboration Agent, los participantes y moderadores pueden realizar múltiples tareas como:

- Ver una lista de otros participantes.
- Levante virtualmente la mano y pida permiso para hablar.
- Enviar mensajes.
- Anotar contenido compartido.
- Grabar o editar minutos.
- Establecer los tonos de entrada y salida.
- Llamar a otros usuarios ya los usuarios de la conferencia.
- Desconectar a los participantes.
- Ascienda a los participantes al rol de moderador.
- Invite a más participantes a unirse a una conferencia activa.

Durante la conferencia, los participantes pueden ver la siguiente información en Collaboration Agent:

- Los participantes que se unieron solo en el puente de audio
- Los participantes activos en la colaboración web
- El participante que habla actualmente
- El presentador actual

Características opcionales

Las siguientes funciones son opcionales y deben ser habilitadas por el administrador del sistema:

- Iniciar conferencias antes de que se unan los moderadores.
- Vídeo integrado
- Promover a todos los participantes al rol de presentador para que todos los participantes puedan compartir contenido
- Marcación desde Collaboration Agent para conectar usuarios a conferencias
- Grabación de conferencias

Espacios de Avaya

Avaya Spaces es una aplicación de reunión y colaboración en equipo basada en la nube. Integra a la perfección voz, video, tareas, uso compartido y más en su navegador o en la aplicación Spaces. Cada usuario de IP Office tiene derecho a una cuenta gratuita de Avaya Spaces Basic que incluye las siguientes actividades de colaboración en equipo a través de Avaya Equinox™cliente:

- Creación de espacios para administrar proyectos en curso: puede usar el área de espacios en el tablero para iniciar una nueva conversación. De hecho, la primera vez que comienza a usar Avaya Spaces, puede ver la opción para crear su propio espacio. Puede invitar a los participantes a su espacio ingresando sus direcciones de correo electrónico. Puede establecer diferentes permisos para cada participante según el tipo de acciones que desea que puedan realizar dentro de su espacio. Si tiene muchos espacios, puede categorizar los que usa con frecuencia como favoritos.
- Conferencias de audio VoIP con hasta cinco participantes.
- Uso compartido de archivos limitado (hasta 1 GB)
- Videollamadas punto a punto, escale sus chats con audio o video.
- Intercambiar mensajes instantáneos con otros usuarios mediante Avaya Spaces Direct Messaging.
- Únase a una reunión de Spaces.

Equinoccio de Avaya®Reuniones en línea

Equinoccio de Avaya®Meetings Online ofrece un servicio de suscripción opcional para comunicaciones unificadas de múltiples partes, es decir, colaboración de audio, video y web. El servicio proporciona una sala de reuniones virtual Over The Top (OTT) con conferencias de audio y video, intercambio de contenido, chat y moderación de reuniones. Los usuarios pueden acceder al servicio a través de un sistema de escritorio, móvil y de sala de video, así como acceso telefónico de audio; También se admite la interoperabilidad de sistemas de salas de video de terceros.

Aplicaciones de instalación y administración.

Las siguientes secciones proporcionan una descripción general de las aplicaciones relacionadas con la instalación y la administración.

Gerente de IP Office

Utilice Manager para administrar sistemas independientes de IP Office o sistemas en una red comunitaria pequeña (SCN). Manager realiza un seguimiento de los cambios de configuración del sistema, gestiona las actualizaciones y las importaciones y exportaciones de configuración.

IP Office tiene una pista de auditoría integrada que rastrea los cambios en la configuración del sistema y quién los ha realizado. El administrador puede mostrar la pista de auditoría para ayudar con la resolución de problemas. La pista de auditoría registra los últimos 15 cambios en la configuración y registra los siguientes elementos:

- Configuración cambiada: para los cambios de configuración, el registro informará a un alto nivel sobre todas las categorías de configuración (usuarios, grupo de búsqueda...) que hayan cambiado.
- Configuración borrada
- Configuración fusionada
- Reiniciar: reinicio instigado por el usuario

- Mejora
- Inicio fresco
- Arranque en caliente
- Escribir en HH:MM: esto es cuando el administrador guardó la configuración a través de la opción de programación
- Escritura con reinicio inmediato
- Escribir con Reiniciar cuando esté libre

IP Office Manager también se utiliza para funciones de mantenimiento como:

- Actualizar al software del sistema IP Office
- Capacidad de enviar software a través de un enlace de red IP a un sistema y validarlo antes de comprometerse con la actualización
- Compatibilidad con versiones anteriores de sistemas de la versión 2.1 en adelante para permitir una sola aplicación de administración
- Importación y exportación de información de configuración de IP Office en archivos ACSII-CSV.

Administrador de la edición del servidor

Server Edition Manager admite la administración centralizada completa para Server Edition Primary, Server Edition Secondary y Server Edition Expansion Systems. Manager también proporciona funciones de telefonía IP Office y comunicaciones unificadas.

Manager permite la gestión de todos los componentes dentro de la solución para actividades como:

- Punto único de configuración para IP Office y correo de voz
- Asistente de instalación inicial simple
- Resumen del sistema con inventario y estado
- Configuraciones comunes consolidadas en Server Edition Primary
- Procliente de correo de voz integrado, aplicación de estado del sistema y acceso a la configuración de la plataforma Linux
- Admite la administración en línea y fuera de línea y la configuración de una solución completa
- Operaciones de plantilla
- Configuración centralizada y almacenamiento de plantillas
- Utilidad de administración de cuentas de administrador
- Conserva la experiencia existente de IP Office
- Ayuda sensible al contexto

Aunque Manager es una aplicación de Windows, Manager se puede instalar directamente desde el portal de administración web del servidor primario de Server Edition. Esto le permite usar cualquier computadora personal con Windows que tenga IP Office Manager preinstalado inmediatamente.

Con Manager, el administrador puede crear plantillas para muchos elementos de administración, como usuarios, extensiones, grupos de búsqueda y líneas. El administrador puede entonces crear cualquier elemento nuevo usando

la configuración predeterminada o la plantilla. Puede crear múltiples usuarios y extensiones usando una plantilla.

Soporte de enrutamiento de llamadas:

- Compatibilidad total con IP Office ARS y plan de marcación
- El enrutamiento predeterminado simplifica la configuración
- Numeración automática de grupos de líneas en toda la solución
- Las rutas comunes de llamadas entrantes brindan resiliencia
- Grupos de búsqueda resistentes

Operación fuera de línea:

- La solución completa se puede crear y/o administrar fuera de línea si es necesario
- Todavía se puede administrar cuando algunos dispositivos están fuera de línea
- Opciones de sincronización de configuración en línea/fuera de línea para armonizar según sea necesario

Gestión de soluciones:

- Vista completa de la solución con estado e inventario
- Los usuarios y los grupos de búsqueda abarcan toda la solución
- Derechos de usuario centralizados, códigos cortos de función, perfiles de tiempo, rutas de llamadas entrantes y códigos de cuenta
- Permite la configuración avanzada por dispositivo si se desea
- Todas las configuraciones almacenadas en el servidor principal
- Directorio de todo el sistema de la solución
- Gestión sencilla de licencias centrales y por dispositivo

Gestión de la resiliencia:

- Puede administrar todos los dispositivos localmente para eventos de 'día lluvioso'
- Puede administrar la solución a través de un servidor secundario cuando el servidor principal falla o en una configuración de WAN dividida
- Opciones de sincronización de configuración On/Offline para armonizar según sea necesario

Agregar o quitar dispositivos:

- Proceso único para agregar o quitar el dispositivo
- Utilidad de configuración inicial (ICU) integrada para simplificar la adición de un nuevo dispositivo
- Los elementos de configuración comunes del servidor principal se completan automáticamente
- Puede configurar antes de instalar un nuevo dispositivo

Validación:

- Validación de la configuración en lectura y cualquier cambio.
- Validaciones de toda la solución

Modelo:

- Cree una plantilla local y centralizada a partir de entradas existentes de Línea, Extensión, Usuario, Grupo de búsqueda, Perfil de tiempo, Perfil de firewall, Ruta IP y Servicio
- Vuelva a crear múltiples extensiones y usuarios a partir de una plantilla

Acceso remoto:

- Admite el acceso desde el servicio a través de SSL VPN

Seguridad:

- Inicio de sesión único para todos excepto para la administración de one-X Portal

Administrador web

Web Manager es una herramienta de administración basada en navegador diseñada para simplificar el proceso de instalación y mantenimiento y proporciona acceso a la mayoría, pero no a todos, los ajustes de configuración de IP Office. Web Manager elimina la necesidad de tener un sistema operativo Windows porque puede ejecutarse en cualquier dispositivo que admita navegadores estándar.

Acceso granular:

Web Manager proporciona a los usuarios del servicio acceso a todos los objetos de configuración si el usuario del servicio tiene acceso a la configuración. Sin embargo, los grandes clientes que tienen varios roles de usuarios de servicios o los clientes que tienen implementaciones en el entorno de la nube deben tener acceso de configuración granular para diferentes usuarios de servicios. Los socios de alojamiento podrán crear una cuenta para el cliente o el revendedor con permisos limitados. Estos permisos impedirán que el cliente o el revendedor realicen actividades que afecten el servicio del sistema.

Panel de configuración:

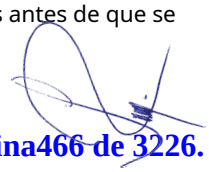
El panel es una versión simplificada del IP Office Web Manager existente y se presenta a los administradores cuando se instala un nuevo sistema IP Office de un solo nodo. El Tablero consiste en un conjunto mínimo requerido de campos de configuración para configurar el sistema. La configuración completa se puede realizar en cualquier momento después.

Administrador de medios de IP Office

IP Office Media Manager es una aplicación nativa de IP Office para archivar, almacenar, buscar, reproducir, descargar, auditar y eliminar grabaciones de llamadas de IP Office. La operación, administración y gestión de (OAM) de la aplicación está integrada dentro de la solución IP Office, por ejemplo, IP Office Web Manager.

Media Manager obtiene las grabaciones de la aplicación IP Office Voicemail Pro a través de un directorio de transferencia preconfigurado. Media Manager mueve las grabaciones del directorio de traspaso a una partición de disco duro adicional en el servidor primario o de aplicaciones de Server Edition y luego archiva las grabaciones en una ubicación de almacenamiento configurada por el administrador. La ubicación de archivo puede ser un almacenamiento conectado a la red (NAS), una unidad de DVD local o un almacenamiento en la nube. Para el almacenamiento en la nube, Media Manager solo es compatible con Google Drive en esta versión.

Media Manager se licencia por sistema. Además de una nueva licencia de IP Office versión 11.0 y posterior de Media Manager, la aplicación también funciona con una licencia anterior de Contact Recorder, para clientes que actualizan desde una versión anterior de IP Office. Media Manager permite un período de prueba de 90 días antes de que se aplique la licencia.



Contact Recorder no es compatible con la versión 11.0 y posteriores de IP Office y no forma parte del software de la versión 11.0 y posteriores de IP Office. Sin embargo, Media Manager admite la migración de datos de Contact Recorder a IP Office versión 11.0 y posteriores.

Media Manager está disponible como parte de la imagen del software IP Office Server Edition y Application Server. La aplicación se ejecuta en la distribución estándar de Linux compatible con las plataformas IP Office Server Edition y Application Server. El software se instala como un RPM de Linux estándar solo en el servidor primario de Server Edition o en el servidor de aplicaciones en caso de implementaciones de IP500 V2. La aplicación no es compatible con las plataformas UCM o Windows. La interfaz de administración está basada en la web y son compatibles con todos los navegadores populares, como Google Chrome, Mozilla Firefox, Microsoft Edge y Microsoft Internet Explorer.

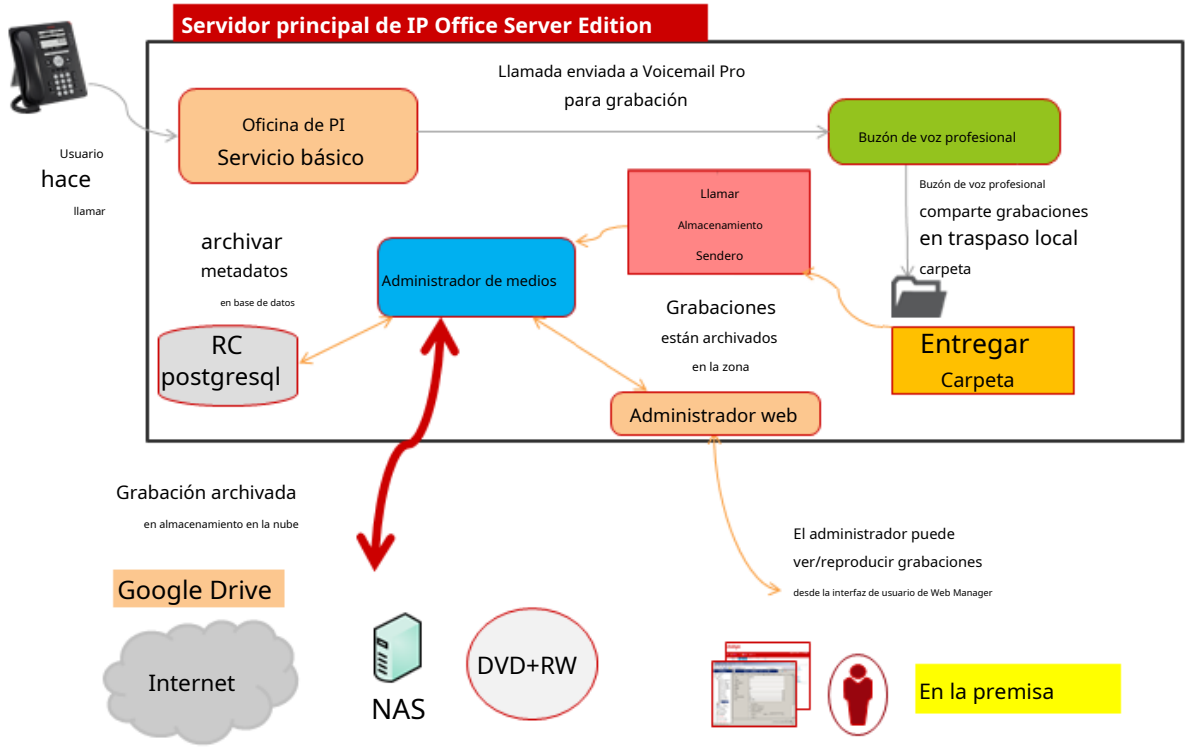
Media Manager en IP Office versión 11.0 Feature Pack 4 admite la eliminación o las grabaciones y realiza un seguimiento del uso de las grabaciones a través de la función de registro de auditoría. La función de seguimiento de auditoría lo ayuda a realizar un seguimiento de las actividades en torno a las grabaciones en la biblioteca. Con esta función, puede averiguar los usuarios que tienen:

- Buscó una grabación
- Reprodujo una grabación
- Descargado una grabación
- Eliminó una grabación

Para cada evento, Media Manager muestra el nombre de usuario, la fecha, la hora y el tipo de acción del usuario. La pista de auditoría se mantiene durante un número predefinido de días y se puede modificar. De forma predeterminada, los datos de la pista de auditoría están disponibles durante 180 días.

Media Manager está disponible como parte de la imagen del software IP Office Server Edition y Application Server. La aplicación se ejecuta en la distribución estándar de Linux compatible con las plataformas IP Office Server Edition y Application Server. El software se instala como un RPM de Linux estándar solo en el servidor primario de Server Edition o en el servidor de aplicaciones en caso de implementaciones de IP500 V2. La aplicación no es compatible con las plataformas UCM o Windows. La interfaz de administración está basada en la web y son compatibles con todos los navegadores populares, como Google Chrome, Mozilla Firefox, Microsoft Edge y Microsoft Internet Explorer.

Una implementación estándar de IP Office Server Edition:



Disponibilidad de las funciones de Contact Recorder en Media Manager

Las capacidades de búsqueda en Media Manager se han mejorado para los administradores y los usuarios.

Funcionalidad	Descripción	Disponibilidad en Contact Recorder	Disponibilidad en medios Gerente
Buscar por administrador	Buscar por administradores utilizando Número de destino, Habilidades, agente e ID de llamada	Sí	Sí
Buscar a través de la Web Autoadministración	Busque por usuarios utilizando los filtros de búsqueda Número objetivo, Habilidades, Agente, e ID de llamada	Sí	Sí
Búsqueda de autoadministración web resultados	Se muestra un máximo de 100 resultados.	Sí	Sí
Conjuntos de llamadas	Facilidad para guardar resultados de búsqueda para recuperarlos en el futuro.	Sí	No
Correo electrónico	Adjuntar grabaciones a correos electrónicos.	Sí	No

La tabla continúa...

Funcionalidad	Descripción	Disponibilidad en Contact Recorder	Disponibilidad en medios Gerente
Exportación a granel	Exportando múltiples grabaciones y la detalles relacionados	Sí	Sí
Dueño	Disponible como una opción de búsqueda.	No	Sí
Pista de auditoría	Se puede realizar una auditoría para rastrear el uso de grabaciones de llamadas.	Sí	Sí
Dominio de Windows Autenticación	-	Sí	No

Aplicación de gestión de soluciones

IP Office Manager y Web Manager utilizan la aplicación de administración de soluciones (SMA) para acceder a la configuración del sistema.

SMA reside en el servidor primario o secundario. Las configuraciones están disponibles para el acceso remoto y Server Edition Central Access. Central Access se comunica con el servidor primario o secundario en lugar de con cada nodo individualmente. Avaya requiere Central Access para un entorno alojado y lo recomienda para entornos no alojados con más de 32 nodos.

Modo Administrador de SoftConsole

Los administradores del sistema pueden iniciar SoftConsole en modo administrador. Cuando se ejecuta en este modo, no hay acceso a las funciones de telefonía.

El modo de administrador de SoftConsole permite a los usuarios configurar las siguientes funciones:

- Crear y editar perfiles de usuario
- Modificar la longitud de las notas de llamada
- Crear y editar plantillas
- Eliminar o mostrar los paneles de interfaz

Consola de administración SNMP

El Protocolo simple de administración de redes (SNMP) es un estándar de la industria diseñado para permitir la administración de equipos de datos de diferentes proveedores mediante una sola aplicación Network Manager. El administrador de la red sondea periódicamente el equipo para solicitar una respuesta, si no se recibe una respuesta, se genera una alarma. Además de responder a las encuestas, IP Office monitorea el estado de sus extensiones, tarjetas de troncales, módulos de expansión y tarjetas de medios para que, si se detecta un error, IP Office notifique al administrador de la red.

Dado que la plataforma IP Office comprende muchas aplicaciones, el software central notifica los eventos SNMP de Voicemail Pro y Embedded Voicemail para advertir acerca de los límites de capacidad de almacenamiento que se aproximan.

IP Office envía notificaciones por correo electrónico directamente al servidor de correo electrónico; no se necesita un cliente de PC adicional.

En los sitios de los clientes donde la administración de SNMP no está disponible, IP Office puede enviar eventos por correo electrónico usando hasta 3 direcciones de correo electrónico, cada una con un conjunto diferente de alarmas.

Las siguientes categorías de eventos del sistema se pueden elegir para la notificación por correo electrónico, si están instaladas en el sistema:

- Genérico
- Líneas troncales
- Tarjeta de correo de voz integrada
- VCM
- Módulos de expansión
- Aplicaciones
- Licencia
- Cambio de teléfono
- Circuito cerrado de CSU

IP Office ha sido probado contra SNMPc-EE de CastleRock™y Network Node Manager de HP (parte del paquete de aplicaciones OpenView).

Solicitud de estado del sistema (SSA)

La aplicación de estado del sistema (SSA) es una herramienta de diagnóstico para que los administradores y administradores de sistemas supervisen y verifiquen el estado de los sistemas IP Office de forma local o remota. SSA muestra el estado actual de un sistema IP Office y los detalles de cualquier problema que haya ocurrido. La información reportada es una combinación de eventos en tiempo real, eventos históricos, estado y datos de configuración para ayudar a encontrar y diagnosticar fallas. SSA proporciona estado en tiempo real, uso histórico e información de alarmas para puertos, módulos y tarjetas de expansión en el sistema. SSA se conecta a todas las variantes de IP Office mediante una conexión IP que puede ser remota o local. Se admiten conexiones de módem a 14,4 kbps o más para diagnósticos remotos.

La SSA proporciona información sobre lo siguiente:

alarmas	SSA muestra todas las alarmas registradas en IP Office para cada dispositivo con error. Se registra el número, la fecha y la hora de la ocurrencia. Las últimas 50 alarmas se almacenan en IP Office para evitar la necesidad de una PC local.
Detalles de la llamada	Información sobre llamadas entrantes y salientes, incluida la duración de la llamada, la identificación de la llamada y la información de enrutamiento.
Extensiones	SSA detalla todas las extensiones (incluido el tipo de dispositivo y la ubicación del puerto) en el sistema IP Office. También se muestra información sobre el estado actual de un dispositivo. SSA muestra las extensiones de IP que se registraron pero que ya no están disponibles y las extensiones de IP que están configuradas pero que no se han registrado después del último reinicio. Esto ayuda a detectar teléfonos inactivos, desconectados o mal configurados. SSA también muestra teléfonos en cuarentena y extensiones y direcciones IP en la lista negra.

Bañador	Se muestran las troncales y conexiones de IP Office (VoIP, analógicas y digitales) y su estado actual. Para troncales VoIP, también se muestra información de QoS (p. ej., retraso de ida y vuelta, fluctuación y pérdida de paquetes).
Sistema Recursos	IP Office incluye recursos centrales que se utilizan para realizar diversas funciones. El diagnóstico de estos recursos suele ser fundamental para el funcionamiento correcto del sistema. Esto incluye detalles sobre recursos para VCM, correo de voz y conferencias.
QoS Vigilancia	Se monitorean los parámetros de QoS de las llamadas conectadas, como la fluctuación y el retraso de ida y vuelta.

SSA se puede iniciar de forma independiente o desde IP Office Manager y puede haber hasta dos (2) clientes SSA conectados a una unidad IP Office a la vez.

Nota: SSA no es una herramienta de configuración para sistemas IP Office.

monitor de sistema

Utilice SysMonitor para solucionar problemas de IP Office desde ubicaciones locales (LAN) y remotas (WAN).

Seleccione los protocolos e interfaces para monitorear y diagnosticar a través de una interfaz gráfica. Capture los rastros directamente en la pantalla o como un archivo de registro para un análisis posterior. Codifique con colores diferentes trazos para mejorar la claridad en archivos grandes. La utilidad también captura las alarmas del sistema y muestra el registro de actividad de las últimas 20 alarmas que ocurrieron.

Gerente de Operaciones en la Nube

Cloud Operations Manager es una herramienta de administración que permite una forma simplificada de gestión de múltiples clientes con un enfoque en los sistemas basados en la nube. La herramienta permite la administración de sistemas IP Office Server Edition y brinda las siguientes capacidades:

- Portal único de administración unificada capaz de administrar hasta 3000 sistemas IP Office.
- Tablero que muestra las condiciones de error, las actividades del sistema en curso y el estado del sistema
- Agrupación de sistemas basada en versiones y etiquetas para acceder a sistemas similares con solo hacer clic en un botón
- Muestra todos los sistemas conectados, como Primario, Secundario, Expansiones y aplicaciones abiertas
- Capacidad para administrar de forma centralizada actualizaciones y parches de software de IP Office en múltiples sistemas y versiones
- Administración basada en roles: Cloud Operations Manager tiene sus propios usuarios del servicio con acceso a IP Office de clientes completos o selectivos. No hay acceso granular a nivel de función disponible en la versión 11.0.
- Ofrece la posibilidad de iniciar aplicaciones de gestión de IP Office nativas. Los usos deben iniciar sesión en las aplicaciones por separado después de iniciar la aplicación. El lanzamiento de IP Office Contact Center, Avaya Contact Center Select y Avaya Workforce Optimization Select no son compatibles con la versión 11.0.

- Alarmas de Configuración, Servicios, Troncales, Enlace y Seguridad por tipo de Severidad
- Alarmas para el estado de los sistemas IP Office que indican si están en línea o fuera de línea
- Alarmas que indican el estado de varias aplicaciones

Administrador de migración de datos (DMM)

El Administrador de migración de datos (DMM) facilita la migración de los sistemas BCM y Norstar a IP Office. Hay tres pasos en el proceso de migración: extraer, convertir y aplicar.

DMM migra:

- Anuncios y saludos
- Mensajes de correo de voz
- Extraer la configuración de Call Pilot

aplicaciones de centros de contacto

Las siguientes secciones proporcionan una descripción general de las aplicaciones del centro de contacto.

Para información general sobre:

- IP Office Contact Center, consulte*Avaya IP Office Contact Center Característica Descripción*.
- Avaya Contact Center Select, consulte*Descripción de la solución Avaya Contact Center Select*.

Descripción general de IP Office Contact Center

Nota:

IP Office Contact Center finaliza la venta de nuevos sistemas en septiembre de 2019.

Avaya es el líder del mercado en tecnología de centros de llamadas e IP Office Contact Center puede llevar su negocio a un nuevo nivel. IP Office Contact Center proporciona capacidades integradas de centro de contacto diseñadas específicamente para empresas que admiten entre 5 y 250 agentes y supervisores de centro de contacto.

IP Office Contact Center ofrece las siguientes funciones y características:

- Solución de servicio al cliente todo en uno que brinda un servicio consistente a los clientes a través de múltiples canales de medios y ubicaciones. IP Office Contact Center incluye una interfaz de usuario (IU) en Microsoft Windows y una interfaz web compatible con varios navegadores.
- Implementación rápida con una interrupción mínima para el negocio. IP Office Contact Center también incluye una función de sincronización automática para la configuración. Esta función se puede habilitar y deshabilitar según sea necesario durante la implementación.
- Acceso a la funcionalidad de la interfaz de usuario del agente, incluido el control de llamadas, desde un complemento de SalesForce (SFDC) o un conector SAP CRM.
- Capacidades de correo electrónico y chat en Windows y Web UI.
- Llamadas de voz entrantes y salientes con capacidades de telefonía y marcador.
- Enrutamiento basado en habilidades.

• Acceso a la libreta de direcciones para que los agentes puedan encontrar rápidamente la información de contacto que necesitan para realizar llamadas y enviar correos electrónicos.

• Informes históricos y en tiempo real para todos los canales de medios.

• Scripts de respuesta de voz interactiva (IVR) y editor de flujo de tareas.

• Configuración de privilegios de perfil de usuario y grupo de agentes para determinar qué funciones están disponibles para los usuarios de la interfaz. Los administradores deben asignar privilegios y crear grupos de agentes.

• Acceso a un portal de administración basado en web. Puede utilizar el portal de administración para realizar tareas de configuración, mantenimiento, supervisión y gestión. También puede cargar certificados, recopilar registros y descargar archivos de correo electrónico y la interfaz de usuario de IP Office Contact Center para Windows. Las tareas de administración avanzada se deben realizar en la interfaz de usuario de IP Office Contact Center para Windows. No puede realizar tareas de administración con la interfaz de usuario web de IP Office Contact Center.

• Acceso a un tablero que muestra las estadísticas de IP Office Contact Center. Para obtener más información acerca de Tablero, consulte *Uso del tablero de IP Office Contact Center de Avaya*.

• Opción para integrar fácilmente la funcionalidad de chat en una página web. Para más información, ver *Guía basada en tareas de servicios de chat y correo electrónico de Avaya IP Office Contact Center*.

• Integración opcional con aplicaciones de grabación de llamadas, como IP Office Media Manager. Las llamadas se graban con Voicemail Pro y los detalles de la grabación completa se almacenan en la base de datos de la aplicación de grabación de llamadas. Puede buscar y administrar grabaciones utilizando un navegador web.

• Interoperabilidad opcional con Avaya Workforce Optimization Select, que es un producto independiente que actualmente no se integra con las IU o las aplicaciones de IP Office Contact Center.

• Integración del Protocolo de control de recursos de medios (MRCP), que brinda soporte para texto a voz (TTS) y reconocimiento de voz automático.

Descripción general de Avaya Contact Center Select

Avaya Contact Center Select es una solución de centro de contacto multimedia, de voz y colaborativa sensible al contexto que permite a las pequeñas y medianas empresas anticipar, acelerar y mejorar las interacciones con los clientes. Avaya Contact Center Select utiliza el sistema telefónico Avaya IP Office para proporcionar una plataforma de telefonía en tiempo real.

Avaya Contact Center Select utiliza interfaces SIP y CTI estándar de la industria para integrarse con IP Office. Esta integración brinda a Avaya Contact Center Select acceso y control de una amplia gama de teléfonos y funciones de IP Office. Los clientes que integran Avaya Contact Center Select con IP Office obtienen enrutamiento basado en habilidades, tratamiento de llamadas, generación de informes, administración unificada de agentes y la utilidad gráfica Diseñador de orquestaciones.

Avaya Agent Desktop es una aplicación de cliente de interfaz única utilizada por los agentes de Avaya Contact Center Select para ayudar a los clientes. Los agentes de Avaya Contact Center Select utilizan el software Agent Desktop para responder a los contactos multimedia y de voz del cliente. Agent Desktop es compatible con una variedad de teléfonos IP Office y una amplia variedad de tipos de contactos multimedia.

De manera predeterminada, las conexiones y los servicios web de Avaya Contact Center Select utilizan comunicación TLS segura. La herramienta de administración de certificados de Avaya Contact Center Select facilita la administración de certificados de seguridad.

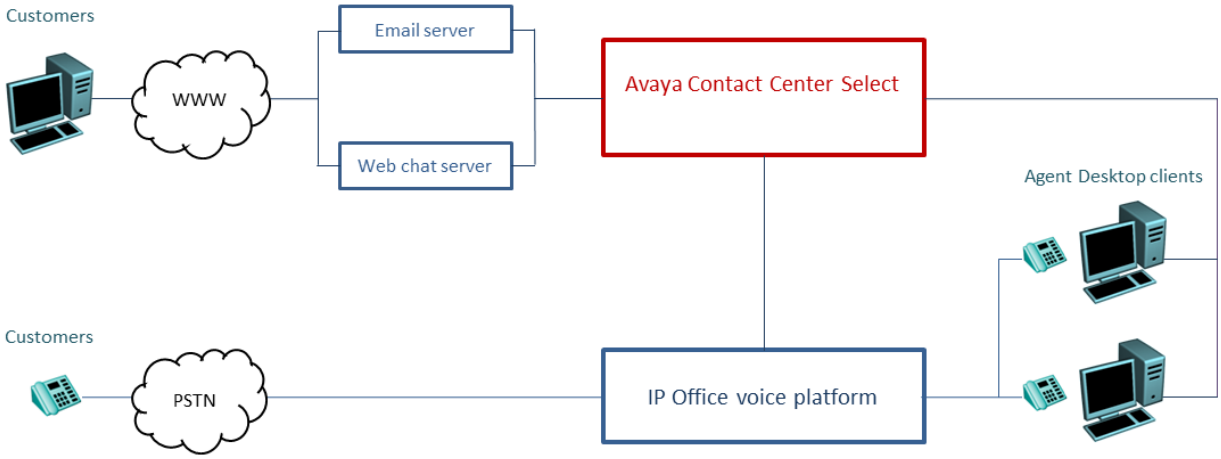


Figura 16: Solución típica de centro de contacto que usa voz y multimedia Avaya Contact Center Select y el sistema telefónico de voz Avaya IP Office

Avaya Contact Center Select proporciona una solución multimedia y de voz rica en funciones con enrutamiento e informes integrados para pequeñas y medianas empresas. Avaya Contact Center Select proporciona un centro de contacto unificado y administración de cuentas de usuario de teléfonos IP Office para agentes y supervisores. Los agentes y supervisores habilitados para voz creados en Avaya Contact Center Select se agregan automáticamente a IP Office. Avaya Contact Center Select sincroniza la información del usuario (agente y supervisor) entre Avaya Contact Center Select e IP Office.

Capítulo 3: Especificaciones de la solución

Configuraciones de referencia

IP Office se vende en diferentes ediciones, configuraciones de referencia y escenarios de implementación para cumplir con los diferentes requisitos de los clientes. Las ediciones se complementan entre sí para ofrecer funciones avanzadas, que incluyen presencia, mensajería instantánea, colaboración web e integración de software de Microsoft.

Las siguientes secciones resumen las ediciones de IP Office y otras opciones de configuración. Estas secciones no proporcionan detalles completos de configuración de referencia para cada opción de IP Office. Los documentos de configuración de referencia separados están disponibles para IP Office Server Edition, IP Office Branch, Powered by Avaya Cloud solutions e IP Office Contact Center.

Ediciones de IP Office

Edición básica de IP Office

IP Office Basic Edition está diseñado para empresas pequeñas y en crecimiento que necesitan una mayor productividad con un toque profesional. Las empresas pueden aumentar la capacidad según sea necesario.

IP Office Basic Edition proporciona funciones básicas de telefonía como:

- Capacidad de 64 troncales: analógica, PRI/T1 y SIP
- Operación del sistema clave
- Capacidad de conferencias para 64 personas
- Operadora automática
- Compatibilidad con varios idiomas
- Reenvío de llamadas
- Identificador de llamadas
- Marcar por nombre
- Salida a recepción
- Correo de voz integrado:
  - Máximo de 6 llamadas simultáneas al correo de voz con aproximadamente 25 horas de almacenamiento
  - Control de mensajes que incluye Guardar, Eliminar, Reenviar, Repetir, Rebobinar, Avance rápido y Omitir mensaje

- Correo de voz visual

- Estampado de fecha y hora del mensaje

Modos de operacion

Las unidades de control IP500V2 se suministran sin firmware ni configuración instalados. Cuando se enciende por primera vez, la unidad de control carga e instala el firmware necesario desde la tarjeta SD del sistema instalada en ella. Crea una configuración predeterminada que coincide con la tarjeta instalada en la unidad de control y los módulos de expansión externos conectados a ella. Las unidades de control IP500V2 pueden operar en varios modos. El modo inicial está determinado por el tipo de tarjeta SD del sistema.

Modo	tarjeta SD
Modo rápido de IP Office Basic Edition	• Operación del sistema PBX de telefonía de ley. • Operación del sistema de clave de telefonía ley µ.
IP Office Basic Edition - Modo SOCIO	El valor predeterminado es el funcionamiento en modo PARTNER de telefonía de ley.
Edición básica de IP Office - Modo NORSTAR	El valor predeterminado es la operación del modo NORSTAR de telefonía de ley µ.

Basic Edition se ejecuta en la unidad de control IP500V2. Se requiere una SD y está instalada en la parte posterior de la unidad de control, que proporciona software operativo, teclas de función y licencias. Se puede instalar una tarjeta SD opcional en la ranura para tarjeta SD opcional, lo que proporciona capacidades de actualización del sistema y copias de seguridad redundantes.

Tabla 5: Tarjetas base admitidas

Basic Edition admite las siguientes tarjetas base:

Tarjeta básica	modo SOCIO Máximo por sistema	Modo NORSTAR Máximo por sistema
combinación analógica	4	4
Combinación BRI		2
ETR6	3	
DS8	3	3
TCM8	4	4
Teléfono 2	4	4
Teléfono 8	4	4

Tabla 6: Tarjetas de troncales admitidas

Basic Edition admite las siguientes tarjetas troncales:

Tarjeta de troncal	modo SOCIO Máximo por sistema	Modo NORSTAR Máximo por sistema
Cajero automático4	4	4
PRI/T1	1	
PRI/E1		1

La tabla continúa...

Tarjeta de troncal	modo SOCIO Máximo por sistema	Modo NORSTAR Máximo por sistema
BRI4		4
BRI8		1

Módulos de expansión

Basic Edition admite los siguientes módulos de expansión:

- DS16A
- DS16B
- DS16B2
- Cajero automático16
- Teléfono 16
- Teléfono 30
- DS30A
- DS30B
- DS30B2

Nota:

Los módulos de estación digital DS16B2 y DS30B2 son compatibles con las versiones 10.1, 9.1 SP12 y 10.0 SP5 de IP Office en adelante.

Edición esencial de IP Office

IP Office Essential Edition ofrece las mismas funciones que Basic Edition además de lo siguiente:

- Control de llamadas móviles con acceso a un número y timbre simultáneo en dispositivos móviles
- Hasta 4 trabajadores remotos a través de una conexión a Internet y un teléfono IP serie 9600 de Avaya
- Acceso las 24 horas con saludos de correo de voz personalizados para cada miembro del personal
- Mensaje de voz:
  - Máximo de 6 llamadas simultáneas al correo de voz
  - Enviar mensajes de voz al correo electrónico
  - Hasta 25 horas de almacenamiento de correo de voz (con 6 puertos)
  - Hasta 40 operadores automáticos con un máximo de 6 llamadas simultáneas
- Compatibilidad con varios idiomas
- Puente de audioconferencia de hasta 128 participantes con 64 en cualquier conferencia

Nota:

La Edición Básica no es un requisito previo para la Edición Esencial o la Edición Preferida, y no se apila bajo la Edición Esencial.

Edición preferida de IP Office

IP Office Preferred Edition proporciona enrutamiento inteligente de llamadas, mensajería, manejo de llamadas e integración de aplicaciones.

Además de las funciones proporcionadas con Essential Edition, IP Office Preferred Edition ofrece lo siguiente:

- Correo de voz escalable:
  - Hasta 40 llamadas simultáneas
  - Envíe un mensaje de voz a todos los empleados, un departamento o un equipo
  - Mensajes de dirección por extensión o por nombre
  - Los mensajes de correo de voz pueden "encontrar" a los usuarios para alertarlos de que hay un mensaje en espera.
- Conferencias seguras para hasta 128 participantes con 64 por conferencia
- Enrutamiento de llamadas automatizado con un número ilimitado de asistentes automáticos que se pueden personalizar según la hora del día, el día de la semana u otras variables, así como para reconocer a las personas que llaman y entregar mensajes personalizados
- Grabación de llamadas para llamadas entrantes y salientes que se pueden enviar al correo de voz o bandejas de entrada de correo electrónico como archivos WAV

Componentes

- Unidad de control IP500 V2
- PC con conexión Ethernet que ejecuta la versión compatible de Windows Server
- PC conectada a Ethernet configurada con el software del servidor de aplicaciones
- Cliente de correo IMAP (Outlook) para sincronización de correo de voz en el correo electrónico y acceso basado en navegador al correo de voz
- Troncales y canales digitales para apoyar a los usuarios
- Teléfonos compatibles con IP Office

Edición de servidor de IP Office

IP Office Server Edition proporciona funciones de telefonía, comunicaciones unificadas, movilidad y colaboración de IP Office. También proporciona alta disponibilidad, facilidad de uso y bajo costo total de propiedad (TCO). Dirigida a la mediana empresa, IP Office Server Edition admite hasta 150 sitios, 3000 usuarios y resiliencia integral.

La solución IP Office Server Edition proporciona lo siguiente:

- Un único servidor primario de Server Edition proporciona IP Office, Voicemail Pro y Avaya one-X® Portal de IP Office.
- Un servidor secundario de Server Edition aumenta la capacidad y proporciona resiliencia.
- Sistemas de expansión, que brindan capacidad adicional, admiten interfaces analógicas o digitales y ubicaciones remotas.
- Una solución Select IP Office Server Edition proporciona capacidad adicional.
- Compatibilidad con una unidad de control IP500 V2 existente optimizada para implementaciones híbridas de analógico/TDM e IP, o un servidor Linux optimizado para implementaciones únicamente de IP.

Traducido del inglés al español - www.onlinedoctranslator.com

- Los usuarios y las extensiones se pueden configurar en el servidor IP Office Server Edition o en el Sistema de expansión Server Edition.
- La distribución de software incluye las diversas aplicaciones de usuario y administración, como IP Office Manager, SSA, Voicemail Pro e IP Office SoftConsole.
- Los componentes pueden estar en la misma ubicación o en diferentes ubicaciones.
- Opcionalmente, configure un servidor de aplicaciones separado dedicado a Avaya one-X®Portal para proporcionar más capacidad de usuarios que la que admite Server Edition Primary.
- Agregue servidores adicionales y sistemas de expansión en cualquier momento.

.

Topología

IP Office Server Edition se basa en una topología de red de doble estrella que brinda funciones integrales y su administración, facilita el uso, la instalación y la administración. La solución general proporciona una arquitectura flexible y modular que comienza con un solo servidor y puede escalar la cantidad de usuarios y ubicaciones mediante la conexión en red de varios servidores. Los componentes actúan automáticamente como una única unidad lógica y puede administrar los componentes desde una única consola a través de un sistema de gestión integrado.

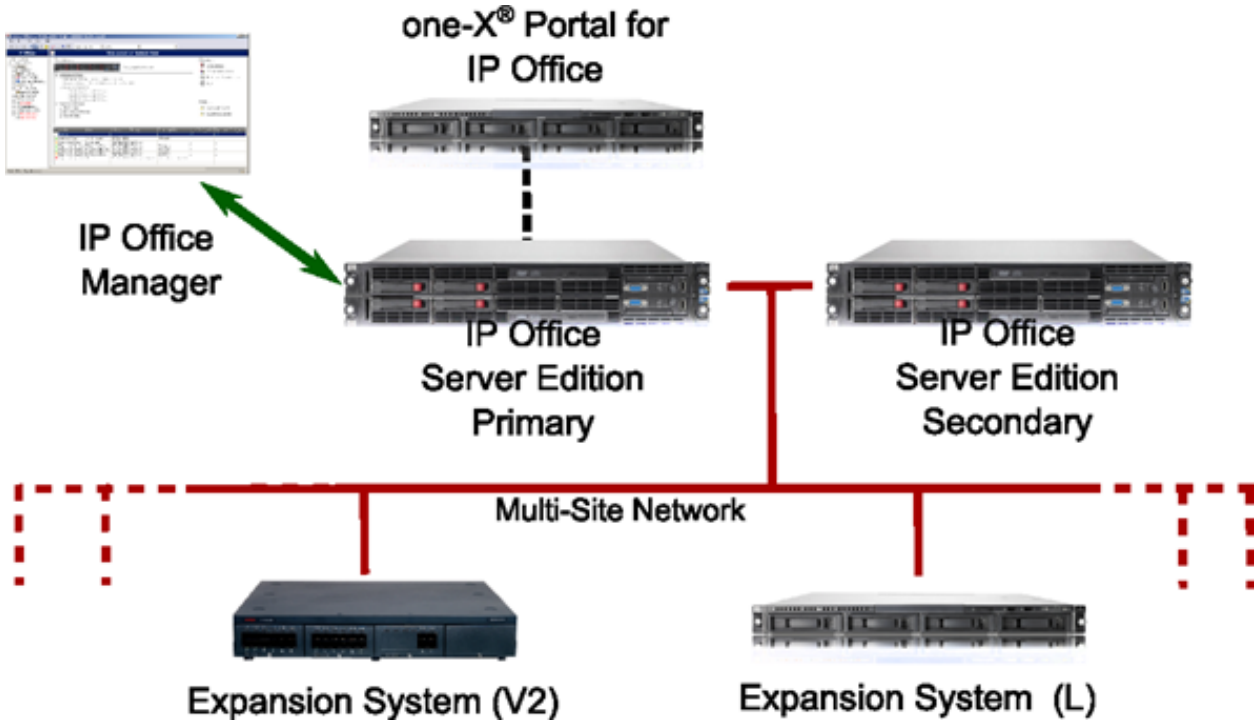


Figura 17: Topología de IP Office Server Edition

Modelos de implementación

Solo IP centralizada	Un servidor principal ubicado en la sede del cliente

IP analógica centralizada y digitales	Un servidor principal y un servidor de expansión ubicados en la sede del cliente
Solo IP distribuida	Un servidor principal ubicado en la sede del cliente y un servidor secundario ubicado en una ubicación remota
IP analógica distribuida y digitales	Un servidor primario y un sistema de expansión ubicado en la sede del cliente y un sistema de expansión ubicado en cada sitio remoto
virtualizado ambiente	Software y hardware proporcionados por el cliente Plataforma VMware vSphere con IP Office Server Edition y servidor de aplicaciones OVA activado como servidor principal, secundario, de expansión o de aplicaciones.

Componentes

Componente	Opciones del servidor	Descripción
Edición del servidor servidor principal	dell r630 dell r620 HP DL360G7 dell r220 dell r210 HP DL120G7	La distribución de software incluye: • Edición de servidor de IP Office • Correo de voz Pro • Avaya one-X®Portal para IP Office • Administrador de IP Office • Solicitud de estado del sistema (SSA) • SoftConsole
Edición del servidor servidor secundario	dell r630 dell r620 HP DL360G7 dell r220 dell r210 HP DL120G7	Componente opcional para soportar la resiliencia ya sea de forma centralizada o en un sitio remoto.
Edición del servidor Expansión Sistema	dell r630 dell r620 HP DL360G7 dell r220 dell r210 HP DL120G7	Componente opcional para admitir ubicaciones remotas. Hasta 148 sistemas de expansión brindan capacidad adicional, admiten interfaces analógicas o digitales y troncales locales en sitios remotos. Se puede configurar de forma centralizada o en un sitio remoto. **Nota:** En un entorno de nube, el sistema de expansión IP500 V2 brinda soporte para puntos finales analógicos y digitales.

La tabla continúa...

Componente	Opciones del servidor	Descripción
Edición del servidor Expansión Sistema	IP500 V2	Componente opcional para admitir ubicaciones remotas y como puerta de enlace. Puede ser un servidor IP500 V2 o IP Office Server Edition existente. Se puede configurar de forma centralizada o en un sitio remoto.
Avaya one-X® Portal de PI aplicación de oficina servidor	dell r630 dell r620 HP DL360G7 dell r220 dell r210 HP DL120G7	Componente opcional. Opcionalmente, puede configurar un servidor de aplicaciones separado dedicado a Avaya one-X®Portal para proporcionar más capacidad de usuarios avanzados por encima del máximo que admite Server Edition Primary.

Componentes del entorno virtualizado

Avaya proporciona un equivalente virtualizado de IP Office Server Edition y un servidor de aplicaciones empaquetado como un solo OVA listo para instalarse en hardware de host compatible con vSphere desde una PC. El OVA está disponible como descarga de Avaya o en un DVD que se puede pedir. Una vez implementado, puede activarse como servidor primario, secundario, de expansión o de aplicaciones.

Otras opciones de implementación

También puede implementar IP Office en:

- Un entorno de sucursal empresarial (sucursal de IP Office centralizada) o un entorno de sucursal distribuida).

  Puede implementar un sistema IP Office como una sucursal independiente o conectarlo a Avaya Aura® la red. También se admite un entorno de sucursal CS 1000.

- Un entorno Cloud con las ofertas Powered by Avaya.

Las opciones del centro de contacto también están disponibles.

Descripción general de IP Office como sucursal empresarial

Puede implementar IP Office como una sucursal empresarial para brindar una solución de comunicaciones adaptable para satisfacer las crecientes necesidades de una red de sucursal empresarial al mismo tiempo que brinda protección de la inversión en la plataforma de hardware y los teléfonos instalados. Puede implementar una sucursal empresarial de IP Office en un sistema de modo estándar, esencial o preferido de IP Office. El sistema IP Office puede instalarse como una sucursal independiente e independiente o conectarse a Avaya Aura®red y migró a una sucursal empresarial distribuida, centralizada o mixta para proporcionar características y aplicaciones específicas para satisfacer las necesidades de los empleados individuales en cada sucursal.

Además de los terminales SIP centralizados o los dispositivos analógicos centralizados configurados como ATA, IP Office puede admitir simultáneamente otros terminales IP y TDM para una comunidad de usuarios centralizados y usuarios de IP Office en la misma sucursal. Ideal para empresas que desean implementar aplicaciones en el cliente

centros de datos o en la sucursal, una sucursal de IP Office puede ofrecer de manera efectiva una variedad de herramientas de comunicación sin infraestructura ni administración complejas.

IP Office también es compatible con un entorno de sucursal de Avaya Communication Server 1000 (CS 1000). Solo se admite la opción de sucursal empresarial distribuida. IP Office se puede implementar como una nueva sucursal en una configuración CS 1000 existente con la adición de Avaya Aura®
Session Manager al que se conecta IP Office a través de la línea SM para la conectividad de la sucursal. Al brindar protección de la inversión telefónica, IP Office también se puede implementar como reemplazo de Business Communications Manager (BCM) o Norstar en una sucursal y conectarse a CS 1000 a través de Avaya Aura.®
Administrador de sesiones. IP Office no puede funcionar como una puerta de enlace recuperable para puntos finales CS 1000 de forma similar a la puerta de enlace remota recuperable (SRG).

Topología

La solución IP Office Branch brinda la flexibilidad para admitir sucursales independientes e independientes de IP Office, así como sucursales de IP Office conectadas a Avaya Aura.®sistema. La solución Branch también es compatible con la integración de CS 1000. Las siguientes opciones de implementación están disponibles para la arquitectura de la solución:

- **Opción de sucursal independiente de IP Office**: Los sistemas IP Office independientes se implementan dentro de la red. Estos sistemas IP Office no están conectados entre sí ni con ninguna otra cosa en la red. Con esta opción, las sucursales de IP Office no están conectadas a un Avaya Aura®
  sistema y los usuarios no pueden acceder a ningún Avaya Aura®servicios.
- **Opción de implementación de sucursales empresariales distribuidas**: Todos los usuarios de esta opción de implementación son usuarios de IP Office. Estos usuarios de IP Office obtienen servicios de telefonía de la IP Office local y no de Avaya Aura.®. Los sistemas IP Office en esta opción de implementación se pueden conectar a Avaya Aura®Session Manager y los administradores pueden obtener servicios de administración centralizados a través de Avaya Aura®Administrador de sistemas. La empresa puede optar por conectar a los usuarios de IP Office en esta opción de implementación a un sistema de correo de voz de IP Office, Embedded Voicemail o Voicemail Pro, o un sistema de correo de voz centralizado, como Avaya Aura.®
  Mensajería o Avaya Modular Messaging. Los usuarios de IP Office en esta implementación también tienen acceso a algunos Avaya Aura centralizados.®aplicaciones y servicios.

  Con la opción de implementación de sucursal distribuida, también puede conectar CS 1000 a IP Office en la sucursal a través de Avaya Aura®Administrador de sesiones. Los usuarios aún obtienen servicios de telefonía de IP Office local, pero pueden usar Avaya CallPilot®como su sistema de correo de voz. Cuando se conecta a CS 1000, IP Office y CS 1000 interoperan como pares a través de Avaya Aura®Administrador de sesiones.

- **Opción de implementación de sucursal empresarial centralizada**: Todos los usuarios de la empresa son usuarios centralizados.

  Registro centralizado de usuarios en Avaya Aura®Session Manager y obtener servicios de telefonía de Avaya Aura®Communication Manager Feature Server o Evolution Server en el núcleo empresarial. Si la conectividad WAN a Avaya Aura®Si se pierde Session Manager, el usuario obtiene automáticamente los servicios básicos de telefonía de la IP Office local. Las funciones de telefonía proporcionadas por IP Office en el modo de supervivencia son limitadas en comparación con las funciones que normalmente se brindan al teléfono centralizado.

  Los usuarios centralizados deben configurarse en Avaya Aura®Administrador de sesiones, administrador de comunicaciones e IP Office. Se debe configurar un usuario centralizado en Avaya Aura®Sesión

Gerente y Avaya Aura®Communication Manager como usuario SIP. En IP Office, el usuario centralizado debe tener una extensión SIP, una extensión analógica o un dispositivo de fax analógico.

- **Opción de implementación de sucursales empresariales mixtas**: una sucursal empresarial con usuarios centralizados y usuarios de IP Office. Los usuarios centralizados y los usuarios de IP Office obtienen los mismos servicios de telefonía descritos anteriormente. Todos los usuarios en esta opción de implementación deben usar un sistema de correo de voz centralizado: Avaya Aura®Mensajería o Avaya Modular Messaging.

Las opciones de implementación en la solución Branch le permiten comenzar con sistemas IP Office independientes y luego evolucionar lentamente la arquitectura de la solución hacia un entorno centralizado a medida que crece su empresa.

La siguiente imagen muestra la topología de la arquitectura de la solución con las opciones de implementación descritas anteriormente. Esta imagen no muestra CS 1000 en la implementación de sucursales distribuidas.

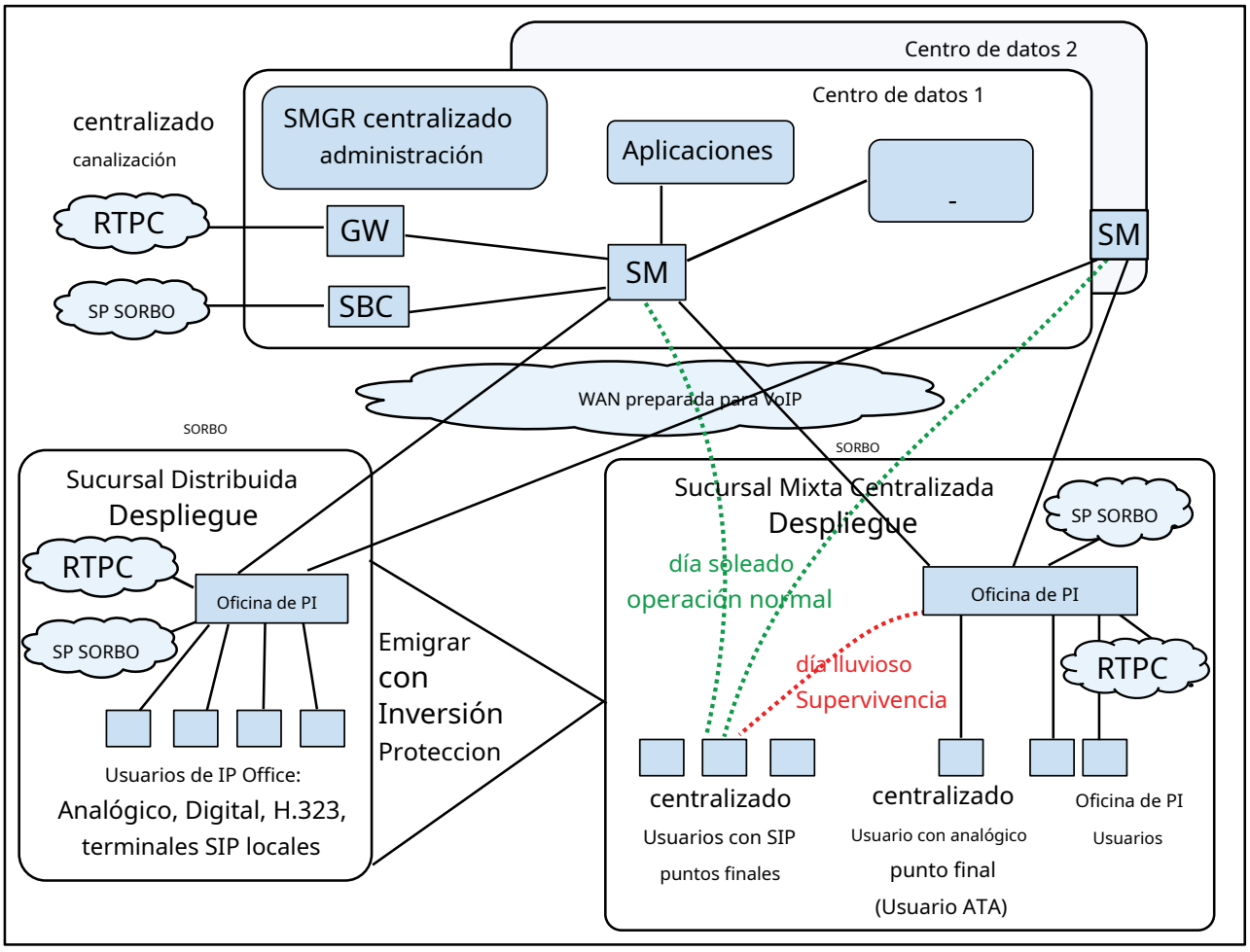


Figura 18: Topología de la arquitectura de la solución

Descripción general de Avaya Cloud

La solución Powered by Avaya Cloud le permite a usted, el BP o el proveedor, vender funciones principales de IP Office y, opcionalmente, IP Office Contact Center o Avaya Contact Center Select, a pequeñas y medianas empresas.

usuarios empresariales. Con Powered by Avaya, instala y aloja las instancias del producto en un centro de datos en la nube en su sitio.

La solución Powered by Avaya Cloud existente le permite a usted, el BP o el proveedor, vender funciones principales de IP Office y, opcionalmente, IP Office Contact Center o Avaya Contact Center Select, telefonía y comunicaciones unificadas (UC) a usuarios de pequeñas y medianas empresas. Con la nueva oferta de IP Office Cloud, los componentes opcionales de IP Office Contact Center y Avaya Contact Center Select no son compatibles. La funcionalidad de nube híbrida, Voicemail Pro y Media Manager tampoco son compatibles con la nueva oferta de IP Office Cloud. Esta oferta actualmente utiliza Embedded Voicemail como su sistema de correo de voz.

Con la oferta Powered by Avaya existente, instala y aloja las instancias del producto en un centro de datos en la nube. La nueva IP Office Cloud está alojada en un entorno de Google Cloud con un clúster de IP Office por proveedor.

Los beneficios clave de la solución en la nube incluyen lo siguiente:

- Reducción de los costos operativos para la empresa al reducir la complejidad de TI del mantenimiento del equipo.
- Reducción de costos de entrega de servicios para la BP a través de virtualización e infraestructura compartida.
- Interfaz programática para admitir instalaciones de licencias, configurar licencias centralizadas o eliminar un archivo de licencia.
- Facturación automatizada con Avaya One Source Cloud Services.
- Flexibilidad para cambiar su orden de Avaya One Source Cloud Services en cualquier momento. Puede agregar o eliminar usuarios en cualquier momento. Puede actualizar su pedido para agregar o eliminar los programas opcionales IP Office Contact Center y Avaya Contact Center Select, según sea necesario.
- Soporte para sistemas de expansión IP500 V2 en el sitio empresarial con Hybrid Cloud. Esto no se aplica a la nueva oferta de IP Office Cloud.
- Compatibilidad con resiliencia con alta disponibilidad (HA).

Desarrollado por la topología de Avaya

Desarrollado por Avaya es compatible con los siguientes modelos de implementación:

- Red pública: este modelo de implementación utiliza una conexión pública a través de Internet entre el centro de datos de la nube y las instalaciones de la empresa. Todos los usuarios que se conectan a través de la red pública se consideran trabajadores remotos.
- Red privada: este modelo de implementación requiere una conexión VPN de sitio a sitio o MPLS entre el centro de datos de la nube y las instalaciones de la empresa.

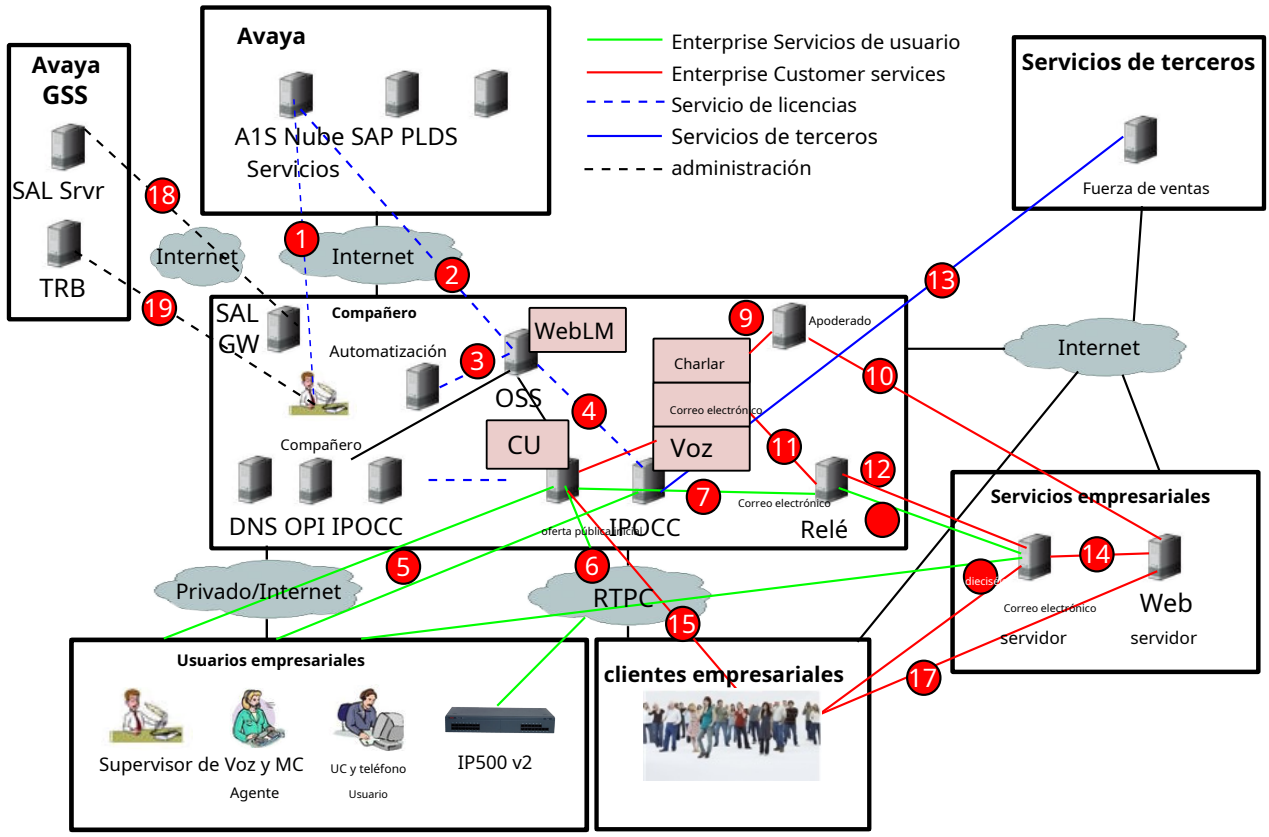


Figura 19: Topología Powered by Avaya

Configuraciones de referencia del centro de contacto

Opciones de implementación de IP Office Contact Center

IP Office Contact Center se puede implementar mediante las siguientes configuraciones y opciones de implementación:

Configuración	Opciones de implementación	Agentes y baúles
Centro de contacto de IP Office con IP500V2	IP500V2, servidor de IP Office Contact Center y un servidor de aplicaciones	Hasta 30 agentes en SIP y troncales digitales.
IP Office Contact Center con IP Office Server Edition	Servidor IP Office Server Edition y servidor IP Office Contact Center *y/o* un servidor de expansión Linux (opcional) *o* Alojado como un servicio en un entorno de nube	Hasta 250 agentes en troncales SIP. Solo se pueden implementar 125 agentes en cada Linux nodo de expansión.

La tabla continúa...

Configuración	Opciones de implementación	Agentes y baúles
IP Office Contact Center con IP Office Server Edition y Expansión IP500V2	Servidor IP Office Server Edition, servidor de expansión IP500V2 y servidor IP Office Contact Center	Hasta 250 agentes en SIP y troncales digitales. Solo se pueden implementar 30 agentes en cada nodo IP500V2.
IP Office Contact Center con IP Office Server Edition en un entorno distribuido	Servidor IP Office Server Edition, servidor de expansión IP500V2, servidor IP Office Contact Center y una expansión de Linux en un sistema distribuido ambiente	Hasta 250 agentes en SIP y troncales digitales. Se pueden implementar hasta 30 agentes en cada nodo IP500V2 y se pueden implementar hasta 125 agentes en cada nodo de expansión de Linux. Los agentes y troncales se distribuyen en cualquier servidor de expansión.

Las topologías detalladas de IP Office Contact Center se muestran en los siguientes documentos:

- *Avaya IP Office Contact Center Característica Descripción*
- *Configuración de referencia de Avaya IP Office Contact Center*

Configuraciones de referencia de Avaya Contact Center Select

Avaya Contact Center Select es una solución de centro de contacto rica en funciones que proporciona enrutamiento basado en habilidades para los contactos multimedia y de voz del cliente. Avaya Contact Center Select proporciona amplias herramientas para la gestión de agentes, informes históricos y en tiempo real, y herramientas gráficas para crear flujos de contacto y reglas de tratamiento. Proporciona administración de licencias, redes y servicios web de interfaces abiertas. Los clientes que integran Avaya Contact Center Select con la plataforma IP Office obtienen enrutamiento basado en habilidades, tratamientos de llamadas, informes, administración unificada de agentes y la utilidad gráfica Orchestration Designer.

En el momento de la implementación, Avaya Contact Center Select inicia automáticamente un asistente de configuración simple para implementar rápidamente una solución de centro de contacto funcional. Está precargado con usuarios de muestra, conjuntos de habilidades y parámetros del centro de contacto. Utilice estos datos de muestra para poner en marcha rápidamente la solución y realizar la primera llamada de cliente enrutada y contacto por correo electrónico.

Avaya Contact Center Select admite los siguientes tipos de contactos enrutados:

- Voz
- Correo electrónico
- Saliente
- Comunicaciones web (chat web)
- Mensajes de texto SMS
- Mensajes de fax
- Documentos escaneados
- Mensajes de correo de voz
- Redes sociales

Avaya Contact Center Select también es compatible con la mensajería instantánea punto a punto. Para admitir los tipos de contacto basados en correo electrónico, debe agregar un servidor de correo electrónico a su solución. Para admitir el tipo de contacto de comunicaciones web, debe agregar un servidor de comunicaciones web a su solución.

Avaya Contact Center Select proporciona una utilidad de administración de mensajes de voz simplificada. El supervisor del centro de contacto puede realizar un trabajo de administración rápido sin necesidad de acceso de administrador al servidor de Avaya Contact Center Select. Avaya Contact Center Select proporciona una serie de utilidades de monitoreo de estado para monitorear los puntos de integración con IP Office.

Contact Center Manager Administration es una interfaz de generación de informes y configuración basada en navegador para Avaya Contact Center Select. Los supervisores de Avaya Contact Center Select utilizan Contact Center Manager Administration para configurar recursos, agentes, conjuntos de habilidades, flujos de contacto, componentes y actividades del centro de contacto. Contact Center Manager Administration proporciona informes históricos y en tiempo real sobre el centro de contacto.

Sincronización de datos de usuario

Avaya Contact Center Select proporciona administración unificada para los agentes del centro de contacto y los usuarios de IP Office. Los usuarios (agentes y agentes-supervisores) que configura en Avaya Contact Center Select se duplican automáticamente en la IP Office conectada.

Cuando crea un agente en Avaya Contact Center Select, se crea una cuenta de usuario coincidente en IP Office. Cuando modifica los detalles del agente en Avaya Contact Center Select, los detalles del usuario de IP Office correspondiente se actualizan automáticamente. Sin embargo, si elimina un agente en Avaya Contact Center Select, el usuario de IP Office correspondiente no se elimina. La sincronización funciona en una dirección: desde Avaya Contact Center Select hasta IP Office. El administrador de IP Office puede forzar manualmente la sincronización de datos desde Avaya Contact Center Select.

Topología

En una solución de centro de contacto que utiliza Avaya Contact Center Select y un sistema telefónico IP Office, se aplican las siguientes consideraciones de topología de red y conectividad:

- El servidor Avaya Contact Center Select se admite en un grupo de trabajo o en un dominio de Windows.
- Cada Avaya Contact Center Select se conecta a un único servidor primario de IP Office Server Edition. De manera alternativa, cada Avaya Contact Center Select puede conectarse a un solo modo estándar de IP Office 500V2 con una licencia de edición avanzada.
- Una red comunitaria pequeña (SCN) es un sistema de sistemas IP Office en red que puede, entre otras funciones, compartir números de extensión y nombres de usuario. Cada IP Office SCN admite un solo Avaya Contact Center Select conectado. Avaya Contact Center Select se conecta al servidor primario de IP Office Server Edition del SCN. Para admitir una SCN de IP Office, Avaya Contact Center Select debe conectarse a un servidor primario de IP Office Server Edition en esa red SCN.
- El servidor Avaya Contact Center Select y el sistema telefónico IP Office conectado deben estar ubicados en la misma ubicación del campus.
- Cada computadora cliente supervisor se comunica con el servidor Avaya Contact Center Select. El supervisor utiliza la interfaz web de Contact Center Manager Administration para configurar agentes y ejecutar informes. El supervisor de agentes utiliza el software Avaya Agent Desktop para manejar llamadas de clientes, aceptar llamadas de emergencia o de supervisor de agentes y observar llamadas o contactos de comunicación web. Cada supervisor habilitado para voz con Agent Desktop requiere un teléfono IP Office asociado.

- Cada equipo cliente del agente se comunica con el servidor de Avaya Contact Center Select. El agente usa Agent Desktop para manejar los contactos multimedia y de voz del cliente. Cada agente habilitado para voz requiere un teléfono IP Office asociado.

Avaya Contact Center Select admite las siguientes opciones de implementación:

- DVD de Avaya Contact Center Select
- Avaya Contact Center Seleccione VMware
- Dispositivo de hardware Avaya Contact Center Select
- Avaya Contact Center Select Business Continuity

Para obtener más información sobre las opciones de implementación de Avaya Contact Center Select, consulte *Descripción de la solución Avaya Contact Center Select*.

Enlaces relacionados

Configuraciones de referencia en la página 67 DVD de Avaya Contact Center Select en la página 80 Avaya Contact Center Select y VMware en la página 81 Dispositivo de hardware Avaya Contact Center Select en la página 82 Continuidad comercial de Avaya Contact Center Select en la página 83

DVD de Avaya Contact Center Select

El DVD de Avaya Contact Center Select contiene el software de la aplicación del centro de contacto. La opción de implementación de DVD es compatible con Platform Vendor Independence (PVI). PVI brinda al cliente la flexibilidad de comprar un servidor que cumpla con los requisitos de servidor de Avaya Contact Center Select y se ajuste a los estándares corporativos propios del cliente.

Avaya Contact Center Select admite una variedad de especificaciones de servidor PVI, cada una de las cuales admite una capacidad máxima de agente y una tasa de llamadas especificadas. Esta gama de especificaciones de PVI brinda al cliente la flexibilidad de usar el hardware mínimo para cumplir con los requisitos de sus soluciones y permite futuras expansiones.

La opción de implementación de Avaya Contact Center Select DVD no requiere recursos ni infraestructura de VMware, lo que mantiene el costo total de propiedad (TCO) y la complejidad de la solución al mínimo.

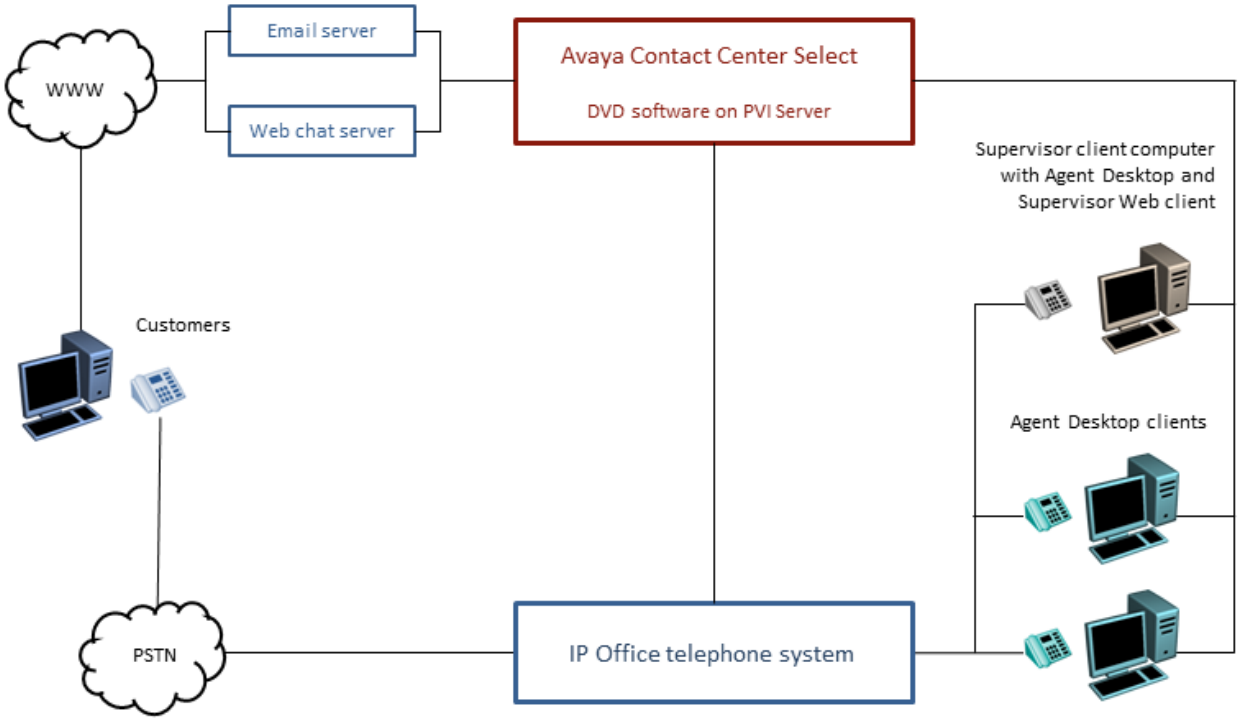


Figura 20: Implementación típica de Avaya Contact Center Select DVD

Para utilizar la opción de implementación de DVD de Avaya Contact Center Select, el cliente debe proporcionar lo siguiente:

- Hardware de servidor que cumple con una de las especificaciones PVI de Avaya Contact Center Select: nivel de entrada, gama media o gama alta.
- Licencia y sistema operativo Microsoft Windows 2012 R2 Standard o Datacenter Edition.

Para obtener más información sobre la opción DVD de Avaya Contact Center Select, consulte *Descripción de la solución Avaya Contact Center Select*.

Avaya Contact Center Select y VMware

Avaya Contact Center Select es compatible con la virtualización de VMware para aumentar la productividad, la flexibilidad y la eficiencia. Todas las opciones de implementación de Avaya Contact Center Select son compatibles con IP Office Server Edition OVA virtualizado en VMware.

Avaya Contact Center Select ofrece un paquete de dispositivo de software que consta de los siguientes componentes:

- Máquina virtual Avaya Contact Center Select
- Aura de Avaya®servidor de medios OVA
- Avaya WebLM OVA

Implemente estas máquinas virtuales e IP Office para crear una solución de centro de contacto escalable y virtualizada.

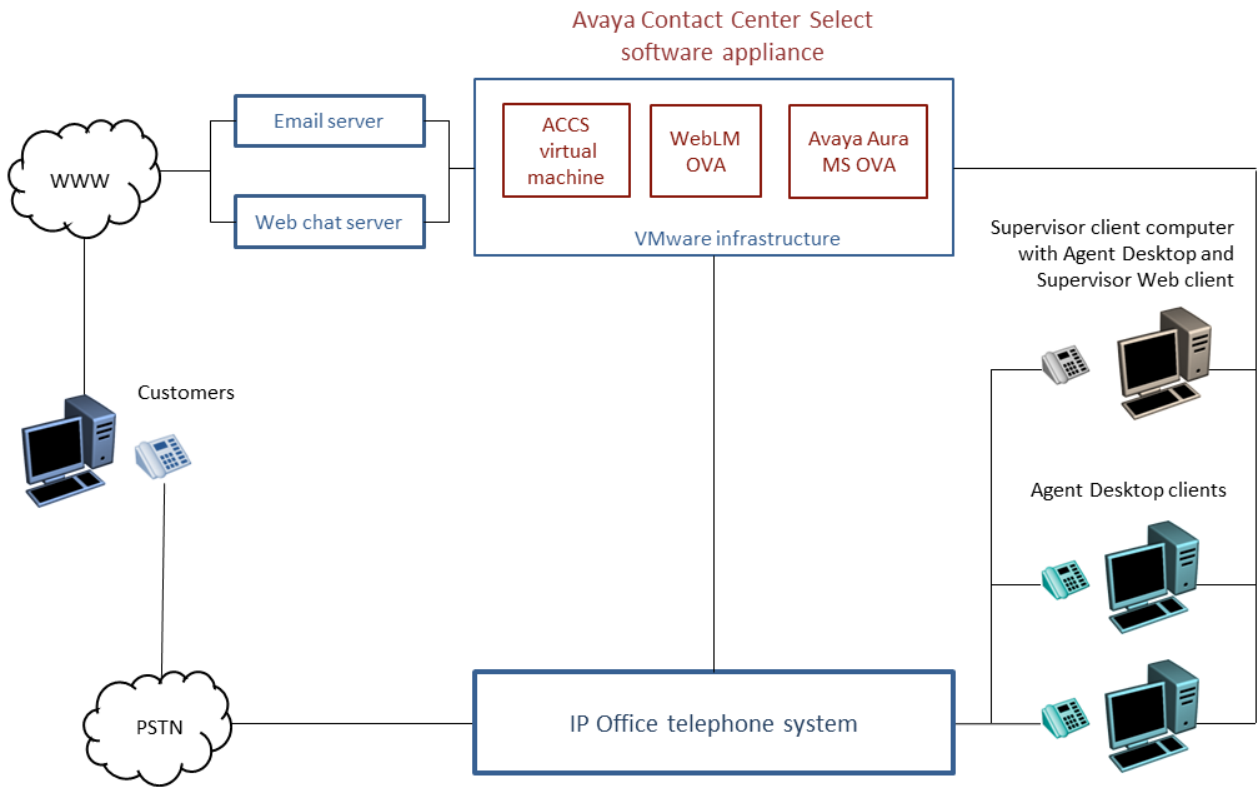


Figura 21: Solución típica de Avaya Contact Center Select y VMware

Avaya Contact Center Select es una colección de aplicaciones que brindan control de llamadas en tiempo real, manejo de multimedia e informes estadísticos. Implemente Avaya Contact Center Select en un entorno virtual VMware de nivel empresarial. Avaya recomienda que aplique la planificación, la ingeniería y la implementación de la virtualización con soporte organizacional completo para la virtualización en lugar de hacer crecer orgánicamente una infraestructura de virtualización.

Avaya Contact Center Select es compatible con VMware ESXi. No se requiere el software VMware vCenter; sin embargo, es compatible y es útil para Avaya Contact Center Select en entornos de centros de contacto de varios hosts.

Para obtener más información sobre Avaya Contact Center Select y VMware, consulte*Descripción de la solución Avaya Contact Center Select*.

Dispositivo de hardware Avaya Contact Center Select

El dispositivo de hardware Avaya Contact Center Select es un servidor físico de montaje en bastidor con el software de aplicación Avaya Contact Center Select ya cargado y parcialmente preconfigurado. Avaya proporciona el hardware del servidor y una licencia para el sistema operativo Microsoft Windows 2012 R2 Standard Edition.

El servidor de dispositivo de hardware de Avaya Contact Center Select ofrece una implementación de centro de contacto rápida y simplificada.

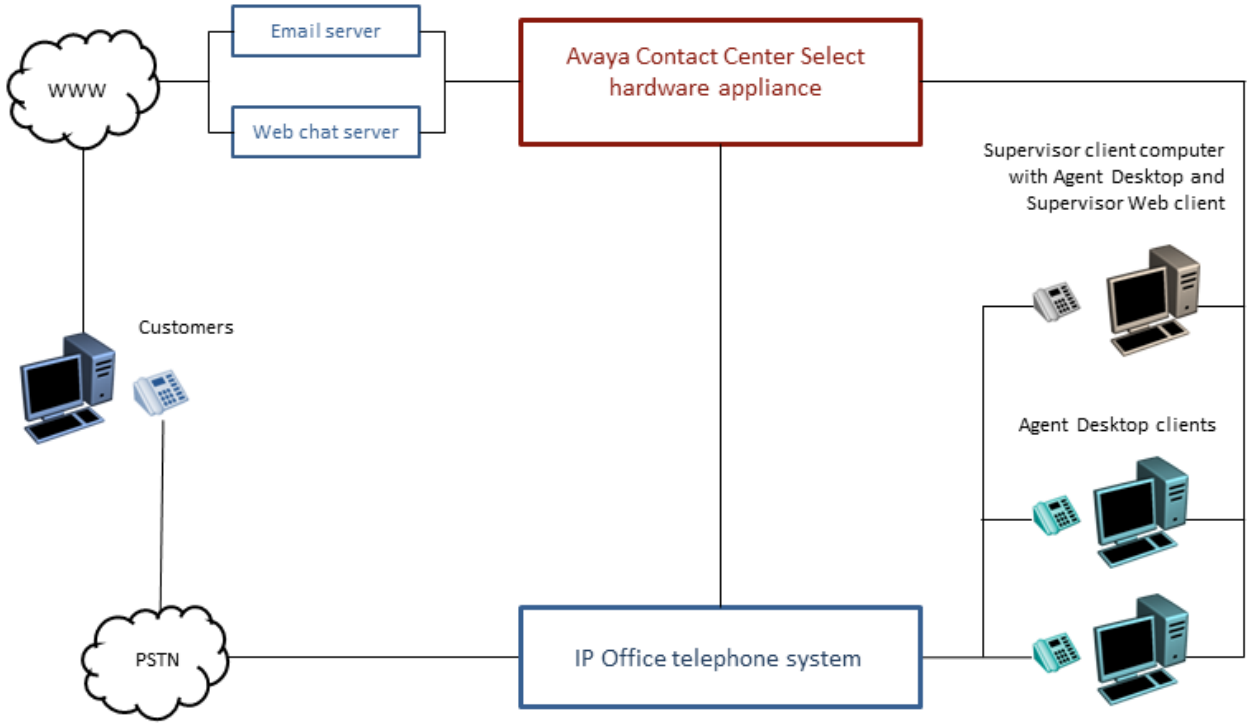


Figura 22: Solución típica de dispositivo de hardware de Avaya Contact Center Select

Después de que las funciones básicas de telefonía y correo electrónico estén funcionando, puede configurar más contactos multimedia, multiplicidad, avisos personalizados y otras funciones y funciones mejoradas para mejorar la experiencia de su cliente.

El servidor de dispositivos de hardware suministrado por Avaya está optimizado para proporcionar todos los recursos informáticos y de registro en tiempo real que requiere Avaya Contact Center Select. El dispositivo de hardware es compatible con la capacidad máxima de tasa de llamada y agente de Avaya Contact Center Select.

Avaya proporciona la clave de producto del sistema operativo Microsoft Windows para el dispositivo de hardware. La clave del producto se muestra en una etiqueta adherida a la parte superior del servidor del dispositivo de hardware de Avaya Contact Center Select.

Para obtener más información sobre el dispositivo de hardware Avaya Contact Center Select, consulte *Descripción de la solución Avaya Contact Center Select*.

Continuidad comercial de Avaya Contact Center Select

Business Continuity es una función con licencia de Avaya Contact Center Select. Las soluciones Avaya Contact Center Select que admiten Business Continuity tienen dos servidores Avaya Contact Center Select. Un servidor, denominado servidor activo, procesa los contactos de los clientes. El otro servidor, denominado standby o nodo geográfico remoto, oculta al servidor activo. Si el servidor activo falla, el otro servidor de Avaya Contact Center Select puede hacerse cargo del procesamiento de contactos. Esta función proporciona redundancia, resiliencia de datos y recuperación ante desastres de Avaya Contact Center Select.

Para respaldar la resiliencia de Business Continuity, los agentes de Avaya Contact Center Select deben tener cada uno una cuenta de usuario de dominio de Windows asociada en el mismo dominio de Windows que el agente activo.

Página491 de 3226.

y servidores de reserva. Los agentes de Avaya Contact Center Select también se admiten en dominios con una relación de confianza bidireccional con el dominio del servidor de Avaya Contact Center Select.

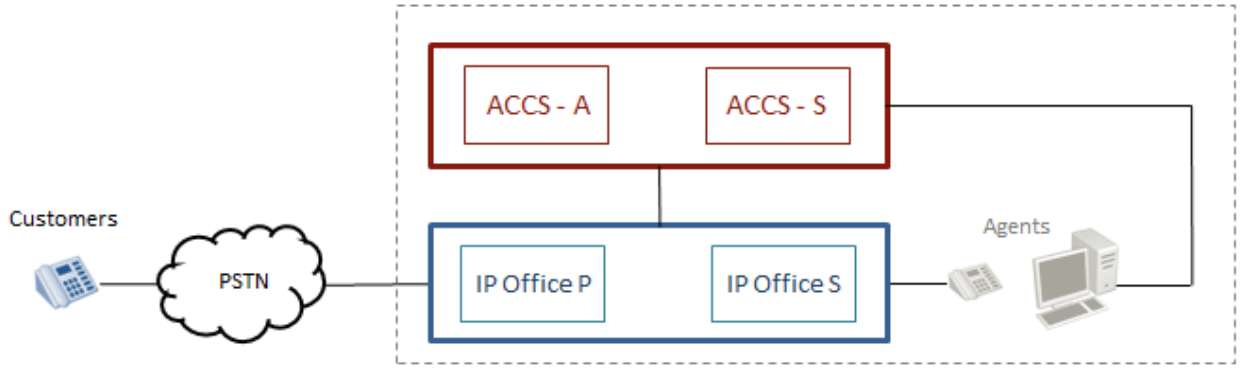


Figura 23: Avaya Contact Center Select Business Continuity con resiliencia de IP Office

Las soluciones IP Office Server Edition admiten la resistencia de la plataforma de voz cuando se agrega un servidor secundario de IP Office a la solución. Avaya Contact Center Select es compatible con esta función de resiliencia de IP Office.

Todas las opciones de implementación de Avaya Contact Center Select, DVD, VMware y Hardware Appliance son compatibles con Contact Center Business Continuity y resiliencia de IP Office. Avaya Contact Center Select Business Continuity agrega requisitos de recursos adicionales, topología, conectividad de red y consideraciones de diseño de dominio a la solución.

Para obtener más información, consulte *Continuidad comercial de Avaya Contact Center Select*.

Opciones de hardware y software

Opciones de hardware

Las opciones de hardware de servidor, tarjeta base, tarjeta troncal y módulo de expansión están disponibles según la edición requerida:

- Dell PowerEdge™R210 o R620
- Hewlett Packard ProLiant DL120 G7 o DL360 G7
- Avaya IP500 V2

Opciones de software

IP Office actúa como un servidor para una variedad de aplicaciones, que incluyen:

- Avaya Communicator for IP Office compatible con dispositivos Windows y iPad
- Avaya one-X®Móvil para IP Office
- Avaya one-X®Portal para IP Office

Página492 de 3226.

- Integración Lync para IP Office
- SoftConsole de IP Office
- Administrador de medios de IP Office
- Equinoccio de Avaya™cliente para IP Office
- Cliente web Avaya IP Office

IP Office también se puede implementar con otros componentes. Puede implementar IP Office con Radvision u otros terminales de video. También puede usar la oferta de la solución IP Office Branch para conectar las sucursales de IP Office a Avaya Aura.®infraestructura, lo que permite a los usuarios aprovechar el núcleo de Avaya Aura®
aplicaciones y servicios que incluyen planes de marcación centralizados, correo de voz, administración y licencias.

Enlaces relacionados

Acceso a las notas de la aplicación Avaya DevConnect en la página 134
interoperabilidad en la página 93

Especificaciones del servidor

Las siguientes tablas enumeran las especificaciones mínimas del servidor para IP Office Server Edition Solution:

opción de servidor	Servidor grande #1	Servidor grande #2	Servidor grande #3
Chasis	Dell R630 1U	Dell R620 1U	HP DL360G7 1U
Procesador	2 E5-2620v3, 2,4 GHz	2 E5-2630, 2,3 GHz	2 x E5620, 2,4 GHz
Memoria (RAM)	32GB	32GB	12 GB
Disco duro	2 de 600GB	2 de 600GB	2x 300GB, 10K
REDADA	Intercambio en caliente RAID 1	Intercambio en caliente RAID 1	Intercambio en caliente RAID 1
Controlador RAID	H730	H710	P410i
Fuentes de alimentación	2x 750W CA Intercambio en caliente	2x 495 W CA Intercambio en caliente	2x 460W CA Intercambio en caliente
NIC	dúplex completo de 6 GB	dúplex completo de 4 GB	4 puertos, placa base
Unidad óptica	1x DVD +/- RW	1x DVD +/- RW	1x DVD+/-RW, SATA, INTERNO
Tipo PCI	2 ranuras x8 Gen2 (PCIe)	2 ranuras x8 Gen2 (PCIe)	1-LP X8 PCIe y 1-FL/FH X16 PCIe elevador

opción de servidor	Pequeño servidor #1	Pequeño servidor #2	Pequeño servidor #3
Chasis	HP DL120G7 1U	Dell R210 1U	Dell R220 1U
Procesador	1 E3-1220, 3,1 GHz	1 E3-1220, 3,1 GHz	1 E3-1220, 3,1 GHz
Memoria (RAM)	12 GB	12 GB	16 GB
Disco duro	1x 250GB, 7.5K	1x 250GB, 7.5K	1x 500GB, 7.2K
REDADA	RAID 0 (ninguno)	RAID 0 (ninguno)	RAID 0 (ninguno)

La tabla continúa...

Página493 de 3226.

opción de servidor	Pequeño servidor #1	Pequeño servidor #2	Pequeño servidor #3
Controlador RAID	P212, 256 MB	A bordo	A bordo
Fuentes de alimentación	1 x 400 W CA	1 x 502 W CA	1 x 250 W CA
NIC	2 puertos, placa base	2 puertos, placa base	2 puertos, placa base
Unidad óptica	1x DVD+/-RW, SATA, INTERNO	1x DVD+/-RW, SATA, INTERNO	1x DVD+/-RW, SATA, INTERNO
Tipo PCI	1-HL/LP X8 PCIe y 1-FL/ FH X16 PCIe elevador	1 x16 ranuras Gen2 (PCIe)	1 x16 ranuras Gen2 (PCIe)

Nota:

En algunas zonas geográficas, donde 12 GB de RAM no son una opción estándar de Dell, use 16 GB de RAM.

Combinaciones y uso de servidores

- Server Edition Primary y Server Edition Secondary deben estar en la misma plataforma. Esta restricción se aplica igualmente a los servidores virtuales. Es posible mezclar servidores centrales nativos y virtuales, pero los recursos asignados al entorno virtual deben coincidir con el servidor nativo.
- Los servidores nativos y virtualizados se pueden combinar en la misma solución de Server Edition en cualquier rol, siempre que Server Edition Primary y Server Edition Secondary sean los mismos que se indicaron anteriormente.
- Es posible utilizar los servidores R210 / DL120 is / R220 de Unified Communication / Application Server ya que se trata del mismo hardware y software que los servidores Server Edition R210 / DL120 / R220. Si el servidor está instalado con el software Server Edition, será compatible con Avaya.
- No puede configurar un Sistema de expansión Server Edition (L) en el modo de funcionamiento estándar de IP Office en IP Office Server Edition Solution.
- No puede reaprovisionar un servidor Server Edition sin una reinstalación completa. Por ejemplo, no puede convertir un servidor principal en un sistema secundario o de expansión.
- No puede configurar un Sistema de expansión Server Edition (L) en el modo de operación estándar de IP Office en IP Office Server Edition Solution. No puede convertir un Sistema de expansión Server Edition (V2) en un servidor Server Edition Primario o Server Edition Secundario.
- No se admite el uso de ningún servidor Voicemail Pro externo (ya sea Linux o Windows).
- El uso de un Avaya one-X externo®El servidor de portal que no ejecuta el software Server Edition y no se ejecuta en un servidor compatible, no es compatible.

Nota:

Salesforce (SFDC) se eliminó de Avaya one-X®Portal.

Compatibilidad con sistema operativo y navegador

Sistema Operativo Windows

Tabla 7: Ediciones de Windows y Service Packs

Sistema operativo*	Paquete de servicio	Edición
ventanas 7	SP1	Profesional, Empresarial, Ultimate
Windows 8.1	N / A	Profesional, Empresa
ventanas 10	N / A	Profesional (PYME), Empresa
Servidor Windows 2012	N / A	Estándar
Servidor Windows 2012 R2	N / A	Estándar
Servidor Windows 2016	N / A	Estándar, Esenciales

*Windows Server 2008 R2 (64 bits) no es compatible con la versión 10.1.

Tabla 8: Compatibilidad con Windows: componentes del servidor

Servidor	ventanas 7		Windows 8.1*		ventanas 10		ventanas Servidor 2012, 2012 R2	ventanas Servidor 2016
	32 bits	64 bits	32 bits	64 bits	32 bits	64 bits	64 bits	64 bits
Edición preferida servidor (correo de voz Pro) Independiente	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Edición preferida servidor con UMS	No	No	No	No	No	No	Sí	Sí
Edición preferida servidor con Campañas	No	No	No	No	No	No	Sí	Sí
Edición preferida servidor con IMS	No	No	No	No	No	No	No	No
Edición preferida servidor con MAPI servicio de correo de voz Profesional en Linux	Sí	Sí	No	No	No	No	Sí	Sí
Avaya one-X®Portal para el servidor de IP Office	No	No	No	No	No	No	Sí	Sí
Primero de TAPI	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
TAPI de terceros	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

La tabla continúa...

Servidor	ventanas 7		Windows 8.1*		ventanas 10		ventanas Servidor 2012, 2012 R2	ventanas Servidor 2016
	32 bits	64 bits	32 bits	64 bits	32 bits	64 bits	64 bits	64 bits
TAPI WAV[2]	Sí	No	Sí	No	Sí	No	No	No

*Windows 8.1 es el paquete de servicio/reemplazo para Windows 8.0. Por lo tanto, ya no admitimos Windows 8.0.

Tabla 9: Soporte de Windows: aplicaciones de cliente pesado

Solicitud	ventanas 7		Windows 8.1*		ventanas 10		Ventana servidor 2012, 2012 R2	Ventana servidor 2016
	32 bits	64 bits	32 bits	64 bits	32 bits	64 bits	64 bits	64 bits
Edición preferida cliente	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Oficina de PI SoftConsole	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
Gerente de IP Office	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
monitor de sistema	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Estado del sistema Solicitud	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Primero de TAPI	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
TAPI WAV[3]	Sí	No	Sí	No	Sí	No	No	No
Equinoccio de Avaya™ para ventanas	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Avaya comunicador para ventanas	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Avaya one-X® Complemento del portal para Microsoft Outlook	Sí	Sí	Sí	Sí	Sí	Sí	No	No
asistente de llamadas	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Complemento para microsoft lync 2013/Skype para Negocio[4]	Sí	Sí	Sí	Sí	Sí	Sí	No	No

La tabla continúa...

2 TAPI WAV no se recomienda para nuevos diseños y no es compatible con un sistema operativo de 64 bits. TAPI
3 WAV no se recomienda para nuevos diseños y no es compatible con un sistema operativo de 64 bits. El
4 complemento para Microsoft Lync 2010 no es compatible con la versión 10.1.

Solicitud	ventanas 7		Windows 8.1*		ventanas 10		Ventana servidor 2012, 2012 R2	Ventana servidor 2016
	32 bits	64 bits	32 bits	64 bits	32 bits	64 bits	64 bits	64 bits
Web conferencias[5]	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Web de IP Office Cliente	Sí	Sí	Sí	Sí	Sí	Sí	No	No

* Windows 8.1 es el paquete de servicio/reemplazo para Windows 8.0. Por lo tanto, ya no admitimos Windows 8.0.

Sistema operativo macOS

Tabla 10: Compatibilidad con macOS: aplicaciones de cliente grueso

Solicitud	mac OS 10.8 (Montaña León)	mac OS 10.9 (Inconformistas)	Mac OS 10.10 (Yosemite)	Mac OS 10.11 (El Capitán)	Mac OS 10.12 (Sierra)	Mac OS 10.13 (Alta Sierra)
Web conferencias[6]	Sí	Sí	Sí	Sí	Sí	
Avaya Equinoccio™por Mac	No	No	No	Sí	Sí	Sí

navegadores

Tabla 11: Navegadores compatibles

Solicitud	Internet Explorador 10*	Internet Explorador 11	Borde	Firefox	Cromo	Safari 8	Safari 9	Safari 10
Buzón de voz profesional Campañas	Sí	Sí	Sí	No	No	No	No	No
Buzón de voz profesional Correo Web UMS	Sí	Sí	Sí	No	No	No	No	No
Avaya one-X® Portal de PI cliente de oficina	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
Web conferencias[7]	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No

La tabla continúa...

[5] Incluye Adobe Flash y Java Applet para compartir.
[6] Incluye Adobe Flash y Java Applet para compartir.
[7] Incluye Adobe Flash y Java Applet para compartir.

Solicitud	Internet Explorador 10*	Internet Explorador 11	Borde	Firefox	Cromo	Safari 8	Safari 9	Safari 10
Administrador web y control web Página	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
DECT D100 Administración	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
IP DECT R4 Administración	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Avaya Comunicador para Internet	No	Sí	No	No	Sí	No	No	No
Medios de IP Office Gerente	Sí	Sí	Sí	Sí	Sí	No	No	No
Oficina IP de Avaya cliente web	No	No	No	No	Sí	No	No	No

* Solo en Windows Server 2012; sin embargo, Server 2012 R2 es compatible con Internet Explorer 11.

Otras aplicaciones

Tabla 12: Microsoft Exchange

Solicitud	Intercambio 2010	Intercambio 2013	Intercambio 2016
Correo de voz Pro UMS	Sí	Sí	Sí
Avaya one-X®Portal para IM y Presencia	Sí	Sí	Sí

Tabla 13: Microsoft Outlook

Solicitud	perspectiva 2010	Perspectivas 2013	Perspectivas 2016
Correo de voz Pro IMS	No	No	No
TAPI (para marcar)	Sí	Sí	Sí
Voicemail Pro UMS con IMAP	Sí	Sí	Sí
Avaya one-X®Complemento de Portal Outlook[8]	Sí	Sí	Sí

[8]Para Outlook 2013 y versiones posteriores, la función de pantalla emergente de contacto no es compatible.

Página498 de 3226.

virtualización

Tabla 14: Soporte de virtualización

hipervisor	Edición de servidor de IP Office	Hospedado por socios de IP Office
VMware ESXi 5.1	Sí	Sí
VMware ESXi 5.5 U2+	Sí	Sí
VMware ESXi 6.0	Sí	Sí
VMware ESXi 6.5	Sí	Sí
VMware ESXi 6.7	Sí	Sí
Microsoft HyperV en el servidor 2012 R2	Sí	Sí
Microsoft HyperV en el servidor 2016	Sí	Sí
KVM	No	Sí
AmazonAWS	Sí	Sí

Nota:

Google KVM es compatible con QEMU con CentOS versión 6 y 7 en el caso de la solución Powered by Avaya (alojada) y no es compatible con CPE. Para más información, ver *Guía de implementación impulsada por Avaya for Business Partners*.

Requisitos de PC proporcionados por el cliente

Los siguientes requisitos de PC proporcionados por el cliente para las aplicaciones son los mínimos requeridos.

Gerente de IP Office

IP Office Manager se utiliza para acceder a todas las partes de la configuración. Se pueden definir diferentes niveles de acceso para controlar qué partes de la configuración puede ver y modificar el usuario de IP Office Manager. IP Office Manager también se usa para actualizar los archivos de software en el sistema. IP Office Manager actúa como un servidor TFTP desde el cual algunos teléfonos Avaya pueden solicitar software nuevo.

RAM	Edición estándar: 4 GB Edición de servidor: 6 GB Edición de servidor seleccionada: 8 GB
Espacio libre en disco duro	1GB
Procesador	Edición estándar: Core i3 Edición de servidor: Core i5 Selección de edición de servidor: Core i5
Sistema operativo	Compatibilidad con sistema operativo y navegador en la página 88

software adicional	. NET Framework 4.0: Instalado con el software si aún no está instalado.

Monitor de sistema de IP Office

RAM	128 MB
Espacio libre en disco duro	10 GB
Procesador	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Sistema operativo	Compatibilidad con sistema operativo y navegador en la página 88

Aplicación de estado del sistema de IP Office

RAM	256 MB
Espacio libre en disco duro	1,4 GB
Procesador	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Sistema operativo	Compatibilidad con sistema operativo y navegador en la página 88
software adicional	Máquina virtual Sun Java Navegador web: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

TAPI

RAM	64 MB
Espacio libre en disco duro	50 MB
Procesador	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Sistema operativo	Compatibilidad con sistema operativo y navegador en la página 88
software adicional	Navegador web: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

Página500 de 3226.

Requisitos del entorno virtual

Asegúrese de tener lo siguiente:

- Software de cliente VMware vSphere para administración (software vSphere ESXi e instancias virtualizadas que se ejecutan en un único servidor host)

  Nota:

  No se requiere el software vCenter, sin embargo, puede ser útil para entornos de servidor de múltiples hosts.

- Host hardware compatible con los requisitos y especificaciones de recursos de VMware vSphere e IP Office Server Edition para satisfacer las necesidades de configuración.

Compatibilidad con VMware ESXi:

- IP Office Server Edition e IP Office Contact Center son compatibles con VMWare ESXi 5.1 y 5.5 U2.
- IP Office Contact Center es compatible con VMWare ESXi 6.0. IP Office Server Edition es compatible con VMWare ESXi 6.0 solo para las versiones 10.0 y posteriores.

  Para obtener más información sobre el soporte y las especificaciones de IP Office Contact Center, consulte *Configuración de referencia de Avaya IP Office Contact Center*.

Nota:

ESXi 4.x ya no es compatible.

Compatibilidad con hipervisor adicional: El

soporte de hipervisor ahora se extiende a:

- Microsoft Hyper-V
- AWS (para Amazon Web Services): se proporciona una AMI (imagen de máquina de Amazon) que puede realizar el encendido automático y la ICU en función de los datos de usuario establecidos en AWS. La AMI se comportará de manera similar a la imagen de Google Compute existente. Consulte los tipos de instancias que admite Amazon EC2 en el sitio web de Amazon AWS.

  En Amazon Dashboard, debe seleccionar Iniciar instancia en Crear instancia. Seleccione Community AMI y busque Avaya IP Office.

- KVM (para máquina virtual basada en kernel)

interoperabilidad

La interoperabilidad significa que dos sistemas pueden comunicarse con una interfaz en cada sistema para manejar la comunicación. Compatibilidad significa que dos componentes en el mismo entorno son compatibles entre sí si se ejecutan o residen en el entorno sin afectar negativamente el comportamiento del otro.

Para obtener información detallada sobre la interoperabilidad de IP Office y las versiones admitidas, consultehttps://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=IP+Office+Platform .

Interfaces de productos de Avaya

IP Office incluye una interfaz para los siguientes productos de Avaya:

- Aura de Avaya®
- Selección del centro de contacto de Avaya
- Aura de Avaya®Mensajería
- Avaya CallPilot®
- Fase de vídeo en la nube de Avaya
- Avaya Communicator para Windows
- Avaya Communicator para iPad
- Equinoccio de Avaya™
- Avaya one-X®Comunicador
- Controlador de borde de sesión de Avaya para empresas
- Gerente de comunicaciones comerciales de Avaya
- Servidor de comunicaciones Avaya 1000
- Mensajería modular de Avaya
- Avaya Scopia®
- Enlace de acceso seguro
- Aura de Avaya®Portal de experiencia

interfaces RDSI

Interfaces de la UE:

- BRI: tomas RJ45. Interfaces ETSI T-Bus y S-Bus a CTR3 para conexión paneuropea
- PRI E1: toma RJ45. Interfaz ETSI T-Bus a CTR4 para conexión paneuropea
- PRI T1/J1: enchufe RJ45: conexión FCC Parte 68/JATE

Interfaces de EE. UU.:

- Servicio PRI T1: Ground Start (GS) - Predeterminado, E&M, datos de 56 K para 5ESS, 56/64/64 restringido para 4ESS
- Compatibilidad con conmutador PRI ISDN: 4ESS, 5ESS, DMS-100, DMS-250 (incluye conformidad con ANSI T1.607 y Bellcore Special Report SR4287, 1992)
- Servicios PRI ISDN: AT&T Megacom 800, AT&T WATS (4ESS), AT&T SDS Accunet 56 Kbps y 64 Kbps (4ESS), AT&T Multiquest (4ESS)

Enlaces relacionados

Interoperabilidad telefónica en la página 95
Interoperabilidad de IP Office y Avaya Aura Communication Manager en la página 99
Interoperabilidad de BCM e IP Office en la página 100 Acceso a las notas de la aplicación Avaya DevConnect en la página 134 Compatibilidad del producto en la página 133 Opciones de hardware y software en la página 84

Página502 de 3226.

Interoperabilidad telefónica

La siguiente tabla resume la comparación de interoperabilidad de teléfonos por edición de IP Office.

Tabla 15: Teléfonos generalmente disponibles

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
Teléfonos de escritorio analógicos:			
OLLAS	Sí	Sí	No
Videoteléfonos Serie 1000:			
1010, 1020, 1030, 1040 (tamaño natural)	No	Sí	No
Serie 1400: Teléfonos DS Digital: IP Office y Communication Manager			
1403, 1408, 1416	Sí	Sí	No
DBM32	Sí	Sí	No
Serie 1600: Teléfonos IP (H.323): IP Office y Communication Manager			
1603, 1603SW, 1603SW–i, 1608, 1608–i, 1616, 1616–I	No	Sí	Sí
Serie 2400: Teléfonos DS Digital: IP Office y Communication Manager			
2402D, 2410D, 2420	Sí	Sí	No
UE24	Sí	Sí	No
Serie 3600: WiFi H.323 – IP Office y Communication Manager			
3641, 3645	No	Sí	Sí
Serie 3700:DECT: IP Office y administrador de comunicaciones			
3720, 3525, 3730, 3735, 3745, 3749	No	Sí	Sí
Serie 9500:DS digital: solo IP Office			
9504, 9508	Sí	Sí	No
BM12	Sí	Sí	No
Serie 9600:IP H.323: IP Office y Communication Manager			
9620L, 9620C, 9630, 9640G, 9650, 9650C	No	Sí	Sí
SBM24 con 96x0	No	Sí	Sí
9608, 9611, 9621, 9641, J169, J179	No	Sí	Sí
BM12	No	Sí	Sí
Teléfonos de conferencia de la serie B100:			
B149, B159	Sí	Sí	No

La tabla continúa...

Página503 de 3226.

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
B179 SORBO	No	Sí	Sí
Teléfonos DECT D100/D160:			
D160	Sí	Sí	Sí
Teléfonos IP de la serie E100:			
E129	No	Sí	Sí
E159	No	Sí	Sí
E169	No	Sí	Sí
Estaciones de colaboración de video de la serie H100:			
H175	No	Sí	Sí
Teléfonos IP de la serie J100 de Avaya:			
Teléfono IP Avaya J139	No	Sí	No
Teléfono IP Avaya J169	No	Sí	No
Teléfono IP Avaya J179	No	Sí	No
Softphone:			
Avaya Communicator Ventanas	No	Sí	Sí
Comunicador Avaya iPad	No	Sí	Sí
Equinoccio de Avaya™	No	Sí	Sí

Tabla 16: Teléfonos NORSTAR/BCM generalmente disponibles

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
Teléfonos SIP de la serie 1100: Migración BCM Unistim			
1120E, 1140E	No	Sí	Sí
BM LED y etiquetas de papel	No	Sí	Sí
BMLCD	No	Sí	Sí
Teléfonos SIP de la serie 1200: Migración BCM Unistim			
1220, 1230	No	Sí	Sí
papel BCM	No	Sí	Sí
BCMLCD	No	Sí	Sí
Teléfonos digitales NORSTAR/BCM:			

La tabla continúa...

Página504 de 3226.

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
T7000, T7100, T7208, T7316, T7316E	Sí	Sí	No
Módulo de llave T24	Sí	Sí	No
M7100(N), M7208(N), M7310(N), M7310BLF, M7324(N)[9]	Sí	Sí	No
Módulo clave CAP	Sí	Sí	No
Teléfono de conferencia digital NORSTAR/BCM	Sí	Sí	No
Teléfonos de movilidad digital de Nortel:			
T7406, T7406E	Sí	Sí	No
7420, 7430, 7434, 7439, 7440, 7449	Sí	Sí	No
4135, 4136, 4145, 4146, 4145EX, 4146EX	Sí	Sí	No

Avaya ha probado la interoperabilidad de los siguientes teléfonos con IP Office. Es posible que estos teléfonos no admitan todas las funciones. Si el teléfono ya pasó el Período de soporte del fabricante de Avaya, la resolución de problemas se limita a los que ya se solucionaron.

Tabla 17: Los teléfonos Avaya compatibles ya no están a la venta

Nota:

Compatible en este contexto significa que los teléfonos han sido probados por Avaya para la interoperabilidad con IP Office. Es posible que los modelos de teléfono más antiguos no admitan nuevas funciones si el modelo de teléfono está fuera del período de soporte del fabricante de Avaya. Si hay una actualización de software relacionada con la versión 11.0, no se proporcionará una corrección de software para los teléfonos que estén fuera del período de soporte de fabricación de Avaya. Los teléfonos que "ya no son compatibles" están fuera del período de soporte de fabricación de Avaya y no están cubiertos por las ofertas de mantenimiento de Avaya (soporte de fin de servicio y soporte de fin de mantenimiento)

1. OSX 10.9 Mavericks es la última versión del sistema operativo compatible con Video Softphone para MAC. Ese cliente ya no está disponible en el software 10.xo 11.0 por la misma razón. Avaya Communicator for Web, Avaya IP Office Web Client y Avaya Equinox™están disponibles para usuarios de Mac en la versión 11.0 de IP Office.

2. Los teléfonos digitales y analógicos son compatibles con Server Edition o Select, según se indica, utilizando IP500 V2 como módulo de expansión.

[9] Solo se admite la versión global de los teléfonos de la serie M7000. Las versiones no globales no son compatibles y pueden identificarse por los niveles de contraste; la versión global tiene 9 niveles de contraste y la versión no global tiene solo 4 niveles de contraste.

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
Teléfonos ETR: Teléfono con funciones analógicas, PARTNER e IP Office			
Display de 34, 18 y 6 botones “Refreshed”	Sí	No	No
Display “Euro” de 34 y 18 botones	Sí	No	No
Display “Euro” de 18 y 6 botones	Sí	No	No

Enlaces relacionados

interoperabilidad en la página 93

Disponibilidad de teléfono en la página 98

Acceso a las notas de la aplicación Avaya DevConnect en la página 134 Uso de la base de conocimientos de Avaya InSite en la página 134 Los telefonos en la página 38

Disponibilidad de teléfono

Teléfonos disponibles en todo el mundo

Los teléfonos de Avaya que se enumeran a continuación son los teléfonos recomendados para usar con IP Office. Estos teléfonos se venden en todo el mundo en todos los países donde está disponible IP Office.

Para obtener especificaciones detalladas, consulte la información específica del teléfono en el sitio de soporte de Avaya enhttp://soporte.avaya.com .

Modelos de teléfonos digitales	Modelos de teléfonos IP
1403	1603
1408	1608
1416	1616
9504	9608
9508	9611
	9621
	9641
	Teléfono IP Avaya J169
	Teléfono IP Avaya J179
	Teléfono IP Avaya J139

Teléfonos solo disponibles en ciertos países

Además de los teléfonos enumerados anteriormente, los siguientes teléfonos de Avaya están disponibles en ciertos países y regiones.

Teléfono digital/analógico modelos	Teléfonos IP
2402	9620L/9620C
2410	9630G/9640/9640G
2420	9650/9650C
3810 inalámbrico	Auricular inalámbrico 3720 DECT R4
Unidad DSS EU24/EU24BL	Auricular inalámbrico 3725 DECT R4
	Auricular inalámbrico 3730 DECT R4
	Auricular inalámbrico 3735 DECT R4
	Teléfono inalámbrico 3745 DECT R4
	Teléfono inalámbrico 3749 DECT R4
	3641 Teléfono inalámbrico (WiFi)
	Teléfono inalámbrico reforzado (WiFi) 3645
	D100

Enlaces relacionados

Interoperabilidad telefónica en la página 95

IP Office y Avaya Aura® Interoperabilidad de Communication Manager

IP Office usa el protocolo H.323 para troncales entre los nodos y Avaya Aura® Gerente de comunicación. El correo de voz centralizado para todos los sistemas IP Office en la red SCN y todos los teléfonos son compatibles con los servidores de llamadas individuales. Las funciones avanzadas de manejo de llamadas están disponibles entre los nodos de IP Office. Esta interfaz funciona en las ediciones Essential y Preferred.

Los teléfonos compatibles incluyen:

- Teléfonos IP de Avaya (H.323)
- Teléfonos digitales Avaya
- Teléfonos digitales de la serie BCM 7000
- Teléfonos IP de la serie BCM 1100/1200 (SIP)
- Teléfonos DECT R4
- Teléfonos analógicos

Estas funciones permiten necesidades de redes simples entre las sucursales remotas de IP Office a un Avaya Aura® Gerente de comunicación en el sitio principal.

Página507 de 3226.

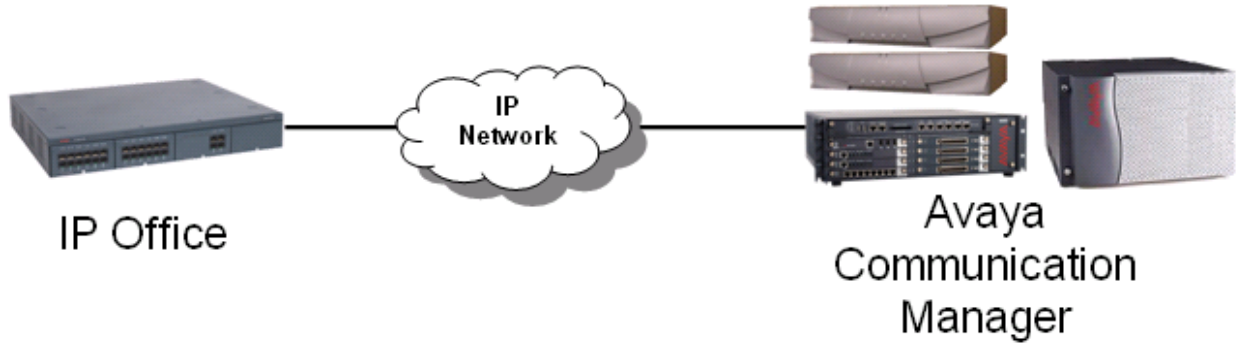


Figura 24: Red VoIP usando H.323

Q.SIG proporciona los siguientes servicios complementarios que también están disponibles entre IP Office y Avaya Aura®Communication Manager equipado con las licencias RFA pertinentes:

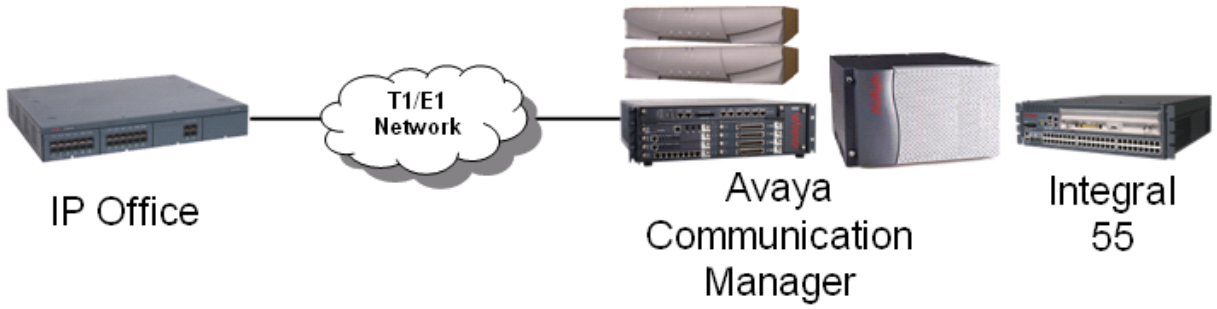


Figura 25: Redes Q.SIG utilizando enlaces T1/E1 (TDM)

Enlaces relacionados

interoperabilidad en la página 93

Interoperabilidad de BCM e IP Office

El soporte de interoperabilidad SIP entre IP Office y BCM50/450 permite a los clientes migrar una red de BCM, paso a paso, a una red IP Office SCN o Server Edition.

Soporte de protocolo	IP Office a BCM: SIP BCM a BCM: SIP o SIP/MCDN IP Office a IP Office H.323: SCN o SIP **Nota:** No es posible conectar IP Office y BCM a través del protocolo MCDN o SCN directamente.
plataforma IP Office requisitos	Versión 8.1 o superior, ediciones Essential, Preferred o Server

plataforma BCM requisitos	BCM50 o BCM450 6.0
centralizado mensaje de voz	IP Office con un sistema Voicemail Pro centralizado en la red SCN BCM con un correo de voz centralizado dentro de la red BCM MCDN. **Nota:** No se admite el correo de voz centralizado en los sistemas IP Office y BCM.
Los telefonos	Todos los teléfonos son compatibles con los servidores de llamadas individuales y las versiones, incluido el teléfono IP de Avaya (H.323), los teléfonos digitales de Avaya, los teléfonos digitales de la serie BCM 7000, los teléfonos IP de la serie BCM1100/1200 (SIP), DECT R4 y los teléfonos analógicos.
Características	Conjunto de funciones avanzadas de IP Office SCN disponible entre IP Office y BCM. Las funciones de MCDN también están disponibles entre IP Office y BCM. Se admiten las funciones SIP estándar.

Enlaces relacionados

interoperabilidad en la página 93

Especificación de seguridad

El Equipo de soporte de seguridad de productos de Avaya (PSST) responde a las vulnerabilidades de seguridad en curso para todos los productos de Avaya. Para más información, ver *Política de respuesta a vulnerabilidades de seguridad de productos de Avaya* y *Clasificación de vulnerabilidades de seguridad de Avaya* en el sitio web de soporte de Avaya en https://support.avaya.com/security .

Seguridad predeterminada

El motor de seguridad del software IP Office es suministrado por Mocana Corporation. Para más información, ver https://www.mocana.com .

Las funciones de seguridad están integradas en la plataforma de software. Estas características consisten en:

- Cortafuegos integrado para evitar ataques de denegación de servicio (DoS)
- Conexiones seguras para asegurar la privacidad e integridad de la información transmitida, incluyendo:
  - TSL en las interfaces de administración
  - Cliente HTTPS
  - Servidor HTTPS
  - IPSec
  - SIP-TLS

Página509 de 3226.

-SSL/VPN

- Integración VMPro/Exchange MAPI (TLS)

Para obtener información detallada sobre el acceso remoto SSL/VPN, consulte*Implementación de IP Office de Avaya™ Plataforma SSL VPN Servicios*y*Oficina IP de Avaya™Matriz de puertos de plataforma*en el sitio web de soporte de Avaya.

Seguridad configurable

Los ajustes de seguridad configurables incluyen las siguientes funciones:

- Cifrado y autenticación de mensajes
- Configuración de los ajustes del cortafuegos integrado
- Certificados digitales
- Prevención del fraude de herramientas mediante la restricción de los privilegios de los usuarios y el uso de la configuración de políticas de seguridad para administrar las credenciales de la cuenta y el control de acceso

Ver*Oficina IP de Avaya™Directrices de seguridad de la plataforma*para más información.

Seguridad de la red

La seguridad de la red aprovecha los recursos como VLAN y firewalls disponibles en la red empresarial e incluye:

- Configuración de cortafuegos externo
- Separación de la funcionalidad de la red mediante la creación de grupos de VLAN y zonas de seguridad independientes
- Fortalecimiento de la capa 2 (capa de enlace de datos) y la capa 3 (capa de red) mediante la configuración de destinos de trampas SNMP, entradas de syslog y una VPN IPSec.
- Acceso remoto SSL/VPN

Seguridad operativa

La seguridad operativa continua para mantener un sistema seguro incluye:

- Aplicación de parches
- Registro y monitoreo
- Protección de virus

Enlaces relacionados

Detalles de seguridad de la plataforma y la aplicación en la página 102

Detalles de seguridad de la plataforma y la aplicación

Para obtener información adicional sobre seguridad, consulte*Oficina IP de Avaya™Directrices de seguridad de la plataforma*

Plataforma

- El sistema operativo IP Office para Linux se basa en Red Hat Enterprise Linux, que se fortalece aún más para los valores predeterminados, los paquetes y los usuarios.
- El sistema operativo de Server Edition Expansion System (L) está desarrollado para IP Office. El sistema operativo es simple, estable y confiable.

Página510 de 3226.

- El sistema operativo de Server Edition Expansion System (V2) está desarrollado para IP Office. El sistema operativo es simple, estable y confiable.
- Componentes que son seguros:
  - Motor de seguridad de software para todos los componentes.
  - Motor de seguridad de hardware para Office Server Edition Expansion System (V2).
  - Políticas del motor de control de acceso interno para solicitudes de servicios externos y aplicaciones internas.

Gerente

- Transport Layer Security (TLS) asegura las comunicaciones entre IP Office Manager e IP Office y los cifrados inseguros están deshabilitados.
- Proporciona control de acceso de usuarios basado en funciones (RBAC).
- Proporciona controles completos de cuentas de usuario y contraseñas.
- Puede habilitar un dominio de confianza de PKI.
- El sistema genera mensajes de advertencia si las contraseñas administrativas están configuradas como predeterminadas. El sistema envía alarmas o falla de inicio de sesión.
- El sistema registra todos los accesos en el registro de auditoría.
- Puede deshabilitar servicios y puertos no utilizados, como HTTP.

Cuentas de usuario de administración

Las cuentas de usuario de administración se pueden controlar para:

- Complejidad de la contraseña
- Historial de contraseñas anteriores (solo cuentas administrativas)
- Cambiar contraseña en el próximo inicio de sesión
- Bloqueo inactivo y bloqueo por falla de inicio de sesión
- Hora y fecha de vencimiento de la cuenta (solo cuentas administrativas)

Inicio de sesión único (SSO)

- Las credenciales de administración para iniciar sesión en la configuración de la plataforma Linux se transfieren de forma segura al cliente Manager, SSA, Voicemail Pro.
- Todos los inicios de sesión administrativos en todos los componentes de IP Office, incluidos Voicemail Pro y Avaya one-X®Portal para IP Office utiliza la configuración de seguridad de IP Office.
- La función de administración de usuarios del servidor en Web Manager sincroniza las credenciales de los usuarios administrativos con todos los componentes de IP Office, incluidos Voicemail Pro y Avaya one-X.®Portal para IP Office en IP Office Server Edition Solution.

Pista de auditoría

- Cada sistema IP Office mantiene un registro de auditoría de acceso y cambio de configuración.
- La configuración de la plataforma Linux también mantiene un registro de auditoría.
- El sistema IP Office muestra la pista de auditoría en IP Office Server Edition Manager y SSA.
-

Infraestructura de clave pública (PKI)

- IP Office admite certificados X.509
- El servidor Primario de Server Edition y el servidor de aplicaciones admiten una Autoridad de certificación (CA) integrada
- El almacén de certificados de confianza se puede configurar y el certificado de identidad está disponible.
- El sistema realiza una Solicitud de firma de certificado (CSR) a través del Protocolo de inscripción de certificado simple (SCEP).
- El sistema crea un certificado de identidad autofirmado que se puede copiar a todas las interfaces HTTPS/TLS.
- Controles flexibles para hacer cumplir el dominio de confianza en servicios específicos. Controles de confianza extendidos para PKI.
- Consola de administración web, Voicemail Pro y Avaya one-X®Portal para IP Office en Linux admite certificados X.509, pero no PKI.

LAN

- Los servidores y los sistemas de expansión se someten a pruebas exhaustivas de resistencia a la denegación de servicio y otros ataques.
- El sistema de expansión Server Edition (V2) es compatible con un cortafuegos configurable
- Perfiles de tiempo en Server Edition Expansion System (V2) únicamente
- NAT estático y NAPT en el sistema de expansión Server Edition (V2)
- Filtrado ICMP
- L2TP/PPP VPN en Sistema de expansión Server Edition (V2) únicamente
- Intercambio de contraseñas PAP o CHAP
- Tiempo de espera inactivo o de cuota
- IPSec VPN en Server Edition Expansion System (V2) solamente

Puntos finales

- El nombre de usuario y el PIN, la contraseña o el código de inicio de sesión se encuentran en la configuración de IP Office y puede administrarlos a través de IP Office Server Edition Manager.
- Puede usar HTTP o HTTPS para configuraciones y actualizaciones de firmware
- No puede hacer llamadas a menos que haya iniciado sesión

Bloqueo de llamadas

- Puede configurar controles de restricción de llamadas flexibles utilizando el nombre de inicio de sesión o el código de cuenta para permitir llamadas internas, locales, nacionales o internacionales en función de cada usuario y sistema.
- No puede usar marcaciones rápidas, transferencias, reenvíos y conferencias para omitir los controles.
- Puede habilitar llamadas de troncal a troncal mediante IP Office Server Edition Manager. Las llamadas de troncal a troncal están deshabilitadas de manera predeterminada.
- La configuración del troncal SIP para las llamadas entrantes debe coincidir con los URI.
- Puede utilizar SMDR (CDR) para crear un registro de todas las llamadas.

Cliente Voicemail Pro

- Puede forzar el inicio de sesión del usuario con un número de identificación personal (PIN) y configurar la complejidad del PIN.
- Puede forzar el cambio de PIN cuando el usuario inicia sesión por primera vez.
- Tiempo de inactividad.

Enlaces relacionados

Especificación de seguridad en la página 101

Asignaciones de puertos

Los detalles del rango de puertos utilizados por IP Office y las aplicaciones de IP Office se encuentran enhttps://support.avaya.com/products/ .

puerto DTE	Conector tipo D hembra de 9 vías tipo D: V.24/V.28
Puertos troncales analógicos	Tomas RJ45: Loop Start/Ground Start (según la región)
Puertos de falla de energía	Tomas RJ45: 2 tomas para ATM16 y 1 toma para ATM4
Tarifas de datos RDSI	BRI: canal B 64 Kbps o 56 Kbps, canal D 16 Kbps
Puertos de teléfono analógico	• Tomas RJ45 • REN: 2. (Sirena externa vía puerto POT: REN = 1) • Corriente descolgada: 25 mA. • Voltaje de timbre: 40 V (nominal) RMS.
LAN	Tomas RJ45. Ethernet 10/100 BaseT de negociación automática (10/100 Mbps)
Audio	• Toma jack estéreo de 3,5 mm. Impedancia de entrada 10 K/canal. • Señal de CA máxima: 200 mV rms.
Puerto de salida externo	• Toma jack estéreo de 3,5 mm. Capacidad de conmutación 0,7 A. • Voltaje Máximo - 55V DC. Sobre la resistencia del estado 0.7. • Corriente de cortocircuito 1 A. Capacidad de corriente de circuito inverso 1,4 A.
Voz integrada memoria	IP500V2: tarjeta de memoria flash compacta (SD) de 512 MB para correo de voz

Rutas de actualización típicas

Actualización de plataformas IP500 V2

Los clientes pueden migrar a la última versión mediante la compra de una licencia de actualización o según los términos de su contrato de soporte de servicios de soporte de IP Office, según corresponda. Los clientes que migren a la última versión deberán tener una unidad de control IP500 V2 o servidores compatibles con Server Edition. Las tarjetas base IP500, las tarjetas de troncales y los módulos de expansión son compatibles con la unidad de control IP500 V2 y pueden migrar a la unidad de control V2. Las licencias requerirán un intercambio de dongle para pasar de la tarjeta llave IP500 a la tarjeta SD IP500 V2.

Para los sistemas que utilizan IP500 V2 con cualquier versión de software anterior a 8.1.1.0, se requiere un proceso de actualización de dos etapas para hacer frente al aumento de tamaño del archivo binario 9.1. Actualice a 8.1.1.0 o cualquier versión 9.0 antes de intentar actualizar a 9.1.

Asegúrese de que los sistemas no contengan hardware no compatible. Actualícelos si es necesario antes de actualizar el software. Instale licencias de actualización antes de la actualización.

Utilice el asistente de actualización de Manager para mostrar el software actualmente presente en la tarjeta SD y las nuevas versiones disponibles para la actualización.

Ya no se admitirá el hardware IP400, incluidas las tarjetas internas de la serie IP400, los módulos de expansión y las tarjetas troncales que se enumeran a continuación:

Tarjetas VCM IP400	VCM4 VCM8 VCM16 VCM24 VCM30
Módulos IP400 y tarjetas de estación	Digital Station V1: variantes de 16 y 30 puertos Teléfono V1: variantes de 8, 16 y 30 puertos So8: compatibilidad con ETSI BRI SO
Tarjetas IP400	Tarjeta de troncales analógicas Uni (ATM4U) Tarjetas de troncales analógicas (ATM4) Tarjetas troncales BRI Tarjetas de troncales PRI T1 Tarjetas de troncales PRI E1 Tarjetas de troncales PRI E1R2

Los siguientes módulos de estación y troncal IP400 seguirán siendo compatibles con la versión actual.

Módulos de expansión IP400	Troncal analógico 16 Digital Station V2: variantes de 16 y 30 puertos

Phone V2: variantes de 16 y 30 puertos

Actualización de la edición del servidor

Actualice los sistemas primario, secundario y de expansión de Server Edition utilizando la imagen iso grabada en un DVD o USB. Instale licencias de actualización antes de actualizar. Hay dos opciones disponibles:

Actualización a IP Office Select

Las licencias de Server Edition existentes deben migrarse mediante la compra de un nuevo conjunto de licencias Select PLDS.

Actualización del servidor de aplicaciones

El proceso de actualización para Application Server es el mismo que para IP Office Server Edition.

Actualización de UCM

Actualice UCM utilizando una llave de memoria USB2 con software nuevo o el proceso de actualización ISO de Web Manager.

Actualización de aplicaciones de servidor de Windows

Descargue las últimas aplicaciones de Windows y cópielas en el servidor o grábelas en un DVD.

Actualización de sistemas en red

En versiones anteriores, la red se lograba mediante líneas H.323 configuradas con servicios complementarios establecidos en SCN. A partir de la versión 9.1 y posterior, estas líneas se migrarán a Líneas de IP Office.

Reemplazo del reportero de llamadas de clientes

Advanced Edition y Customer Call Reporter (CCR) ya no están disponibles para la venta. Además, los clientes existentes de Advanced Edition deberán migrar su CCR a IP Office Contact Center mediante la compra de la solución IP Office Contact Center antes de la actualización. Sin embargo, CCR seguirá vendiéndose y recibiendo soporte en la versión anterior de acuerdo con la política de soporte del ciclo de vida de Avaya.

Avaya brindará a los clientes de CCR un camino claro para migrar a IP Office Contact Center. Además, como resultado de este cambio, Preferred Edition ahora vendrá con la base de datos Voicemail Pro y Visual Basic Scripting (anteriormente formaban parte de Advanced Edition).

Proceso de pedido

Los socios de Avaya pueden pedir las aplicaciones de software a su distribuidor autorizado de Avaya. Los socios de Avaya deben comunicarse directamente con sus respectivos distribuidores para comprar todas las aplicaciones de software de IP Office. Cada distribuidor implementa un proceso personalizado de compra y distribución de software IP Office para su red de socios de Avaya. Estos procesos internos específicos del distribuidor no están cubiertos por este documento.

Migración de BCM con CS1000 a IP Office

Esta configuración permite migrar una red de BCM y CS1000 a IP Office paso a paso al agregarle sistemas IP Office.

Soporte de protocolo	IP Office a BCM: SIP

	IP Office a CS1000: SIP IP Office a IP Office: SIP o H323 - SCN Networking BCM a BCM: SIP o SIP/MCDN BCM a CS1000: SIP o SIP/MCDN **Nota:** Solo se admitirá UDP y no TCP. IP Office a CS1000 mediante troncales H.323 o PRI no es compatible.
plataforma IP Office requisitos	Versión 8.1 o superior, ediciones Essential, Preferred o Server
plataforma BCM requisitos	BCM50 o BCM450 6.0
plataforma CS1000 requisitos	CS1000 7.5 con NRS
centralizado mensaje de voz	Correo de voz centralizado para todos los sistemas IP Office en la red SCN. Los sistemas BCM pueden usar el correo de voz centralizado del CS1000. Los sistemas IP Office no pueden usar el correo de voz centralizado de CS1000.
Los telefonos	Todos los teléfonos son compatibles con los servidores de llamadas individuales y las versiones, incluidos Avaya IP Phone (H.323), teléfonos Avaya Digital, teléfonos digitales de la serie BCM 7000, teléfonos IP (SIP) de la serie BCM1100/1200, teléfonos DECT R4 y teléfonos analógicos.

Migración de sucursales de IP Office

Hoja de ruta de migración y limitaciones

Puede actualizar desde un B5800 Branch Gateway a la versión actual de IP Office, o desde una versión anterior de IP Office a la versión actual de IP Office. El proceso de actualización para la solución IP Office Branch varía según cómo se implemente la arquitectura.

Si la versión de B5800 Branch Gateway o IP Office desde la que está actualizando está conectada a Avaya Aura®infraestructura y usos Avaya Aura®System Manager para administración centralizada, use Avaya Aura®System Manager para actualizar el firmware y el software del sistema.

Si la arquitectura se implementa en un entorno de sucursal independiente de IP Office sin centralización ni conexión a Avaya Aura®red, debe usar IP Office Manager para las actualizaciones. Desde IP Office Manager, puede realizar una actualización mediante el asistente de actualización o la tarjeta SD del sistema.

Para conocer los procedimientos sobre cómo realizar actualizaciones de System Manager o IP Office Manager para su solución de sucursal, consulte*Migración de IP Office o B5800 Branch Gateway a IP Office Enterprise Branch*.

Licencias

Muchas soluciones, aplicaciones y funciones de los sistemas IP Office tienen licencia y solo funcionan cuando se detecta una licencia válida. Esto incluye funciones dentro de las aplicaciones de IP Office conectadas al sistema IP Office.

Esta sección describe los requisitos de licencia para las funciones de IP Office. Para obtener información y procedimientos sobre la gestión de licencias, consulte "Solicitud de licencias" en los siguientes documentos:

- *Administración de IP Office de Avaya™Plataforma con Gerente*
- *Administración de IP Office de Avaya™Plataforma con Web Manager*

Puertos, canales y usuarios

Algunas licencias permiten varios puertos, canales o usuarios. Dependiendo de la licencia en particular, cada instancia admitida se puede consumir cuando está configurada para su uso o cuando realmente se está utilizando. Cuando no hay más instancias de una licencia disponibles, no se permite el uso posterior de la función con licencia.

Se pueden agregar varias licencias para brindar una mayor cantidad de puertos, canales o usuarios admitidos. Sin embargo, las licencias por encima de la capacidad admitida por la unidad de control de IP Office en particular no funcionarán.

Licencias PLDS

IP Office utiliza el Sistema de entrega y licencias de productos (PLDS) de Avaya para administrar las licencias. PLDS es una herramienta en línea basada en la web para administrar los derechos de licencia y la entrega electrónica de software y archivos de licencia relacionados. PLDS brinda a los clientes, socios de Avaya, distribuidores y asociados de Avaya herramientas fáciles de usar para administrar los derechos de licencia y la entrega electrónica de software y archivos de licencia relacionados. Con PLDS, puede realizar operaciones como activaciones de licencias, actualizaciones de licencias, movimientos de licencias y descargas de software. Puede acceder a PLDS desdehttp://plds.avaya.com/ .

Archivos de licencia PLDS

Las licencias se entregan desde PLDS con archivos de licencia. Se genera un archivo de licencia PLDS para instalar en una máquina específica. Hay dos opciones de implementación:

- Los archivos de licencia de PLDS Nodal se generan e instalan en nodos particulares de IP Office.
- Los archivos de licencia PLDS WebLM se generan e instalan en un servidor WebLM que puede otorgar licencias a varios nodos de IP Office.

Las licencias centralizadas de WebLM se admiten en IP Office Server Edition y en las implementaciones de IP Office Branch, pero no en las implementaciones que no son de sucursal del modo estándar de IP Office.

Página517 de 3226.

Id. de host PLDS

Cada archivo de licencia PLDS debe crearse con el ID de host PLDS del sistema donde se cargará el archivo de licencia. Los archivos de licencia de PLDS Nodal son específicos de la máquina y debe especificar el ID de host en el**Id. de host PLDS**campo en IP Office Manager o Web Manager.

Sistemas IP500 V2: Puede encontrar el ID de host de PLDS en el**Licencia**pestaña de IP Office Manager y Web Manager. La ID de host PLDS consta de dos dígitos "11", seguidos del número de serie de la clave de función de 10 dígitos impreso en la tarjeta SD de IP Office. Si se cambia la tarjeta SD, la ID de host PLDS también cambiará.

Servidores IP Office Linux: El ID de host de PLDS se puede encontrar en la etiqueta del servidor, la etiqueta del paquete del servidor y la pantalla de inicio de sesión de encendido del sistema. El ID de host de PLDS se deriva del ID del sistema. Si la ID del sistema cambia, la ID del host PLDS también cambiará.

WebLM: El ID de host de WebLM es la dirección Mac del servidor WebLM. En un entorno virtual, la ID de host de WebLM es una dirección Mac virtual que comienza con la letra "V". La ID de host de WebLM se debe usar al generar un archivo de licencia PLDS para el servidor WebLM a fin de implementar un esquema de licencia centralizado para múltiples sistemas IP Office. El ID de host de WebLM se puede encontrar en la etiqueta del servidor, la etiqueta del paquete del servidor, la pantalla de inicio de sesión del sistema y a través de la interfaz de administración de WebLM.

Administrador de licencias web (WebLM)

Web License Manager (WebLM) es una aplicación basada en web para administrar licencias. Si usa el servidor WebLM que se ejecuta en el servidor IP Office, puede usar IP Office Web Manager para iniciar sesión en el servidor WebLM seleccionando**Aplicaciones**>**Administrador de licencias web**. Las credenciales de WebLM se administran por separado de las contraseñas del sistema de IP Office y no forman parte del inicio de sesión único (SSO).

Nota:

- La administración de licencias de WebLM es compatible con las implementaciones de Server Edition y para las implementaciones de Enterprise Branch mediante el servidor WebLM de System Manager. No es compatible con los sistemas de modo estándar.
- Al actualizar desde una versión anterior, todos los sistemas deben ejecutar el mismo nivel de software. IP Office Server Edition no admite versiones mixtas.

Para obtener más información sobre WebLM, consulte*Administración de Avaya WebLM independiente*.

Migración de licencias ADI

Las licencias ADI ya no se admiten a partir de la versión 10.0. Las nuevas licencias deben obtenerse de PLDS.

Con One Source Configurator (OSC), todas las licencias ADI de versiones anteriores se actualizan a PLDS. los **Migración de licencia**La opción en IP Office Manager se puede usar para extraer información de licencia sobre el sistema, y esta información se puede cargar luego en OSC. Después de extraer la información, IP Office Manager firma el archivo para que no se pueda modificar.

Creación de licencia PLDS

La licencia PLDS debe crearse con la ID de host PLDS del sistema donde se cargará la licencia. Si las licencias se cargan localmente en IP Office, la ID de host PLDS está disponible en IP Office Manager o Web Manager. Para IP500 V2, también es el número de clave de función en la tarjeta SD, que comienza con "11". Si el archivo PLDS se carga en un servidor WebLM, la ID de host está disponible en la interfaz WebLM en **Propiedades del servidor**.

Para obtener más información sobre la migración de licencias de IP Office a PLDS, consulte*Administración de IP Office de Avaya™Plataforma con Gerente*o*Administración de IP Office de Avaya™Plataforma con Web Manager*.

Licencias virtuales

Como parte del proceso de migración, las siguientes licencias virtuales se proporcionan como licencias PLDS reales solo a través del proceso de migración XML:

- Edición esencial virtual
- Virtual Preferred Edition para sistemas con módulo UCMv1
- Terminales IP virtuales de Avaya para sistemas con:
  - Módulos VCM32/64 v1 que proporcionaron 12 terminales IP de Avaya
  - Licencias de migración de canal de VCM heredadas
- Puertos Voicemail Pro virtuales adicionales para Server Edition

  El sistema de licencias PLDS agrega dos puertos de Voicemail Pro a cualquier licencia de Server Edition o Server Edition Select.

Los clientes con sistemas más antiguos (IP500 V1 / IP406 V2 / IP412 en la versión 6.0 o posterior) pueden actualizar a través de la carga de BOM del configurador A1S y el proceso de validación de licencia ADI. Las licencias virtualizadas en estos sistemas más antiguos no se transferirán y se deben comprar como nuevas.

Nota:

El teléfono basado en software heredado de Windows no es compatible con la versión 11.0 de IP Office y no funcionará. Las licencias virtuales anteriores proporcionadas al actualizar ya no se proporcionan en la versión 11.0. Equinoccio de Avaya™para Windows es el reemplazo. La licencia Teleworker permite el uso de Avaya Equinox™para ventanas. En versiones anteriores, esto solo estaba disponible con Office Worker y Power User.

Licenciamiento centralizado y nodal de Server Edition

Antes de la versión 10, las implementaciones de Server Edition usaban licencias nodales. Este tipo de licencia aún se puede usar en la versión 10 y posteriores. Sin embargo, se espera que la mayoría de las implementaciones prefieran centralizar la administración de licencias mediante el servidor Avaya Web License Management (WebLM). El servidor WebLM se instala automáticamente en el servidor Primario de Server Edition. Para los sistemas recién instalados, la licencia centralizada es la configuración predeterminada.

Todos los sistemas de la solución Server Edition deben utilizar el mismo**Fuente de licencia**.

Licencias nodales

Con la licencia de nodo, los archivos de licencia deben instalarse en cada nodo del sistema. Para algunas funciones con licencia, la licencia requerida se puede instalar en el servidor Primario de Server Edition y

utilizado por todos los nodos del sistema. Sin embargo, para otras funciones con licencia, la licencia requerida debe instalarse en el nodo donde se usa la función.

Licencias centralizadas

A partir de la versión 10, puede usar el servidor WebLM que se ejecuta en el servidor Primario de Server Edition para centralizar completamente la administración de licencias. Con la gestión de licencias centralizada, todas las licencias están contenidas en un solo archivo PLDS cargado en WebLM. Todos los nodos de la solución obtienen sus licencias de WebLM.

El servidor secundario de IP Office y los sistemas de expansión se pueden configurar para solicitar licencias directamente desde el servidor WebLM o para usar una opción de proxy. Cuando se configura para usar la opción de proxy, las solicitudes de licencia se envían a través del servidor primario de IP Office, que envía las solicitudes al servidor WebLM. El servidor primario no asigna licencias, solo actúa como proxy.

Los sistemas que usan licencias nodales se pueden convertir para usar licencias centralizadas. Dado que los archivos de licencia PLDS se generan utilizando la ID de host del servidor donde residen, debe volver a generar el archivo de licencia utilizando la ID de host del servidor WebLM que alojará el archivo de licencia.

Distribución centralizada de licencias

Cuando el origen de la licencia es WebLM, el**Licencias reservadas**los campos de solo lectura indican las licencias que se requieren para las funciones configuradas actualmente. Los campos editables se pueden utilizar para:

- Solicitar licencias adicionales del servidor WebLM.
- Eliminar licencias del nodo de IP Office para aplicarlas en otro lugar.

Importante:

Al reasignar licencias, siempre reduzca el número en el nodo de IP Office donde se aplican actualmente antes de aplicarlas en otro nodo. Si supera el número de licencias disponibles, recibirá un mensaje de error.

Distribución después de la conversión de licencias nodales a centralizadas

- Si el nodo de IP Office necesita alguna de las siguientes licencias, debe configurar manualmente la respectiva**Licencias reservadas**campos editables. Esto permitirá que el nodo de IP Office solicite las licencias del servidor WebLM.
  - **Administradores de grabaciones de VMPro**
  - **VMPro TTS profesional**
  - **Enlace CTI Pro**

Configuración de licencia reservada de extensión: Cuando la fuente de la licencia es**Local**, el ajuste **Extensión**> **VoIP**>**Licencia de reserva**se establece en**Ninguna**. Cambiar la fuente de licencia a WebLM cambia la configuración a**Reservar la licencia de endpoint IP de Avaya**. Si es necesario, debe cambiar manualmente esta configuración a**Reservar licencia de terminal de terceros**o**Ambas cosas**.

Asignación de licencias en WebLM

Puede utilizar WebLM para ver las licencias utilizadas por cada nodo en IP Office Server Edition. En el panel de navegación de WebLM a la izquierda, haga clic en**Productos con licencia**. La tabla Licencias adquiridas muestra información sobre las licencias adquiridas para cada ID de cliente. En IP Office, la ID de cliente de WebLM para cada nodo se muestra en la página del servidor remoto de la licencia.

Distribución de licencias nodales

Cuando el**Fuente de licencia**es**Local**, la**Licencias reservadas**los campos de solo lectura indican las licencias que se requieren para las funciones configuradas actualmente.

La licencia nodal para una solución Server Edition se basa en una combinación de licencias realizadas a través del servidor Primario de Server Edition más algunas licencias específicas del servidor. Todas las licencias específicas del usuario y del sistema se pueden administrar desde el servidor primario de Server Edition que también actúa como un servidor de licencias. Las licencias se ingresan en la configuración del servidor Primario de Server Edition y se basan en la ID del sistema de ese servidor.

Cuando se usa una licencia para habilitar funciones, como canales SIP Trunk, en otros sistemas, el servidor Primario de Server Edition solo asigna esas licencias a otros sistemas después de haber satisfecho sus propias necesidades de licencia.

Cuando otro sistema pierde la conexión con el servidor Primario de Server Edition, cualquier requisito de licencia basado en las licencias ingresadas en la configuración del servidor Primario de Server Edition se admite durante un período de gracia de 30 días.

Otras licencias específicas del servidor se ingresan en la configuración del servidor que requiere la función y se basan en el ID del sistema de ese sistema.

Licencia	servidor principal	Específico del servidor
Edición del servidor	Sí	No
Terminales IP de Avaya	Sí	No
Puntos finales de IP de terceros	Sí	No
Canales troncales SIP	Sí	No
Canales PRI universales IP500	No	Sí
Puertos de correo de voz adicionales [3]	Sí	No
Colaboración web	No	Sí
Servicios Web UMS [1]	No	Sí
Empleado de oficina	Sí	No
Usuario de poder	Sí	No
Actualización de Office Worker a Power User	Sí	No
Recepcionista	No	Sí
Enlace CTI Pro	No	Sí
Mensajería TTS Pro [3]	Sí	No
Administrador de grabaciones de Voicemail Pro [2] [3]	Sí	No
Usuario WAV	No	Sí
tunelización IPSec	No	Sí

1. Las licencias del servicio web UMS son solo para grupos de búsqueda.
2. La licencia de administrador de grabación de Voicemail Pro hace referencia a Contact Store. Solo se requiere una licencia para una red Server Edition.

3. Para implementaciones con dos servidores Voicemail Pro, Messaging TTS Pro, Voicemail Pro Recording Administrator y las licencias de puertos de correo de voz adicionales deben estar en el servidor secundario.

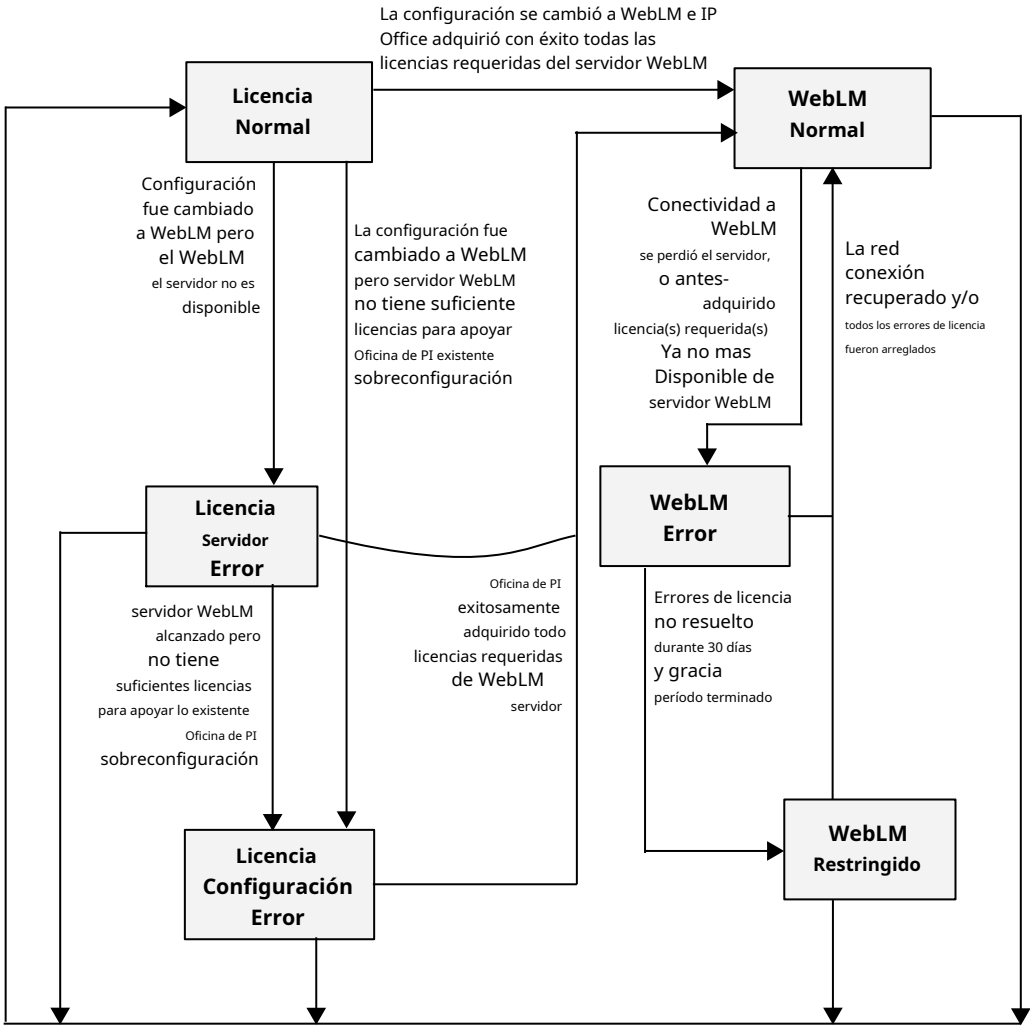
Licencias WebLM

Modos de licencia

Los siguientes son los modos de licencia de IP Office cuando utiliza licencias WebLM. El modo de licencia se muestra en IP Office Manager, Web Manager y System Status Application (SSA).

Modo	Descripción
Licencia Normal	La licencia de WebLM no está configurada. Licenciamiento Nodal Tradicional. Sin período de gracia. Se permite la sobreconfiguración.
Servidor de licencias Error	La configuración se cambió a WebLM, pero el servidor WebLM no está disponible. Sin período de gracia. Hasta que se resuelva el problema, IP Office no tiene licencia y no se puede usar de manera similar a las licencias tradicionales de Nodal si no se instalan licencias.
Licencia Configuración Error	La configuración se cambió a WebLM y el servidor WebLM está disponible, pero no tiene suficientes licencias para admitir la configuración de IP Office existente. Sin período de gracia. Hasta que se resuelva el problema, IP Office no tiene licencia y no se puede usar de manera similar a las licencias tradicionales de Nodal si no se instalan licencias. Las licencias se deben agregar al archivo de licencia de WebLM o se debe modificar la configuración de IP Office para corregir la sobreconfiguración.
WebLM normal	IP Office está configurado para licencias WebLM, el servidor WebLM está disponible e IP Office adquirió con éxito todas las licencias necesarias para admitir todas sus funciones configuradas. Se adquieren nuevas licencias para funciones recién configuradas y se evita la sobreconfiguración de funciones con licencia si no se pueden adquirir licencias. IP Office renueva periódicamente sus licencias adquiridas. Si no se renueva, se activará el modo de error de WebLM con un período de gracia.
Error de WebLM	IP Office está configurado para licencias de WebLM y anteriormente estaba en el modo normal de WebLM. Pero IP Office ahora no puede renovar ni volver a adquirir todas las licencias requeridas para admitir todas sus funciones configuradas. Se evita la sobreconfiguración de las funciones con licencia si no se pueden adquirir las licencias. IP Office sigue funcionando durante un período de gracia de 30 días según su configuración existente (las licencias perdidas se reemplazan con licencias de gracia virtuales).
WebLM Restringido	IP Office estaba en el modo de error de WebLM, pero el período de gracia de 30 días venció y los problemas de este error no se resolvieron. Las funciones sin licencia dejarán de funcionar (se eliminarán las licencias virtuales de gracia). No se permite ninguna configuración de IP Office, excepto los cambios de configuración que reducen los errores de licencia.

Transiciones de estado del modo de licencia



Configuración de licencias de WebLM

En las licencias de WebLM, las licencias deben ser totalmente compatibles con la configuración de IP Office. No se permite la sobreconfiguración. IP Office, según su configuración, solicita las licencias requeridas del servidor WebLM.

Para algunos tipos de licencias, como para usuarios, extensiones, recepcionistas y colaboración web, el tipo y la cantidad de licencias requeridas está determinado por la configuración de los elementos respectivos. Por ejemplo, los registros de Usuario y Extensión en la configuración de IP Office. Estas cantidades se muestran en campos de solo lectura en la lista 'Licencias reservadas' en la pestaña Licencia de configuración de IP Office > Servidor remoto.

Para otros tipos de licencias, como sesiones de troncales SIP y puertos Voicemail Pro, la cantidad de licencias requeridas debe configurarse explícitamente. Estas cantidades deben configurarse en campos editables en la lista de Licencias reservadas en la pestaña Licencia de configuración de IP Office > Servidor remoto.

Advertencias y alarmas de configuración de licencias

Modo de error de configuración de licencia

- IP Office entra en el modo de error de configuración de licencia cuando cambia el origen de la licencia de IP Office de "Local" a "WebLM" y tiene una licencia insuficiente o una configuración excesiva.

  En este modo, IP Office no tiene licencia y no se puede utilizar. Este modo es un estado de error de transición y no se admite como estado estable. Intente evitar entrar en este modo y, si sucede, corrija los errores de inmediato.
- Los sistemas instalados con licencias tradicionales pueden tener una licencia insuficiente o una configuración excesiva. Si se actualizan a la versión 10.0 y se migran mediante licencias WebLM sin adquirir las licencias adicionales necesarias o eliminar la sobreconfiguración, los sistemas instalados entran en el modo Error de configuración de licencia después de la migración.

  Para ayudar a evitar este problema, la herramienta de migración de licencias de IP Office Manager emite advertencias. Si IP Office tiene una configuración excesiva en relación con sus licencias antiguas existentes, la herramienta de migración de licencias muestra una advertencia y también incluye información de advertencia detallada en el archivo de información de migración de licencias.
- Si IP Office se encuentra en el modo Error de configuración de licencia, la página de alarmas de Systems Status Application (SSA) muestra alarmas que indican la causa del problema.

  Si encuentra este modo, revise los errores de alarma de SSA y resuélvalos adquiriendo las licencias requeridas que faltan o modificando la configuración de IP Office para que no requiera estas licencias.

Otras advertencias

Cuando el administrador establece el Origen de la licencia en “WebLM”, IP Office Manager e IP Office Web Manager muestran una advertencia que le indica al administrador que revise y verifique que haya suficientes licencias disponibles en el servidor WebLM.

Licencias de usuario WebLM y punto final de IP

Licencias de terminales de IP

Cuando IP Office utiliza licencias WebLM, cada extensión H.323 o SIP configurada requiere una licencia e IP Office solicita las licencias requeridas del servidor WebLM. Se requieren licencias suficientes para todas las extensiones H.323 y SIP configuradas y no solo para el número máximo de extensiones registradas simultáneamente. Esto es coherente con las licencias de WebLM para usuarios y recepcionistas.

Nota:

Con las licencias de WebLM, IP Office no admite la configuración de una gran cantidad de extensiones con una pequeña cantidad de licencias para cubrir solo un subconjunto de las extensiones que se registran al mismo tiempo. Por ejemplo, configurar tres extensiones con una licencia de terminal de IP para cubrir solo una de las tres extensiones que se registran al mismo tiempo. Sin embargo, si desea compatibilidad con este comportamiento, puede utilizar un archivo de licencia PLDS local en lugar de una licencia WebLM centralizada y establecer el **Licencia de reserva**campo para las extensiones aNinguna.

Para cada extensión H.323 o SIP configurada, IP Office solicita al servidor WebLM una licencia de terminal IP de Avaya o de un tercero, según el**Licencia de reserva**campo del registro de extensión configurado. Cuando IP Office utiliza licencias WebLM, el**Licencia de reserva**El campo para cada extensión H. 323 y SIP configurada se establece de forma predeterminada en la licencia de terminal IP de Avaya. Este campo es editable y el

el administrador puede cambiarla a una licencia de terminal IP de terceros o a Avaya y terminales IP de terceros.

Nota:

Para el**Licencia de reserva**campo, el valorNingunano está disponible con licencias WebLM porque IP Office debe solicitar una licencia del servidor WebLM.

Licencias de usuario

Cuando IP Office utiliza licencias WebLM, se requieren suficientes licencias de usuario según la configuración de usuarios de IP Office y no solo para la cantidad máxima de usuarios registrados simultáneamente. Esto es coherente con las licencias de WebLM para recepcionistas y terminales de IP. IP Office solicita del servidor WebLM las licencias de usuario requeridas (por ejemplo, licencias de usuario avanzado) según el perfil de usuario de todos los usuarios configurados.

Nota:

Con las licencias de WebLM, IP Office no admite la configuración de una gran cantidad de usuarios con una pequeña cantidad de licencias para cubrir solo un subconjunto de usuarios que se registran al mismo tiempo. Por ejemplo, configurar tres usuarios con una licencia de usuario para cubrir solo uno de los tres usuarios que se registran al mismo tiempo. Sin embargo, si desea compatibilidad con este comportamiento, puede utilizar un archivo de licencia PLDS local en lugar de una licencia WebLM centralizada.

Licencias de recepcionista

Cuando IP Office usa licencias de WebLM, se requieren licencias de recepcionista para todos los usuarios que están configurados como recepcionista y no solo para la cantidad máxima de usuarios que ejecutarían su aplicación IP Office SoftConsole simultáneamente. Esto es coherente con las licencias de WebLM para puntos finales y usuarios de IP. Con WebLM, se requieren licencias de acuerdo con los objetos configurados, y no se permite la sobreconfiguración ni la sublicencia.

Nota:

Con las licencias de WebLM, IP Office no admite la configuración de una gran cantidad de usuarios Receptionist con una pequeña cantidad de licencias para cubrir solo un subconjunto de usuarios que se conectan al mismo tiempo mediante IP Office SoftConsole. Por ejemplo, configurar tres usuarios de recepcionista con una licencia de recepcionista para cubrir solo uno de los tres usuarios que se conectan al mismo tiempo mediante IP Office SoftConsole. Sin embargo, si desea compatibilidad con este comportamiento, puede utilizar un archivo de licencia PLDS local en lugar de una licencia WebLM centralizada.

Soporte de creación automática para usuarios y extensiones

Cuando IP Office utiliza licencias WebLM, no puede crear automáticamente usuarios y extensiones, ya que no es compatible. El administrador debe configurar manualmente los usuarios y las extensiones. Para extensiones DECT, se debe utilizar el método “Preconfigurado”.

Sin embargo, se admite la creación automática de usuarios y extensiones si utiliza un archivo de licencia PLDS local en lugar de una licencia WebLM centralizada.

Licencia Basic Edition para nuevos sistemas

Para actualizar a la versión 11.0, la nueva licencia de tiempo de ejecución de actualización PLDS R11.0 se utiliza en combinación con el software R11.0. La actualización a IP Office R11.0 desde versiones anteriores a la R10.0 implica una transición completa a las licencias PLDS. Para actualizar los sistemas IP Office existentes a IP Office R11.0, se requieren licencias de actualización o migración pagadas o transaccionales o autorizadas de la Edición R11.0.

Código material	Licencia	Descripción
396490	ACTUALIZACIÓN DE MIG DE LA EDICIÓN BÁSICA DE IP OFFICE R11 plds	R11 Edición básica a partir de PLDS
369472	MIGRACIÓN DE LA EDICIÓN BÁSICA DE IP OFFICE R11 MEJORA	Actualización de ADI o PLDS a R11 Edición básica

Los clientes también deben comprar tarjetas SD, que están configuradas, de manera predeterminada, con la Edición básica.

Los clientes deben obtener este código de material, que es comercializable y no tiene que configurarse, antes de solicitar los servicios de soporte de IP Office. Esto es especialmente importante para los clientes que ya tienen la Edición básica o para compras de servicios de soporte de IP Office posventa, incluidos los clientes que primero configuran la Edición básica sin los servicios de soporte de IP Office, pero luego eligen obtener los servicios de soporte de IP Office. Estos clientes deben realizar un pedido de mercadería para este código de material primero y luego realizar su compra posventa de servicios de soporte de IP Office y registrar su equipo para servicio.

Nota:

La Edición Básica no es un requisito previo para la Edición Esencial o la Edición Preferida, y no se apila bajo la Edición Esencial.

Licencias Essential Edition y Preferred Edition

Una licencia de Essential Edition es un requisito previo en los sistemas IP500 V2 e incluye hermanamiento móvil para todos los usuarios y cuatro trabajadores remotos.

Una licencia de Preferred Edition es un requisito previo para cualquier licencia de perfil de usuario. En una red multisitio, la licencia Preferred Edition del sistema central se comparte automáticamente con otros sistemas en la red, lo que permite licencias de perfil de usuario en esos otros sistemas. Sin embargo, cada sistema que admita un servidor de Voicemail Pro aún requiere su propia licencia Preferred Edition para el funcionamiento de Voicemail Pro. Para un sistema IP500 V2 equipado con un módulo de comunicaciones unificadas (UCM V2), la tarjeta requiere una licencia Preferred Edition separada.

La licencia Preferred Edition incluye soporte para 4 puertos de mensajería. El número total de puertos de mensajería admitidos se puede aumentar agregando licencias de puertos de mensajería adicionales, en el momento de la compra o posteriormente, hasta el máximo admitido por la unidad de control en particular.

Código de orden	Licencia	Descripción
396491	ACTUALIZACIÓN DE IP OFFICE R11 ESSENTIAL EDITION PLDS LIC:DS	Edición esencial (actualizaciones de PLDS)
396474	IP OFFICE R11 ESSENTIAL EDITION MIG UPG LICENCIA:DS	Migraciones de ADI a PLDS y actualizaciones a R11.0 Essential Edition
396492	IP OFFICE R11 PREFERENCIAL VOICEMAIL PRO ACTUALIZAR PLDS LIC:DS	Edición preferida (actualizaciones de PLDS)
396476	IP OFFICE R11 PREFERIDO VOICEMAIL PRO MIG UPG LIC:DS	Migraciones de ADI a PLDS y actualizaciones a R11.0 Preferred Edition

Licencias de edición de servidor

Una licencia de Server Edition incluye:

- Características de la Edición Esencial
- Características de la edición preferida
- Voicemail Pro centralizado
- Dos puertos de Voicemail Pro
- Canales ilimitados de redes multisitio (líneas de IP Office)

Una licencia de Server Edition permite:

- Conferencia Meet-Me
- Mensajería avanzada
- Asistente automático
- Grabacion de llamada
- Enrutamiento de llamadas condicional
- Anuncios de cola
- Hermanamiento móvil
- Control de llamadas
- Llamar de vuelta

Se requiere una licencia de Server Edition para el servidor principal, el servidor secundario y para cada sistema de expansión Linux o IP500 V2. Las licencias permiten redes de voz entre sistemas en la red de Server Edition.

Código de orden	Licencia	Descripción
Actualizaciones de PLDS (a partir de PLDS)		
396493	IPO R11 SE/VRTLZD UPG PLDS LIC	Código de actualización pagado
Migraciones de ADI a PLDS y actualización a R11.0		
396480	IP Office R11 SE ADI MIG UPG LIC	Código de actualización pagado
396478	IPO R11 VRTLZD SE Migración ADI UPG LIC	Código de actualización pagado
Actualizaciones de PLDS de IP Office		
396519	IPO-SL 11 SE/VRTLZD UPG PLDS LIC	Código de actualización pagado

Licencias de sucursales

La siguiente tabla describe las licencias clave de IP Office que son de particular interés para las implementaciones de sucursales.

Nombre para mostrar	Descripción
Modelo WebLM de Avaya	Esta licencia es requerida por IP Office en implementaciones de sucursales para poder conectarse al servidor WebLM y usar licencias centralizadas de WebLM.
Sistema de Sucursales	Esta licencia es necesaria para IP Office en implementaciones de sucursales. Se utiliza únicamente con fines de seguimiento.
Licencia de terminales centralizados de IP Office	Se requiere una licencia para cada usuario centralizado configurado en IP Office con una extensión SIP o una extensión analógica. **Importante:** Además de esta licencia de IP Office, cada usuario centralizado también requiere una licencia en Avaya Aura central.®sistema.
Canal troncal SM	Se requiere esta licencia con la cantidad suficiente para permitir que se habilite en el sistema la cantidad máxima de llamadas de línea SM simultáneas. La cantidad total de requisitos de licencias de canal troncal SM depende de los patrones de tráfico esperados en la implementación en particular. **Nota:** IP Office también admite conexiones de línea SM a Avaya Aura® Session Manager en otras implementaciones de IP Office Server Edition. Estas conexiones no se limitan a implementaciones de sucursales.

Licencias de red comunitaria pequeña

En una red comunitaria pequeña (SCN), debe haber al menos una edición preferida de IP Office. Se requieren dos con resiliencia.

Los diferentes tipos de usuarios en un SCN tienen la misma funcionalidad, independientemente de dónde esté instalado IP Office Preferred Edition.

En una red multisitio, si uno o más sistemas IP Office Preferred Edition están instalados, todos los sistemas IP Office en la red multisitio tendrán automáticamente licencias Preferidas como requisitos previos para los siguientes tipos de usuarios:

- Usuarios avanzados
- Teletrabajadores
- Trabajadores móviles
- Trabajadores de oficina

Licencias troncales

Las tablas de esta sección incluyen todos los códigos de material de licencia de software IP Office PLDS nuevos y actualizados. Los códigos de material con indicación de R10+ se conocen como códigos "CUALQUIERA" y se pueden usar para implementaciones de sistemas de la versión 10.0 y posteriores. Las descripciones de SAP se han modificado para mostrar 10+ para este cambio, mientras que el código de material sigue siendo el mismo. Otros códigos son específicos de la versión R11.0 y contienen R11.0 en la descripción.

Sesiones de troncales SIP

Estas licencias se utilizan para permitir sesiones en troncales SIP y líneas SM agregadas al sistema. Se pueden combinar varias licencias para el número total de canales necesarios.

Código de orden	Licencia	Descripción
383085	IPO R10+ SIP TRNK 1 LIC	Troncal SIP 1 sesión
307332	IIPO-SL R10+ SIP TRNK 1 LIC	Sesión de troncal SIP 1: seleccione
383120	IPO R10+ SM LÍNEA SIP TRNK LIC	Sesión de línea SM
382917	IPO-SL R10+ LÍNEA SM SIP TRK LIC	Sesión de línea IP Office Select SM

Canales adicionales IP500 Universal PRI

La tarjeta troncal universal (UTC) IP500 PRI está disponible en variantes de 1 o 2 puertos, cada puerto admite una única conexión de circuito PRI. Los puertos se pueden cambiar entre los tipos de línea compatibles E1, E1R2 o T1 según sea necesario para el enlace troncal que se está conectando. Cada puerto admite 8 canales B ("Portador") que no necesitan licencia. Si se requieren canales B adicionales, se deben licenciar mediante la adición de las licencias a continuación. Se pueden agregar varias licencias para lograr el número total de canales necesarios. Los canales D no están sujetos a licencia. Las licencias son consumidas por esos canales, que están configurados como*en servicio*, en el orden de las tarjetas IP500 PRI-U instaladas.

IP500 Universal PRI canales E1 adicionales

Estas licencias se utilizan para habilitar canales B E1 adicionales para tarjetas IP500 PRI-U configuradas para operación E1. Cada puerto puede admitir hasta 30 canales B en este modo.

Código de orden	Licencia	Descripción
383092	IPO R10+ IP500 E1 AGREGAR LICENCIA DE 2 CANALES	2 canales E1
383093	IPO R10+ IP500 E1 AGREGAR LICENCIA DE 8 CANALES	8 canales E1
383094	IPO R10+ IP500 E1 AGREGAR LICENCIA DE 22 CANALES	22 canales E1
307337	IPO-SL R10+ IP500 E1 AGREGAR LICENCIA DE 2 CANALES	2 canales E1 – Seleccionar
307338	IPO-SL R10+ IP500 E1 AGREGAR LICENCIA DE 8 CANALES	8 canales E1 – Seleccione
307339	IPO-SL R10+ IP500 E1 LICENCIA DE 22 CANALES	22 canales E1 – Seleccionar

IP500 Universal PRI canales adicionales E1R2

Estas licencias se utilizan para habilitar canales B E1R2 adicionales para tarjetas IP500 PRI-U configuradas para la operación E1R2. Cada puerto puede admitir hasta 30 canales B en este modo.

Código de orden	Licencia	Descripción
275637	IPO R10 IP500 E1R2 AGREGAR 2CH PLDS LIC	2 canales E1R2
383096	IPO R10+ IP500 E1R2 AGREGAR LICENCIA DE 8 CANALES	8 canales E1R2
383097	IPO R10+ IP500 E1R2 AGREGAR LICENCIA DE 22 CANALES	22 canales E1R2
307340	IPO-SL R10+ IP500 E1R2 2CH LIC	2 canales E1R2 – Seleccionar
307341	IPO-SL R10+ IP500 E1R2 8CH LIC	8 canales E1R2 – Seleccione
307342	IPO-SL R10+ IP500 E1R2 LICENCIA DE 22 CANALES	22 canales E1R2 – Seleccionar

IP500 V2 Universal PRI canales T1 adicionales

Estas licencias se utilizan para habilitar canales T1 B adicionales para tarjetas IP500 PRI-U configuradas para operación T1 PRI o T1 con bits robados. Cada puerto puede admitir hasta 23 canales B (T1 PRI) o 24 canales B (bit T1 robado) en este modo.

Código de orden	Licencia	Descripción
383091	IPO R10+ IP500 T1 AGREGAR LICENCIA DE 2 CANALES	2 canales T1
307336	IPO-SL R10+ IP500 T1 AGREGAR LICENCIA DE 2 CANALES	2 canales T1 – Seleccione

Redes de voz IP500 V2

El uso de troncales de redes de voz privadas entre unidades de control IP500 V2 y otros sistemas requiere licencias de canales de redes de voz dentro de IP500 V2. Esto se aplica a las troncales IP H.323 configuradas en IP500 V2, incluidas las troncales IP que se utilizan para una red comunitaria pequeña (SCN) de IP Office. También se requiere una licencia de redes de voz para el uso de troncales configuradas para operación Q.SIG. En un troncal IP H.323, se consume una instancia de licencia para cada llamada saliente simultánea. En un troncal Q.SIG, la cantidad de llamadas está limitada por el tipo de troncal en lugar de las licencias disponibles.

Se pueden agregar licencias adicionales para lograr la cantidad de canales de red de voz necesarios.

Código de orden	Licencia	Descripción
383087	IPO R10+ IP500 VCE NTWK 4 LIC	4 canales de red de voz, incluidas las funciones de red avanzada (grupos distribuidos y escritorio compartido en Small Community Network)

Licencias de usuario

Un perfil controla si los usuarios pueden configurarse para una serie de funciones. Todos los usuarios del sistema, excepto los usuarios con perfil de usuario básico y los usuarios sin licencia, requieren uno de los tipos de licencia de usuario.

La siguiente tabla enumera los diferentes perfiles de usuario y las funciones a las que puede acceder cada perfil. Establecer un usuario en un perfil particular habilita esas funciones de forma predeterminada, pero se pueden deshabilitar manualmente si es necesario. El número de usuarios que se pueden configurar para cada perfil está controlado por las licencias de usuario presentes en la configuración.

Excepto para un usuario básico, una licencia del sistema Preferred Edition es un requisito previo para cualquier licencia de perfil de usuario. En una red de sitios múltiples, la licencia de Preferred Edition para el sistema central se comparte automáticamente con otros sistemas en la red, lo que permite licencias de perfil de usuario en esos otros sistemas. Sin embargo, cada sistema que admita un servidor de Voicemail Pro aún requiere su propia licencia Preferred Edition para el funcionamiento de Voicemail Pro.

Rasgo		Modo estandar					Edición del servidor		
	No- con licencia Usuario [1]	Básico Usuario	Oficina Trabajador	teletrabajo ker	Móvil Trabajador	Energía Usuario	Básico Usuario	Oficina Trabajador	Energía Usuario
una-X Portal Servicios	–	–	Sí	Sí	–	Sí	–	Sí	Sí
telecomunicaciones útero opciones	–	–	–	Sí	–	Sí	–	–	Sí
Web de la UMS Servicios	–	–	Sí	Sí	–	Sí	–	Sí	Sí
TTS para Correo electrónico Lectura	–	–	–	–	Sí	Sí	–	–	Sí
Remoto trabajador [2]	–	–	–	Sí	–	Sí	Sí	Sí	Sí
Avaya comun gato [3]	–	–	Sí	Sí	–	Sí	Sí	Sí	Sí
WebRTC	–	–	Sí	–	–	Sí	–	Sí	Sí
Avaya Equinoccio™	–	–	Sí	Sí	–	Sí	–	Sí	Sí

Notas de perfil de usuario:

1. Se pueden crear usuarios sin licencia en los sistemas Standard Mode y Server Edition.
2. El sistema admite usuarios que utilizan extensiones remotas H.323 o SIP. En los sistemas que no son Server Edition, se admiten hasta 4 usuarios como extensiones remotas sin necesidad de configurarlos ni obtener una licencia para un perfil de usuario. Se admiten usuarios remotos adicionales si tienen licencia y están configurados para un **teletrabajador**o**Usuario de poder**perfil del usuario. En los sistemas Server Edition, el trabajador remoto es compatible con todos los perfiles de usuario.
3. Compatible con el uso avanzado de Avaya Communicator para IP Office si también están instaladas las aplicaciones one-X Portal y Voicemail Pro. De lo contrario, solo se admite el uso básico de Avaya Communicator para IP Office.
4. Equinoccio de Avaya™se puede utilizar con una licencia de usuario básico o de trabajador móvil junto con una licencia de IP Softphone, pero solo en modo estándar. En tales casos, el modo simultáneo, la función de control compartido y el soporte de presencia no estarán disponibles.

Usuario sin licencia

Un usuario sin licencia:

- Se permite acceso telefónico y paginación.
- Se puede utilizar como puerto de buscapersonas analógico o de música en espera.
- Se puede autenticar para permitir el acceso remoto para la administración remota.
- Puede realizar llamadas internas y de emergencia como NoUser.
- Puede reenviar al buzón de correo de voz para usuarios de buzón de correo de voz únicamente.
- Se puede utilizar para hermanamiento interno.

Usuarios básicos

Los nuevos usuarios se crean como usuarios básicos de forma predeterminada. Los usuarios básicos pueden realizar hot-desking, realizar y recibir llamadas, desviar llamadas y realizar hermanamiento móvil.

Las licencias de usuario básicas ya no se proporcionan. Tanto para los sistemas nuevos como para las actualizaciones, el**Usuarios básicos**el campo está atenuado.

Se requieren licencias de usuario básicas solo en el entorno de la nube.

licencias de oficinista

Esta opción está dirigida a usuarios que trabajan en la oficina. Junto con un teléfono Avaya con cable o inalámbrico, estos usuarios cuentan con funciones para controlar su comunicación con una PC. Por ejemplo, estos usuarios pueden controlar conferencias de audio o administrar el correo de voz con un cliente de correo electrónico (requiere una licencia Preferred Edition).

Una licencia de Office Worker habilita Avaya Communicator, Avaya Equinox™para Windows y Mac, y Avaya Communicator for Web. La licencia de Office Worker permite a un usuario utilizar el Servicio de mensajería unificada (UMS) y Avaya one-X®Portal para IP Office sin funcionalidad Telecommuter. Las instancias de licencia se consumen para cada usuario que se configura.

Código de orden	Licencia	Descripción
383105	IPO R10+ TRABAJADOR MÓVIL 5 TRL LIC	5 licencias para trabajadores móviles
383107	IPO R10+ TRABAJADOR DE OFICINA 5 TRL LIC	5 licencias para oficinistas
307347	IPO-SL R10+ OFICINA TRABAJADOR 5 TRL LIC	5 usuarios – Seleccionar

Licencias de teletrabajador

Esta opción está dirigida a usuarios que trabajan desde casa o en otro lugar con conexión a Internet a la oficina. Se les proporciona la capacidad de aprovechar el PLDS o ISDN usando el modo Telecommuter, sin incurrir en cargos telefónicos remotos. Como alternativa, se puede usar el nuevo IP Office Video Softphone si la calidad del servicio de la conexión a Internet local es adecuada.

Teleworker incluye la capacidad de trabajador remoto con el paquete. Una licencia de Essential Edition proporciona 4 puestos de trabajo remoto. Los clientes que requieran asientos adicionales deberán comprar la solución Teleworker.

La licencia Teleworker permite a un usuario utilizar Avaya Communicator, Avaya Equinox™para Windows y Mac, y Avaya one-X® Portal de IP Office. La funcionalidad UMS para correo de voz o integración de correo electrónico también está habilitada, proporcionando sincronización con cualquier cliente de correo electrónico IMAP. Las instancias de licencia se consumen para cada usuario que se configura.

Código de orden	Licencia	Descripción
383103	Licencia IPO R10+ TELEWORKER 5 TRL	5 usuarios

Licencias de trabajadores móviles

Esta opción está dirigida a usuarios con dispositivos móviles. Por ejemplo, el personal de servicio y ventas de campo que a menudo está de viaje. Estos usuarios cuentan con funciones, como acceso a un número y control de llamadas como si estuvieran en la oficina, lo que les permite no perder nunca una llamada. La licencia de Mobile Worker permite el uso del cliente one-X Mobile Preferred en modo de devolución de llamada (pero no en modo VoIP).

Licencias de usuario avanzado

Esta opción está dirigida a trabajadores clave del conocimiento que necesitan la funcionalidad de trabajador móvil y teletrabajador. Una licencia de usuario avanzado habilita Avaya Communicator, Avaya Equinox™ (escritorio y móvil), Avaya Communicator for Web y modo VoIP en one-X Mobile Preferred.

La licencia de usuario avanzado le permite a un usuario usar Avaya one-X®Portal para IP Office, todas las funciones de movilidad y UMS. Se requiere una licencia de usuario avanzado para habilitar la programación de conferencias en Avaya one-X®Portal de IP Office.

Las instancias de licencia se consumen para cada usuario que se configura.

Código de orden	Licencia	Descripción
396319	IP Office R11 OFICINA DE TRABAJADOR PARA USUARIO POTENCIAL 1 UPLIFT LIC	Actualización de Office Worker a Power User: 1 usuario
396505	IP OFFICE: SELECCIONE R11 OFFICE WORKER PARA EL USUARIO ENERGÉTICO 1 UPLIFT LIC	Actualizar de Office Worker a Power User – 1 usuario – Seleccione
396318	IP Office R11 MOBILE TO POWER USER 1 UPLIFT LIC	Actualización de trabajador móvil a usuario avanzado: 1 usuario
396316	LICENCIA DE USUARIO 1 DE IP Office R11	1 usuario
396503	IP Office-Select R11 POWER USER 1 LIC	1 usuario – Seleccionar

Licencias de recepcionista

Esta opción está dirigida a operadores o recepcionistas y proporciona una interfaz de computadora visual para el manejo y administración de llamadas para múltiples sitios. Se admiten hasta 10 usuarios recepcionistas en cada nodo. Server Edition admite hasta 32 usuarios Receptionist y Server Edition Select admite hasta 50.

La licencia de recepcionista también permite que un usuario use IP Office SoftConsole, una aplicación de Windows diseñada para recepcionistas y operadores. Se pueden ejecutar hasta 4 clientes IP Office SoftConsole al mismo tiempo y tener licencia en un solo sistema IP Office. Se pueden agregar licencias adicionales.

Código de orden	Licencia	Descripción
307318	IPO-SL R10+ RECEPTA 1 LIC	1 usuario
382687	IPO R10+ RECEPCIONISTA 1 LICENCIA	1 usuario

Licencia de usuario centralizada

En implementaciones de sucursales de IP Office, donde IP Office se implementa como una sucursal de un Avaya Aura central® sistema, los usuarios con una extensión SIP o analógica se pueden configurar como usuarios centralizados. Cada usuario centralizado requiere una licencia de punto final centralizado.

Licencias de colaboración web

Código de orden	Licencia	Descripción
383122	IPO R10+ WEB COLLAB USUARIO 1 LICENCIA	1 usuario
382918	IPO-SL 10+ WEB COLLAB USR 1 LIC	1 usuario – Seleccionar

Licencias de terminales de IP

Todos los puntos finales de IP, Avaya y de terceros, requieren una licencia de punto final.

Licencias de terminales IP de Avaya

Todos los teléfonos IP de Avaya, incluidos los teléfonos DECT y Wi-Fi, requieren una licencia de terminal IP de Avaya y consumirán una instancia de esa licencia. Esto no se aplica a Avaya Softphone o Avaya Communicator. Los teléfonos IP de Avaya sin licencia aún podrán registrarse, pero se limitarán a realizar llamadas de emergencia únicamente. El teléfono mostraráNo hay licencia disponibleySolo llamadas de emergencia.Si una licencia está disponible, se asignará primero a cualquier teléfono DECT sin licencia y luego a cualquier otro teléfono IP de Avaya sin licencia en el orden en que se registraron los teléfonos.

Código de orden	Licencia	Descripción
307350	IPO-SL R10+ AV IP PTO FINAL 1 LIC	1 punto final: seleccione
383110	IPO R10+ AV IP PTO FINAL 1 LIC	1 punto final

Licencias de terminales de IP de terceros

Los teléfonos IP que no son de Avaya, incluidos los dispositivos SIP o H.323, requieren una licencia de terminal IP de terceros para registrarse en IP Office y consumirán una instancia de esa licencia.

Código de orden	Licencia	Descripción
307323	IPO-SL R10+ 3ER PTY IP EXTREMO 1 LIC	1 punto final: seleccione
383072	IPO R10+ 3ER PTY IP ENDPT 1 LIC	1 punto final

Licencias de prueba

Código de orden	Licencia	Descripción
396446	LICENCIA DE PRUEBA DE IP OFFICE R11 ESSENTIAL EDITION	Edición esencial
396448	LICENCIA DE PRUEBA DE IP OFFICE R11 PREFERED VOICEMAIL PRO	Edición preferida

La tabla continúa...

Código de orden	Licencia	Descripción
383123	IPO R10+ WEB COLLAB 5 TRL LIC	5 licencias de colaboración web
382919	IPO-SL R10+ WEB COLLAB 5 TRL LIC	5 licencias de colaboración web: seleccione
396504	IP OFFICE-SELECT R11 POWER USER 5 LICENCIA DE PRUEBA	5Licencia de usuario avanzado: seleccione
396317	IP OFFICE R11 POWER USER 5 LICENCIA DE PRUEBA	5 licencias de usuario avanzado
383103	Licencia IPO R10+ TELEWORKER 5 TRL	5 licencias de teletrabajador
383105	IPO R10+ TRABAJADOR MÓVIL 5 TRL LIC	5 licencias de trabajador móvil
307347	IPO-SL R10+ OFICINA TRABAJADOR 5 TRL LIC	5 licencias para trabajadores de oficina: seleccione
383107	IPO R10+ TRABAJADOR DE OFICINA 5 TRL LIC	5 licencias de oficinista
307319	IPO-SL R10+ RECEPTA 5 TRL LIC	5 Licencias de recepcionista — Seleccionar
382688	IPO R10+ RECEPCIONISTA 5 TRL LIC	5 licencias de recepcionista
307324	IPO-SL 10 3ER PTY IP 5 TRL LIC	Licencia de prueba de punto final de IP de terceros: seleccione
383073	IPO R10 3RDPTY IPENDPT 5 TRL LIC	Licencia de prueba de punto final de IP de terceros
382913	IPO-SL R10+ AV IP ENDPT 5 TRL LIC	5 Licencias para terminales IP de Avaya: seleccione
383111	IPO R10+ AV IP ENDPT 5 TRL LIC	5 licencias de terminal IP de Avaya
383090	IPO R10+ VMPRO UMS 5 TRL LIC	5 licencias Voicemail Pro UMS
307335	IPO-SL R10+ VMPRO UMS 5 TRL LIC	5 licencias Voicemail Pro UMS: seleccione
383078	IPO R10+ 3ER PTY TTS TRL LIC	Licencia TTS de Voicemail Pro de terceros
383076	IPO R10+ TTS WNDWS TRL LIC	Licencia Voicemail Pro Windows TTS
307327	IPO-SL R10+ TTS PROLINUX TRL LIC	Licencia Voicemail Pro Linux TTS: seleccione
383080	Licencia IPO R10+ TTS PRO LINUX TRL	Licencia Voicemail Pro Linux TTS
307329	IPO-SL R10+ IPSEC VPN TRL LIC	Tunelización IPSec — Seleccionar
383082	IPO R10+ IPSEC VPN TRL LIC	Tunelización IPSec
307333	IPO-SL R10+ SIP TRNK 5 TRL LIC	Sesiones de troncales SIP — Seleccionar
383086	IPO R10+ SIP TRNK 5 TRL LIC	Sesiones de troncales SIP
383088	IPO R10+ IP500 VCE NTWK 4	Redes de voz IP500
307321	IPO-SL R10+ CTI TRL LIC	CIT Link Pro — Seleccionar
383070	IPO R10+ CTI TRL LIC	Enlace CIT Pro

Licencias de actualización

Para actualizar los sistemas existentes a la versión más reciente, se requieren licencias de actualización. Las licencias de actualización se venden por separado. Los clientes solo pueden actualizar al último equivalente de su edición existente.

Nota:

La actualización de una versión anterior de Basic Edition a la última versión de Essential Edition no es una ruta de actualización válida.

Código de orden	Licencia	Descripción
383738	IPO-SL R10+ RECEPTA 1 UPG PLDS LIC	Seleccione la actualización de recepcionista
383696	IPO R10+ RECEPCIONISTA 1 UPG PLDS LIC	Actualización de recepcionista
383739	IPO-SL 10+ CTI UPG PLDS LIC	Seleccione la actualización de CTI
383697	IPO R10+ TI UPG PLDS LICENCIA	actualización CTI
383740	IPO-SL 10+ MPRO 1 UPG PLDS LIC	Seleccione la actualización de Voicemail Pro
383698	IPO R10+ VM PRO 1 UPG PLDS LIC	Actualización de Voicemail Pro
383741	IPO-SL 10+ 3RDPTY IPEND1 UPG PLDS LIC	Seleccione la actualización de punto final de IP de terceros
383699	IPO R10+ 3RDPTY IPENDPT1 UPG PLDS LIC	Actualización de punto final de IP de terceros
383742	IPO-SL 10+ TAPI WAV 1 UPG PLDS LIC	Seleccione la actualización TAPI WAV
383700	IPO R10+ TAPI WAV 1 UPG PLDS LIC	Actualización TAPI WAV
383702	IPO R10+ 3ER PTY TTS UPG PLDS LIC	Actualización de TTS de terceros
383744	IPO-SL 10+ IPSEC VPN UPG PLDS LIC	Seleccione la actualización de VPN IPSec
383704	IPO R10+ IPSEC VPN UPG PLDS LIC	Actualización de VPN IPSec
383747	IPO-SL 10+ VMPRO UMS 1 UPG PLDS LIC	Seleccione la actualización del servidor de mensajería unificada de Voicemail Pro
383708	IPO R10+ VM PRO UMS 1 UPG PLDS LIC	Actualización del servidor de mensajería unificada de Voicemail Pro
383748	IPO-SL 10+ IP500 T1 CH1 UPG PLDS LIC	Seleccione la actualización de canal adicional IP500
383709	IPO R10+ IP500 T1 CH1 UPG PLDS LIC	Actualización de canal adicional IP500
383749	IPO-SL 10+ IP500 E1 CH1 UPG PLDS LIC	Seleccione la actualización de canal adicional IP500
383710	IPO R10+ IP500 E1 CH1 UPG PLDS LIC	Actualización de canal adicional IP500
383752	IPO-SL 10+ IP500 E1R2 CH1 UPG PLDS LIC	Seleccione la actualización de canal adicional IP500
383713	IPO R10+ IP500 E1R2 CH1 UPG PLDS LIC	Actualización de canal adicional IP500

La tabla continúa...

Código de orden	Licencia	Descripción
383707	IPO R10+ IP500 VCE NTWK1 UPG PLDS LIC	Actualización de red de voz IP500
383757	IPO-SL 10+ AV IP ENDPT 1 UPG PLDS LIC	Seleccione la actualización de punto final IP de Avaya
383722	IPO R10+ SFTPH 1 PLDS UPG LIC	Actualización de teléfono suave
383760	IPO-SL 10+ SMLINE SIPTRK UPG PLDS LIC	Seleccione la actualización del troncal SIP de la línea SM
383726	IPO R10+ SM LINE SIPTRNK UPG PLDS LIC	Actualización del troncal SIP de la línea SM
383706	IPO R10+ SIP TRNK 1 UPG PLDS LIC	Actualización de troncales SIP
383761	IPO-SL 10+ WEBCOLLB USR1 UPG PLDS LIC	Seleccione la actualización de usuario de Web Collaboration
383728	IPO R10+ WEBCOLLAB USER1 UPG PLDS LIC	Actualización de usuario de Web Collaboration
383730	IPO R10 ESS ED EVM 1CH UPG PLDS LIC	Actualización del canal de correo de voz incorporado Essential Edition

Capítulo 4: Recursos

Documentación

Consulte los siguientes documentos relacionados en el sitio web de soporte de Avaya ensoporte.avaya.com y la base de conocimientos de IP Office enherramientas de marketing.avaya.com/knowledgebase .

Documento número	Título	Utilice este documento para:	Audiencia
Visión general			
16–604278	*Oficina IP de Avaya™Plataforma Comience aquí primero*	Vea una lista de todos los documentos relacionados con la solución.	Todo el mundo
no numerado	*Oficina IP de Avaya™Característica de la plataforma Descripción*	Comprender las características de la solución a un alto nivel.	Todo el mundo
no numerado	*Avaya IP Office Contact Center Característica Descripción*	Comprender las funciones y capacidades de IP Office Contact Center.	Todo el mundo
Planificación			
15–604135	*Oficina IP de Avaya™ Configuración de referencia de Platform Server Edition*	Comprender las especificaciones técnicas y planificar la implementación de IP Office Server Edition.	Ingenieros de Ventas Implementación Ingenieros
15–604253	*Oficina IP de Avaya™Plataforma en un entorno de sucursal Configuración de referencia*	Comprender las especificaciones técnicas y planificar IP Office en la implementación de un entorno de sucursal.	Ingenieros de Ventas Implementación Ingenieros
no numerado	*en Avaya™y con la tecnología de referencia de Avaya Configuración para socios comerciales*	Comprenda las especificaciones técnicas de ambas soluciones IP Office Cloud y planifique la implementación.	Ingenieros de Ventas Implementación Ingenieros
no numerado	*Oficina IP de Avaya™Directrices de seguridad de la plataforma*	Comprender y seguir pautas de seguridad recomendadas.	Ingenieros de Ventas Implementación Ingenieros
no numerado	*Referencia de Avaya IP Office Contact Center Configuración*	Comprender las especificaciones técnicas de IP Office Contact Center y planificar la implementación.	Ingenieros de Ventas Implementación Ingenieros

Búsqueda de documentos en el sitio web de soporte de Avaya

Acerca de esta tarea

Utilice este procedimiento para buscar la documentación del producto en el sitio web de soporte de Avaya.

Procedimiento

1. Use un navegador para navegar al sitio web de soporte de Avaya enhttp://soporte.avaya.com/ .
2. En la parte superior de la pantalla, ingrese su nombre de usuario y contraseña y haga clic en**Acceso**.
3. Coloque el cursor sobre**Soporte por producto**.
4. Haga clic en**Documentos**.
5. En el**Ingrese su producto aquí**cuadro de búsqueda, escriba el nombre del producto y luego seleccione el producto de la lista desplegable.
6. Si hay más de un lanzamiento, seleccione el número de lanzamiento apropiado de la**Elija Liberar**la lista desplegable.
7. Usa el**Tipo de contenido**filtro a la izquierda para seleccionar el tipo de documento que está buscando, o haga clic en **Seleccionar todo**para ver una lista de todos los documentos disponibles.

   Por ejemplo, si está buscando guías de usuario, seleccione**Guías de usuario**en el**Tipo de contenido** filtrar. Solo los documentos de la categoría seleccionada aparecerán en la lista de documentos.
8. Haga clic en**Ingresar**.

Capacitación

La capacitación y las credenciales de Avaya están diseñadas para garantizar que nuestros Business Partners tengan las capacidades y habilidades para vender, implementar y respaldar con éxito las soluciones de Avaya y superar las expectativas de los clientes. Las siguientes credenciales están disponibles:

- Especialista en ventas certificado de Avaya (APSS)
- Especialista profesional en implementación de Avaya (AIPS)
- Especialista en soporte certificado de Avaya (ACSS)

Los mapas de credenciales están disponibles en el sitio web de Avaya Learning enhttp://avaya-learning.com/ .

Los siguientes cursos también están disponibles en el sitio web de Avaya Learning. Después de iniciar sesión en el sitio web, ingrese el código del curso o el título del curso en el**Búsqueda**campo.

Código del curso	Título del curso
2S00012W	APSS – Comunicaciones de mercado pequeño y mediano – IP Office™Descripción general de la plataforma y selección

La tabla continúa...

Código del curso	Título del curso
4601W	Oficina IP de Avaya™Plataforma — Componentes
4602W	Oficina IP de Avaya™Plataforma — Ediciones
2S00015O	Comunicaciones para pequeñas y medianas empresas — IP Office — Endpoints
10S00005E	Acceso al conocimiento: IP Office de Avaya™Implementación de la plataforma
5S00004E	Acceso al conocimiento: IP Office de Avaya™Soporte de plataforma

Incluido en todas las ofertas de Knowledge Collection Access anteriores hay un área separada llamada IP Office Supplemental Knowledge. Este piso en el Campus Virtual contiene objetos de aprendizaje autodirigidos, que cubren la información delta de IP Office. Este material puede ser consumido por técnicos con experiencia en IP Office.

Visualización de videos de mentores de Avaya

Los videos de orientación de Avaya brindan contenido técnico sobre cómo instalar, configurar y solucionar problemas de los productos de Avaya.

Acerca de esta tarea

Los videos están disponibles en el sitio web de soporte de Avaya, enumerados bajo el tipo de documento de video y en el canal administrado por Avaya en YouTube.

Procedimiento

- Para encontrar videos en el sitio web de soporte de Avaya, vaya ahttp://soporte.avaya.com y realice una de las siguientes acciones:
  - En**Búsqueda**, escribeVídeos de orientación de Avayapara ver una lista de los videos disponibles.
  - En**Búsqueda**, escriba el nombre del producto. En la página Resultados de la búsqueda, seleccione**Video**en el **Tipo de contenido**columna de la izquierda.
- Para encontrar los videos de Avaya Mentor en YouTube, vaya awww.youtube.com/AvayaMentor y realice una de las siguientes acciones:
  - Ingrese una palabra clave o palabras clave en el**Canal de búsqueda**para buscar un producto o tema específico.
  - Desplácese hacia abajo en Listas de reproducción y haga clic en el nombre de un tema para ver la lista disponible de videos publicados en el sitio web.

Nota:

Los videos no están disponibles para todos los productos.

Recursos adicionales de IP Office

Puede encontrar información en los siguientes sitios web de recursos adicionales.

Avaya

http://www.avaya.com es el sitio web oficial de Avaya. La página principal también brinda acceso a sitios web individuales de Avaya para diferentes países.

Portal de socios y ventas de Avaya

http://ventas.avaya.com es el sitio web oficial de todos los Business Partners de Avaya. El sitio requiere el registro de un nombre de usuario y contraseña. Una vez accedido, el portal se puede personalizar para productos específicos y tipos de información que desea ver y recibir notificaciones por correo electrónico.

Base de conocimientos de IP Office de Avaya

http://herramientas de marketing.avaya.com/knowledgebase proporciona acceso a una versión en línea actualizada periódicamente de la base de conocimientos de IP Office.

Información de mantenimiento, ciclo de vida y garantía de Avaya

Los servicios de soporte de Avaya complementan las políticas estándar de mantenimiento, ciclo de vida y garantía de Avaya que se publican enhttp://soporte.avaya.com . Para obtener más información, envíe un correo electrónico a support@avaya.com .

Grupo internacional de usuarios de Avaya

http://www.iaug.org es el foro de discusión oficial para los usuarios de productos de Avaya.

Compatibilidad del producto

Para obtener la información de compatibilidad más reciente y precisa, vaya ahttps://support.avaya.com/CompatibilityMatrix/Index.aspx .

Enlaces relacionados

Acceso a las notas de la aplicación Avaya DevConnect en la página 134
interoperabilidad en la página 93

Apoyo

Vaya al sitio web de soporte de Avaya enhttp://soporte.avaya.com para obtener la documentación, los avisos de productos y los artículos de conocimiento más actualizados. También puede buscar notas de la versión, descargas y resoluciones de problemas. Utilice el sistema de solicitud de servicio en línea para crear una solicitud de servicio. Chatea con agentes en vivo para obtener respuestas a tus preguntas o solicita a un agente que te conecte con un equipo de soporte si un problema requiere experiencia adicional.

Página541 de 3226.

Uso de la base de conocimientos de Avaya InSite

Avaya InSite Knowledge Base es un motor de búsqueda basado en la web que proporciona:

- Procedimientos de resolución de problemas y consejos técnicos actualizados
- Información sobre paquetes de servicios
- Acceso a la documentación técnica y del cliente
- Información sobre programas de capacitación y certificación
- Enlaces a otra información pertinente

Si es un socio autorizado de Avaya o un cliente actual de Avaya con un contrato de soporte, puede acceder a la base de conocimiento sin costo adicional. Debe tener una cuenta de inicio de sesión y un número de cliente válido.

Utilice la base de conocimientos de Avaya InSite para buscar posibles soluciones a los problemas.

1. Ir ahttp://www.avaya.com/support .
2. Inicie sesión en el sitio web de Avaya con una ID de usuario y una contraseña válidas de Avaya. Aparece la página de soporte.
3. Bajo**Soporte por producto**, haga clic**Soporte específico del producto**.
4. Introduce el producto en**Introduzca el nombre del producto**cuadro de texto y presione Entrar.
5. Seleccione el producto de la lista desplegable y elija la versión correspondiente.
6. Seleccione el**Soluciones Técnicas**pestaña para ver artículos.
7. Seleccione artículos relevantes.

Enlaces relacionados

Los telefonos en la página 38

Interoperabilidad telefónica en la página 95

Acceso a las notas de la aplicación Avaya DevConnect

El programa Avaya DevConnect realiza pruebas con proveedores de servicios para establecer la compatibilidad con los productos de Avaya.

Procedimiento

1. Ir ahttp://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp .
2. Inicie sesión o regístrese.
3. Haga clic en un período de tiempo para buscar dentro.

   Aparece una lista de todas las notas de la aplicación para ese período de tiempo.

4. En el**Búsqueda**Tipo de campoOficina de PIy presiona**Ingresar**.

   Aparece una lista de notas de aplicación relevantes.

Enlaces relacionados

Los telefonos en la página 38

Interoperabilidad telefónica en la página 95 Compatibilidad del producto en la página 133 Opciones de hardware y software en la página 84 interoperabilidad en la página 93

lista del glosario

Ruta Automática Selección	Característica de algunos sistemas telefónicos en la que el sistema elige automáticamente la forma más rentable de enviar una llamada interurbana.
Llamada en hora pico Terminaciones	Una medida de llamadas de tráfico dinámico que se pueden completar en una hora pico promedio.
Comunicación Gerente	Un componente clave de Avaya Aura®. Ofrece capacidades ricas de voz y video y proporciona una red distribuida resistente para puertas de enlace de medios y dispositivos de comunicación analógicos, digitales y basados en IP. Incluye funciones de movilidad avanzadas, conferencias telefónicas integradas, aplicaciones de centros de contacto y capacidades E911.
Soportado por computadora telecomunicaciones Solicitud (CSTA)	Una interfaz estándar para aplicaciones de integración de telefonía informática (CTI), como correo de voz y operadora automática, para interactuar con equipos de telefonía.
Digital Comunicaciones Protocolo	Un protocolo propietario que se utiliza para transmitir tanto voz digitalizada como datos digitalizados a través del mismo enlace de comunicaciones. Un enlace de Protocolo de comunicaciones digitales (DCP) consta de dos canales de información (I) de 64 kbps y un canal de señalización (S) de 8 kbps. El protocolo DCP admite dos canales portadores de información y dos teléfonos o módulos de datos.
Directorio habilitado administración	Una interfaz que utiliza Avaya Directory Server para facilitar la administración de Modular Messaging desde una ubicación centralizada.
Repartido Comunicaciones Sistema	Un protocolo de interconexión de redes patentado de Avaya con el que puede configurar dos o más redes de comunicación privadas basadas en Avaya para que funcionen como una gran red.
Nombre de dominio Sistema (DNS)	Un estándar del Grupo de trabajo de ingeniería de Internet (IETF) para cadenas ASCII para representar direcciones IP. El DNS es un servicio de directorio interno distribuido que se utiliza principalmente para traducir entre nombres de dominio y direcciones IP. Los teléfonos IP de la serie 9600 de Avaya pueden usar DNS para convertir nombres en direcciones IP. En los archivos DHCP, TFTP y HTTP, los nombres DNS se pueden usar siempre que haya direcciones IP disponibles, siempre que se identifique primero un servidor DNS válido.

Datos dinámicos Intercambio (DDE)	Un método de comunicación entre procesos (IPC).
Anfitrión dinámico Configuración Protocolo (DHCP)	Un protocolo del Grupo de trabajo de ingeniería de Internet (IETF) que se utiliza para automatizar la asignación y administración de direcciones IP.
Enrutamiento Ethernet Interruptor (ERS)	El sistema de chasis apilable de Avaya que proporciona conectividad de conmutación Ethernet de alto rendimiento, preparada para la convergencia, segura y resistente.
Interfaz de expansión	Paquete de circuitos de puertos en una red de puertos (PN) que proporciona la interfaz entre un bus de multiplexación por división de tiempo (TDM) o un bus de paquetes en la PN y un enlace de fibra óptica. La interfaz de expansión (EI) transporta datos de conmutación de circuitos, datos de conmutación de paquetes, control de red, control de temporización y control de señal digital 1 (DS1). EI en una red de puertos de expansión (EPN) también se comunica con la tarjeta de mantenimiento maestra para proporcionar el estado ambiental y el estado de alarma de la EPN al elemento de procesamiento del conmutador (SPE).
Puerto de expansión la red	En las configuraciones de Intuity Audix Server, una red de puertos (PN) que está conectada al bus de multiplexación por división de tiempo (TDM) y al bus de paquetes de una red de puertos de procesador (PPN). El control se logra mediante la conexión indirecta de la EPN a la PPN a través de un enlace de red de puerto (PNL).
Extensión a Celular número de acceso	El número de teléfono marcado para conectarse al servidor de Avaya que ejecuta Communication Manager. El número de acceso de Extension to Cellular inicia el proceso de habilitar o deshabilitar Extension to Cellular o cambiar el código de seguridad de la estación.
Federal Comunicaciones Comisión (FCC)	Una agencia federal de los Estados Unidos que regula las comunicaciones, como las comunicaciones por cable e Internet.
técnico mundial Servicios	Un equipo de Avaya que responde a las llamadas de los clientes sobre productos en Avaya Integrated Management.
protocolo de Internet	Un protocolo sin conexión que opera en la capa 3 del modelo de interconexión de sistemas abiertos (OSI). El Protocolo de Internet (IP) se utiliza para el direccionamiento de Internet y el enrutamiento de paquetes a través de múltiples redes hasta un destino final. IP funciona junto con el Protocolo de control de transmisión (TCP) y se identifica como TCP/IP.
Superviviente local Procesador	Una configuración del servidor de medios S8300 en la que el servidor actúa como servidor alternativo o controlador de acceso para entidades IP como teléfonos IP y puertas de enlace de medios G700. Estas entidades de IP utilizan el Procesador recuperable local (LSP) cuando las entidades de IP pierden la conectividad con el servidor principal.

Pasarela de medios

Un elemento de hardware habilitador de aplicaciones que forma parte de una familia de dichos elementos. Esta familia incluye conectividad dentro del switch, interfaces de control, interfaces de puerto y gabinetes. Los gateways de medios de Avaya admiten tráfico portador y tráfico de señalización que se enruta entre redes de conmutación de paquetes y redes de conmutación de circuitos para brindar capacidades de datos, voz, fax y mensajería. Los gateways de medios brindan conversión de protocolo, como IP a ATM a TDM, conferencias, presencia, como colgado o descolgado, conectividad a redes privadas y redes públicas, como IP, ATM, TDM y redes, como QSIG. , DCS, RDSI. Los gateways de medios admiten factores de forma opcionales.

Dirección de red
Traducción de puertos

Una técnica de enrutamiento de red. La traducción de puertos de direcciones de red (NAPT) se utiliza para acceder a los sistemas en la misma subred que IP Office.

Enrutamiento de red
Política

Una aplicación para gestionar de forma centralizada el enrutamiento SIP para las instancias de Session Manager. Una política de enrutamiento describe cómo se enruta una llamada: de dónde viene, hacia dónde se dirige, cuál es su patrón de marcación, a qué hora del día se enruta y su costo para una ruta en particular.

novela®directorio electrónico™

Un producto de software de servicio de directorio compatible con X.500 lanzado inicialmente en 1993 por Novell®para administrar de forma centralizada el acceso a los recursos en múltiples servidores y computadoras dentro de una red determinada. novela®directorio electrónico™ antes conocido como Novell®Directorio de Servicios. A veces se denomina Servicios de directorio de Netware. novela®directorio electrónico™es una base de datos jerárquica orientada a objetos que se utiliza para representar ciertos activos en una organización en un árbol lógico, que incluye personas, puestos, servidores, estaciones de trabajo, aplicaciones, impresoras, servicios y grupos.

OFCOM

La Oficina de Comunicaciones del Reino Unido para la regulación de las telecomunicaciones.

COMPAÑERO®Contacto
Adjunto de cierre

Un dispositivo que está conectado al chasis de un portal de medios y proporciona cierres de contactos. El complemento de cierre de contacto (CCA) cierra un relé en respuesta a un comando de acceso telefónico desde el portal de medios para operar una puerta o realizar una acción similar.

Información del Producto
Sistema de presentación

Los informes del Sistema de presentación de información del producto (PIPS) proporcionan datos del Experto en información del producto (PIE), una herramienta de minería de datos que extrae la información de configuración adjunta y del interruptor del cliente de Avaya y la almacena en una base de datos.

Licencias de productos
y sistema de entrega
(PLDS)

El sitio web y el sistema de administración de licencias y descargas de Avaya. Los socios comerciales y los clientes de Avaya utilizan este sitio para obtener archivos de imágenes ISO y otras descargas de software.

Conmutado público
Red Telefónica
(RTPC)

Una red telefónica que incluye muchas tecnologías de comunicación, como transmisión de microondas, satélites y cables submarinos.

Función remota Activación
Una aplicación de Avaya basada en la web para activar funciones de forma remota y aumentar las capacidades en el sistema de un cliente mediante la entrega de un nuevo archivo de licencia.

Administrador de sistemas
Un marco de gestión común para Avaya Aura®que proporciona funciones de gestión centralizadas para el aprovisionamiento y la administración para reducir la complejidad de la gestión.

Estado del sistema
Una aplicación de IP Office que muestra el estado de cosas como las llamadas salientes.

Solicitud teletrabajador
La configuración en la que Communication Manager establece la conexión de voz a un teléfono con conmutación de circuitos. Requiere dos conexiones: una conexión TCP/IP para control de señalización y una conexión de conmutación de circuitos para voz.

Telefonía Programa de aplicación Interfaz (TAPI)
un microsoft®API de Windows que permite que las computadoras que ejecutan Windows usen servicios de telefonía. TAPI se utiliza para comunicaciones de datos, FAX y voz. Las aplicaciones pueden usar TAPI para controlar las funciones de telefonía, como marcar, contestar y colgar.

Servicio de Telefonía Interfaz de proveedor (TSPI)
Una interfaz definida por Microsoft para el proveedor de servicios de telefonía (TSP). microsoft®Windows viene con un TSP H.323, un TSP de conferencia IP, un TSP de controlador de dispositivo en modo kernel y un TSP unimodem.

Índice

A

a-ley PCM 31
notas de aplicación 134
Soporte de aplicaciones 87
arquitectura 71
soporte de creación automática para usuarios y extensiones en WebLM... 117 Comunicador Avaya 45
ipad 46
Ventanas 47
Selección del centro de contacto de Avaya
Continuidad del negocio 83
opciones de implementación ..... 80 –83 DVD 80
dispositivo de hardware 82
visión general ..... sesenta y cinco
configuraciones de referencia 78
topología ..... 78 ,80 –83
sincronización de datos de usuario 78
Vmware 81
Reunión en línea de Avaya Equinox 55
Descripción general de Avaya Spaces 55

B

cartas base 31
Edición básica 67
Migración de BCM ..... 100 ,107 compatibilidad con navegadores 87

C

CA 61
Acceso Centro 61
gerente de operaciones en la nube 63
visión general de la nube 75
componentes 72
Integración de telefonía informática 27
llamadas de conferencia 51
configuración de licencias WebLM 115
avisos y alarmas 116
centro de contacto 64
unidad de control 29
TIC 27
requisitos de PC proporcionados por el cliente 91

D

red de datos 18
opciones de implementación 67
Selección del centro de contacto de Avaya ..... 78 ,80 –83 DVD ..... 80 ,83
opciones de implementación *(continuado)*
dispositivo de hardware 82
Vmware 81
DevConnect 134
DMM 64
cambios en el documento 7

mi

Correo de voz integrado 50
puntos finales 126
aplicaciones de usuario final 40
Equinoccio para IP Office
Equinoccio
Equinoccio de Avaya 42
Edición Esencial 69
módulos de expansión externos 35

F

teclas de función 31
caracteristicas 13
Descripción de las características 54

GRAMO

porteros 22
puertas de enlace 22
pautas
WebRTC 38

H

H.323 22
opciones de hardware 84

yo

Base de conocimientos de InSite 134
interfaces 105
interoperabilidad ..... 93 ,99
IP500 V2 29
ipad 46
Licencias de terminales de IP 126
Licencias de terminales de IP para WebLM 116
aplicaciones de IP Office
aplicaciones de centros de contacto 64
Aplicaciones de instalación y administración 55
aplicaciones de usuario 40
Centro de contacto de IP Office
opciones de implementación 77
topología 77

Página548 de 3226.

ediciones de ip office 10
Telefonía IP 19

L

Migración de licencias
IDA 110
licencias 109
Edición básica 118
Rama 120
Edición Esencial 118
Puntos finales IP 126
Edición preferida 118
ESCN 120
Edición del servidor 119
pequeña red comunitaria 120
Modo estandar 118
juicios 126
baúles 121
actualizaciones ..... 106 ,127
usuarios 122

METRO

Gerente 55
MCU 22
Administrador de medios
visión general 58
Conferencia Meet-Me 52
Migración
Hoja de ruta y limitaciones 108
Unidades de Conexión Multipunto 22

norte

nuevas características 11

O

Preferido de one-X Mobile 40
Portal one-X para IP Office 41
soporte del sistema operativo 87
opciones
despliegue 73
visión general ..... 10 ,64 ,75
Selección del centro de contacto de Avaya ..... sesenta y cinco
Reunión en línea de Avaya Equinox 55
Espacios de Avaya 55
sucursal de la empresa 73
oficina de PI 73

PAGS

Redes de voz y datos basadas en paquetes 18
PCM 31
Los telefonos 38
Los telefonos *(continuado)*
compatibilidad 95
disponibilidad del país 98
remoto 39
Licencias PLDS 109
puertos 105
Edición preferida 70
red privada de voz conmutada por circuito 14
Compatibilidad del producto 133
Redes de voz pública 15
modulación de código de pulso 31

R

Radvisión 53
licencias de recepcionista para WebLM 117
configuración de referencia
Centro de contacto de IP Office 77
configuraciones de referencia ..... 67 ,73
documentos relacionados 130
telefonos remotos 39
sitios web de recursos 133

S

Licencias SCN 120
Escopia 53
tarjetas SD 31
seguridad ..... 101 ,102
Edición del servidor 70
Licenciamiento centralizado 111
licencias 119
Licencias nodales 111
Administrador de la edición del servidor 56
Protocolo de Iniciacion de Sesion 23
SORBO ..... 23,25 Agentes de usuario de punto final SIP 26
SMA 61
Consola de administración SNMP 61
Consola suave 49
Administración de SoftConsole 61
opciones de software 84
Aplicación de gestión de soluciones 61
especificación de la solución 85
especificaciones
interfaces de puerto 105
SSA 62
Modo estandar 118
apoyo 133
Monitor de sistema 63

T

telefonos 38
topología ..... 14 ,71 ,74
Selección del centro de contacto de Avaya ..... 78 ,80 –83

Página549 de 3226.

topología*(continuado)*
Alojado por BP 76
Continuidad del negocio 83
DVD 80
dispositivo de hardware 82
Impulsado por socios 76
Vmware 81
capacitación 131
juicios 126
tarjetas de troncales 33
bañador
licencias 121

tu

licencias de actualización 127
actualizaciones 106
licencias de usuario 122
licencias de usuario para WebLM 117

V

VCM 22
Solución de videocolaboración 53
videoconferencia 53
vídeos 132
ambiente virtual 93
licencias virtuales 111
Módulos de compresión de voz 22
Correo de voz Pro 50
red de voz ..... 14 , 15 , 18

W

cliente web
cliente web oficina ip
webrtc 44
Administrador de licencias web 110
WebLM 110
Modos de licencia de WebLM 114
Transiciones de estado del modo de licencia de WebLM 115
Licencias WebLM
creación automática de soporte para usuarios y extensiones 117
configuración 115
advertencias y alarmas de configuración 116
Licencias de terminales de IP 116
modos de licencia 114
transiciones de estado del modo de licencia 115
licencias de recepcionista 117
licencias de usuario 117
Administrador web 58
WebRTC 38

Traducido del inglés al español - www.onlinedoctranslator.com

Oficina IP de Avaya™Plataforma Solución Descripción

Versión 11.0.4
Mayo 2019

©2018-2019, Avaya Inc. Todos
los derechos reservados.

Aviso

Si bien se han realizado esfuerzos razonables para garantizar que la información de este documento sea completa y precisa en el momento de la impresión, Avaya no asume ninguna responsabilidad por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información de este documento sin la obligación de notificar a ninguna persona u organización sobre dichos cambios.

Descargo de responsabilidad de la documentación

"Documentación" se refiere a la información publicada en diversos medios que pueden incluir información sobre el producto, instrucciones de funcionamiento y especificaciones de rendimiento que generalmente se ponen a disposición de los usuarios de los productos. La documentación no incluye materiales de marketing. Avaya no será responsable de ninguna modificación, adición o eliminación de la versión original publicada de la Documentación, a menos que dichas modificaciones, adiciones o eliminaciones hayan sido realizadas por Avaya o en su nombre expreso. El usuario final acepta indemnizar y eximir de responsabilidad a Avaya, a los agentes, servidores y empleados de Avaya frente a todos los reclamos, juicios, demandas y juicios que surjan de, o en relación con, modificaciones, adiciones o eliminaciones posteriores a esta documentación, en la medida en que lo haga End Usuario.

Descargo de responsabilidad del enlace

Avaya no es responsable del contenido o la confiabilidad de los sitios web vinculados a los que se hace referencia en este sitio o la documentación proporcionada por Avaya. Avaya no es responsable de la precisión de la información, declaración o contenido proporcionado en estos sitios y no respalda necesariamente los productos, servicios o información descritos u ofrecidos en ellos. Avaya no garantiza que estos enlaces funcionen todo el tiempo y no tiene control sobre la disponibilidad de las páginas enlazadas.

Garantía

Avaya proporciona una garantía limitada para el hardware y el software de Avaya. Consulte su contrato de venta para establecer los términos de la garantía limitada. Además, el lenguaje de la garantía estándar de Avaya, así como la información sobre el soporte para este producto mientras está bajo garantía, está disponible para los clientes de Avaya y otras partes a través del sitio web de Soporte de Avaya:https://support.avaya.com/ helpcenter/ getGenericDetails?detailId=C20091120112456651010 bajo el enlace "Garantía y ciclo de vida del producto" o el sitio sucesor designado por Avaya. Tenga en cuenta que si adquirió los productos de un socio de canal autorizado de Avaya fuera de los Estados Unidos y Canadá, dicho socio de canal de Avaya le proporciona la garantía y no Avaya.

"Servicio alojado" hace referencia a una suscripción de servicio alojado de Avaya que adquiere de Avaya o de un socio de canal autorizado de Avaya (según corresponda) y que se describe con más detalle en SAS alojado u otra documentación de descripción del servicio con respecto al servicio alojado aplicable. Si compra una suscripción al Servicio alojado, es posible que la garantía limitada anterior no se aplique, pero puede tener derecho a servicios de soporte en relación con el Servicio alojado, como se describe más adelante en los documentos de descripción del servicio para el Servicio alojado correspondiente. Comuníquese con Avaya o con el socio de canal de Avaya (según corresponda) para obtener más información.

Servicio alojado

LO SIGUIENTE SE APLICA ÚNICAMENTE SI COMPRA UNA SUSCRIPCIÓN AL SERVICIO ALOJADO DE AVAYA DE AVAYA O DE UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA), LOS TÉRMINOS DE USO PARA LOS SERVICIOS ALOJADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA,HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO BAJO EL ENLACE "Términos de uso de Avaya para servicios alojados" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, Y SON APLICABLES A CUALQUIER PERSONA QUE ACCEDA O UTILICE EL SERVICIO ALOJADO. AL ACCEDER O UTILIZAR EL SERVICIO ALOJADO, O AL AUTORIZAR A OTROS A HACERLO, USTED, EN NOMBRE DE USTED Y DE LA ENTIDAD PARA LA QUE LO ESTÁ HACIENDO (EN ADELANTE DENOMINADO INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA LOS TÉRMINOS DE USO. SI USTED ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR DICHA ENTIDAD A ESTOS TÉRMINOS DE USO. SI USTED NO TIENE DICHA AUTORIDAD, O SI USTED NO DESEA ACEPTAR ESTOS TÉRMINOS DE USO, NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO.

Licencias

LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA,HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, BAJO EL ENLACE "TÉRMINOS DE LICENCIA DE SOFTWARE DE AVAYA (Productos de Avaya)" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, SON APLICABLES A CUALQUIER PERSONA QUE DESCARGUE, UTILICE Y/O INSTALE SOFTWARE DE AVAYA, COMPRADO DE AVAYA INC., CUALQUIER AFILIADO DE AVAYA O UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA) BAJO UN ACUERDO COMERCIAL CON AVAYA O UN SOCIO DE CANAL DE AVAYA. A MENOS QUE AVAYA ACORDE LO CONTRARIO POR ESCRITO, AVAYA NO EXTENDERÁ ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE CUALQUIER PERSONA QUE NO SEA AVAYA, UNA AFILIADA DE AVAYA O UN SOCIO DE CANAL DE AVAYA; AVAYA SE RESERVA EL DERECHO DE TOMAR ACCIONES LEGALES CONTRA USTED Y CUALQUIER OTRA PERSONA QUE UTILICE O VENDA EL SOFTWARE SIN LICENCIA. AL INSTALAR, DESCARGAR O UTILIZAR EL SOFTWARE, O AUTORIZAR A OTROS A HACERLO, USTED, EN SU NOMBRE Y EN EL DE LA ENTIDAD PARA LA QUE ESTÁ INSTALANDO, INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA ESTOS TÉRMINOS Y CONDICIONES Y CREA UN CONTRATO VINCULANTE ENTRE USTED Y AVAYA INC. O LA AFILIADA DE AVAYA CORRESPONDIENTE ("AVAYA").

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el cual el alcance de la licencia se detalla a continuación. Cuando la documentación del pedido no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de Sistema Designado como se establece a continuación en la sección Licencia de Sistema(s) Designado(s) (DS) según corresponda. El número aplicable de licencias y unidades de capacidad para las que se otorga la licencia será uno (1), a menos que se especifique un número diferente de licencias o unidades de capacidad en la documentación u otros materiales disponibles para Usted. "Software" hace referencia a los programas informáticos en código objeto, proporcionados por Avaya o un socio de canal de Avaya, ya sea como productos independientes, preinstalados en productos de hardware y cualquier mejora, actualización, parche, corrección de errores, o versiones modificadas de los mismos. "Procesador designado" significa un único dispositivo informático independiente. "Servidor" hace referencia a un conjunto de Procesadores designados que aloja (física o virtualmente) una aplicación de software a la que acceden varios usuarios. "Instancia" significa una única copia del Software que se ejecuta en un momento determinado: (i) en una máquina física; o (ii) en una máquina virtual de software implementada ("VM") o implementación similar.

Tipos de licencia

Licencia de sistema(s) designado(s) (DS). El Usuario final puede instalar y utilizar cada copia o una Instancia del Software únicamente: 1) en una cantidad de Procesadores designados hasta la cantidad indicada en el pedido; o 2) hasta el número de Instancias del Software que se indique en el pedido, la Documentación o que Avaya autorice por escrito. Avaya puede solicitar que los Procesadores designados se identifiquen en el pedido por tipo, número de serie, clave de función, Instancia, ubicación u otra designación específica, o que el Usuario final los proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este objetivo.

Licencia de Usuario Concurrente (CU). El Usuario final puede instalar y utilizar el Software en varios Procesadores designados o en uno o más Servidores, siempre que solo el número de Unidades con licencia acceda y utilice el Software en un momento dado. Una "Unidad" hace referencia a la unidad en la que Avaya, a su exclusivo criterio, basa el precio de sus licencias y puede ser, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o correo de voz a nombre de una persona. o función corporativa (por ejemplo, webmaster o servicio de asistencia), o una entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software. Las Unidades pueden vincularse a un Servidor específico e identificado oa una Instancia del Software.

Licencia de clúster (CL). El Usuario final puede instalar y usar cada copia o una Instancia del Software solo hasta la cantidad de Clústeres que se indica en el pedido con un valor predeterminado de un (1) Clúster si no se indica. "Cluster" significa un grupo de Servidores y otros recursos que actúan como un solo sistema.

Licencia de empresa (EN). El usuario final puede instalar y usar cada copia o una instancia del software solo para el uso de una cantidad ilimitada de instancias del software en toda la empresa, según se indica en el pedido o según lo autorice Avaya por escrito.

Licencia de usuario nominal (NU). Usted puede: (i) instalar y usar cada copia o Instancia del Software en un solo Procesador o Servidor Designado por Usuario Designado autorizado (definido a continuación); o (ii) instalar y usar cada copia o Instancia del Software en un Servidor, siempre que solo los Usuarios designados autorizados accedan y usen el Software. “Usuario designado” significa un usuario o dispositivo que ha sido expresamente autorizado por Avaya para acceder y utilizar el Software. A discreción exclusiva de Avaya, un "Usuario designado" puede ser, entre otros, designado por nombre, función corporativa (por ejemplo, webmaster o servicio de asistencia técnica), una cuenta de correo electrónico o correo de voz en nombre de una persona o función corporativa, o un entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software.

Licencia Shrinkwrap (SR). Usted puede instalar y usar el Software de acuerdo con los términos y condiciones de los acuerdos de licencia aplicables, como la licencia "shrinkwrap" o "clickthrough" que acompaña o se aplica al Software ("Licencia Shrinkwrap").

Software de la herencia de Nortel

“Software Heritage Nortel” significa el software que fue adquirido por Avaya como parte de su compra de Nortel Enterprise Solutions Business en diciembre de 2009. El software Heritage Nortel es el software incluido en la lista de productos Heritage Nortel ubicada enhttps://support.avaya.com/LicenseInfo bajo el enlace "Productos de Heritage Nortel" o el sitio sucesor designado por Avaya. Para el software Heritage Nortel, Avaya le otorga al Cliente una licencia para usar el software Heritage Nortel proporcionado en virtud del presente únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la Documentación, y únicamente como integrado, para ejecución en, o para comunicación con equipos Avaya. Los cargos por el software Heritage Nortel pueden basarse en el grado de activación o uso autorizado según se especifica en un pedido o factura.

Derechos de autor

Salvo que se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, la documentación, el software, el servicio alojado o el hardware proporcionado por Avaya. Todo el contenido de este sitio, la documentación, el Servicio alojado y el producto proporcionado por Avaya, incluida la selección, disposición y diseño del contenido, es propiedad de Avaya o de sus otorgantes de licencias y está protegido por derechos de autor y otras leyes de propiedad intelectual, incluida la ley sui generis. derechos relativos a la protección de las bases de datos. No puede modificar, copiar, reproducir, volver a publicar, cargar, publicar, transmitir o distribuir de ninguna manera ningún contenido, en su totalidad o en parte, incluido cualquier código y software, a menos que Avaya lo autorice expresamente. La reproducción, transmisión, difusión, almacenamiento o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede ser un delito,

virtualización

Lo siguiente se aplica si el producto se implementa en una máquina virtual. Cada producto tiene su propio código de pedido y tipos de licencia. A menos que se indique lo contrario, cada Instancia de un producto se debe licenciar y pedir por separado. Por ejemplo, si el cliente usuario final o el socio de canal de Avaya desea instalar dos instancias del mismo tipo de productos, entonces se deben pedir dos productos de ese tipo.

Componentes de terceros

"Componentes de terceros" significa que ciertos programas de software o partes de los mismos incluidos en el Software o el Servicio alojado pueden contener software (incluido el software de código abierto) distribuido bajo acuerdos de terceros ("Componentes de terceros"), que contienen términos relacionados con los derechos de uso de ciertos partes del Software ("Términos de terceros"). Según sea necesario, la información sobre el código fuente del sistema operativo Linux distribuido (para aquellos productos que tienen el código fuente del sistema operativo Linux distribuido) y la identificación de los titulares de derechos de autor de los componentes de terceros y los términos de terceros que se aplican está disponible en los productos, la documentación o en el sitio web de Avaya. a:https://support.avaya.com/Copyright o el sitio sucesor designado por Avaya. Los términos de licencia de software de código abierto proporcionados como Términos de terceros son consistentes con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del código abierto.

software. Los Términos de terceros prevalecerán sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables en la medida en que estos Términos de licencia de software le impongan mayores restricciones que los Términos de terceros aplicables.

Lo siguiente se aplica solo si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO TIENE LICENCIA BAJO LA LICENCIA DE CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS POR LOS QUE NO RECIBE REMUNERACIÓN PARA (i) CODIFICAR VÍDEO EN CUMPLIMIENTO CON EL ESTÁNDAR AVC (“AVC VIDEO”) Y/O (ii) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL DE MPEG LA, LLC VERHTTP://WWW.MPEGLA.COM .

Proveedor de servicio

LO SIGUIENTE SE APLICA AL ALOJAMIENTO DE PRODUCTOS O SERVICIOS DE AVAYA POR PARTE DEL SOCIOS DE CANAL DE AVAYA. EL PRODUCTO O EL SERVICIO ALOJADO PUEDE UTILIZAR COMPONENTES DE TERCEROS SUJETOS A TÉRMINOS DE TERCEROS Y REQUIERE QUE UN PROVEEDOR DE SERVICIOS TENGA UNA LICENCIA INDEPENDIENTE DIRECTAMENTE DEL PROVEEDOR DE TERCEROS. EL ALOJAMIENTO DE PRODUCTOS DE AVAYA POR PARTE DE UN SOCIO DE CANAL DE AVAYA DEBE SER AUTORIZADO POR ESCRITO POR AVAYA Y SI DICHOS PRODUCTOS ALOJADOS UTILIZAN O INTEGRAN DETERMINADO SOFTWARE DE TERCEROS, INCLUYENDO, ENTRE OTROS, SOFTWARE O CÓDECS DE MICROSOFT, EL SOCIO DE CANAL DE AVAYA DEBE
OBTENGA DE FORMA INDEPENDIENTE CUALQUIER ACUERDO DE LICENCIA CORRESPONDIENTE, POR CUENTA DEL SOCIO DE CANAL DE AVAYA, DIRECTAMENTE DEL PROVEEDOR TERCERO CORRESPONDIENTE.

CON RESPECTO A LOS CÓDECS, SI EL SOCIO DE CANAL DE AVAYA ALOJA CUALQUIER PRODUCTO QUE UTILICE O INTEGRA EL CÓDEC H.264 O EL CÓDEC H.265, EL SOCIO DE CANAL DE AVAYA RECONOCE Y ACEPTA QUE EL SOCIO DE CANAL DE AVAYA ES RESPONSABLE DE TODAS LAS TARIFAS RELACIONADAS Y/O O REGALÍAS. EL CÓDEC H.264 (AVC) TIENE LICENCIA BAJO LA LICENCIA DE LA CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS EN LOS QUE NO RECIBE REMUNERACIÓN PARA: (I) CODIFICAR VÍDEO DE CONFORMIDAD CON EL ESTÁNDAR AVC (“AVC VIDEO ”) Y/O (II) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO CON LICENCIA PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL PARA LOS CÓDECS H.264 (AVC) Y H.265 (HEVC) DE MPEG LA, LLC VERHTTP://WWW.MPEGLA.COM .

De acuerdo con las leyes

Usted reconoce y acepta que es su responsabilidad cumplir con las leyes y reglamentaciones aplicables, incluidas, entre otras, las leyes y reglamentaciones relacionadas con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude y los derechos de interpretación musical, en el país o territorio donde se utiliza el producto Avaya.

Prevención del fraude de llamadas

El "fraude interurbano" es el uso no autorizado de su sistema de telecomunicaciones por parte de una parte no autorizada (por ejemplo, una persona que no es un empleado corporativo, agente, subcontratista o que no trabaja en nombre de su empresa). Tenga en cuenta que puede haber un riesgo de fraude de llamadas asociado con su sistema y que, si ocurre, puede resultar en cargos adicionales sustanciales para sus servicios de telecomunicaciones.

Intervención de fraude de llamadas de Avaya

Si sospecha que está siendo víctima de fraude de llamadas y necesita asistencia o soporte técnico, llame a la línea directa de intervención de fraude de llamadas del Centro de Servicio Técnico al +1-800-643-2353 para los Estados Unidos y Canadá. Para obtener números de teléfono de soporte adicionales, consulte el sitio web de soporte de Avaya:https://soporte.avaya.com o el sitio sucesor designado por Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de soporte de seguridad de Avaya en la sección Políticas de seguridad y soporte dehttps://support.avaya.com/security .

Las sospechas de vulnerabilidades de seguridad de productos de Avaya se manejan según el Flujo de soporte de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Descarga de documentación

Para obtener las versiones más recientes de la documentación, consulte el sitio web de soporte de Avaya:https://soporte.avaya.com , o el sitio sucesor designado por Avaya.

Comuníquese con el soporte de Avaya

Consulte el sitio web de soporte de Avaya:https://soporte.avaya.com para avisos y artículos sobre productos o Servicios alojados, o para informar un problema con su producto o Servicio alojado de Avaya. Para obtener una lista de números de teléfono y direcciones de contacto de soporte, vaya al sitio web de Soporte de Avaya:https://soporte.avaya.com (o el sitio sucesor designado por Avaya), desplácese hasta la parte inferior de la página y seleccione Contactar con el soporte de Avaya.

Marcas registradas

Las marcas comerciales, los logotipos y las marcas de servicio ("Marcas") que se muestran en este sitio, la Documentación, los Servicios alojados y los productos proporcionados por Avaya son Marcas registradas o no registradas de Avaya, sus afiliados, sus licenciantes, sus proveedores u otros terceros. Los usuarios no pueden usar dichas Marcas sin el consentimiento previo por escrito de Avaya o de un tercero que pueda ser propietario de la Marca. Nada de lo contenido en este sitio, la Documentación, los Servicios alojados y los productos debe interpretarse como una concesión, por implicación, impedimento legal o de otro modo, de cualquier licencia o derecho sobre las Marcas sin el permiso expreso por escrito de Avaya o el tercero aplicable.

Avaya es una marca registrada de Avaya Inc.

Todas las marcas comerciales que no son de Avaya son propiedad de sus respectivos dueños. linux®es la marca registrada de Linus Torvalds en los EE. UU. y otros países.

Contenido

Capítulo 1 Introducción..... 7
Objetivo..... 7
Cambia la historia..... 7
Capítulo 2: Oficina IP de Avaya™Descripción general de la plataforma..... 10
Ediciones de IP Office..... 10
Nuevo en esta versión..... 11
Características..... 13
Topología..... 14
Redes..... 14
Redes de voz conmutadas por circuito privado..... 14
Redes de voz públicas..... 15
Redes de voz y datos basadas en paquetes..... 18
Telefonía con protocolo de Internet..... 19
Integración de telefonía informática..... 27
Componentes..... 29
Componentes de hardware..... 29
Los telefonos..... 38
Aplicaciones de IP Office..... 40
Capítulo 3: Especificaciones de la solución..... 67
Configuraciones de referencia..... 67
Ediciones de IP Office..... 67
Otras opciones de implementación..... 73
Opciones de hardware y software..... 84
Especificaciones del servidor..... 85
Compatibilidad con el sistema operativo y el navegador..... 87
Requisitos de PC proporcionados por el cliente..... 91
Requisitos del entorno virtual..... 93
Interoperabilidad..... 93
Interoperabilidad del teléfono..... 95
IP Office y Avaya Aura®Interoperabilidad de Communication Manager..... 99
Interoperabilidad de BCM e IP Office..... 100
Especificación de seguridad..... 101
Detalles de seguridad de la plataforma y la aplicación..... 102
Asignaciones de puertos..... 105
Rutas de actualización típicas..... 106
Migración de BCM con CS1000 a IP Office..... 107
Migración de sucursales de IP Office..... 108
Licencias..... 109
Licencias PLDS..... 109

Migración de licencias ADI..... 110
Licenciamiento centralizado y nodal de Server Edition..... 111
Licencia de edición básica para nuevos sistemas..... 118
Licencias Essential Edition y Preferred Edition..... 118
Licencias de la edición del servidor..... 119
Licencias de sucursal 120
Licencias de Redes Comunitarias Pequeñas 120
Licencias troncales..... 121
Licencias de usuario..... 122
Licencias de punto final de IP..... 126
Licencias de prueba..... 126
Licencias de actualización..... 127
Capítulo 4: Recursos..... 130
Documentación..... 130
Búsqueda de documentos en el sitio web de soporte de Avaya..... 131
Capacitación..... 131
Visualización de videos de orientación de Avaya..... 132
Recursos adicionales de IP Office 133
Compatibilidad del producto..... 133
Apoyo..... 133
Uso de la base de conocimientos de Avaya InSite..... 134
Acceso a las notas de la aplicación Avaya DevConnect 134
lista del glosario..... 136

Capítulo 1 Introducción

Objetivo

Este documento describe IP Office desde una perspectiva holística que se centra en las vistas estratégica, empresarial y funcional de la arquitectura. Este documento también incluye una descripción de alto nivel de las especificaciones de la solución y las configuraciones de referencia disponibles.

Cambia la historia

La siguiente tabla describe los principales cambios realizados en este documento para cada versión.

Tema	Fecha de lanzamiento	Resumen de Cambios
Versión 11.0 FP4	febrero 2019	• Se actualizó el tema Novedades con las funciones de la versión 11.0 FP4. • Avaya Equinox actualizado™tema para agregar contenido en Shared Control y Avaya Vantage™apoyo. • Avaya one-X actualizado®Tema del portal para agregar mejoras de capacidad de servicio. • Se actualizó la información de licencias. • Se actualizó la sección de navegadores compatibles. • Se actualizó la sección Media Manager para agregar nuevas funciones admitidas en la versión 11.0 FP4 de IP Office. • Incluyó VMWare ESXi 6.7 como hipervisor compatible.

La tabla continúa...

Tema	Fecha de lanzamiento	Resumen de Cambios
Versión 11.0	mayo 2018	• Se actualizó el tema Novedades con las funciones de la versión 11.0. • Se eliminaron las referencias a IP Office Integrated Contact Reporter. • Se eliminaron las referencias a IP Office Video SoftPhone, ya que no es compatible con la versión 11.0. • Contenido agregado sobre las siguientes aplicaciones: - Gerente de Operaciones en la Nube - Equinoccio de Avaya™cliente para IP Office - Cliente web Avaya IP Office • Se actualizó la sección Administrador web para agregar contenido sobre el Panel de configuración. • Se actualizó la sección Media Manager para agregar nuevas funciones compatibles con la versión 11.0 de IP Office. • Se agregaron los teléfonos J169 y J179 a las secciones de interoperabilidad y disponibilidad de teléfonos.
Versión 10.1, Número 1	junio 2017	• Se actualizó la sección "Novedades en esta versión". • Información agregada sobre dos nuevas aplicaciones: IP Office Integrated Contact Reporter e IP Office Media Manager • Se agregó información sobre la compatibilidad con hipervisores adicionales en la sección "Requisitos del entorno virtual". • Información agregada sobre dos nuevos teléfonos DECT: 3730 y 3735 • Se agregó información sobre una nueva API/SDK de administración y dos nuevas interfaces de CTI: API de servicio web de CTI centralizado y SSI sobre servicios web. • Información agregada sobre dos nuevos módulos de expansión: DS16B2 y DS30B2 • Se agregó información de acceso granular en la sección "Administrador web". • Información de extensión agregada en la sección "Solicitud de estado del sistema (SSA)" • Se actualizó la sección "Sistema operativo y compatibilidad con navegadores"

La tabla continúa...

Tema	Fecha de lanzamiento	Resumen de Cambios
Versión 10.0, Número 1	julio de 2016	• Se actualizó la sección "Novedades en esta versión". • Se reemplazaron las referencias del teléfono 3740 DECT con 3745 DECT. • Contenido actualizado de Avaya Contact Center Select. • Hizo las siguientes actualizaciones importantes de licencias: - Se agregó más información contextual. - Nombres de licencia actualizados y sus códigos asociados. - Contenido de licencias de Server Edition reorganizado. - Se agregaron licencias de la Edición Básica. - Soporte de licencia de usuario básico aclarado.
Versión 9.1, Problema 01.18	febrero 2016	Este documento fue creado para reemplazar el*Descripción del producto Avaya IP Office*.

Capítulo 2: Oficina IP de Avaya™Plataforma

visión general

La oficina IP de Avaya™Platform es un sistema de telefonía rentable que admite una fuerza de trabajo móvil y distribuida con voz y video en prácticamente cualquier dispositivo. IP Office es una solución de comunicaciones modular e integrada que se amplía hasta 3000 extensiones y 150 sitios en una red multisitio con resiliencia. Haga coincidir un modelo de implementación con las necesidades de infraestructura, desde dispositivos simples hasta software virtualizado en un centro de datos con opciones intermedias. Mejore la experiencia del cliente y la eficiencia de los agentes del centro de contacto con una potente y asequible funcionalidad multicanal para voz, correo electrónico y chat web. La solución combina software de colaboración más centros de contacto multicanal, redes, seguridad y video.

IP Office proporciona un PBX híbrido con multiplexación por división de tiempo (TDM) y telefonía IP con compatibilidad con troncales, que se usan en cualquiera de los dos modos o en ambos al mismo tiempo. IP Office tiene capacidades de datos integradas, que brindan enrutamiento IP, conmutación y protección de firewall, entre LAN y WAN (LAN2).

Además de los servicios básicos de telefonía y correo de voz, IP Office ofrece opciones de telefonía fija y virtual. Las aplicaciones de softphone están diseñadas para brindar flexibilidad a los trabajadores remotos y permitirles acceder a servicios de telefonía, como hacer y recibir llamadas, correo de voz y desvío de llamadas desde su computadora o dispositivo móvil.

Ediciones de IP Office

IP Office también ofrece funciones avanzadas como conferencias de audio y video y voz sobre IP para satisfacer las necesidades cambiantes de las pequeñas, medianas y grandes empresas.

IP Office está disponible en muchos modelos de implementación según el tamaño de la empresa y las funciones requeridas mediante uno o todos los siguientes elementos:

- Software IP Office virtualizado que se ejecuta en una máquina virtual
- Servidor dedicado
- Unidad de control IP Office 500 V2 (IP500 V2)

Edición	Plataforma	tamaño de la empresa (usuarios)	Aborda las necesidades comerciales
Edición básica	IP500 V2	menos de 25	Capacidades simples de telefonía y mensajería solamente
Edición esencial	IP500 V2	20–99	Capacidades simples de telefonía y mensajería más telefonía IP con movilidad esencial
Edición preferida	IP500 V2	21–250	Capacidades de Essential Edition más comunicaciones unificadas con movilidad preferida
Edición del servidor	servidor linux, IP500 V2 y Expansión Linux	100 — 2000	Preferred Edition en una solución basada en software.
Seleccionar IP Office	servidor linux, IP500 V2 y Expansión Linux	100 — 3000	Preferred Edition en una solución basada en software con mayor escala y resiliencia.
Server Edition o IP Office Select con Software virtualizado	virtualizado	100 — 2000 (o) 100 — 3000	Preferred Edition en una solución basada en software con mayor escala y resiliencia.
Server Edition o IP Office Select alojado en la nube	Potencializado por la nuve por Avaya)	100–2000 (o) 25–3000	Preferred Edition en una solución basada en software con mayor escala y resiliencia.

IP Office Essential Edition y Preferred Edition también se denominan Modo estándar de IP Office. Cada edición se basa en la siguiente para ofrecer funcionalidad adicional.

Nuevo en esta versión

Oficina de PI™Platform Release 11.0 Feature Pack 4 ofrece las siguientes características y capacidades nuevas:

Nota:

Las funciones están disponibles en todo el mundo a menos que se especifique lo contrario. No todas las funciones son compatibles con todas las plataformas y teléfonos. Vea las descripciones para más detalles.

Hermanamiento alternativo

Con esta función, IP Office redirige las llamadas al número de teléfono móvil hermanado de los usuarios cuando no se puede acceder a las extensiones principales, incluso si la hermanación móvil está deshabilitada. Esta función proporciona un mecanismo para la conmutación por error a un dispositivo externo, como un dispositivo móvil y PSTN, si el sitio de un cliente que admite teléfonos IP Office pierde la conectividad con el centro de datos en la nube. Los siguientes dos códigos cortos están disponibles para deshabilitar y habilitar el hermanamiento alternativo móvil:

- **Desactivar el hermanamiento alternativo**: para deshabilitar el hermanamiento alternativo

- **Activar el hermanamiento alternativo**: Para habilitar el hermanamiento alternativo

Mejoras de IP Office Media Manager

Se agregaron las siguientes funciones a IP Office Media Manager:

- Eliminar grabaciones
- Registro de auditoría: los administradores pueden realizar un seguimiento del uso de los archivos de grabación en IP Office Media Manager. El siguiente tipo de uso de una grabación se puede rastrear usando esta característica:
  - Borrar
  - Descargar
  - Repetir
  - Búsqueda

Mejoras de seguridad para el registro de dispositivos SIP

Las nuevas mejoras de seguridad permiten a los administradores permitir o rechazar el registro de dispositivos SIP en IP Office en función de sus cadenas de Agente de usuario. Los administradores pueden usar los ajustes de configuración para agregar, modificar o eliminar cadenas de SIP User Agent en la lista negra de SIP UA, la lista blanca de SIP UA y la lista blanca de IP. Posteriormente, el**Agentes de usuario SIP permitidos**La configuración se puede utilizar para seleccionar qué agentes de usuario SIP pueden registrarse en IP Office.

Sincronización automática de usuarios con Avaya Spaces

Usuarios del sistema IP Office R 11.0 FP4 y detalles de usuario creados para Avaya Equinox™se puede sincronizar automáticamente con el servidor de Avaya Spaces. Para usar y recibir funciones adicionales de Avaya Spaces, los detalles de los usuarios configurados para Avaya Equinox™necesita usuarios coincidentes configurados en el servidor de Avaya Spaces. La sincronización se puede realizar de forma manual o automática.

Contraseña de extensión predeterminada

La contraseña de extensión predeterminada o PIN es diferente a la contraseña de usuario y es mucho más segura con un mínimo de nueve dígitos. Las implementaciones de IP Office R11.0 FP4 proporcionan un PIN de extensión predeterminado generado automáticamente de 10 dígitos, que se puede ver y modificar más adelante. Un ícono de ojo al lado del **Contraseña de extensión predeterminada**El campo en la interfaz de usuario se puede usar para ver la contraseña de extensión predeterminada existente.

Equinoccio de Avaya™soporte en Avaya Vantage™

Equinoccio de Avaya™es compatible con Avaya Vantage™teléfonos K165 y K175 en implementaciones de IP Office R 11.0 FP4.

Enrute las llamadas de troncales SIP entrantes en función de un encabezado SIP opcional

IP Office se puede configurar para usar el opcional**P-persona-llamada**encabezado en el mensaje SIP entrante para el enrutamiento de llamadas. IP Office lee elID de la parte llamada Pencabezado en el mensaje SIP y enruta las llamadas SIP entrantes en función de él.

Registradores SIP y H.323 deshabilitados por defecto

Para proteger IP Office R 11.0 FP4 de vulnerabilidades, el**H.323 Gatekeeper Habilitar**y**Habilitar registrador SIP**Los campos están deshabilitados por defecto. Cada vez que se agrega una nueva extensión H.323 o SIP y el registrador correspondiente no está habilitado, el sistema IP Office muestra un mensaje de error y solicita habilitar los campos. Cuando el soporte de resiliencia está habilitado en una línea de IP Office en sistemas que tienen extensiones de IP y los sistemas no tienen habilitados los registradores correspondientes,

El sistema IP Office muestra un mensaje de error y solicita a los administradores que habiliten los registradores correspondientes.

Equinoccio de Avaya™control compartido

Equinoccio de Avaya™ahora se puede usar en modo de control compartido con teléfonos de escritorio. La función de control compartido está disponible incluso cuando Avaya Equinox™los teléfonos cliente y de escritorio están registrados en diferentes sistemas dentro de la misma red.

Unirse a la conferencia

La función Unirse a la conferencia permite unir dos conferencias separadas en una sola conferencia que contiene a todos los participantes anteriores de ambas conferencias anteriores. Una vez que se han unido las conferencias, no es posible volver a las dos conferencias separadas nuevamente.

Compatibilidad con el módulo de 24 botones JEM en el teléfono IP Avaya J169/J179

Avaya J169/J179 IP Phone puede admitir hasta tres módulos de botones JEM24. Cada JEM24 tiene 24 botones de doble LED con pantalla de etiqueta de botón adyacente. Los LED de los botones se usan para indicar el estado de la función del botón, mientras que presionar el botón se usa para acceder a la función. Un solo JEM24 admite 72 espacios para botones programables. Estos están organizados en 3 páginas, a las que se accede mediante el botón de desplazamiento de página del módulo. Cuando se conectan varios módulos a un teléfono, cada módulo solo admite una sola página de 24 ranuras de botones programables.

Los módulos coinciden automáticamente con la configuración de pantalla del teléfono al que están conectados: color con Avaya J179 IP Phone o escala de grises con Avaya J169 IP Phone, tamaño de fuente, imagen de fondo, protector de pantalla. Los módulos de botones se alimentan a través del teléfono. Para obtener más información, consulte el*IP Office Platform R11.0 Guía del usuario del teléfono de la serie J100*.

Teléfono IP Avaya J139

Compatibilidad con IP Office para el teléfono IP Avaya J139. Avaya J139 IP Phone es un teléfono de escritorio SIP avanzado que admite la programación de botones y los menús interactivos de IP Office. Avaya J139 IP Phone no es compatible con todas las funciones avanzadas de trabajadores del conocimiento y centros de contacto que están disponibles en los teléfonos Avaya J169 IP Phone y Avaya J179 IP Phone. Para obtener más información, consulte el*IP Office Platform R11.0 Guía del usuario del teléfono de la serie J100*.

Mejoras en la capacidad de servicio en Avaya one-X®Portal

Avaya one-X®Portal admite una serie de funciones de mantenimiento, como mostrar el recuento de sesiones iniciadas, el avatar del usuario, la opción para bloquear versiones de clientes, la opción para rastrear intentos de inicio de sesión fallidos repetidos y la opción para borrar todas las sesiones de un usuario.

Autoadministración web simplificada

La interfaz mejorada se enfoca en simplificar la configuración y hacerla más fácil para los usuarios no técnicos y proporciona un asistente autoguiado de tres pasos para configurar la cuenta básica. De manera predeterminada, la nueva capacidad, que ejecuta el asistente, está habilitada para todos los usuarios, pero el administrador puede deshabilitar la capacidad o modificarla según sea necesario.

Características

Ver*Oficina IP de Avaya™Característica de la plataforma Descripción*para obtener descripciones detalladas de las funciones.

Topología

Hay muchas opciones para la topología de IP Office. Para obtener información detallada sobre todos los escenarios de implementación, consulte el*Configuración de referencia*documentos para cada escenario de implementación.

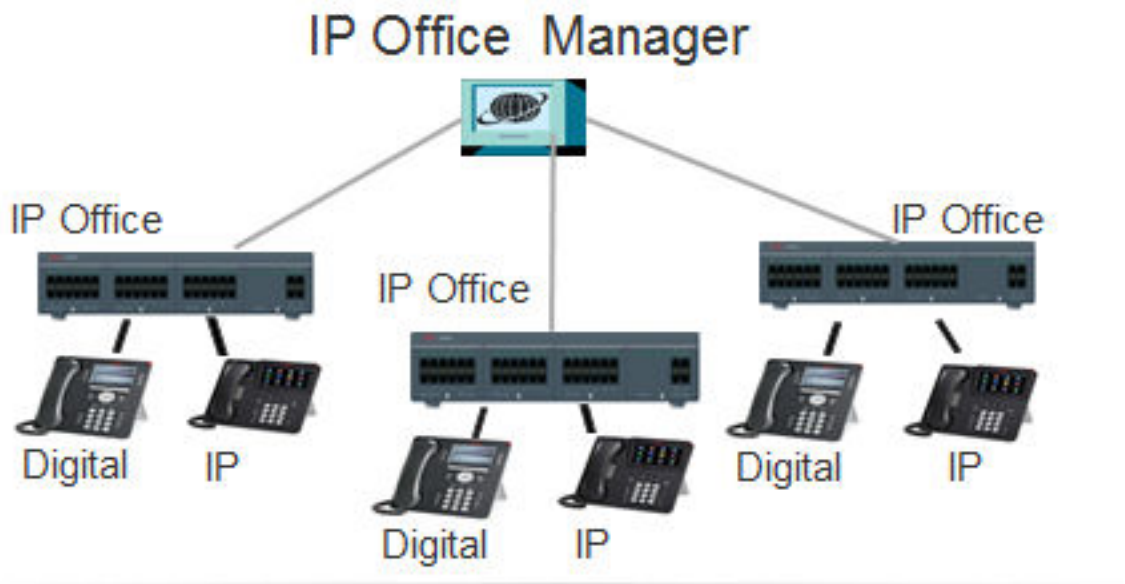


Figura 1: Sistemas IP Office conectados a un solo terminal de IP Office Manager

Redes

Redes de voz conmutadas por circuito privado

Cuando los circuitos de línea alquilada se usan en un escenario de red privada, estas interfaces E1 o T1 generalmente se configuran para usar señalización Q.SIG entre sitios.

Q.SIG proporciona un nivel de transparencia de funciones de voz entre PBX y es el estándar de señalización preferido dentro de múltiples proveedores y redes de voz internacionales. El módulo IP Office E1 o T1 termina una conexión QSIG con una interfaz RJ45 de 120 ohmios.

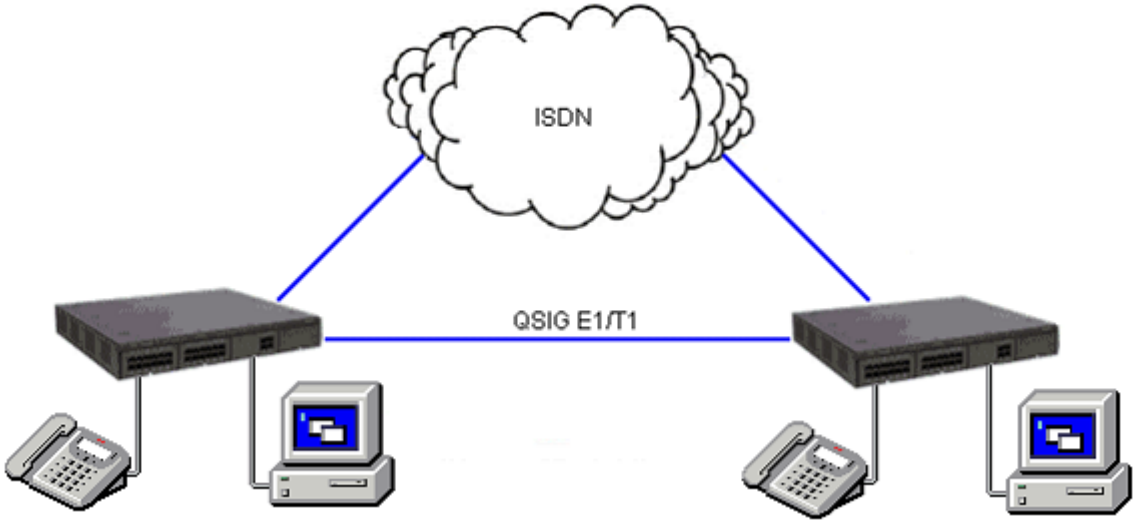


Figura 2: Redes de voz con conmutación de circuitos

IP Office admite los siguientes servicios Q.SIG en esta red: **Llamada de**

Telefonía Simple/Llamada Básica	ETS300 171/172
Llamada de datos con conmutación de circuitos/llamada básica	ETS300 171/172
Presentación de ID de línea llamada/llamante	ETS300 173
Presentación del llamado/nombre del llamante	(SS-CNIP, SS-CONP, SS-CNIR) ETS300 237/238
mensaje en espera	(SS-MWI) EN301 260/255
Transferir	(SS-CT) ETS 300 260/261

Redes de voz pública

IP Office admite una variedad de troncales y modos de señalización para la conexión a la red telefónica pública conmutada (oficina central). Algunas de estas líneas solo están disponibles en ciertos territorios; consulte con su distribuidor para conocer la disponibilidad local. Las troncales de tasa primaria están disponibles con una troncal simple (24/30 canales) o doble (48/60 canales).

Tarifa primaria ISDN (ETSI CTR4)

El servicio es provisto por tarjetas IP500V2 Universal PRI. ISDN Primary Rate proporciona 30 canales de voz PCM de 64K sobre un circuito E1 y un canal de señalización. Señalización Cumple con el estándar ETSI Q. 931 con verificación de errores de redundancia cíclica (CRC).

Se admiten los siguientes servicios complementarios:

línea de llamada Identificación Presentación (CLIP)	Proporciona el número de teléfono de la llamada entrante.
línea de llamada Identificación Restricción (CLIR)	Evita que se presente el número de teléfono de IP Office en una llamada saliente.
Marcación directa (DDI)	Donde el intercambio proporciona los últimos x dígitos del número marcado en una llamada entrante. Esto permite que IP Office enrute la llamada a diferentes usuarios o servicios.
subdireccionamiento	Permite la transmisión/recepción de hasta 20 dígitos, adicionales a cualquier información DDI/DID o CLIP, para fines de enrutamiento e identificación de llamadas.

IP Office admite las siguientes funciones en troncales PRI y BRI.

Nota:

La disponibilidad de funciones depende del proveedor de servicios ISDN por el cual puede haber cargos.

Llamada maliciosa Identificación (MCID)	(2400, 4600, 5400, 5600, T3, IP T3, 9500, 9600) Los códigos cortos y las funciones de programación de botones están disponibles para que los usuarios puedan activar esta actividad en el intercambio ISDN cuando sea necesario. Esta función NO está disponible en teléfonos ISDN DSS1 estándar.
Consejo de Cargo (COA)	(Solo teléfonos IP y digitales T3; Phone Manager) Se admite el aviso de cargo durante una llamada (AOC-D) y al final de una llamada (AOC-E) para llamadas ISDN salientes que no sean Q.SIG. El costo de la llamada se puede mostrar en los teléfonos T3 para fines de contabilidad de llamadas. IP Office permite la configuración de la moneda del costo de la llamada y un recargo del costo de la llamada para cada usuario.
Finalización de llamadas ocupado Abonado (CCBS)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, teléfonos DECT; Phone Manager) CCBS se puede utilizar cuando lo proporcione el proveedor de servicios ISDN. Permite establecer una devolución de llamada en llamadas RDSI externas que regresan ocupadas. También se puede utilizar para llamadas ISDN entrantes a un usuario ocupado. Esta función no está disponible en teléfonos ISDN DSS1 estándar.
Cambio de ruta parcial (PR)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, teléfonos DECT; Phone Manager) Al reenviar una llamada en un canal ISDN a un número externo mediante otro canal ISDN, el reenrutamiento parcial informa a la central ISDN que realice el reenvío, liberando así los canales a IP Office. Esta función no está disponible en teléfonos estándar ISDN DSS1 y no es compatible con Q.SIG.

Llamada explícita Transferencia (TEC)	(Usado normalmente por una aplicación de terceros) ECT es compatible con la interfaz S0. Una llamada a un terminal S0 se puede transferir a cualquier otro dispositivo, como un terminal analógico, digital o IP, o a cualquier troncal. El uso normal de esta función es por parte de una aplicación de terceros conectada a través de una o más interfaces S0 a IP Office. Un ejemplo es VoiceDirector, un asistente automático de llamadas.

Tarifa básica RDSI (ETSI CTR3)

El servicio es proporcionado por tarjetas IP500 V2 BRI. ISDN Basic Rate proporciona 2 canales de voz PCM de 64K y un canal de señalización mediante señalización Q.931 y comprobación de errores CRC. Se admite la operación punto a punto y punto a multipunto. Las líneas multipunto permiten que múltiples dispositivos compartan la misma línea; sin embargo, punto a punto es el modo preferido.

La tarifa básica admite todos los servicios que se admiten en la versión de tarifa principal con la adición de número de suscriptor múltiple. Este servicio suele ser mutuamente excluyente con el servicio DDI/DID y proporciona hasta 10 números para propósitos de enrutamiento, muy similar a DDI/DID.

Señalización asociada al canal E1R2

El servicio es proporcionado por tarjetas IP500 V2 Universal PRI.

La tarjeta IP500 Universal PRI configurada como PRI E1R2 admite una conexión de red RJ45 simple o doble. Cada tarjeta proporciona canales que se pueden configurar para marcación MFC, Pulse o DTMF según los requisitos de la red.

Tarifa primaria T1 norteamericana

El servicio es proporcionado por tarjetas IP500 V2 Universal PRI. T1 Primary Rate proporciona hasta 24 canales de 64K en un circuito de 1,54M. Cada canal del troncal T1 puede configurarse (canalizarse) de forma independiente para admitir las siguientes emulaciones de señalización con tipos de protocolo de enlace inmediato, retardado o parpadeante.

- Inicio de bucle
- Inicio en tierra
- Línea de enlace E&M
- E&M HIZO
- E&M conmutado 56K
- DID: los canales configurados para DID/DDI solo admiten llamadas entrantes. El operador o la oficina central proporcionará los últimos x dígitos que se marcaron para que se utilicen para el enrutamiento de llamadas.
- Guiño-Inicio

Las troncales T1 de IP Office admiten servicios DNIS y ANI, cuando estén disponibles en la oficina central.

Número marcado Cadena de identificación (DNIS)	Proporciona una cadena de dígitos a IP Office según el número marcado por la persona que llama. Esta cadena se puede usar para enrutar a las personas que llaman a extensiones, grupos o servicios individuales.
Número automático Identificación (ANI)	Proporciona a IP Office un número que identifica quién es la persona que llama. Esto puede usarse para enrutamiento o aplicaciones de telefonía informática.

Las tarjetas de troncales T1 incorporan una CSU/DSU integral, lo que elimina la necesidad de una unidad externa. La función CSU permite que la troncal se ponga en modo de bucle invertido para fines de prueba. Esto se puede configurar

manualmente, usando la aplicación de monitoreo, o automáticamente desde una Oficina Central enviando un patrón de Line Loop Back (LLB). La función DSU permite compartir el troncal T1 entre los servicios de datos y de voz.

Interfaz de velocidad primaria de América del Norte (PRI)

El servicio es proporcionado por las tarjetas IP500V2 Universal PRI. IP Office es compatible con troncales ISDN de tasa primaria en conmutadores de oficina central 5ESS o DMS100 proporcionados por AT&T, Sprint, WorldCom y otras empresas de telecomunicaciones locales. Los canales pueden configurarse previamente para los servicios admitidos o negociarse llamada por llamada.

Se pueden configurar servicios especiales para enrutar llamadas a operadores locales o proveedores pre-suscritos para llamadas nacionales e internacionales (SSS). También se pueden seleccionar operadores alternativos a través de la configuración de las tablas de selección de red de tránsito (TNS) de IP Office.

IP Office también es compatible con el servicio de nombre y número de llamada a través de troncales de velocidad primaria (NI2).

Troncales analógicos

Círculo comienzo Las troncales de inicio de bucle están disponibles en las tarjetas de troncales analógicas de IP Office instaladas dentro de la unidad de control de IP Office o en los módulos de expansión de 16 puertos de troncales analógicas (ATM16). Los primeros dos troncales en el ATM16 se cambian automáticamente a enchufes de falla de energía en caso de que se interrumpa la energía. Powerfail también está disponible en la tarjeta de troncales cuando se instala en una tarjeta combinada o telefónica. Cumplen con el estándar TIA/EIA-646-B. Los troncales de inicio de bucle también admiten la identificación de línea de llamadas entrantes (ICLID) conforme a los estándares GR-188-CORE y GR-31-CORE. IP Office puede usar esta información para enrutar llamadas o proporcionarla a aplicaciones informáticas para mostrar información adicional sobre la persona que llama.

Terrestre comienzo Las troncales Ground Start solo están disponibles en el ATM16, configurado a través de IP Office Manager. Los dos primeros troncales del módulo se cambian automáticamente a la toma de corriente en caso de que se interrumpa la alimentación. Cumplen con las normas ANSI T1.401 y TIA/EIA-646-B. No disponible en todos los territorios.

Redes de voz y datos basadas en paquetes

IP Office admite el uso de la red de datos para la comunicación de voz, llamada voz sobre IP (VoIP).

IP Office admite comunicaciones de voz y datos en red con los siguientes servicios:

- Enrutador IP incorporado
- Un enlace para redes de voz y datos
- Acceso común a Internet; compartir archivos y enviar correos electrónicos a otros sitios
- Compatibilidad con el protocolo RIP-2 para el enrutamiento dinámico de datos; IPSec VPN, cortafuegos y NAT (traducción de direcciones de red) y para seguridad; Gestión centralizada y gestión proactiva de fallos a través de SNMP.

IP Office admite redes de voz basadas en paquetes IP entre sitios a través de VoIP en la LAN del campus o VoIP en la red pública.

En un entorno de fábrica o campus, las llamadas de voz se pueden enviar a través de conexiones LAN de 10/100 Mbps en sistemas equipados con módulos de compresión de voz (VCM) opcionales. IP Office es compatible con Diffserve al marcar adecuadamente tanto los paquetes RTP como los paquetes de señalización para facilitar la administración del ancho de banda de la red.

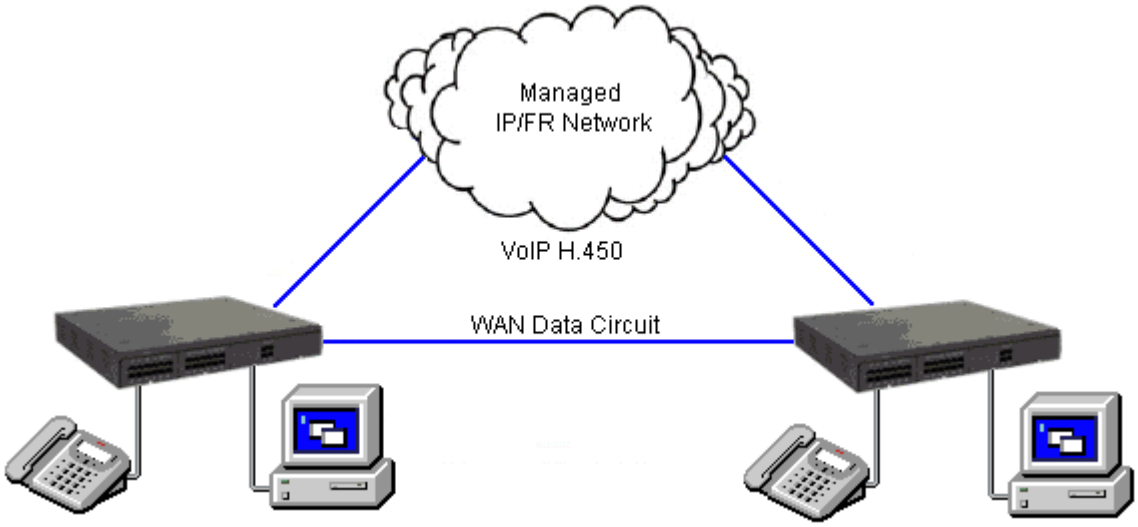


Figura 3: Red VoIP a través de una red IP o WAN

IP Office puede obtener los beneficios del soporte de servicios complementarios Q.931 y H.450 a través de una conexión pública donde se puede establecer una conexión QoS adecuada.

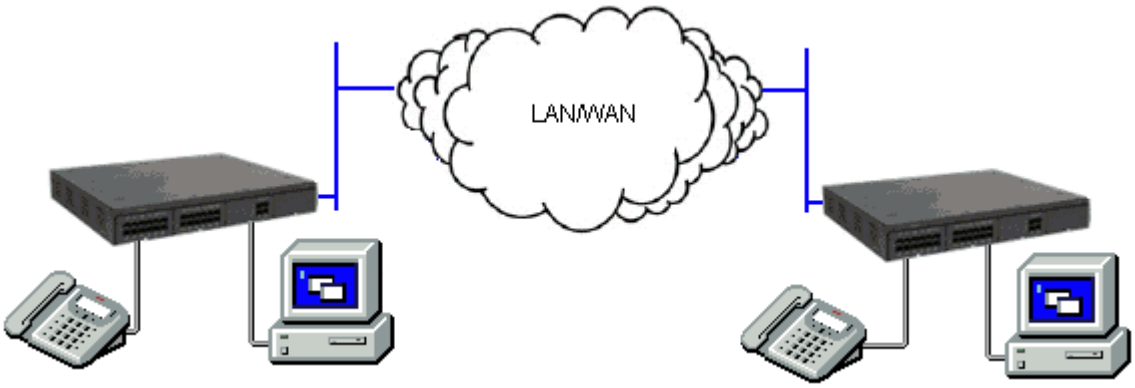


Figura 4: Red VoIP en la LAN

Telefonía con protocolo de Internet

El Protocolo de Internet (IP) se refiere al tipo de reglas que utiliza la red para enviar y recibir señales. La telefonía IP convierte las comunicaciones de voz en paquetes de datos. Convenientemente, funciona con tecnología Ethernet LAN (red de área local). La telefonía IP une las muchas ubicaciones de una empresa, incluidos los trabajadores móviles, en una única red de comunicaciones convergente.

IP Office es un sistema de telefonía convergente; combina aspectos de los sistemas de telefonía PABX tradicionales y los sistemas de telefonía y datos IP. IP Office es compatible con PSTN, SIP, POT, hora digital

Teléfonos multiplexados de división y teléfonos IP digitales todos en el mismo sistema. IP Office permite que todas las tecnologías coexistan.

IP Office se conecta a la PSTN ya los troncales IP proporcionando una función PABX "híbrida", donde las tecnologías heredadas y futuras se pueden usar juntas para minimizar los costos operativos y optimizar las comunicaciones comerciales a través de voz y datos. La funcionalidad convergente funciona en múltiples niveles:

- Los usuarios de teléfonos individuales pueden controlar el funcionamiento de su teléfono a través de aplicaciones que se ejecutan en su PC.
- El tráfico de datos se puede enrutar desde la interfaz LAN a una interfaz troncal de telefonía.
- El tráfico de voz se puede enrutar a través de enlaces de datos internos y externos. Esta opción se conoce como voz sobre IP (VoIP).

Voz sobre IP (VoIP) y evaluaciones de red

Voz sobre IP (VoIP) significa voz transmitida a través de una red de paquetes de datos. VoIP a menudo se denomina telefonía IP porque utiliza los protocolos de Internet para posibilitar comunicaciones de voz mejoradas dondequiera que existan conexiones IP.

El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas de clientes y/o teléfonos IP H.323 o SIP para usuarios. En cualquier caso, se deben considerar los siguientes factores:

- La unidad de control de IP Office debe estar equipada con canales de compresión de voz. Estos se utilizan cuando un dispositivo IP (troncal o extensión) necesita comunicarse con un dispositivo que no es IP (troncal o extensión) o con un dispositivo que utiliza un códec diferente.
- Una evaluación de la red es un requisito obligatorio para todos los sistemas que utilizan VoIP. Para problemas de soporte con VoIP, Avaya puede solicitar acceso a los resultados de la evaluación de la red y puede rechazar el soporte si no están disponibles o no son satisfactorios.

Una evaluación de la red incluiría una determinación de lo siguiente:

- Una auditoría de red para revisar el equipo existente y evaluar sus capacidades, incluida su capacidad para satisfacer las necesidades de voz y datos actuales y planificadas.
- Una determinación de los objetivos de la red, incluido el tipo de tráfico dominante, la elección de tecnologías y el establecimiento de objetivos de calidad de voz.
- La evaluación debe dejarle la confianza de que la red implementada tendrá la capacidad para el tráfico de voz y datos previsto, y puede admitir H.323, DHCP, TFTP y búferes de fluctuación en aplicaciones H.323.

Un resumen de los objetivos esperados de la evaluación de la red es:

Prueba	Objetivo mínimo de evaluación
Latencia	Menos de 150ms
Paquete perdido	Menos de 3%
Duración	Supervise las estadísticas una vez cada minuto durante una semana completa

Protocolos de señalización

Para hacer uso de VoIP, IP Office utiliza protocolos de señalización llamados H.323 y Protocolo de inicio de sesión (SIP), para establecer conexiones de extremo a extremo para la ruta de voz a través de una red IP. Este

Página570 de 3226.

La conexión garantiza que cada extremo pueda transmitir y recibir voz y proporciona el direccionamiento de red para la transmisión de paquetes de extremo a extremo. IP Office también conecta las diferentes tecnologías al traducir las señales que utilizan. Por ejemplo, un teléfono analógico puede conectarse a un destino de VoIP. Esta conexión requiere que se traduzcan tanto la señalización como la transmisión de voz. IP Office realiza esta traducción mediante puertas de enlace y guardianes.

Con la telefonía IP se conecta un teléfono IP a una IP PBX a través de una LAN. Hay dos tipos básicos de teléfonos IP:

- Un teléfono físico, que se parece mucho a un teléfono estándar, denominado "teléfono fijo"
- Una aplicación de software, denominada "softphone", que se ejecuta en la PC del usuario y le permite usar un auricular y un micrófono para realizar y recibir llamadas en cualquier lugar donde tenga una conexión IP.

Consideraciones de calidad de servicio

Al hacer uso de la telefonía IP, hay una serie de consideraciones centradas en los datos, como qué tipos de datos tienen prioridad en la red IP cuando hay contención. Esto se configura con calidad de servicio IP/TCP y no debe ignorarse. En situaciones en las que el ancho de banda de la LAN es limitado, se debe utilizar un conmutador de LAN con capacidad de calidad de servicio para garantizar que los paquetes de voz se transmitan con la prioridad requerida en la red. De lo contrario, la conversación transmitida a través de IP parece interrumpida debido a retrasos o se han introducido retrasos inaceptables en la conversación que causan latencia y fluctuación. Con los teléfonos fijos IP, existe la necesidad de alimentación a través de Ethernet (PoE), o suministros de energía telefónicos locales para los teléfonos, ya que los teléfonos IP no reciben alimentación de IP Office.

Canales de compresión de voz

Las llamadas hacia y desde dispositivos IP pueden requerir la conversión al formato de códec de audio que utiliza el dispositivo IP. Los sistemas IP Office utilizan canales de compresión de voz para realizar la conversión. Estos canales admiten los códecs de audio IP comunes G.711, G.723 y G.729a.

La aplicación de estado del sistema se puede usar para mostrar el uso del canal de compresión de voz. Dentro de**Recursos**sección muestra el número de canales en uso. También muestra con qué frecuencia ha habido canales insuficientes disponibles y la última vez que ocurrió tal evento.

Tabla 1: Canales de compresión de voz

Tipo de llamada	Uso del canal de compresión de voz
Dispositivo IP a dispositivo no IP	Requiere un canal de compresión de voz durante la duración de la llamada. Si no hay ningún canal disponible, la indicación de ocupado se devuelve a la persona que llama.

La tabla continúa...

Tipo de llamada	Uso del canal de compresión de voz
Dispositivo IP a dispositivo IP	Los tonos de progreso de llamada (por ejemplo, tono de marcado, tono de marcado secundario, etc.) no requieren canales de compresión de voz con las siguientes excepciones: • Los tonos de confirmación de código corto, activación de ARS y entrada de código de cuenta requieren un canal de compresión de voz. • Los dispositivos que utilizan G723 requieren un canal de compresión de voz para todos los tonos excepto para llamada en espera. Cuando se conecta una llamada: • Si los dispositivos IP utilizan el mismo códec de audio, no se utiliza ningún canal de compresión de voz. • Si los dispositivos usan diferentes códecs de audio, se requiere un canal de compresión de voz para cada uno.
Dispositivo no IP a dispositivo no IP	No se requieren canales de compresión de voz.
Música en espera reproducida en dispositivo IP	Se proporciona desde el bus TDM y, por lo tanto, requiere un canal de compresión de voz cuando se reproduce en un dispositivo IP.
Recursos de la conferencia y dispositivos IP	Gestionado por el chip de conferencia que está en el bus TDM. Por lo tanto, se requiere un canal de compresión de voz para cada dispositivo IP involucrado en una conferencia. Esto incluye servicios que usan recursos de conferencia como escucha de llamadas, intrusión, grabación de llamadas y monitoreo silencioso.
Llamada de buscapersonas a dispositivo IP	Utiliza G729a para llamadas de buscapersonas, por lo que solo requiere un canal, pero también solo admite búsquedas a dispositivos compatibles con G729a.
Servicios de correo de voz y dispositivos IP	Se tratan como llamadas de datos desde el bus TDM. Por lo tanto, las llamadas desde un dispositivo IP al correo de voz requieren un canal de compresión de voz.
Llamadas de fax	Estas son llamadas de voz pero con un rango de frecuencia ligeramente más amplio que las llamadas de voz habladas. IP Office solo admite fax a través de IP entre sistemas IP Office con la opción de transporte de fax seleccionada. Actualmente no es compatible con T38.
Llamadas de fax T38	IP Office admite fax T38 en troncales SIP y extensiones SIP. Cada llamada de fax T38 utiliza un canal VCM. Dentro de una red comunitaria pequeña, una llamada de fax T38 se puede convertir en una llamada a través de líneas SCN H323 utilizando el protocolo de soporte de transporte de fax de IP Office. Esta conversión utiliza 2 canales VCM. Para utilizar la conexión de fax T38, se puede configurar la Clasificación de equipo de una extensión analógica conectada a una máquina de fax. Además, está disponible una nueva función de código corto Marcar fax.

Nota:

Los dispositivos IP T3 deben configurarse con un tamaño de paquete de 20 ms para que se apliquen las condiciones anteriores. Si se deja configurado para un tamaño de paquete de 10 ms, se necesita un canal de compresión de voz para todos los tonos y para llamadas de medios no directos.

Protocolo de señalización H.323

Los sistemas de telefonía IP de IP Office utilizan estándares abiertos. Los teléfonos IP digitales, gateways y gatekeepers soportan el estándar H.323 y es este el que permite que dispositivos de diferentes

fabricantes a trabajar juntos. IP Office también es compatible con una puerta de enlace integral opcional, módulos de compresión de voz (VCM) y funcionalidad de controlador de acceso.

IP Office utiliza el protocolo de señalización H.323 mediante los siguientes componentes arquitectónicos:

telefonos ip	Dispositivos de extremo de servicio H.323 que admiten llamadas de audio. Otros tipos de dispositivos H.323 pueden admitir video como parte de H.323.
Pasarelas	Proporcione traducción de medios para permitir que se realicen llamadas a dispositivos que no sean H.323, por ejemplo, un teléfono analógico o la red pública para conectarse con un dispositivo H.323.
porteros	Controle el procesamiento de llamadas y la seguridad de los dispositivos H.323.
multipunto Unidades de conexión (MCU)	Controle las conferencias agregando flujos de medios.

Estos elementos forman una zona H.323 que es análoga a una PABX. Cada zona tiene un único gatekeeper para controlar la distribución de llamadas, el control de llamadas y la gestión de recursos. Al encenderse, los teléfonos IP, las puertas de enlace y las MCU realizan solicitudes de registro a un controlador de acceso que luego autentica (acepta o rechaza) la solicitud para convertirse en miembro de la zona. Una vez aceptado, un teléfono que desea realizar una llamada envía un mensaje de establecimiento de llamada al portero, que luego determina cómo enrutar la llamada y luego envía una alerta al teléfono llamado, o si la llamada es a un no-H. El teléfono 323 establece la llamada a través de un Gateway dentro de la zona.

Troncalización del protocolo de inicio de sesión

IP Office utiliza troncales del Protocolo de inicio de sesión (SIP) para permitir que los usuarios aprovechen los servicios de telefonía que ofrecen los proveedores de servicios de Internet (ISP). En muchos casos, los servicios de telefonía ofrecen ahorros sustanciales en comparación con las líneas de intercambio tradicionales. Para ayudar a habilitar el proveedor de servicios SIP, Avaya ofrece un programa de prueba de cumplimiento de SIP (GSSCP) que validará el funcionamiento de IP Office con la oferta de troncales SIP de los ISP. Para obtener más información sobre el Programa de prueba de cumplimiento de SIP (GSSCP) de Avaya, consulte https://www.devconnectprogram.com/site/global/compliance_testing/overview/index.gsp .

IP Office permite que todos los usuarios, independientemente de su tipo de teléfono, realicen y reciban llamadas SIP. Los troncales SIP se manejan como cualquier otra línea en IP Office, lo que brinda todo el enrutamiento de llamadas y el control de peaje necesarios para administrar las llamadas entrantes y salientes.

Los troncales SIP requieren el aprovisionamiento de canales de compresión de voz a través de la instalación de módulos VCM dentro de la unidad de control. También se necesita una licencia para el número máximo requerido de llamadas SIP simultáneas. Se admiten hasta 128 llamadas simultáneas.

IP Office también es compatible con el protocolo T38 que permite el envío de fax por IP.

Existen varias topologías de red posibles para los sistemas troncales SIP, como se muestra en los siguientes diagramas:

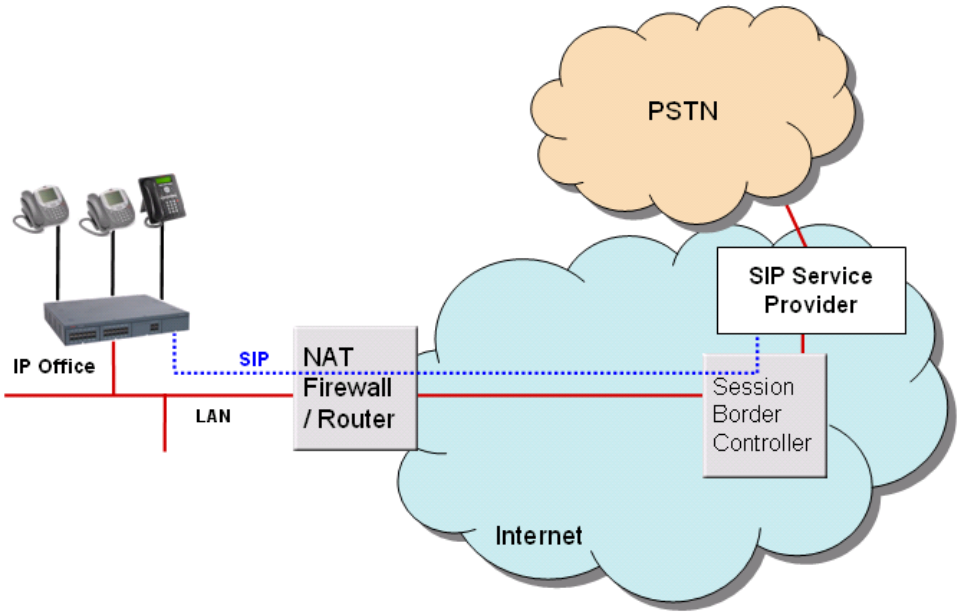


Figura 5: Proveedor de servicios con Avaya Session Border Controller for Enterprise (recomendado)

Para que esta configuración sea segura, el firewall de IP Office está configurado para descartar todos los paquetes excepto SIP.

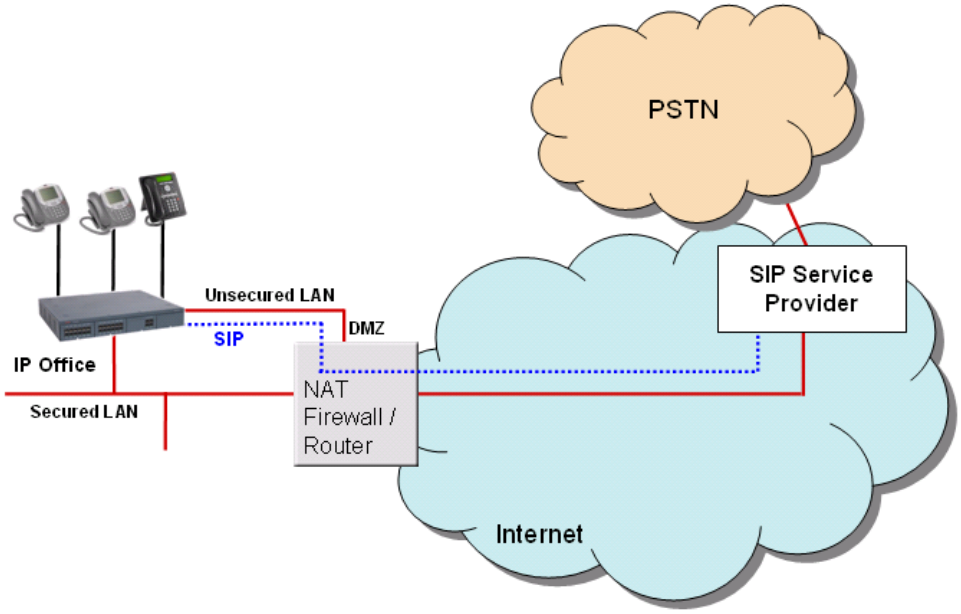


Figura 6: Conexión directa desde el segundo puerto Ethernet a Internet a través de un puerto DMZ en el enrutador

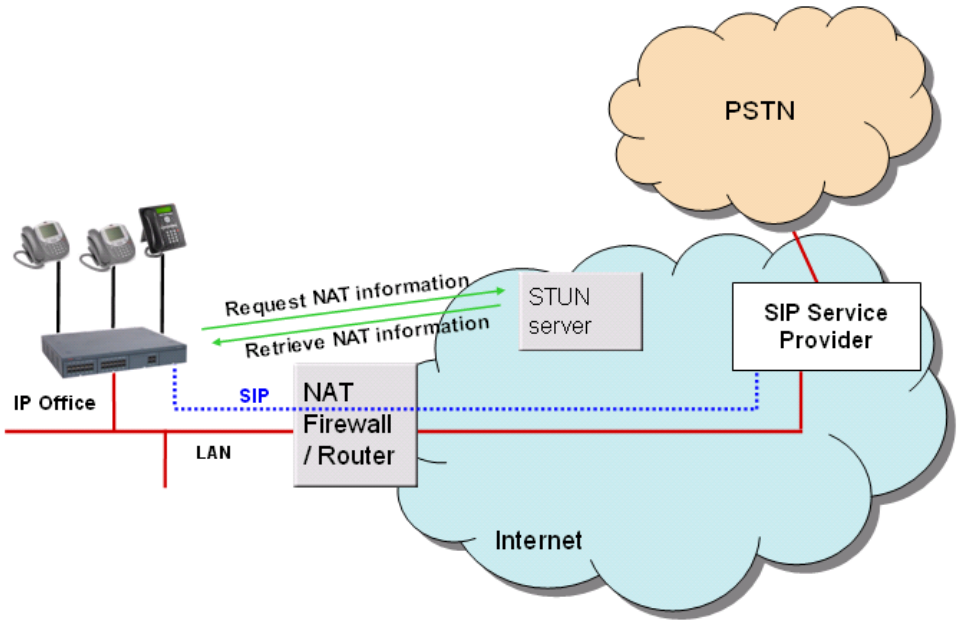


Figura 7: Conexión a ITSP sobre NAT utilizando servidores STUN de terceros

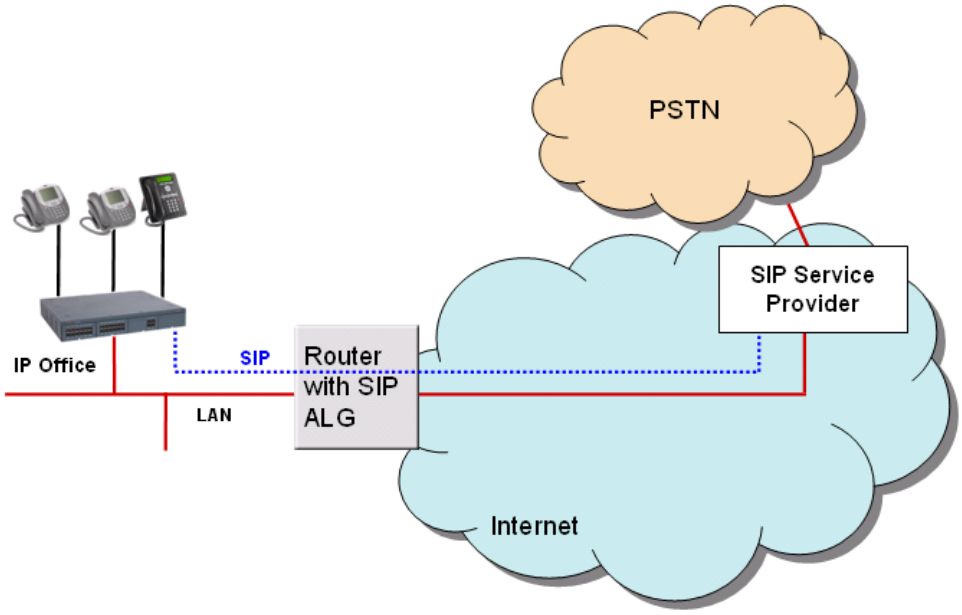


Figura 8: Conexión a ITSP a través del enrutador con ALG para resolver problemas de NAT

servidores SIP

La implementación del terminal SIP de IP Office se basa en dos componentes SIP principales: Componentes del servidor SIP Aplicaciones del agente de usuario del terminal SIP.

Los servidores SIP brindan compatibilidad con extremos SIP para permitir la interoperabilidad total entre extremos SIP, otros teléfonos IP basados en H.323, teléfonos digitales y analógicos, así como troncales de IP Office (analógicos, digitales o basados en SIP).

Los servidores SIP brindan información centralizada y servicios de habilitación en un ecosistema SIP. Los servidores SIP centrales y sus funciones se resumen aquí. IP Office proporciona las funciones de los siguientes dos servidores para comunicaciones de voz y fax.

- **servidor de registro**

  Cuando los teléfonos IP SIP se conectan, deben asegurarse de que los demás sepan que están disponibles para recibir y realizar llamadas. El registrador autentica y registra el teléfono IP (a menudo directamente relacionado con un usuario específico) cuando se conecta y luego almacena información sobre las identidades lógicas de los teléfonos.

- **Servidor proxy**

  Un servidor proxy toma las solicitudes SIP, las procesa y las pasa en sentido descendente mientras envía respuestas en sentido ascendente a otros servidores o dispositivos SIP. Un servidor proxy puede actuar como servidor y como cliente, y puede modificar una solicitud SIP antes de transmitirla. Un proxy solo participa en la configuración y finalización de una sesión de comunicación. Después de que los agentes de usuario establecen una sesión, las comunicaciones ocurren directamente entre las partes.

La funcionalidad de los siguientes dos servidores SIP generalmente está disponible para IP Office utilizando la funcionalidad existente de IP Office. Por lo tanto, si bien se proporciona la funcionalidad, por ejemplo, que permite compartir escritorios en una pequeña red comunitaria, se utiliza una metodología coherente entre los extremos SIP y no SIP para ofrecer esas funciones.

- **Servicio de localización**

  A medida que los usuarios se desplazan, la red debe estar continuamente al tanto de sus ubicaciones. El servicio de ubicación es una base de datos que realiza un seguimiento de los usuarios y sus ubicaciones. El servicio de ubicación obtiene su entrada del servidor de registro y proporciona información clave a los servidores proxy y de redirección. IP Office brinda soporte de escritorio compartido, brindando una funcionalidad similar pero trabajando consistentemente entre terminales SIP y no SIP.

- **servidor de redirección**

  Si los usuarios no están en sus dominios de origen, las sesiones vinculadas a ellos deben redirigirse a ellos.

  El servidor de redirección asigna una solicitud SIP destinada a un usuario al dispositivo más cercano al usuario. En IP Office, la función de desvío de llamadas y Sígueme se utiliza para brindar nuevamente una funcionalidad consistente entre todo tipo de terminales.

Agentes de usuario de punto final SIP

Los terminales SIP, como teléfonos SIP, teléfonos móviles, PDA o estaciones de trabajo, utilizan aplicaciones de agente de usuario (UA) para proporcionar la interfaz entre los usuarios y la red SIP.

La compatibilidad con terminales SIP está completamente integrada en IP Office. No se necesitan otros componentes. Los terminales SIP requieren la capacidad del módulo VCM como cualquier otro teléfono IP.

Las extensiones SIP funcionan como cualquier otra extensión de IP Office. IP Office proporciona la siguiente funcionalidad:

• Hacer y recibir llamadas a cualquier otra extensión, independientemente del tipo de extensión.

- Entregar medios de extremo a extremo. Durante las llamadas entre dos extensiones SIP o una extensión SIP y un teléfono IP de Avaya, IP Office transmite audio de extremo a extremo para llamadas telefónicas básicas. Las conferencias requieren un recurso de VCM.
- Utilice códigos cortos y códigos de autorización.
- Transmitir tonos de progreso de llamada en banda.
- Registrar punto final mediante autenticación con nombre de usuario y contraseña.
- Admite creación automática. El registro correcto de puntos finales utiliza una licencia de terceros.
- Varias extensiones pueden registrarse en una dirección IP, cada una usando una licencia. Esto permite la conexión de adaptadores de terminal SIP con más de un puerto analógico, dando un número de extensión diferente a cada puerto.

Integración de telefonía informática

Computer Telephony Integration (CTI) cierra la brecha entre el sistema telefónico y las aplicaciones comerciales. Con IP Office, esto se logra con IP Office CTI Link, un producto de middleware CTI y un kit para desarrolladores de software (SDK).

En IP Office, CTI se entrega mediante el cumplimiento de estándares abiertos. Esto brinda a las empresas acceso a una amplia gama de soluciones de terceros, dirigidas a mercados verticales y diseñadas para cumplir con sus requisitos. Para los desarrolladores, migrar su oferta desde otras plataformas a IP Office es rápido y fácil, y las funciones avanzadas de CTI que ofrece IP Office facilitan la demostración de la integración completa y más beneficios comerciales.

IP Office proporciona dos niveles de interoperabilidad de CTI:

Enlace CTI Lite	Gratis y proporciona toda la funcionalidad necesaria para admitir la gran mayoría de las aplicaciones, incluidas las pantallas emergentes y muchos productos de terceros.
Enlace CTI Pro	Brinda una funcionalidad mejorada, incluida la capacidad de controlar varios teléfonos y brinda acceso a la operación avanzada del centro de llamadas.

Debido a que las redes IP están integradas en el sistema IP Office, todo el CTI se realiza a través de la LAN. Esto introduce puntos adicionales de falla, además de depender de interfaces y teléfonos no estándar. En IP Office, todos los dispositivos se pueden usar con CTI.

Interfaces CTI compatibles

IP Office es compatible con las siguientes interfaces:

TAPI Link Lite	Proporciona compatibilidad con CTI de primera mano para Microsoft TAPI 2.1 y TAPI 3.0, por lo que cada PC puede controlar o monitorear un teléfono. Los componentes de software se suministran con el sistema IP Office en el CD del usuario y no requieren una clave de licencia para su uso. La especificación requiere que se implemente una cierta cantidad de funciones básicas y, además, define una serie de funciones opcionales que también pueden implementar los proveedores de conmutadores.

TAPI Link Pro

Proporciona compatibilidad con CTI de terceros para TAPI 2.1 y 3.0. Estos componentes son idénticos a su equivalente original; la presencia de la clave de licencia CTI Link Pro RFA (que se puede comprar de la forma habitual para los productos) habilita esta funcionalidad adicional. TAPILink Pro proporciona todas las características y funcionalidades de TAPILink Lite, pero además proporciona operación CTI de terceros. Esto significa que un solo servidor puede controlar y monitorear cualquier número de dispositivos telefónicos. Además, TAPILink Pro brinda la capacidad de monitorear y controlar grupos. Esto permite que una aplicación sea notificada cuando una llamada ingresa a una cola y también puede redirigirla a otra ubicación.

TAPI-WAV
conductor

Proporciona soporte basado en software para procesamiento de voz. El controlador TAPI-WAV solo se usa con TAPI 2.1; para TAPI 3.0, IP Office es compatible con la interfaz del proveedor de servicios multimedia (MSP), definida por Microsoft en TAPI 3.0. Esta funcionalidad solo funcionará junto con CTI Link Pro y también requiere licencias TAPI-WAV. Cada licencia habilita 4 puertos de procesamiento de voz.

DevLink Pro

Proporciona un flujo de eventos en tiempo real además de la interfaz SMDR proporcionada en IP Office SMDR. El flujo de eventos en tiempo real toma la forma de un registro de llamada, que se emite cada vez que cambia el estado de cualquier punto final de una llamada (normalmente hay dos puntos finales en una llamada, pero en algunas circunstancias, como llamadas en conferencia, llamadas intrusas puede haber más).

REDCE IP Office

Proporciona una interfaz para obtener eventos SMDR. Se emite un registro separado por comas para cada llamada, cuando se completa la llamada. Esta interfaz está diseñada para aplicaciones de contabilidad y facturación de llamadas. IP Office SMDR puede enviarse directamente desde la unidad de control de IP Office a una dirección IP y un puerto designados.

Oficina de PI
Software
Desarrollo
Equipo

Este kit de herramientas se entrega en un solo CD que contiene la documentación para desarrolladores de TAPILink Lite, TAPILink Pro, DevLink Lite y DevLink pro, así como programas precompilados para explorar TAPI 2.1 y 3.0. Además, se incluye código fuente de ejemplo, lo que facilita que los desarrolladores se familiaricen con las interfaces CTI de IP Office. El programa Developer Connection (DevConnect) es el programa de socios desarrolladores de Avaya y está diseñado para empresas de terceros que están creando un producto para la venta y que desean recibir soporte técnico. La membresía del programa queda a la sola discreción de Avaya. Los miembros de DevConnect pagan una tarifa anual, por la cual reciben soporte técnico directamente de Avaya. Además, Avaya realizará pruebas de interoperabilidad entre IP Office y el producto del miembro, y también puede crear oportunidades para el marketing conjunto, incluidas exhibiciones, el uso del logotipo de Avaya y otros beneficios. Puede encontrar más información sobre el programa DevConnect enhttp://www.devconnectprogram.com .

CTI centralizado
Servicio web
API

Proporciona una plataforma más abierta para permitir que terceros agreguen valor y desarrollen soluciones. Admite entornos distribuidos (SE/SCN) y, por lo tanto, no se limita a nodos como TAPI. Tiene una dependencia de Avaya one-X® Portal de acceso para los usuarios. Al crear un nuevo usuario en IP Office, no es necesario reiniciar.

SSI a través de la Web Servicios	Proporciona información de monitoreo del sistema de SSI a través de un servicio web REST de solo lectura disponible solo a través de https. Los datos de llamadas en tiempo real y el control de llamadas no están disponibles a través de esta interfaz, pero estarán disponibles a través del programa DevConnect. Esta función ya tiene varias áreas instrumentadas, pero los datos son para SSA y se entregan a través de la interfaz SSI patentada, y hay un pequeño conjunto de datos disponible en SNMP. No requiere licencia.

Abrir API/SDK

Con la versión 10.1, IP Office admite una nueva API/SDK de administración para abordar las necesidades de las configuraciones de "botón fácil". Mejoras para cubrir más áreas, específicamente lo que cubren los servicios web de configuración "XO" heredados para que la API heredada pueda llegar al final de su vida útil. La API de administración proporciona una interfaz API basada en REST a los desarrolladores de aplicaciones de terceros para consumir objetos de configuración de IP Office.

- Brinda todas las capacidades de los servicios de configuración de IP Office compatibles actualmente (servicios XO).
- La solicitud y la respuesta están en formato XML y JSON.
- Proporciona acceso de lectura/escritura únicamente a usuarios de servicios privilegiados.
- No se requiere una licencia por separado para acceder a las API.

Componentes

Componentes de hardware

unidad de control de IP Office

La unidad de control de IP Office (IP500 V2) es una unidad apilable con un kit de montaje en rack de 19" opcional y un kit de montaje en pared opcional para configuraciones más pequeñas.

La unidad de control IP500 V2 es compatible con todas las tarjetas de módulo de compresión de voz (VCM) y extensión base IP500, así como con todos los módulos de expansión IP500 externos.

La centralita IP500 V2 dispone de 4 slots para la inserción de tarjetas base IP500. Las ranuras están numeradas del 1 al 4 de izquierda a derecha. Normalmente se pueden usar en cualquier orden, sin embargo, si se excede la capacidad de un tipo de tarjeta en particular, la tarjeta en la ranura más a la derecha se desactivará. Cada tarjeta base incluye un panel frontal integral con puertos para conexiones de cable. Por lo general, los primeros 8 puertos de la izquierda son para la conexión de dispositivos de extensión. Los 4 puertos de la izquierda se utilizan para la conexión de troncales si se agrega una tarjeta secundaria de troncales a la tarjeta base.

La unidad de control proporciona la siguiente funcionalidad:

Máximo extensiones	Hasta 384 extensiones.
Conferencia fiestas	128 como estándar pero máximo 64 en cualquier conferencia individual. La supresión de silencio se aplica a conferencias con más de 10 participantes.
Tarjetas troncales	Hasta 4. Cualquier combinación de tarjetas secundarias de troncales.
Voz compresión canales	Hasta 148 canales usando hasta VCM y tarjetas combinadas.
Mensaje de voz canales	Se admiten hasta 250 canales de correo de voz/grabación en el servidor principal. Para implementaciones seleccionadas, el servidor secundario también puede admitir hasta 250 canales de correo de voz/grabación.
locales	Compatible en los siguientes países: Argentina, Australia, Baréin, Bélgica, Brasil, Canadá, Chile, China, Colombia, Personalizar, Dinamarca, Egipto, Finlandia, Francia, Alemania, Grecia, Hong Kong, Hungría, Islandia, India, Irlanda, Italia , Japón, Corea, Kuwait, Malasia, México, Marruecos, Países Bajos, Nueva Zelanda, Noruega, Omán, Pakistán, Perú, Polonia, Portugal, Qatar, Rusia, Arabia Saudita, Singapur, Sudáfrica, España, Suecia, Suiza, Taiwán, Turquía, Emiratos Árabes Unidos, Reino Unido, Estados Unidos, Venezuela.
Fuente de alimentación	Unidad de fuente de alimentación interna.
Montaje	Independiente, montado en bastidor o montado en la pared (requiere kits de montaje).
Memoria	Tamaño máximo del archivo de configuración: 2048 KB.

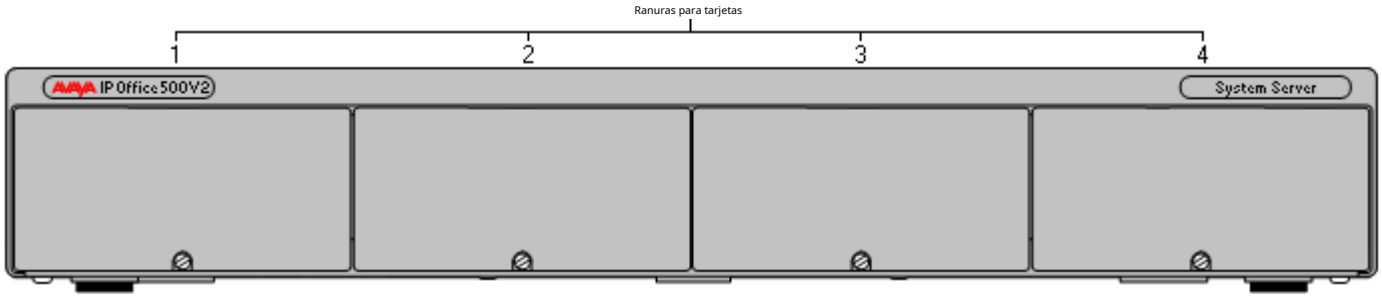


Figura 9: Vista frontal de IP500 V2

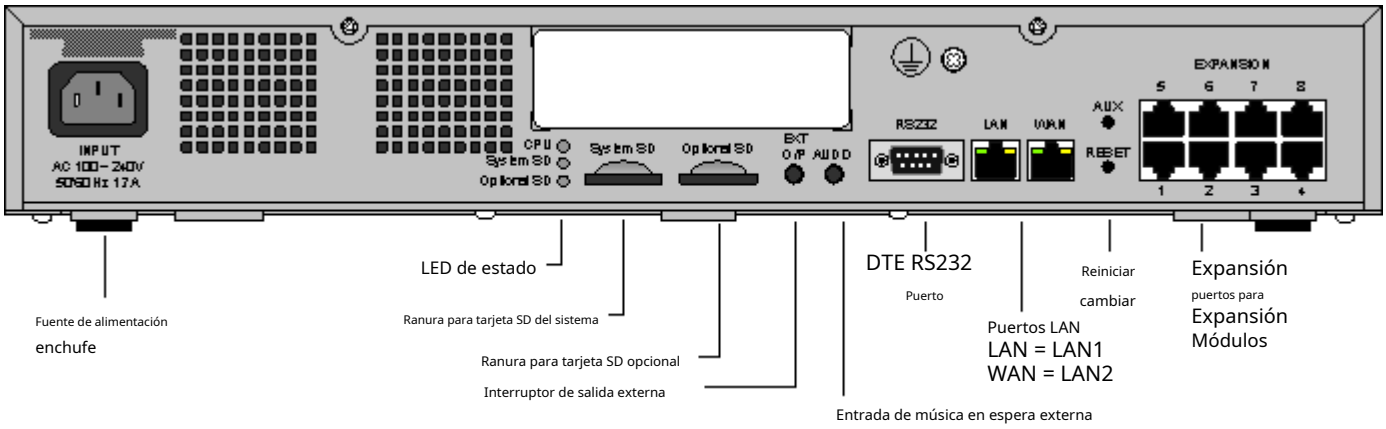


Figura 10: Vista trasera de IP500 V2

Teclas de función

El número de serie de la tarjeta SD de llave de función instalada en la unidad de control de IP Office se usa como base para todas las licencias emitidas para ese sistema IP Office y se usa para validar las licencias con regularidad. Si se extrae la tarjeta SD de la llave de funciones, en las próximas horas las funciones con licencia dejarán de funcionar.

Codificación de modulación de código de pulso

La modulación de código de pulso (PCM) es un método para codificar voz como datos. En telefonía, se utilizan ampliamente dos métodos de codificación PCM, a-law y μ-law (también llamado mu-law o u-law). Por lo general, la ley μ se usa en América del Norte y en algunos otros lugares, mientras que la ley a se usa en el resto del mundo. Además de configurar la codificación PCM correcta para la región, la configuración de ley a o ley μ de IP Office cuando se inicia por primera vez afecta una amplia gama de valores predeterminados regionales relacionados con la configuración de línea y otros valores.

Tarjetas base

Las siguientes tarjetas base están disponibles:

Tabla 2: Tarjetas base IP500 V2

Tarjeta básica	Máximo m por sistema	Puerto RJ45 asignación descripción	Teléfonos compatibles
Estación digital (DS8)	3	Puertos 1–8: digitales estaciones Con tarjeta de troncal: Puertos 9–12: Central Líneas de oficina	Teléfonos Avaya series 2400, 5400 y 9500 seleccionados Teléfonos T3 (solo EMEA) Teléfonos inalámbricos 3810 (solo en Norteamérica) **Nota:** Los teléfonos de la serie 4400 no son compatibles con esta tarjeta. Son compatibles con los puertos DS del módulo de expansión externo. Los teléfonos 4100, 7400, serie M y serie T utilizan la tarjeta de estación digital TCM8.

La tabla continúa...

Página581 de 3226.

Tarjeta básica	Máximo m por sistema	Puerto RJ45 asignación descripción	Teléfonos compatibles
Teléfono analógico 2	4	Puertos 1–2: Analógico estaciones Con tarjeta de troncal: Puertos 9–12: Troncal conexiones	Teléfonos analógicos
Teléfono analógico 8	4	Puertos 1–8: Analógico estaciones Con tarjeta de troncal: Puertos 9–12: Troncal conexiones	Teléfonos analógicos
Estación digital (TCM8)	4	Puertos 1–8: BST estaciones digitales Con tarjeta de troncal: Puertos 9–12: Central Líneas de oficina	Norstar®/teléfonos BCM Teléfonos de la serie BST Teléfonos globales de la serie M Controladores de movilidad digital (DMC) Teléfonos inalámbricos 7406e Unidad de audioconferencia digital
Voz Compresión Módulo (VCM V2)	2	Puertos 1–8: No presente Con tarjeta de troncal: Puertos 9–12: Central Líneas de oficina	Llamadas VoIP incluyendo extensiones IP o troncales IP. Hasta 128 canales de compresión de voz según el códec utilizado. La unidad de control IP500V2 admite hasta 148 canales de compresión de voz, usando la tarjeta más los puertos de compresión de voz en la tarjeta combinada.
Cajero automático Combinación (cajero automático V2)	2	Puertos 1–6: digitales estaciones Puertos 7–8: Analógico estaciones Puertos 9–12: Central Líneas de oficina 10 voz compresión canales códec el soporte es G.711, G729a y G.723 con eco de 64ms cancelación. G.722 Es apoyado por versión 8.0 y más alto.	Teléfonos digitales de Avaya excepto teléfonos de las series 3800 y 4400 Teléfonos analógicos Tarjetas de troncales preinstaladas

La tabla continúa...

Tarjeta básica	Máximo m por sistema	Puerto RJ45 asignación descripción	Teléfonos compatibles
BRI Combinación	2	Puertos 1–6: digitales estaciones Puertos 7–8: Analógico estaciones Puertos 9–10: BRI puertos troncales (4 canales BRI) 10 voz compresión canales códec el soporte es G.711, G729a y G.723 con eco de 64ms cancelación. G.722 es compatible con la versión 8.0 de IP Office y más alto.	Teléfonos digitales de Avaya, excepto teléfonos de las series 3800 y 4400 (tipo DS, no TCM) Teléfonos analógicos Tarjetas de troncales preinstaladas
unificado Comunicación Módulo ns (UCM V2)	1		Requiere una licencia Preferred Edition por separado. No compatible con Server Edition. Más de 200 usuarios cuando solo se ejecuta Voicemail Pro. Hasta 200 usuarios cuando se ejecuta Voicemail Pro y Avaya one-X®Portal de IP Office. 50 Avaya one-X simultáneos®Portal para usuarios de IP Office. Sin tarjetas troncales
ETR6	3	Puertos 1 a 6: ETR estaciones Con ATM4: Puertos 7–8: Alimentación Transferencia de fallas Puertos 9–12: Central Líneas de oficina	No compatible con Server Edition. Teléfono SOCIO ACS Tarjetas SD ATM4, PRI/T1 o PARTNER en modo µ-law (solo Norteamérica)

Tarjetas troncales

Las tarjetas de troncales se pueden instalar en tarjetas base existentes para brindar soporte a los puertos de troncales. La tarjeta troncal utiliza los puertos proporcionados en la tarjeta base para la conexión de cables. Cada tarjeta de troncal viene con clavijas espaciadoras para la instalación y etiquetas de identificación de puertos.

Nota:

Estas tarjetas se utilizan para puertas de enlace PSTN/FXS con IP Office para Linux.

Consejo:

En sistemas con tarjetas base de Analog Phone 8 y tarjetas de troncales analógicas, se recomienda combinar los dos tipos porque brinda soporte de falla de energía analógica para una troncal por extensión (no aplicable a la tarjeta base de Analog Phone 2).

Tabla 3: Tarjetas de troncales IP500 V2

Tarjeta de troncal	Máximo m por sistema	Funciona con estas tarjetas base.	Descripción
Analógico (V2)	4	ETR6 DS8 TCM8 Teléfono analógico 2/8	4 troncales de inicio de bucle analógico Módem V.32 para acceso remoto 1 extensión de falla de energía a conexión troncal en tarjetas Phone 8

La tabla continúa...

Tarjeta de troncal	Máximo m por sistema	Funciona con estas tarjetas base.	Descripción
PRI universal (PRI-U)	4	ETR6 DS8 TCM8 Teléfono analógico 2/8 VCM	Hasta 2 conexiones troncales PRI. La tarjeta está disponible en variantes de puerto único y doble. La tarjeta se puede configurar para troncales E1 PRI, T1 bit robado, T1 PRI o E1R2 PRI. Admite troncales digitales de tasa primaria. En cada tarjeta, 8 canales por interfaz están habilitados por defecto. Esto significa que el PRI simple tiene 8 canales habilitados, mientras que el PRI dual tiene 8 canales habilitados en cada uno de los dos circuitos. Se pueden habilitar más canales mediante la compra de licencias adicionales en incrementos de 2 u 8 canales. Disponible en versión simple y doble. La variante única puede admitir hasta 24 canales T1 o hasta 30 canales E1. La variante dual puede admitir hasta 48 canales T1 o 60 canales E1. Configurable para uso de MFC T1, E1, E1R2, según el territorio. Incluye una CSU/DSU integrada: • CSU permite que las troncales se pongan en modo de bucle invertido para fines de prueba. Esto se puede configurar manualmente, usando la aplicación de monitoreo, o automáticamente desde una oficina central enviando un patrón de bucle de línea (LLB). • DSU permite que el troncal T1 se comparta entre los servicios de datos y voz. Incluye capacidades de diagnóstico: indicadores visuales para mostrar el estado del servicio y puntos de prueba físicos para monitorear el tráfico. Admite funciones de movilidad: Mobile Call Control y clientes one-X Mobile
BRI (Euro RDSI)	4	DS8 TCM8 Teléfono analógico 2/8 VCM	Hasta 4 conexiones troncales BRI, cada troncal proporciona 2 canales digitales B+D. Disponible en 2 (4 canales) y 4 (8 canales) opciones. Admite funciones de movilidad: Mobile Call Control y clientes one-X Mobile.

Módulos de expansión externos

Los módulos de expansión externos se pueden utilizar con la unidad de control IP500 V2.

Módulos de expansión de teléfonos analógicos

En los puertos analógicos, la información de la llamada se envía mientras suena el teléfono y no se puede actualizar durante una llamada ni configurar en una llamada saliente (el teléfono puede hacer una coincidencia local, pero esto no está controlado por IP Office). El propósito principal de las pantallas es dar información sobre las llamadas entrantes. Cuando el estándar de visualización de la persona que llama elegido admite la entrega de texto (nombre de la extensión), así como el número, se entregan ambos.

Se puede configurar un puerto de extensión analógico para la operación de megafonía externa. No funciona como una extensión normal y se conecta a un equipo externo a través de un dispositivo de aislamiento (también se puede utilizar como fuente de MoH). El puerto siempre estará ocupado, por lo que no se puede llamar directamente y solo se puede acceder mediante una función de paginación. Cuando no reciba una página, el puerto permanecerá en silencio. Al ser buscado, el tono de buscapersonas se envía antes de que se abra la ruta de voz.

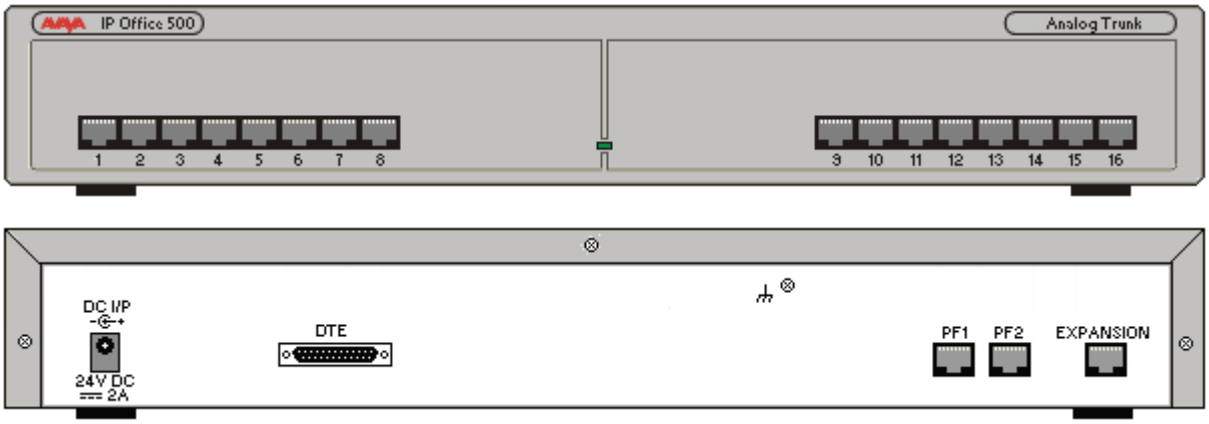
Para instalaciones en rack, este módulo requiere el kit de montaje en rack IP500 V2.

Expansión módulo	Teléfonos compatibles	Interfaces compatibles
Teléfono analógico 16	16 estaciones analógicas con presentación de línea de llamada	Señalización DTMF (sin desconexión rotativa ni de bucle) Recuperación de tiempo de descanso (sin recuperación de tierra) Indicación de mensaje en espera (MWI): 51 V escalonado, 81 V, 101 V e inversión de línea y Bellcore FSK
Teléfono analógico 30	30 estaciones analógicas con presentación de línea de llamada	

Módulos troncales analógicos

Este tipo de módulo se puede usar para agregar 16 troncales analógicas adicionales a un sistema IP500 V2. El módulo admite troncales de inicio por bucle y de inicio por tierra. El módulo también proporciona dos puertos de falla de energía para la conexión directa de teléfonos analógicos a los dos primeros troncales analógicos.

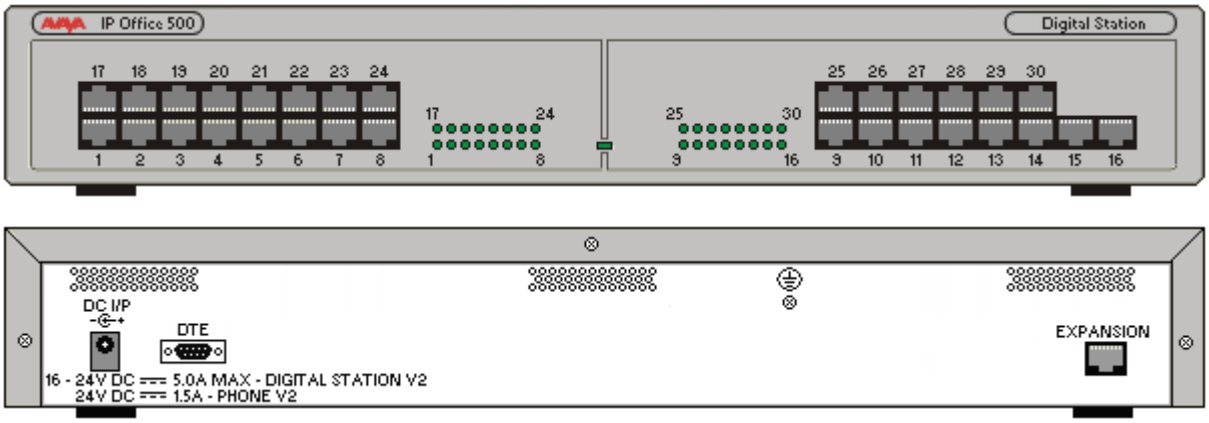
Los sistemas Basic Edition solo admiten un único módulo de expansión ATM16. Para instalaciones en rack, este módulo requiere el kit de montaje en rack IP500 V2.



Expansión módulo	Descripción	Interfaces compatibles
cajero automático16	16 troncales analógicas	Inicio de bucle Comienzo de tierra

Módulos de expansión de estaciones digitales

Para instalaciones en rack, este módulo requiere el kit de montaje en rack IP500 V2.



Expansión módulo	Teléfonos compatibles	Descripción
DS16A	Norstar®/Teléfonos BCM	16 puertos de estación digital
DS30A	Teléfonos de la serie BST Teléfonos de la serie Global M Controladores de movilidad digital (DMC) Teléfonos inalámbricos 7406e Unidad de audioconferencia digital	30 puertos de estación digital
DS16B, DS16B2[1]	Teléfonos Avaya	16 puertos de estación digital
DS30B, DS30B2[1]	Modo DS o TCM compatible con los teléfonos conectados a las tarjetas DS8 o TCM8.	30 puertos de estación digital

Servidor de aplicaciones

El servidor de aplicaciones de IP Office brinda confiabilidad, escalabilidad y potencia de procesamiento para implementaciones de IP Office a mayor escala. Es un servidor externo montado en rack que brinda escalabilidad para instalaciones más grandes e implementaciones en múltiples sitios que actualmente no son compatibles con Unified Communications Module (UCM V2).

El servidor de aplicaciones de IP Office es una instalación única de IP Office seleccionado™Aplicaciones de la plataforma que se ejecutan en Linux. El sistema operativo Linux se incluye como parte de la instalación. Sin embargo, la instalación requiere un conocimiento mínimo de Linux debido a la inclusión de una interfaz de administración basada en web para permitir que el servidor se administre de forma remota a través del navegador web.

[1]DS16B2 y DS30B2 son compatibles con 10.1, 9.1 SP 12 y 10.0 SP5 en adelante.

El servidor de aplicaciones de IP Office alberga las siguientes aplicaciones:

- Servicios de gestión
- Portal one-X para IP Office
- Correo de voz Pro
- Administrador de licencias web (WebLM)
- Administrador web
- Servicios opcionales
  - Administrador de medios
  - Colaboración web
  - Puerta de enlace WebRTC

Pautas de configuración de la puerta de enlace WebRTC

Use las siguientes pautas al configurar una puerta de enlace WebRTC:

- Definir extensiones SIP de WebRTC en:
  - Servidor SIP que forma parte de la configuración de la puerta de enlace WebRTC.
  - Servidor principal si forma parte de la topología de implementación.
- Con las implementaciones de IP500 V2, WebRTC debe estar habilitado en el servidor de aplicaciones.

Limitaciones de la puerta de enlace

La puerta de enlace WebRTC no es compatible con la resiliencia.

Controlador de borde de sesión de Avaya para empresas

Un controlador de borde de sesión actúa como un enrutador entre la empresa y el servicio del operador, lo que permite que solo las sesiones autorizadas pasen por el punto de conexión (borde). El controlador de borde de sesión para empresas (SBCE) de Avaya brinda seguridad a una red de comunicaciones unificadas basada en SIP.

Para obtener información sobre la SBCE, consulte*Resumen y especificaciones de Avaya Session Border Controller para empresas*.

Para obtener información sobre la implementación de SBCE con IP Office, consulte "Configuración de Avaya Session Border Controller para trabajadores remotos de IP Office" en

- *Administración de IP Office de Avaya™Plataforma con Web Manager*
- *Administración de IP Office de Avaya™Plataforma con Gerente*

Los telefonos

IP Office es compatible con varias soluciones telefónicas:

- Teléfonos IP

- Teléfonos digitales
- Teléfonos ETR
- Teléfonos analógicos
- Teléfonos inalámbricos
- Terminales SIP de terceros, como teléfonos de escritorio, softphones y teléfonos con altavoz para conferencias

Para obtener especificaciones detalladas, consulte la información telefónica específica en el sitio de soporte de Avaya en http://soporte.avaya.com .

Enlaces relacionados

Soporte telefónico remoto en la página 39
Acceso a las notas de la aplicación Avaya DevConnect en la página 134 Uso de la base de conocimientos de Avaya InSite en la página 134 Interoperabilidad telefónica en la página 95

Soporte telefónico remoto

Teléfonos IP que usan enrutador NAT

IP Office admite teléfonos IP remotos de la serie 9600 con el FW H.323 que reside detrás de un enrutador NAT para IP Office. La configuración no requiere ningún equipo concentrador VPN. Los teléfonos IP 9600 H.323 remotos pueden conectarse a IP Office incluso si está ubicado detrás de un enrutador NAT. Los teléfonos se autentican del mismo modo que los teléfonos de la red privada. IP Office determina que un teléfono está ubicado fuera de la red privada y retransmite el tráfico RTP de VOIP para garantizar que atraviese el enrutador NAT.

Nota:

La señalización H.323 y el tráfico de medios no están encriptados.

Para acceder a IP Office desde la red privada remota, los teléfonos IP H.323 remotos deben configurarse con la dirección IP pública del enrutador NAT que aloja IP Office. Los puertos configurables deben reenviarse a IP Office. IP Office requiere que se configure una dirección IP pública válida y la dirección IP pública puede configurarse estáticamente o descubrirse dinámicamente a través de un servidor STUN. La función de trabajador remoto requiere la licencia de Essential Edition, que proporciona 4 puestos de trabajo remoto. Habilite la función de trabajador remoto mediante IP Office Manager. La capacidad de trabajo remoto adicional está disponible con las licencias de usuario de teletrabajador o usuario avanzado y una licencia de edición preferida.

Teléfonos VPN

Los teléfonos VPN brindan comunicación segura a través de redes ISP públicas con IP Office en la sede de la empresa. Es un producto de solo software que se ejecuta en teléfonos IP 5610/5620/5621 o 4610/21. En combinación con uno de estos teléfonos y los productos de puerta de enlace VPN más populares, el software extiende la telefonía empresarial a ubicaciones remotas. La funcionalidad VPN es compatible con los teléfonos IP 9600 y no requiere una carga de software independiente. El teléfono VPN ha sido probado con varias puertas de enlace VPN de proveedores importantes como Cisco o Juniper, así como con dispositivos de acceso VPN más pequeños de compañías como Adtran, Kentrox, Netgear y SonicWall. Consulte el sitio web de soporte de Avaya para obtener una lista de las notas de aplicación disponibles en las puertas de enlace VPN probadas con cada línea de teléfonos.

Página589 de 3226.

Teléfonos SIP que utilizan Avaya SBCE

El controlador de borde de sesión de Avaya para empresas (Avaya SBCE) se encuentra en el borde de la red del cliente con interfaces IP internas y externas. Con estas interfaces IP, Avaya SBCE funciona como puerta de enlace para el tráfico SIP hacia y desde la red. Cuando se usan internamente, los clientes SIP se registran directamente en IP Office. Cuando se usan externamente, los clientes SIP se conectan a Avaya SBCE. Esto se logra mediante DNS dividido, que resuelve automáticamente los FQDN en la dirección IP interna de IP Office o la dirección IP pública de Avaya SBCE, según la ubicación actual de los clientes. Además de actuar como puerta de enlace, Avaya SBCE también brinda protección contra cualquier ataque externo basado en SIP. Para la privacidad en la Internet pública,

---

aplicaciones de IP Office

Aplicaciones de usuario

Las siguientes secciones proporcionan una descripción general de las aplicaciones destinadas a los usuarios finales.

Avaya one-X®Móvil

Avaya one-X®Mobile es una aplicación que los usuarios móviles utilizan para conectarse a IP Office.

Avaya one-X®El móvil funciona en modo de devolución de llamada telefónica. Por ejemplo, cuando un usuario inicia una llamada desde el cliente, IP Office inicia una llamada al dispositivo móvil de la persona que llama y luego marca el destino. Este modo ofrece ahorros de costos a los usuarios en países donde las llamadas de voz entrantes son gratuitas o para usuarios que tienen un plan de voz ilimitado más económico en comparación con un plan de datos.

El cliente de movilidad preferido de one-X Mobile también funciona en el modo Voz sobre IP (VoIP). En el modo VoIP, el cliente realiza llamadas a través de redes de datos Wi-Fi/3G/4G. El cliente, utilizando su pila SIP subyacente, se registra en IP Office a través de la red de datos y funciona como una extensión de la oficina.

Los usuarios de países en los que se cobran las llamadas entrantes verán un importante ahorro de costes en el modo VoIP, especialmente en redes Wi-Fi. La disponibilidad de los modos de devolución de llamada y VoIP en el cliente de movilidad permitirá a los usuarios alternar entre los modos en función de sus conexiones de red. Esto permitirá a los usuarios finales elegir el modo apropiado según su plan de voz y datos, así como la disponibilidad y calidad de su conexión de datos (WiFi/3G/4G). Por ejemplo,

- El usuario puede elegir el modo de devolución de llamada cuando no tiene acceso a Wi-Fi y la conexión de datos 3G no proporciona una buena calidad para la voz.
- El usuario puede elegir el modo VoIP cuando tiene acceso a un punto de acceso móvil donde hay disponible una conexión de datos Wi-Fi o cuando la conexión de datos 3G o 4G es buena.

Un cliente de movilidad preferente de one-X Mobile es compatible con el modo VoIP en dispositivos iOS y Android. El modo VoIP está disponible con el perfil de usuario avanzado. Los usuarios con perfiles de trabajador móvil solo pueden

usar el modo de devolución de llamada. El modo VoIP no requiere una licencia de terminal IP. Las siguientes características están disponibles:

- Selección de tono de llamada
- Selección de códec de ancho de banda alto o de banda estrecha según la conexión de red disponible
- Control de audio de auriculares Bluetooth en llamadas VoIP
- Pantalla de conferencia
- Selección de número de teléfono de contacto
- Indicador de prioridad de correo de voz
- Soporte de deslizamiento para mensajería instantánea en la pantalla de inicio
- Apoyo a la acción de grupo
- Emoticones
- Búsqueda CLID en contactos para llamadas
- Enviar correo de voz como WAV en el correo electrónico
- Habilitar o deshabilitar el hermanamiento móvil (anillo simultáneo)
- Activar o desactivar DND (enviar todas las llamadas)
- Registro de llamadas combinado con correos de voz en el historial de eventos
- Monitoreo de llamadas para ver e interactuar con todas las llamadas
- Plan de marcación del modo VoIP
- Transferir llamadas como un controlador de llamadas de terceros (3PCC)

Avaya one-X®Portal para IP Office

Avaya one-X®Portal for IP Office proporciona a los usuarios el control de su teléfono desde una PC en red. Utilice esta aplicación con cualquier extensión; analógico, digital o cualquier teléfono IP, alámbrico o inalámbrico, que esté disponible como parte de las licencias de usuario de Office Worker, Power User o Teleworker.

Avaya one-X®Portal for IP Office es una aplicación basada en servidor a la que el usuario accede a través de un navegador web.

Para el modo Teletrabajador, las aplicaciones One-X requieren supervisión de respuesta y detección de desconexión para un funcionamiento adecuado. Como resultado, las aplicaciones one-X no funcionarán con troncales que no admitan supervisión de respuesta y detección de desconexión.

Nota:

Las aplicaciones one-X funcionan en tipos de troncales como PRI, BRI y SIP; sin embargo, no funcionarán en E1R2, T1 RBS y troncales de inicio de bucle analógico.

Los administradores del sistema pueden controlar si Avaya one-X®Se puede acceder a Portal for IP Office solo a través de un protocolo seguro, recomendado para implementaciones alojadas para proporcionar acceso "solo seguro". La otra opción es permitir que los usuarios accedan al cliente a través de un protocolo seguro y no seguro (HTTP/ HTTPS). La aplicación cliente obliga a los usuarios a cambiar sus contraseñas y códigos de correo de voz para cumplir con la configuración de complejidad configurada por el administrador.

A través de dispositivos, Avaya one-X®Portal para IP Office ofrece las siguientes funciones:

- Información de llamadas
- Control de llamadas y conferencias
- Notificaciones de presencia y mensajería instantánea, monitoreo y archivo
- Importación y exportación de contactos
- Grupos XMPP mostrados en la**Directorio del sistema**pestaña
- Marcar al propio puente del usuario e invitar a otros usuarios a unirse
- Programación de conferencias telefónicas y otras reuniones, incluidas reservas de puertos, asistencia por correo electrónico y creación automática de informes, disponibles en la interfaz de Outlook
- Alojamiento de conferencias web con un solo clic e inicio de sesión único para unirse a conferencias web como participante

Equinoccio de Avaya™para IP Office

Equinoccio de Avaya™para IP Office es un cliente de comunicaciones unificadas (UC) basado en SIP que brinda a los usuarios capacidades de colaboración en tiempo real y permite a los usuarios comerciales administrar fácilmente sus comunicaciones diarias desde una única interfaz. IP Office es compatible con los siguientes sistemas operativos:

- Escritorio:
  - Ventanas
  - Mac OS
- Teléfono móvil:
  - Android: Desde un teléfono móvil, tableta o un Avaya Vantage™dispositivo
  - iOS

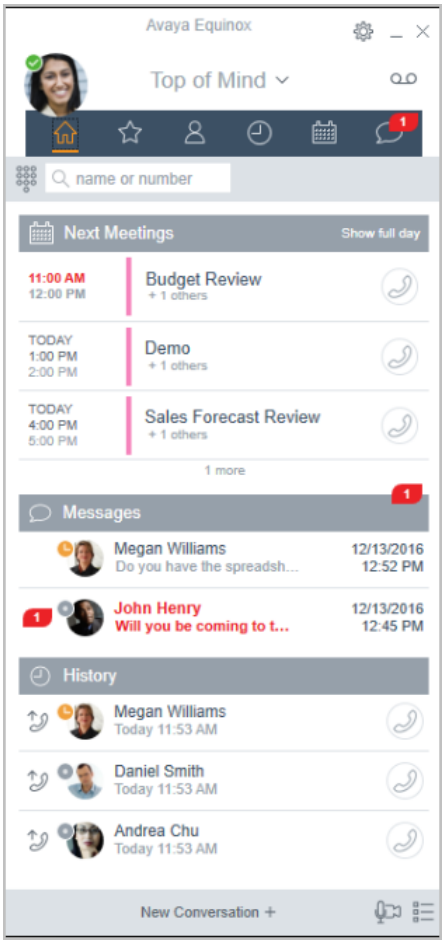
Nota:

En Avaya Vantage™Versión 2.0.1, los dispositivos K165 y K175 son compatibles con Avaya Equinox™cliente. El dispositivo K155 no es compatible con Avaya Equinox™cliente.

Equinoccio de Avaya™es un cliente multiplataforma común. Las capacidades del cliente varían según la plataforma en la que esté registrado. Las funciones admitidas en Avaya Equinox™para IP Office son:

- Pantalla de inicio de elementos destacados
  - Próximas reuniones que muestran el horario del calendario local o el servicio web de Exchange/Office 365
  - Historial de llamadas locales
  - Mensajes
  - Panel de inicio de reuniones/lanzamiento de espacios
- Opción Top of Mind Lite para teléfonos móviles
- Directorio de IP Office y contactos locales
- Mensajería a través de Avaya Spaces

- Presencia a través del servidor de IP Office
- Historial de llamadas locales
- Teclado con rellamada
- Integración de escritorio con Microsoft Outlook y navegadores
- Llamadas de audio y video del cliente Softphone
- Control compartido de un teléfono de escritorio de IP Office asociado.



Equinoccio de Avaya™se registra con el servidor de IP Office como un softphone SIP para llamadas de audio y video, y funciones de telefonía. Se admiten las siguientes características:

- Llamadas de audio y video punto a punto (realizar, recibir y finalizar)
- Manejo de múltiples llamadas (entrantes y salientes)
- Retener y recuperar (llamadas de audio y video)
- Transferencia (ciega y consultiva)
- Conferencia de consulta
- Escalar audio a videollamada
- Comparta el control con teléfonos de escritorio compatibles en Avaya Equinox™cliente de escritorio

- Equinoccio de Avaya™en Avaya Vantage™
- Integración de presencia y directorio con Avaya Equinox™en Avaya Vantage™
- Introducir DTMF durante una llamada

Equinoccio de Avaya™cliente en Avaya Vantage™admite las siguientes características:

- Realización de llamadas salientes.
- Manejo de llamadas entrantes.
- Poner una llamada en espera y reanudarla.
- Silenciar y reactivar una llamada.
- Transferir una llamada.
- Escalar una llamada de audio a una videollamada y desescalar una videollamada a una llamada de audio.
- Introducir dígitos DTMF mediante el teclado.
- Accede a tus contactos locales
- Acceda a sus contactos de IP Office mediante el directorio de IP Office.
- Administrar su estado de presencia y mensajes de estado de presencia.

Equinoccio de Avaya™para las limitaciones de IP Office:

- Control CTI: Avaya Equinox™para IP Office no se puede controlar a través de otras aplicaciones, como Avaya Contact Center Select, IP Office Contact Center o IP Office SoftConsole.
- Trabajador de sucursal: Avaya Equinox™para IP Office no admite conmutación por error entre Avaya Aura®Núcleo y sucursal de IP Office.
- Para mensajería instantánea, Avaya Equinox™para IP Office depende de la disponibilidad de la cuenta de Avaya Spacesbasic en la nube.
- El equinoccio de Avaya™el cliente accede a Avaya Equinox®Reuniones en línea mediante HTTPS, desde la pestaña Reuniones de Equinox del cliente. El equinoccio de Avaya™El cliente puede acceder a Equinox Conferencing local local de la misma manera mediante HTTPS, es decir, si la URL de acceso está configurada en Equinox Meetings. Sin embargo, si Avaya Equinox™el cliente accede a Equinox Conferencing local en las instalaciones a través de troncales SIP, el audio y el video estarán disponibles pero no se compartirán ni la lista de conferencias. Lo mismo se aplica para acceder a Scopia a través de troncales SIP. Incluso cuando Avaya Equinox™el cliente accede a IP Office Meet Me Conferencing local en las instalaciones, el audio estará disponible pero no se compartirá ni la lista de conferencias.

Cliente web Avaya IP Office

Avaya IP Office Web Client es una aplicación WebRTC que brinda varias capacidades de comunicación. El cliente aprovecha las mejoras de resiliencia de WebRTC Gateway proporcionadas en R11.0 y es compatible con Server Edition e IP500 V2. Los usuarios deben tener una licencia de Office Worker o Power User para usar las funciones de Avaya IP Office Web Client. El cliente es compatible con los siguientes entornos:

- Navegadores Google Chrome en el sistema operativo Windows
- Navegadores Google Chrome en macOS
- Cliente independiente en el sistema operativo Windows

Avaya IP Office Web Client ofrece las siguientes funciones:

- Llamadas de audio y video punto a punto
- Acceso al correo de voz
- Registros de llamadas
- Conferencias:
  - Conferencia ad-hoc mediante la fusión de llamadas
  - Iniciar o unirse a una conferencia Meet Me de IP Office
  - Acceder a la colaboración web de IP Office
- Presencia y mensajería instantánea punto a punto al integrarse con Avaya one-X®Portal para IP Office
- Hacer clic para llamar con la extensión de Google Chrome
- Compatibilidad con inicio de sesión único (SSO) para Avaya one-X®Portal para IP Office y colaboración web de IP Office
- Directorio del sistema y favoritos (Directorio personal)

Comunicador de Avaya

Avaya Communicator es un cliente de software de colaboración que ofrece una interfaz innovadora para comunicaciones en tiempo real para Windows y iPad. Permite a los usuarios manejar llamadas telefónicas, mensajes instantáneos, conferencias, colaboración web, presencia, contactos empresariales y correo electrónico, todo desde una única interfaz. Avaya Communicator ofrece el diseño gráfico intuitivo de focos, menú de medios, barra de notificaciones y tarjetas de contacto.

Avaya Communicator for IP Office se comunica tanto con IP Office como con Avaya one-X®Portal para proporcionar funciones de comunicación y colaboración. IP500 V2 proporciona funciones de telefonía como hacer/recibir llamadas, poner en espera/retirar, silenciar/activar, DTMF, MWI, etc. y Avaya one-X proporciona funciones de UC como mensajería instantánea, presencia y contactos empresariales.®Servidor de portales.

Si Avaya one-X®El servidor del portal no está disponible, ya sea debido a restricciones de licencia o problemas de conectividad, el cliente de Avaya Communicator funcionará en un modo de solo telefonía y brindará solo funciones de telefonía. La interoperabilidad con Avaya Session Border Controller for Enterprise permite que los usuarios con el perfil de trabajador remoto utilicen el cliente Flare Communicator y se registren en IP Office sin necesidad de una conexión VPN.

Avaya Communicator ofrece las siguientes funciones:

- Agregue participantes usando el teclado de marcación o arrastrando y soltando
- Silenciar y cancelar el silencio de todos o un subconjunto de participantes
- Bloquear y desbloquear la conferencia
- Colocar la conferencia en modo conferencia
- Habilitar y deshabilitar los tonos de entrada y salida
- Eliminar a todos o algunos participantes de la conferencia
- Terminar la conferencia

- Habilite y deshabilite la continuación para permitir que la conferencia continúe después de que el moderador se retire.
- Ascender a los participantes a moderadores
- Cree conferencias ad-hoc fusionando llamadas P2P
- Autorización y códigos de cuenta (solo Windows)
- Recordatorio de tiempo de espera en espera (solo Windows)
- Experiencia de usuario compacta
- Compatibilidad con TSL/SRTP
- Filtrado de contactos
- Integración de conferencias web
- Transferencia sin supervisión
- Respuesta automática
- Modo simultáneo
- Cambio de contraseña
- Códigos de cuenta
- Configuración automática (solo iOS)
- Compatibilidad y selección de dispositivos Bluetooth y auriculares (solo iOS)
- Interoperabilidad con Scopia (Radvision XT5000)

Nota:

Avaya Communicator no admite la grabación ni el indicador de altavoz activo.

Avaya Communicator para iPad

Avaya Communicator para iPad integra voz, video, presencia, mensajería instantánea, directorios en una interfaz unificada a través de conexiones Wi-Fi o celular 3G y VPN.

Avaya Communicator es una solución solo de software que se puede descargar fácilmente desde Apple iTunes Store y es compatible con iPad2, iPad3, iPad4, iPad Mini (con y sin pantalla retina), iPad Air, modelos Wi-Fi y 3G y las siguientes versiones de iOS: 6.1.x, 7.0.x, 7.1.x y 8.0.x.

Nota:

Avaya Communicator no es compatible con iOS 6.0.x.

Con Avaya Communicator, los usuarios de IP Office pueden usar dispositivos iPad para:

- Fácil acceso a las herramientas de comunicación en tiempo real en las que confían todos los días (teléfono, presencia, mensajería instantánea, etc.)
- Combinar las comunicaciones en tiempo real y los procesos comerciales, como las ventas móviles
- Aprovechar la conectividad Wi-Fi y 3G para VoIP económico
- Señalización segura sobre TLS e intercambio seguro de medios sobre SRTP en entornos de nube

- Como moderador de conferencias web, la capacidad de compartir pizarras y documentos
- Cambio de contraseñas
- Soporte de respuesta automática
- Transferencias no supervisadas
- Servicios de configuración automática utilizando un perfil de configuración alojado en un servidor web por dirección de correo electrónico o URL
- Compatibilidad y selección de dispositivos Bluetooth y auriculares
- Búsqueda en el directorio del sistema
- Agregar/eliminar miembros de un equipo (Grupo XMPP)
- Buscar en el directorio del sistema y agregar a un equipo o contacto personal
- Compatibilidad con Radvision XT5000 para videollamadas punto a punto

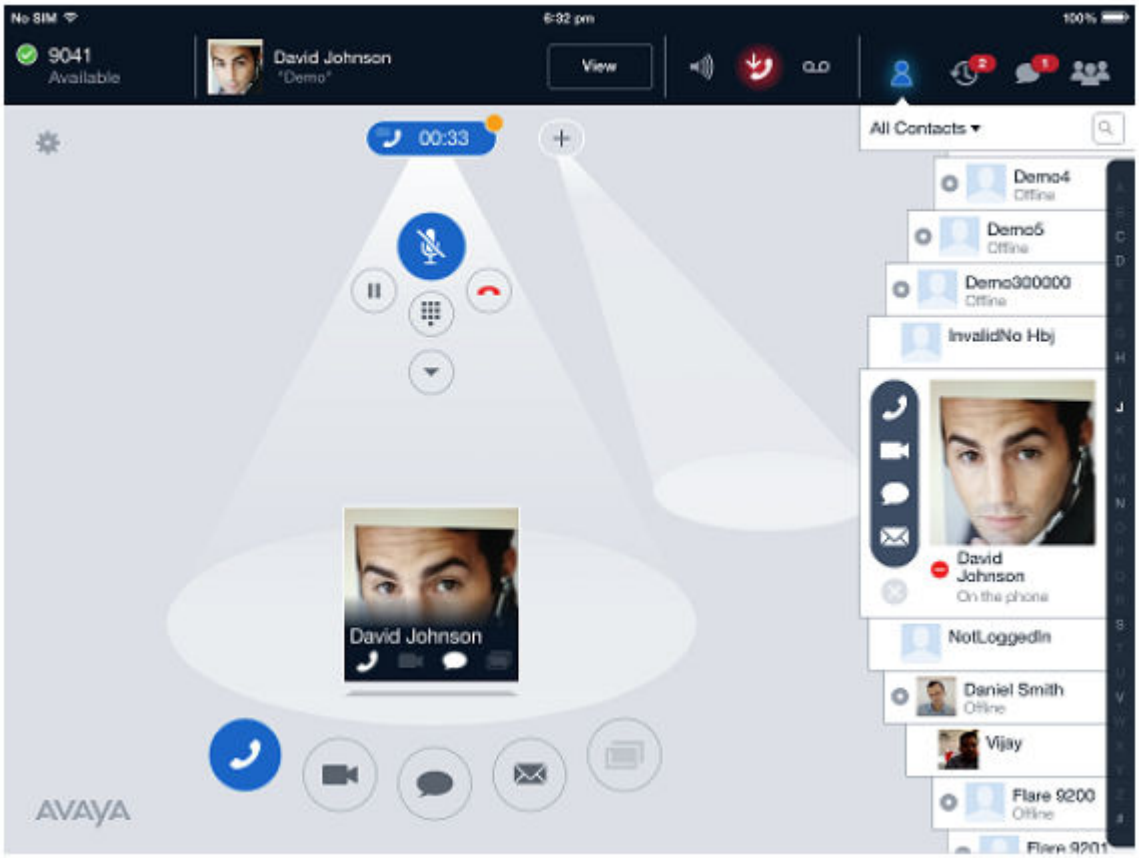


Figura 11: Avaya Communicator para iPad

Avaya Communicator para Windows

Avaya Communicator for Windows integra voz, presencia, mensajería instantánea y directorios en una oferta unificada para computadoras portátiles y de escritorio con Windows a través de una conexión LAN.

Avaya Communicator ofrece las siguientes funciones:

• Modo compacto que ocupa menos espacio en la pantalla

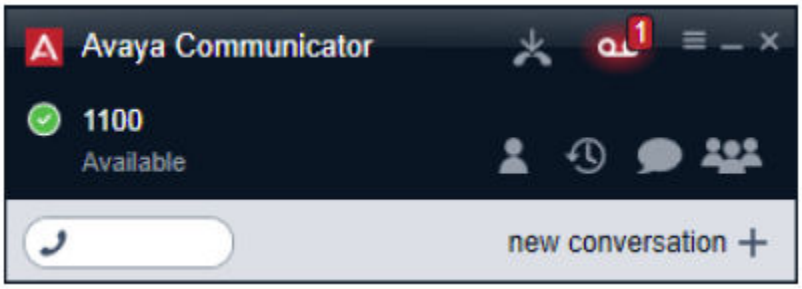


Figura 12: Vista compacta de Avaya Communicator for Windows

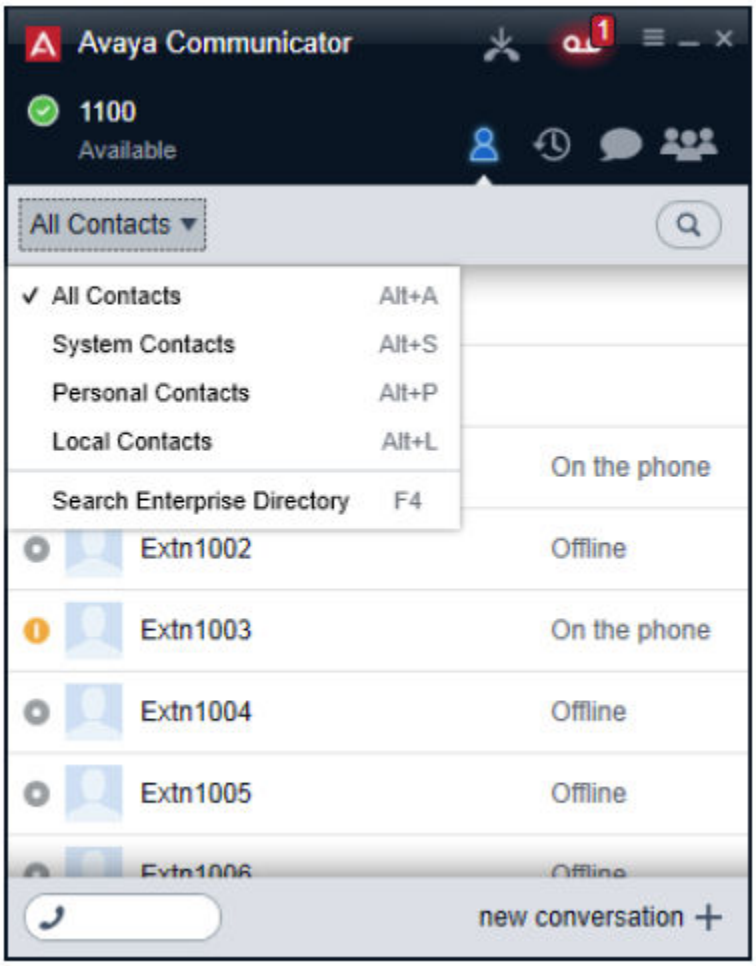


Figura 13: Vista completa de Avaya Communicator para Windows

• Señalización segura sobre TLS e intercambio seguro de medios sobre SRTP para entornos de nube

• Filtrado de contactos según criterios y opción de ver solo contactos del sistema, locales o personales

- Integración de conferencias web
- Transferencias no supervisadas
- Respuesta automática
- Modo simultáneo para interfaces con one-X Portal, Outlook y Salesforce
- Cambio de contraseña
- Códigos de cuenta

SoftConsole

SoftConsole es la aplicación de recepcionista de Windows basada en PC para IP Office. Se puede adquirir con la licencia de usuario Recepcionista.

SoftConsole proporciona a los recepcionistas y operadores empresariales información de llamadas y acciones de llamadas para simplificar el manejo de llamadas y la mensajería instantánea. Con SoftConsole, los usuarios ven el estado de otros usuarios y ajustan la configuración básica de telefonía de otros usuarios, como los números de desvío. Avaya recomienda usar teléfonos que admitan Respuesta automática. Los usuarios pueden usar las funciones de mensajería instantánea proporcionadas por Avaya one-X®Portal, si está disponible.

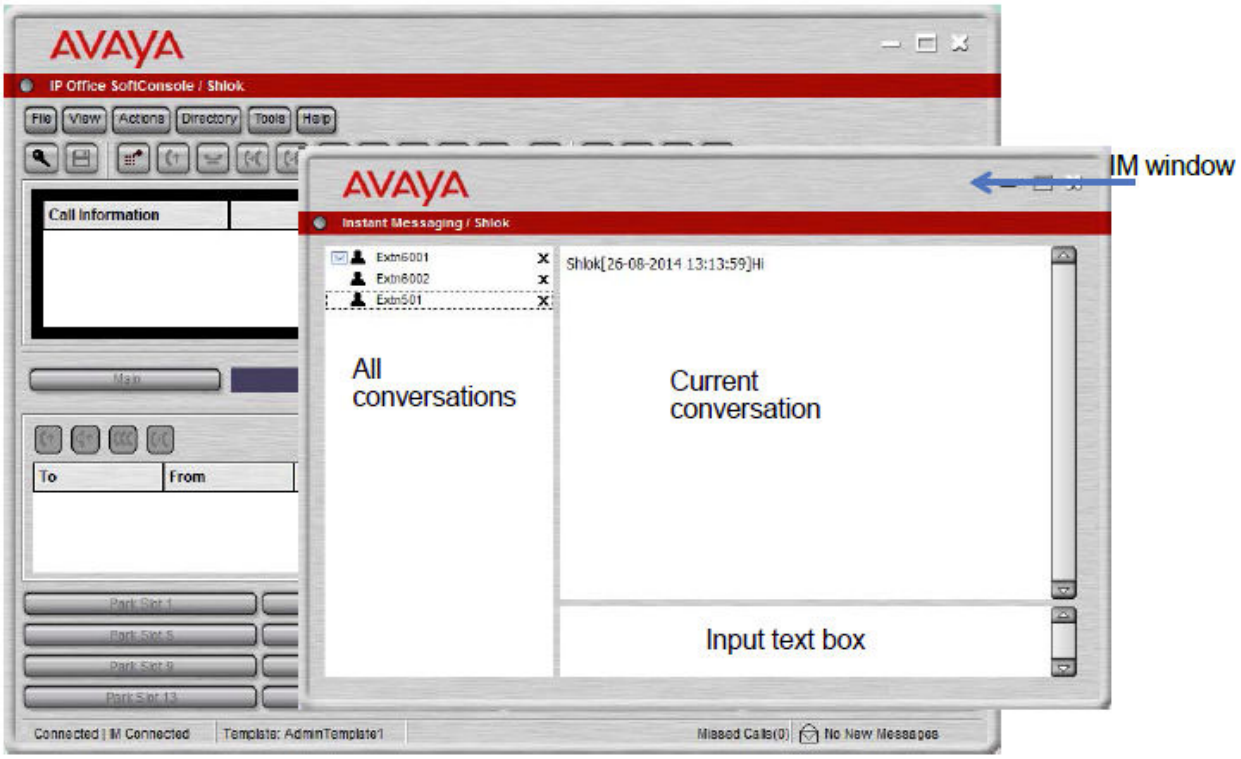


Figura 14: ventana de mensajería instantánea de SoftConsole

La comunicación WebSocket permite a los clientes de SoftConsole comunicarse con IP Office y Avaya one-X® Portal. El protocolo WebSocket es bidireccional entre el cliente y el servidor. Como la comunicación se realiza a través del puerto 80 o 443 (el mismo puerto utilizado para HTTP), no hay problemas con el cruce del cortafuegos. En un entorno alojado, la comunicación WebSocket proporciona seguridad.

SoftConsole se puede minimizar en la bandeja del sistema de Windows cuando no está en uso, pero aparecerá en la pantalla cuando se reciba una llamada. Los archivos de sonido y multimedia se pueden asociar con llamadas. Si se utiliza esta característica, la PC requiere una tarjeta de sonido y parlantes.

SoftConsole admite las siguientes características:

- Contestar llamadas
- Realización de llamadas salientes
- Transferencias supervisadas y no supervisadas
- Transferir llamadas al correo de voz
- Retener y estacionar llamadas
- Supervisión de colas y respuesta de llamadas en cola
- Uso y visualización de salas de conferencias
- Conferencia de llamadas retenidas
- Adición de usuarios a una conferencia
- Agregar texto a una llamada
- Liberación de la puerta
- entrometerse
- Envío de mensajes de texto
- Paginación
- Grabación de llamadas
- Envío de correo electrónico
- Uso del teclado de marcación
- Soporte de múltiples idiomas, los usuarios pueden seleccionar el idioma

Correo de voz integrado

En entornos como el comercio minorista o la oficina en el hogar, donde las consideraciones de espacio, ruido o costo descartan el uso de una PC para el correo de voz, Embedded Voicemail brinda servicios básicos de correo de voz. Embedded Voicemail está en la unidad de control IP500 V2 y no requiere un servidor de correo de voz separado.

Embedded Voicemail está disponible con IP Office Essential Edition. No se requieren licencias adicionales.

Buzón de voz profesional

Voicemail Pro se proporciona con IP Office Preferred Edition y es una aplicación avanzada de mensajería y flujo de llamadas para sistemas IP Office. Voicemail Pro puede manejar 40 (hasta 250/500 en Server Edition/ Server Edition Select) llamadas simultáneas según la licencia y la configuración del sistema. Cada usuario tiene la opción de activar o desactivar su correo de voz. Cuando está activado, el sistema contesta automáticamente su teléfono cuando no están disponibles para atender una llamada, reproduce un saludo personal y graba un mensaje.

Cuando se ha dejado un mensaje, el usuario verá una luz de mensaje en espera encendida en su teléfono y podrá presionar un botón de recuperación para recoger sus mensajes.

Voicemail Pro también puede llamar al usuario para entregar cualquier mensaje nuevo. Los mensajes de correo de voz se marcan con la fecha y la hora y se registra el número de la persona que llama. Voicemail Pro se puede configurar para eliminar los mensajes leídos automáticamente, a menos que el usuario elija guardar el mensaje de forma permanente.

Los correos de voz se pueden recopilar de forma remota llamando al servidor de Voicemail Pro. Si se reconoce el número desde el que está marcando el usuario (número de casa o teléfono móvil/celular, por ejemplo), el usuario escuchará su correo de voz de inmediato. Si no se reconoce el número de origen, se le solicitará al usuario un número de buzón y un código PIN para ese buzón, antes de que pueda escuchar su correo de voz. Los usuarios tienen la capacidad de establecer y cambiar sus propios códigos PIN.

Cuando es necesario reenviar un correo de voz a otros usuarios, Voicemail Pro ofrece muchas opciones:

- Los correos de voz se pueden reenviar a otro buzón o grupo de buzones
- Los destinatarios pueden agregar sus comentarios al correo de voz antes de reenviarlos a otro buzón o buzones.
- Los correos de voz se pueden reenviar como archivos adjuntos WAV de correo electrónico.

Todas las opciones están disponibles en varios idiomas; tanto indicaciones de voz habladas como interfaces de programación gráfica y tiene la opción de TUI de IP Office y TUI de emulación INTUITY.

conferencias

Los usuarios pueden poner llamadas en espera y crear una conferencia usando el teléfono o las aplicaciones de escritorio. Se pueden agregar miembros adicionales a la conferencia; sin embargo, una sola conferencia no puede tener más de 64 miembros (solo con IP500 V2 y más en Server Edition).

Para conferencias ad-hoc, el sistema requiere tantos troncales digitales/canales VoIP como participantes externos (así como Preferred Edition para conferencias Meet-Me). El sistema admite 128 canales de conferencia en el IP500 V2, lo que permite múltiples conferencias de cualquier tamaño de 3 a 64 participantes. El sistema admite 42 conferencias de 3 participantes, 2 conferencias de 64 participantes o cualquier combinación intermedia. Las capacidades Meet-Me requieren Preferred Edition para marcación directa en un puente de conferencia con seguridad de código PIN. En una red SCN, solo se requiere una licencia Preferred Edition centralizada para organizar conferencias Meet-Me en cualquiera de los sitios. Los ID de conferencia también se comparten en los sitios de SCN.

Están disponibles las siguientes capacidades de canal de conferencia:

Tabla 4: Capacidades del canal de conferencia

Plataforma	no seleccionado	Seleccione	Contacto Avaya Seleccionar centro	Contacto de la oficina de PI Centro
HP DL120 dell r210	128	128	414	414
HP DL360	256	256	825	825
dell r620	256	512	825	825

La tabla continúa...

Página601 de 3226.

Plataforma	no seleccionado	Seleccione	Contacto Avaya Seleccionar centro	Contacto de la oficina de PI Centro
ÓVULO	256	512	825	825
IP500V2	128	128	128	128

Para iniciar una conferencia, los usuarios marcan el número directo asignado al puente de la conferencia, ingresan el PIN (se requiere Preferred Edition y Voicemail Pro) si es necesario. Para conferencias ad-hoc con pocos participantes, los usuarios pueden configurar fácilmente conferencias inmediatas llamando a todas las partes y llevándolas al puente de conferencia. Con Avaya one-X®Portal para IP Office, el originador de la conferencia puede mantener el control: se muestra el número de identificación de llamadas (y el nombre asociado si se reconoce) de cada participante. Si es necesario, pueden colgar selectivamente a un participante específico. El sistema emite un solo pitido al entrar y un doble pitido a la salida. El propietario de la conferencia puede usar su número de extensión como ID de la conferencia. El propietario de la conferencia tiene el control de la conferencia con la capacidad de silenciar y desconectar las llamadas de los participantes. Todos los participantes escucharán la música en espera (MOH) del sistema hasta que el propietario se una, y escucharán MOH cuando el propietario se retire. Tenga en cuenta que cualquier parte interna tiene la opción de ver y eliminar participantes (no solo el originador de la conferencia).

Los usuarios pueden grabar un saludo personalizado para una conferencia (requiere Preferred Edition y Voicemail Pro).

Los usuarios pueden grabar la conferencia usando Avaya one-X®Portal para IP Office, teléfono con pantalla IP o digital o un código corto (requiere Preferred Edition y Voicemail Pro). Para evitar el acceso no autorizado al puente de conferencia, se pueden configurar códigos PIN, filtrado de números de identificación de llamadas y perfiles de fecha y hora mediante Voicemail Pro. Un usuario puede administrar la instalación del puente de conferencias desde cualquier ubicación.

Las conferencias tienen las siguientes restricciones:

- Solo se permiten dos llamadas conectadas a través de troncales analógicas en una sola conferencia.
- Cada llamante externo requiere un canal troncal/VoIP digital (por ejemplo, 1 T1 permite 23/24 interlocutores externos, 1 E1 permite 30 interlocutores y un VCM-64 con licencia completa permite 64 interlocutores).
- No hay límites en la combinación de llamadas internas y externas en la conferencia, pero si todos los participantes internos se desconectan del puente de conferencia, el sistema puede desconectar automáticamente a los participantes externos para mayor seguridad (configuración configurable del sistema).
- Las funciones del sistema, como la intrusión de llamadas, la grabación de llamadas y la supervisión silenciosa, utilizan recursos de conferencia, al igual que la grabación automática si está habilitada. Cuando alguna de estas funciones está activa, se reduce el número de espacios disponibles para los participantes en la conferencia. Por ejemplo, una llamada de conferencia entre 3 participantes y que se está grabando utilizará 4 espacios de conferencia.

Conferencia Meet-Me

La conferencia Meet-Me permite que varias personas que llaman hablen en una audioconferencia. Las personas que llaman pueden ser personal en el sitio, así como partes externas, ya sean ingenieros de campo, personal de ventas en el camino, clientes o proveedores. Las conferencias telefónicas se pueden planificar con anticipación o establecer ad-hoc cuando sea necesario.

Colaboración de vídeo

IP Office brinda compatibilidad con Bring Your Own Device (BYOD) y sistema de sala HD para la colaboración de video.

IP Office admite la colaboración de video con el intercambio de datos a través de Avaya Scopia®aplicaciones móviles y de escritorio al usar Radvision MCU o Video Collaboration para IP Office. Los clientes de Flare también pueden participar en videoconferencias multipartitas. Avaya Scopia®se conecta a IP Office como punto final SIP mediante una licencia IP de Avaya.

Avaya Video Collaboration for IP Office ofrece las siguientes funciones:

- Integración directa que incluye un plan de marcación común con IP Office
- "Sala de conferencias virtual" para hasta ocho participantes con capacidades de hacer clic para unirse desde cualquier sistema de sala basado en estándares, computadora de escritorio o dispositivo móvil
- Clientes de video móviles y de escritorio de distribución gratuita para PC, Mac y los dispositivos iOS y Android más populares, lo que permite a las personas dentro y fuera de una organización unirse fácilmente a una reunión de video
- Videoconferencia multipartita HD de bajo ancho de banda con colaboración de datos usando SIP/H nativo. 323
- Cortafuegos transversal automático para interactuar con participantes fuera de la red

El siguiente diagrama muestra la topología de IP Office implementada con terminales de video.

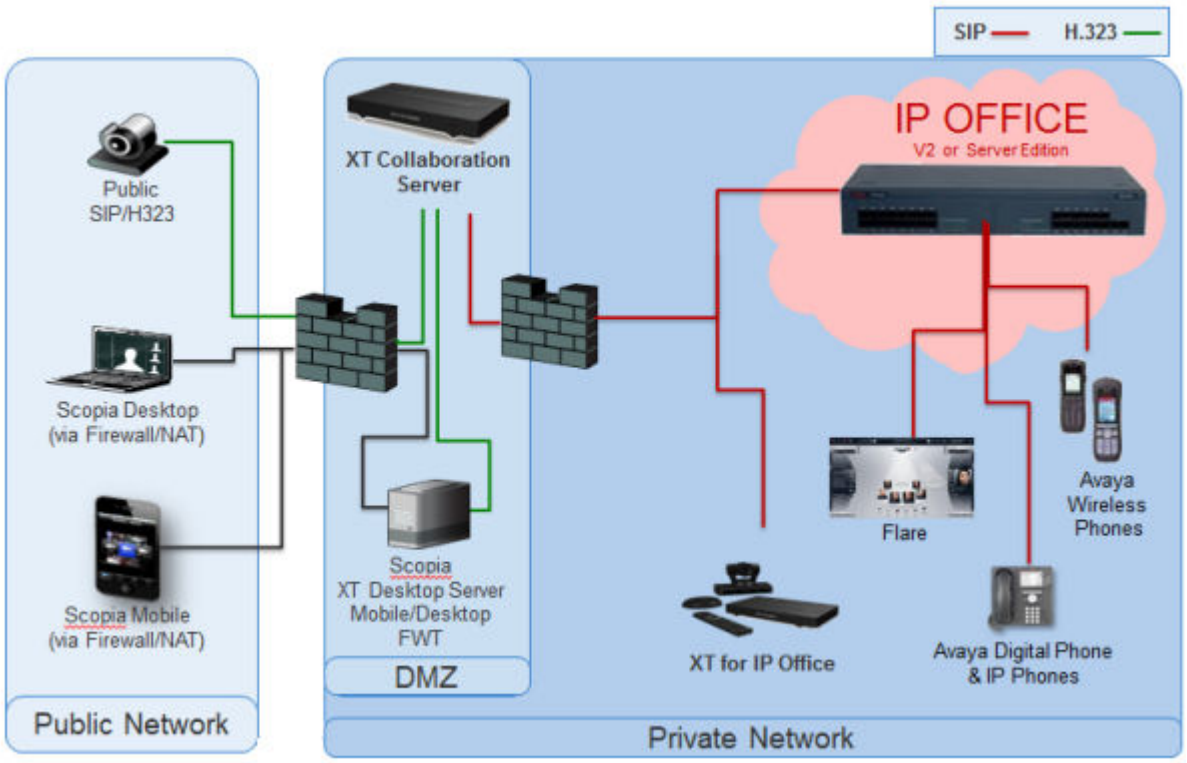


Figura 15: Puntos finales de video

Agente de colaboración

Collaboration Agent es una aplicación que proporciona herramientas de conferencia y colaboración web. Usuarios con Avaya Aura®Las cuentas de conferencias y los invitados pueden usar las herramientas para administrar conferencias y participar y colaborar en conferencias.

Los participantes de la conferencia pueden unirse a conferencias iniciando sesión en Collaboration Agent y llamando al puente de audio asignado a la conferencia. Los participantes también pueden usar la función integrada de audio y video de Collaboration Agent. Los participantes pueden usar las herramientas de Collaboration Agent para aumentar la productividad y realizar un seguimiento de los elementos de acción incluso después de que finaliza la conferencia. Los moderadores de la conferencia pueden:

- Grabar todos los aspectos de las conferencias.
- Grabar y editar actas de reuniones.
- Crear y distribuir informes de reuniones basados en las actas de las reuniones.

Características del Agente de colaboración

En Collaboration Agent, los participantes y moderadores pueden realizar múltiples tareas como:

- Ver una lista de otros participantes.
- Levante virtualmente la mano y pida permiso para hablar.
- Enviar mensajes.
- Anotar contenido compartido.
- Grabar o editar minutos.
- Establecer los tonos de entrada y salida.
- Llamar a otros usuarios ya los usuarios de la conferencia.
- Desconectar a los participantes.
- Ascienda a los participantes al rol de moderador.
- Invite a más participantes a unirse a una conferencia activa.

Durante la conferencia, los participantes pueden ver la siguiente información en Collaboration Agent:

- Los participantes que se unieron solo en el puente de audio
- Los participantes activos en la colaboración web
- El participante que habla actualmente
- El presentador actual

Características opcionales

Las siguientes funciones son opcionales y deben ser habilitadas por el administrador del sistema:

- Iniciar conferencias antes de que se unan los moderadores.
- Vídeo integrado
- Promover a todos los participantes al rol de presentador para que todos los participantes puedan compartir contenido
- Marcación desde Collaboration Agent para conectar usuarios a conferencias
- Grabación de conferencias

Espacios de Avaya

Avaya Spaces es una aplicación de reunión y colaboración en equipo basada en la nube. Integra a la perfección voz, video, tareas, uso compartido y más en su navegador o en la aplicación Spaces. Cada usuario de IP Office tiene derecho a una cuenta gratuita de Avaya Spaces Basic que incluye las siguientes actividades de colaboración en equipo a través de Avaya Equinox™cliente:

- Creación de espacios para administrar proyectos en curso: puede usar el área de espacios en el tablero para iniciar una nueva conversación. De hecho, la primera vez que comienza a usar Avaya Spaces, puede ver la opción para crear su propio espacio. Puede invitar a los participantes a su espacio ingresando sus direcciones de correo electrónico. Puede establecer diferentes permisos para cada participante según el tipo de acciones que desea que puedan realizar dentro de su espacio. Si tiene muchos espacios, puede categorizar los que usa con frecuencia como favoritos.
- Conferencias de audio VoIP con hasta cinco participantes.
- Uso compartido de archivos limitado (hasta 1 GB)
- Videollamadas punto a punto, escale sus chats con audio o video.
- Intercambiar mensajes instantáneos con otros usuarios mediante Avaya Spaces Direct Messaging.
- Únase a una reunión de Spaces.

Equinoccio de Avaya®Reuniones en línea

Equinoccio de Avaya®Meetings Online ofrece un servicio de suscripción opcional para comunicaciones unificadas de múltiples partes, es decir, colaboración de audio, video y web. El servicio proporciona una sala de reuniones virtual Over The Top (OTT) con conferencias de audio y video, intercambio de contenido, chat y moderación de reuniones. Los usuarios pueden acceder al servicio a través de un sistema de escritorio, móvil y de sala de video, así como acceso telefónico de audio; También se admite la interoperabilidad de sistemas de salas de video de terceros.

Aplicaciones de instalación y administración.

Las siguientes secciones proporcionan una descripción general de las aplicaciones relacionadas con la instalación y la administración.

Gerente de IP Office

Utilice Manager para administrar sistemas independientes de IP Office o sistemas en una red comunitaria pequeña (SCN). Manager realiza un seguimiento de los cambios de configuración del sistema, gestiona las actualizaciones y las importaciones y exportaciones de configuración.

IP Office tiene una pista de auditoría integrada que rastrea los cambios en la configuración del sistema y quién los ha realizado. El administrador puede mostrar la pista de auditoría para ayudar con la resolución de problemas. La pista de auditoría registra los últimos 15 cambios en la configuración y registra los siguientes elementos:

- Configuración cambiada: para los cambios de configuración, el registro informará a un alto nivel sobre todas las categorías de configuración (usuarios, grupo de búsqueda...) que hayan cambiado.
- Configuración borrada
- Configuración fusionada
- Reiniciar: reinicio instigado por el usuario

- Mejora
- Inicio fresco
- Arranque en caliente
- Escribir en HH:MM: esto es cuando el administrador guardó la configuración a través de la opción de programación
- Escritura con reinicio inmediato
- Escribir con Reiniciar cuando esté libre

IP Office Manager también se utiliza para funciones de mantenimiento como:

- Actualizar al software del sistema IP Office
- Capacidad de enviar software a través de un enlace de red IP a un sistema y validarlo antes de comprometerse con la actualización
- Compatibilidad con versiones anteriores de sistemas de la versión 2.1 en adelante para permitir una sola aplicación de administración
- Importación y exportación de información de configuración de IP Office en archivos ACSII-CSV.

Administrador de la edición del servidor

Server Edition Manager admite la administración centralizada completa para Server Edition Primary, Server Edition Secondary y Server Edition Expansion Systems. Manager también proporciona funciones de telefonía IP Office y comunicaciones unificadas.

Manager permite la gestión de todos los componentes dentro de la solución para actividades como:

- Punto único de configuración para IP Office y correo de voz
- Asistente de instalación inicial simple
- Resumen del sistema con inventario y estado
- Configuraciones comunes consolidadas en Server Edition Primary
- Procliente de correo de voz integrado, aplicación de estado del sistema y acceso a la configuración de la plataforma Linux
- Admite la administración en línea y fuera de línea y la configuración de una solución completa
- Operaciones de plantilla
- Configuración centralizada y almacenamiento de plantillas
- Utilidad de administración de cuentas de administrador
- Conserva la experiencia existente de IP Office
- Ayuda sensible al contexto

Aunque Manager es una aplicación de Windows, Manager se puede instalar directamente desde el portal de administración web del servidor primario de Server Edition. Esto le permite usar cualquier computadora personal con Windows que tenga IP Office Manager preinstalado inmediatamente.

Con Manager, el administrador puede crear plantillas para muchos elementos de administración, como usuarios, extensiones, grupos de búsqueda y líneas. El administrador puede entonces crear cualquier elemento nuevo usando

la configuración predeterminada o la plantilla. Puede crear múltiples usuarios y extensiones usando una plantilla.

Soporte de enrutamiento de llamadas:

- Compatibilidad total con IP Office ARS y plan de marcación
- El enrutamiento predeterminado simplifica la configuración
- Numeración automática de grupos de líneas en toda la solución
- Las rutas comunes de llamadas entrantes brindan resiliencia
- Grupos de búsqueda resistentes

Operación fuera de línea:

- La solución completa se puede crear y/o administrar fuera de línea si es necesario
- Todavía se puede administrar cuando algunos dispositivos están fuera de línea
- Opciones de sincronización de configuración en línea/fuera de línea para armonizar según sea necesario

Gestión de soluciones:

- Vista completa de la solución con estado e inventario
- Los usuarios y los grupos de búsqueda abarcan toda la solución
- Derechos de usuario centralizados, códigos cortos de función, perfiles de tiempo, rutas de llamadas entrantes y códigos de cuenta
- Permite la configuración avanzada por dispositivo si se desea
- Todas las configuraciones almacenadas en el servidor principal
- Directorio de todo el sistema de la solución
- Gestión sencilla de licencias centrales y por dispositivo

Gestión de la resiliencia:

- Puede administrar todos los dispositivos localmente para eventos de 'día lluvioso'
- Puede administrar la solución a través de un servidor secundario cuando el servidor principal falla o en una configuración de WAN dividida
- Opciones de sincronización de configuración On/Offline para armonizar según sea necesario

Agregar o quitar dispositivos:

- Proceso único para agregar o quitar el dispositivo
- Utilidad de configuración inicial (ICU) integrada para simplificar la adición de un nuevo dispositivo
- Los elementos de configuración comunes del servidor principal se completan automáticamente
- Puede configurar antes de instalar un nuevo dispositivo

Validación:

- Validación de la configuración en lectura y cualquier cambio.
- Validaciones de toda la solución

Modelo:

- Cree una plantilla local y centralizada a partir de entradas existentes de Línea, Extensión, Usuario, Grupo de búsqueda, Perfil de tiempo, Perfil de firewall, Ruta IP y Servicio
- Vuelva a crear múltiples extensiones y usuarios a partir de una plantilla

Acceso remoto:

- Admite el acceso desde el servicio a través de SSL VPN

Seguridad:

- Inicio de sesión único para todos excepto para la administración de one-X Portal

Administrador web

Web Manager es una herramienta de administración basada en navegador diseñada para simplificar el proceso de instalación y mantenimiento y proporciona acceso a la mayoría, pero no a todos, los ajustes de configuración de IP Office. Web Manager elimina la necesidad de tener un sistema operativo Windows porque puede ejecutarse en cualquier dispositivo que admita navegadores estándar.

Acceso granular:

Web Manager proporciona a los usuarios del servicio acceso a todos los objetos de configuración si el usuario del servicio tiene acceso a la configuración. Sin embargo, los grandes clientes que tienen varios roles de usuarios de servicios o los clientes que tienen implementaciones en el entorno de la nube deben tener acceso de configuración granular para diferentes usuarios de servicios. Los socios de alojamiento podrán crear una cuenta para el cliente o el revendedor con permisos limitados. Estos permisos impedirán que el cliente o el revendedor realicen actividades que afecten el servicio del sistema.

Panel de configuración:

El panel es una versión simplificada del IP Office Web Manager existente y se presenta a los administradores cuando se instala un nuevo sistema IP Office de un solo nodo. El Tablero consiste en un conjunto mínimo requerido de campos de configuración para configurar el sistema. La configuración completa se puede realizar en cualquier momento después.

Administrador de medios de IP Office

IP Office Media Manager es una aplicación nativa de IP Office para archivar, almacenar, buscar, reproducir, descargar, auditar y eliminar grabaciones de llamadas de IP Office. La operación, administración y gestión de (OAM) de la aplicación está integrada dentro de la solución IP Office, por ejemplo, IP Office Web Manager.

Media Manager obtiene las grabaciones de la aplicación IP Office Voicemail Pro a través de un directorio de transferencia preconfigurado. Media Manager mueve las grabaciones del directorio de traspaso a una partición de disco duro adicional en el servidor primario o de aplicaciones de Server Edition y luego archiva las grabaciones en una ubicación de almacenamiento configurada por el administrador. La ubicación de archivo puede ser un almacenamiento conectado a la red (NAS), una unidad de DVD local o un almacenamiento en la nube. Para el almacenamiento en la nube, Media Manager solo es compatible con Google Drive en esta versión.

Media Manager se licencia por sistema. Además de una nueva licencia de IP Office versión 11.0 y posterior de Media Manager, la aplicación también funciona con una licencia anterior de Contact Recorder, para clientes que actualizan desde una versión anterior de IP Office. Media Manager permite un período de prueba de 90 días antes de que se aplique la licencia.

Contact Recorder no es compatible con la versión 11.0 y posteriores de IP Office y no forma parte del software de la versión 11.0 y posteriores de IP Office. Sin embargo, Media Manager admite la migración de datos de Contact Recorder a IP Office versión 11.0 y posteriores.

Media Manager está disponible como parte de la imagen del software IP Office Server Edition y Application Server. La aplicación se ejecuta en la distribución estándar de Linux compatible con las plataformas IP Office Server Edition y Application Server. El software se instala como un RPM de Linux estándar solo en el servidor primario de Server Edition o en el servidor de aplicaciones en caso de implementaciones de IP500 V2. La aplicación no es compatible con las plataformas UCM o Windows. La interfaz de administración está basada en la web y son compatibles con todos los navegadores populares, como Google Chrome, Mozilla Firefox, Microsoft Edge y Microsoft Internet Explorer.

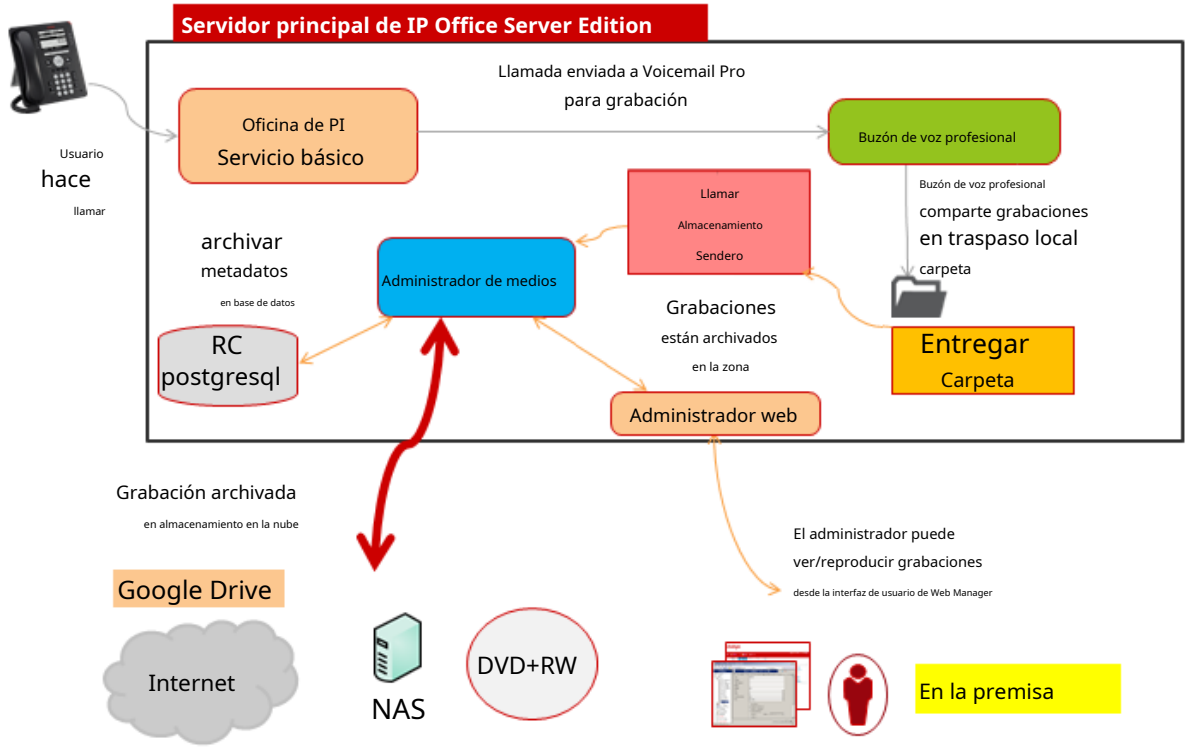
Media Manager en IP Office versión 11.0 Feature Pack 4 admite la eliminación o las grabaciones y realiza un seguimiento del uso de las grabaciones a través de la función de registro de auditoría. La función de seguimiento de auditoría lo ayuda a realizar un seguimiento de las actividades en torno a las grabaciones en la biblioteca. Con esta función, puede averiguar los usuarios que tienen:

- Buscó una grabación
- Reprodujo una grabación
- Descargado una grabación
- Eliminó una grabación

Para cada evento, Media Manager muestra el nombre de usuario, la fecha, la hora y el tipo de acción del usuario. La pista de auditoría se mantiene durante un número predefinido de días y se puede modificar. De forma predeterminada, los datos de la pista de auditoría están disponibles durante 180 días.

Media Manager está disponible como parte de la imagen del software IP Office Server Edition y Application Server. La aplicación se ejecuta en la distribución estándar de Linux compatible con las plataformas IP Office Server Edition y Application Server. El software se instala como un RPM de Linux estándar solo en el servidor primario de Server Edition o en el servidor de aplicaciones en caso de implementaciones de IP500 V2. La aplicación no es compatible con las plataformas UCM o Windows. La interfaz de administración está basada en la web y son compatibles con todos los navegadores populares, como Google Chrome, Mozilla Firefox, Microsoft Edge y Microsoft Internet Explorer.

Una implementación estándar de IP Office Server Edition:



Disponibilidad de las funciones de Contact Recorder en Media Manager

Las capacidades de búsqueda en Media Manager se han mejorado para los administradores y los usuarios.

Funcionalidad	Descripción	Disponibilidad en Contact Recorder	Disponibilidad en medios Gerente
Buscar por administrador	Buscar por administradores utilizando Número de destino, Habilidades, agente e ID de llamada	Sí	Sí
Buscar a través de la Web Autoadministración	Busque por usuarios utilizando los filtros de búsqueda Número objetivo, Habilidades, Agente, e ID de llamada	Sí	Sí
Búsqueda de autoadministración web resultados	Se muestra un máximo de 100 resultados.	Sí	Sí
Conjuntos de llamadas	Facilidad para guardar resultados de búsqueda para recuperarlos en el futuro.	Sí	No
Correo electrónico	Adjuntar grabaciones a correos electrónicos.	Sí	No

La tabla continúa...

Funcionalidad	Descripción	Disponibilidad en Contact Recorder	Disponibilidad en medios Gerente
Exportación a granel	Exportando múltiples grabaciones y la detalles relacionados	Sí	Sí
Dueño	Disponible como una opción de búsqueda.	No	Sí
Pista de auditoría	Se puede realizar una auditoría para rastrear el uso de grabaciones de llamadas.	Sí	Sí
Dominio de Windows Autenticación	-	Sí	No

Aplicación de gestión de soluciones

IP Office Manager y Web Manager utilizan la aplicación de administración de soluciones (SMA) para acceder a la configuración del sistema.

SMA reside en el servidor primario o secundario. Las configuraciones están disponibles para el acceso remoto y Server Edition Central Access. Central Access se comunica con el servidor primario o secundario en lugar de con cada nodo individualmente. Avaya requiere Central Access para un entorno alojado y lo recomienda para entornos no alojados con más de 32 nodos.

Modo Administrador de SoftConsole

Los administradores del sistema pueden iniciar SoftConsole en modo administrador. Cuando se ejecuta en este modo, no hay acceso a las funciones de telefonía.

El modo de administrador de SoftConsole permite a los usuarios configurar las siguientes funciones:

- Crear y editar perfiles de usuario
- Modificar la longitud de las notas de llamada
- Crear y editar plantillas
- Eliminar o mostrar los paneles de interfaz

Consola de administración SNMP

El Protocolo simple de administración de redes (SNMP) es un estándar de la industria diseñado para permitir la administración de equipos de datos de diferentes proveedores mediante una sola aplicación Network Manager. El administrador de la red sondea periódicamente el equipo para solicitar una respuesta, si no se recibe una respuesta, se genera una alarma. Además de responder a las encuestas, IP Office monitorea el estado de sus extensiones, tarjetas de troncales, módulos de expansión y tarjetas de medios para que, si se detecta un error, IP Office notifique al administrador de la red.

Dado que la plataforma IP Office comprende muchas aplicaciones, el software central notifica los eventos SNMP de Voicemail Pro y Embedded Voicemail para advertir acerca de los límites de capacidad de almacenamiento que se aproximan.

IP Office envía notificaciones por correo electrónico directamente al servidor de correo electrónico; no se necesita un cliente de PC adicional.

En los sitios de los clientes donde la administración de SNMP no está disponible, IP Office puede enviar eventos por correo electrónico usando hasta 3 direcciones de correo electrónico, cada una con un conjunto diferente de alarmas.

Las siguientes categorías de eventos del sistema se pueden elegir para la notificación por correo electrónico, si están instaladas en el sistema:

- Genérico
- Líneas troncales
- Tarjeta de correo de voz integrada
- VCM
- Módulos de expansión
- Aplicaciones
- Licencia
- Cambio de teléfono
- Circuito cerrado de CSU

IP Office ha sido probado contra SNMPc-EE de CastleRock™y Network Node Manager de HP (parte del paquete de aplicaciones OpenView).

Solicitud de estado del sistema (SSA)

La aplicación de estado del sistema (SSA) es una herramienta de diagnóstico para que los administradores y administradores de sistemas supervisen y verifiquen el estado de los sistemas IP Office de forma local o remota. SSA muestra el estado actual de un sistema IP Office y los detalles de cualquier problema que haya ocurrido. La información reportada es una combinación de eventos en tiempo real, eventos históricos, estado y datos de configuración para ayudar a encontrar y diagnosticar fallas. SSA proporciona estado en tiempo real, uso histórico e información de alarmas para puertos, módulos y tarjetas de expansión en el sistema. SSA se conecta a todas las variantes de IP Office mediante una conexión IP que puede ser remota o local. Se admiten conexiones de módem a 14,4 kbps o más para diagnósticos remotos.

La SSA proporciona información sobre lo siguiente:

alarmas	SSA muestra todas las alarmas registradas en IP Office para cada dispositivo con error. Se registra el número, la fecha y la hora de la ocurrencia. Las últimas 50 alarmas se almacenan en IP Office para evitar la necesidad de una PC local.
Detalles de la llamada	Información sobre llamadas entrantes y salientes, incluida la duración de la llamada, la identificación de la llamada y la información de enrutamiento.
Extensiones	SSA detalla todas las extensiones (incluido el tipo de dispositivo y la ubicación del puerto) en el sistema IP Office. También se muestra información sobre el estado actual de un dispositivo. SSA muestra las extensiones de IP que se registraron pero que ya no están disponibles y las extensiones de IP que están configuradas pero que no se han registrado después del último reinicio. Esto ayuda a detectar teléfonos inactivos, desconectados o mal configurados. SSA también muestra teléfonos en cuarentena y extensiones y direcciones IP en la lista negra.

Bañador	Se muestran las troncales y conexiones de IP Office (VoIP, analógicas y digitales) y su estado actual. Para troncales VoIP, también se muestra información de QoS (p. ej., retraso de ida y vuelta, fluctuación y pérdida de paquetes).
Sistema Recursos	IP Office incluye recursos centrales que se utilizan para realizar diversas funciones. El diagnóstico de estos recursos suele ser fundamental para el funcionamiento correcto del sistema. Esto incluye detalles sobre recursos para VCM, correo de voz y conferencias.
QoS Vigilancia	Se monitorean los parámetros de QoS de las llamadas conectadas, como la fluctuación y el retraso de ida y vuelta.

SSA se puede iniciar de forma independiente o desde IP Office Manager y puede haber hasta dos (2) clientes SSA conectados a una unidad IP Office a la vez.

Nota: SSA no es una herramienta de configuración para sistemas IP Office.

monitor de sistema

Utilice SysMonitor para solucionar problemas de IP Office desde ubicaciones locales (LAN) y remotas (WAN).

Seleccione los protocolos e interfaces para monitorear y diagnosticar a través de una interfaz gráfica. Capture los rastros directamente en la pantalla o como un archivo de registro para un análisis posterior. Codifique con colores diferentes trazos para mejorar la claridad en archivos grandes. La utilidad también captura las alarmas del sistema y muestra el registro de actividad de las últimas 20 alarmas que ocurrieron.

Gerente de Operaciones en la Nube

Cloud Operations Manager es una herramienta de administración que permite una forma simplificada de gestión de múltiples clientes con un enfoque en los sistemas basados en la nube. La herramienta permite la administración de sistemas IP Office Server Edition y brinda las siguientes capacidades:

- Portal único de administración unificada capaz de administrar hasta 3000 sistemas IP Office.
- Tablero que muestra las condiciones de error, las actividades del sistema en curso y el estado del sistema
- Agrupación de sistemas basada en versiones y etiquetas para acceder a sistemas similares con solo hacer clic en un botón
- Muestra todos los sistemas conectados, como Primario, Secundario, Expansiones y aplicaciones abiertas
- Capacidad para administrar de forma centralizada actualizaciones y parches de software de IP Office en múltiples sistemas y versiones
- Administración basada en roles: Cloud Operations Manager tiene sus propios usuarios del servicio con acceso a IP Office de clientes completos o selectivos. No hay acceso granular a nivel de función disponible en la versión 11.0.
- Ofrece la posibilidad de iniciar aplicaciones de gestión de IP Office nativas. Los usos deben iniciar sesión en las aplicaciones por separado después de iniciar la aplicación. El lanzamiento de IP Office Contact Center, Avaya Contact Center Select y Avaya Workforce Optimization Select no son compatibles con la versión 11.0.

- Alarmas de Configuración, Servicios, Troncales, Enlace y Seguridad por tipo de Severidad
- Alarmas para el estado de los sistemas IP Office que indican si están en línea o fuera de línea
- Alarmas que indican el estado de varias aplicaciones

Administrador de migración de datos (DMM)

El Administrador de migración de datos (DMM) facilita la migración de los sistemas BCM y Norstar a IP Office. Hay tres pasos en el proceso de migración: extraer, convertir y aplicar.

DMM migra:

- Anuncios y saludos
- Mensajes de correo de voz
- Extraer la configuración de Call Pilot

aplicaciones de centros de contacto

Las siguientes secciones proporcionan una descripción general de las aplicaciones del centro de contacto.

Para información general sobre:

- IP Office Contact Center, consulte*Avaya IP Office Contact Center Característica Descripción*.
- Avaya Contact Center Select, consulte*Descripción de la solución Avaya Contact Center Select*.

Descripción general de IP Office Contact Center

Nota:

IP Office Contact Center finaliza la venta de nuevos sistemas en septiembre de 2019.

Avaya es el líder del mercado en tecnología de centros de llamadas e IP Office Contact Center puede llevar su negocio a un nuevo nivel. IP Office Contact Center proporciona capacidades integradas de centro de contacto diseñadas específicamente para empresas que admiten entre 5 y 250 agentes y supervisores de centro de contacto.

IP Office Contact Center ofrece las siguientes funciones y características:

- Solución de servicio al cliente todo en uno que brinda un servicio consistente a los clientes a través de múltiples canales de medios y ubicaciones. IP Office Contact Center incluye una interfaz de usuario (IU) en Microsoft Windows y una interfaz web compatible con varios navegadores.
- Implementación rápida con una interrupción mínima para el negocio. IP Office Contact Center también incluye una función de sincronización automática para la configuración. Esta función se puede habilitar y deshabilitar según sea necesario durante la implementación.
- Acceso a la funcionalidad de la interfaz de usuario del agente, incluido el control de llamadas, desde un complemento de SalesForce (SFDC) o un conector SAP CRM.
- Capacidades de correo electrónico y chat en Windows y Web UI.
- Llamadas de voz entrantes y salientes con capacidades de telefonía y marcador.
- Enrutamiento basado en habilidades.

• Acceso a la libreta de direcciones para que los agentes puedan encontrar rápidamente la información de contacto que necesitan para realizar llamadas y enviar correos electrónicos.

• Informes históricos y en tiempo real para todos los canales de medios.

• Scripts de respuesta de voz interactiva (IVR) y editor de flujo de tareas.

• Configuración de privilegios de perfil de usuario y grupo de agentes para determinar qué funciones están disponibles para los usuarios de la interfaz. Los administradores deben asignar privilegios y crear grupos de agentes.

• Acceso a un portal de administración basado en web. Puede utilizar el portal de administración para realizar tareas de configuración, mantenimiento, supervisión y gestión. También puede cargar certificados, recopilar registros y descargar archivos de correo electrónico y la interfaz de usuario de IP Office Contact Center para Windows. Las tareas de administración avanzada se deben realizar en la interfaz de usuario de IP Office Contact Center para Windows. No puede realizar tareas de administración con la interfaz de usuario web de IP Office Contact Center.

• Acceso a un tablero que muestra las estadísticas de IP Office Contact Center. Para obtener más información acerca de Tablero, consulte *Uso del tablero de IP Office Contact Center de Avaya*.

• Opción para integrar fácilmente la funcionalidad de chat en una página web. Para más información, ver *Guía basada en tareas de servicios de chat y correo electrónico de Avaya IP Office Contact Center*.

• Integración opcional con aplicaciones de grabación de llamadas, como IP Office Media Manager. Las llamadas se graban con Voicemail Pro y los detalles de la grabación completa se almacenan en la base de datos de la aplicación de grabación de llamadas. Puede buscar y administrar grabaciones utilizando un navegador web.

• Interoperabilidad opcional con Avaya Workforce Optimization Select, que es un producto independiente que actualmente no se integra con las IU o las aplicaciones de IP Office Contact Center.

• Integración del Protocolo de control de recursos de medios (MRCP), que brinda soporte para texto a voz (TTS) y reconocimiento de voz automático.

Descripción general de Avaya Contact Center Select

Avaya Contact Center Select es una solución de centro de contacto multimedia, de voz y colaborativa sensible al contexto que permite a las pequeñas y medianas empresas anticipar, acelerar y mejorar las interacciones con los clientes. Avaya Contact Center Select utiliza el sistema telefónico Avaya IP Office para proporcionar una plataforma de telefonía en tiempo real.

Avaya Contact Center Select utiliza interfaces SIP y CTI estándar de la industria para integrarse con IP Office. Esta integración brinda a Avaya Contact Center Select acceso y control de una amplia gama de teléfonos y funciones de IP Office. Los clientes que integran Avaya Contact Center Select con IP Office obtienen enrutamiento basado en habilidades, tratamiento de llamadas, generación de informes, administración unificada de agentes y la utilidad gráfica Diseñador de orquestaciones.

Avaya Agent Desktop es una aplicación de cliente de interfaz única utilizada por los agentes de Avaya Contact Center Select para ayudar a los clientes. Los agentes de Avaya Contact Center Select utilizan el software Agent Desktop para responder a los contactos multimedia y de voz del cliente. Agent Desktop es compatible con una variedad de teléfonos IP Office y una amplia variedad de tipos de contactos multimedia.

De manera predeterminada, las conexiones y los servicios web de Avaya Contact Center Select utilizan comunicación TLS segura. La herramienta de administración de certificados de Avaya Contact Center Select facilita la administración de certificados de seguridad.

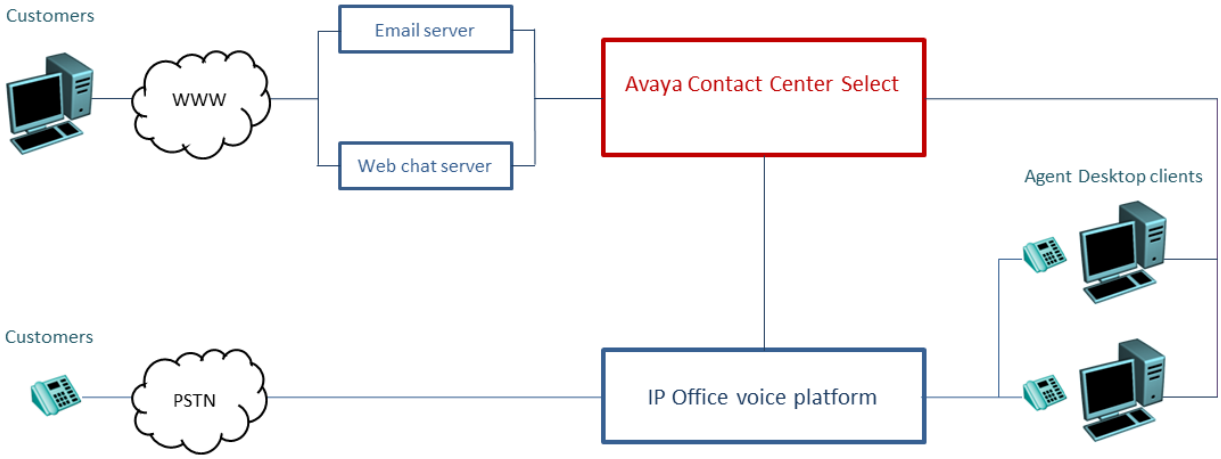


Figura 16: Solución típica de centro de contacto que usa voz y multimedia Avaya Contact Center Select y el sistema telefónico de voz Avaya IP Office

Avaya Contact Center Select proporciona una solución multimedia y de voz rica en funciones con enrutamiento e informes integrados para pequeñas y medianas empresas. Avaya Contact Center Select proporciona un centro de contacto unificado y administración de cuentas de usuario de teléfonos IP Office para agentes y supervisores. Los agentes y supervisores habilitados para voz creados en Avaya Contact Center Select se agregan automáticamente a IP Office. Avaya Contact Center Select sincroniza la información del usuario (agente y supervisor) entre Avaya Contact Center Select e IP Office.

Capítulo 3: Especificaciones de la solución

Configuraciones de referencia

IP Office se vende en diferentes ediciones, configuraciones de referencia y escenarios de implementación para cumplir con los diferentes requisitos de los clientes. Las ediciones se complementan entre sí para ofrecer funciones avanzadas, que incluyen presencia, mensajería instantánea, colaboración web e integración de software de Microsoft.

Las siguientes secciones resumen las ediciones de IP Office y otras opciones de configuración. Estas secciones no proporcionan detalles completos de configuración de referencia para cada opción de IP Office. Los documentos de configuración de referencia separados están disponibles para IP Office Server Edition, IP Office Branch, Powered by Avaya Cloud solutions e IP Office Contact Center.

Ediciones de IP Office

Edición básica de IP Office

IP Office Basic Edition está diseñado para empresas pequeñas y en crecimiento que necesitan una mayor productividad con un toque profesional. Las empresas pueden aumentar la capacidad según sea necesario.

IP Office Basic Edition proporciona funciones básicas de telefonía como:

- Capacidad de 64 troncales: analógica, PRI/T1 y SIP
- Operación del sistema clave
- Capacidad de conferencias para 64 personas
- Operadora automática
- Compatibilidad con varios idiomas
- Reenvío de llamadas
- Identificador de llamadas
- Marcar por nombre
- Salida a recepción
- Correo de voz integrado:
  - Máximo de 6 llamadas simultáneas al correo de voz con aproximadamente 25 horas de almacenamiento
  - Control de mensajes que incluye Guardar, Eliminar, Reenviar, Repetir, Rebobinar, Avance rápido y Omitir mensaje

Página617 de 3226.

- Correo de voz visual

- Estampado de fecha y hora del mensaje

Modos de operacion

Las unidades de control IP500V2 se suministran sin firmware ni configuración instalados. Cuando se enciende por primera vez, la unidad de control carga e instala el firmware necesario desde la tarjeta SD del sistema instalada en ella. Crea una configuración predeterminada que coincide con la tarjeta instalada en la unidad de control y los módulos de expansión externos conectados a ella. Las unidades de control IP500V2 pueden operar en varios modos. El modo inicial está determinado por el tipo de tarjeta SD del sistema.

Modo	tarjeta SD
Modo rápido de IP Office Basic Edition	• Operación del sistema PBX de telefonía de ley. • Operación del sistema de clave de telefonía ley µ.
IP Office Basic Edition - Modo SOCIO	El valor predeterminado es el funcionamiento en modo PARTNER de telefonía de ley.
Edición básica de IP Office - Modo NORSTAR	El valor predeterminado es la operación del modo NORSTAR de telefonía de ley µ.

Basic Edition se ejecuta en la unidad de control IP500V2. Se requiere una SD y está instalada en la parte posterior de la unidad de control, que proporciona software operativo, teclas de función y licencias. Se puede instalar una tarjeta SD opcional en la ranura para tarjeta SD opcional, lo que proporciona capacidades de actualización del sistema y copias de seguridad redundantes.

Tabla 5: Tarjetas base admitidas

Basic Edition admite las siguientes tarjetas base:

Tarjeta básica	modo SOCIO Máximo por sistema	Modo NORSTAR Máximo por sistema
combinación analógica	4	4
Combinación BRI		2
ETR6	3	
DS8	3	3
TCM8	4	4
Teléfono 2	4	4
Teléfono 8	4	4

Tabla 6: Tarjetas de troncales admitidas

Basic Edition admite las siguientes tarjetas troncales:

Tarjeta de troncal	modo SOCIO Máximo por sistema	Modo NORSTAR Máximo por sistema
Cajero automático4	4	4
PRI/T1	1	
PRI/E1		1

La tabla continúa...

Tarjeta de troncal	modo SOCIO Máximo por sistema	Modo NORSTAR Máximo por sistema
BRI4		4
BRI8		1

Módulos de expansión

Basic Edition admite los siguientes módulos de expansión:

- DS16A
- DS16B
- DS16B2
- Cajero automático16
- Teléfono 16
- Teléfono 30
- DS30A
- DS30B
- DS30B2

Nota:

Los módulos de estación digital DS16B2 y DS30B2 son compatibles con las versiones 10.1, 9.1 SP12 y 10.0 SP5 de IP Office en adelante.

Edición esencial de IP Office

IP Office Essential Edition ofrece las mismas funciones que Basic Edition además de lo siguiente:

- Control de llamadas móviles con acceso a un número y timbre simultáneo en dispositivos móviles
- Hasta 4 trabajadores remotos a través de una conexión a Internet y un teléfono IP serie 9600 de Avaya
- Acceso las 24 horas con saludos de correo de voz personalizados para cada miembro del personal
- Mensaje de voz:
  - Máximo de 6 llamadas simultáneas al correo de voz
  - Enviar mensajes de voz al correo electrónico
  - Hasta 25 horas de almacenamiento de correo de voz (con 6 puertos)
  - Hasta 40 operadores automáticos con un máximo de 6 llamadas simultáneas
- Compatibilidad con varios idiomas
- Puente de audioconferencia de hasta 128 participantes con 64 en cualquier conferencia

Nota:

La Edición Básica no es un requisito previo para la Edición Esencial o la Edición Preferida, y no se apila bajo la Edición Esencial.

Edición preferida de IP Office

IP Office Preferred Edition proporciona enrutamiento inteligente de llamadas, mensajería, manejo de llamadas e integración de aplicaciones.

Además de las funciones proporcionadas con Essential Edition, IP Office Preferred Edition ofrece lo siguiente:

- Correo de voz escalable:
  - Hasta 40 llamadas simultáneas
  - Envíe un mensaje de voz a todos los empleados, un departamento o un equipo
  - Mensajes de dirección por extensión o por nombre
  - Los mensajes de correo de voz pueden "encontrar" a los usuarios para alertarlos de que hay un mensaje en espera.
- Conferencias seguras para hasta 128 participantes con 64 por conferencia
- Enrutamiento de llamadas automatizado con un número ilimitado de asistentes automáticos que se pueden personalizar según la hora del día, el día de la semana u otras variables, así como para reconocer a las personas que llaman y entregar mensajes personalizados
- Grabación de llamadas para llamadas entrantes y salientes que se pueden enviar al correo de voz o bandejas de entrada de correo electrónico como archivos WAV

Componentes

- Unidad de control IP500 V2
- PC con conexión Ethernet que ejecuta la versión compatible de Windows Server
- PC conectada a Ethernet configurada con el software del servidor de aplicaciones
- Cliente de correo IMAP (Outlook) para sincronización de correo de voz en el correo electrónico y acceso basado en navegador al correo de voz
- Troncales y canales digitales para apoyar a los usuarios
- Teléfonos compatibles con IP Office

Edición de servidor de IP Office

IP Office Server Edition proporciona funciones de telefonía, comunicaciones unificadas, movilidad y colaboración de IP Office. También proporciona alta disponibilidad, facilidad de uso y bajo costo total de propiedad (TCO). Dirigida a la mediana empresa, IP Office Server Edition admite hasta 150 sitios, 3000 usuarios y resiliencia integral.

La solución IP Office Server Edition proporciona lo siguiente:

- Un único servidor primario de Server Edition proporciona IP Office, Voicemail Pro y Avaya one-X® Portal de IP Office.
- Un servidor secundario de Server Edition aumenta la capacidad y proporciona resiliencia.
- Sistemas de expansión, que brindan capacidad adicional, admiten interfaces analógicas o digitales y ubicaciones remotas.
- Una solución Select IP Office Server Edition proporciona capacidad adicional.
- Compatibilidad con una unidad de control IP500 V2 existente optimizada para implementaciones híbridas de analógico/TDM e IP, o un servidor Linux optimizado para implementaciones únicamente de IP.

Traducido del inglés al español - www.onlinedoctranslator.com

- Los usuarios y las extensiones se pueden configurar en el servidor IP Office Server Edition o en el Sistema de expansión Server Edition.
- La distribución de software incluye las diversas aplicaciones de usuario y administración, como IP Office Manager, SSA, Voicemail Pro e IP Office SoftConsole.
- Los componentes pueden estar en la misma ubicación o en diferentes ubicaciones.
- Opcionalmente, configure un servidor de aplicaciones separado dedicado a Avaya one-X®Portal para proporcionar más capacidad de usuarios que la que admite Server Edition Primary.
- Agregue servidores adicionales y sistemas de expansión en cualquier momento.

.

Topología

IP Office Server Edition se basa en una topología de red de doble estrella que brinda funciones integrales y su administración, facilita el uso, la instalación y la administración. La solución general proporciona una arquitectura flexible y modular que comienza con un solo servidor y puede escalar la cantidad de usuarios y ubicaciones mediante la conexión en red de varios servidores. Los componentes actúan automáticamente como una única unidad lógica y puede administrar los componentes desde una única consola a través de un sistema de gestión integrado.

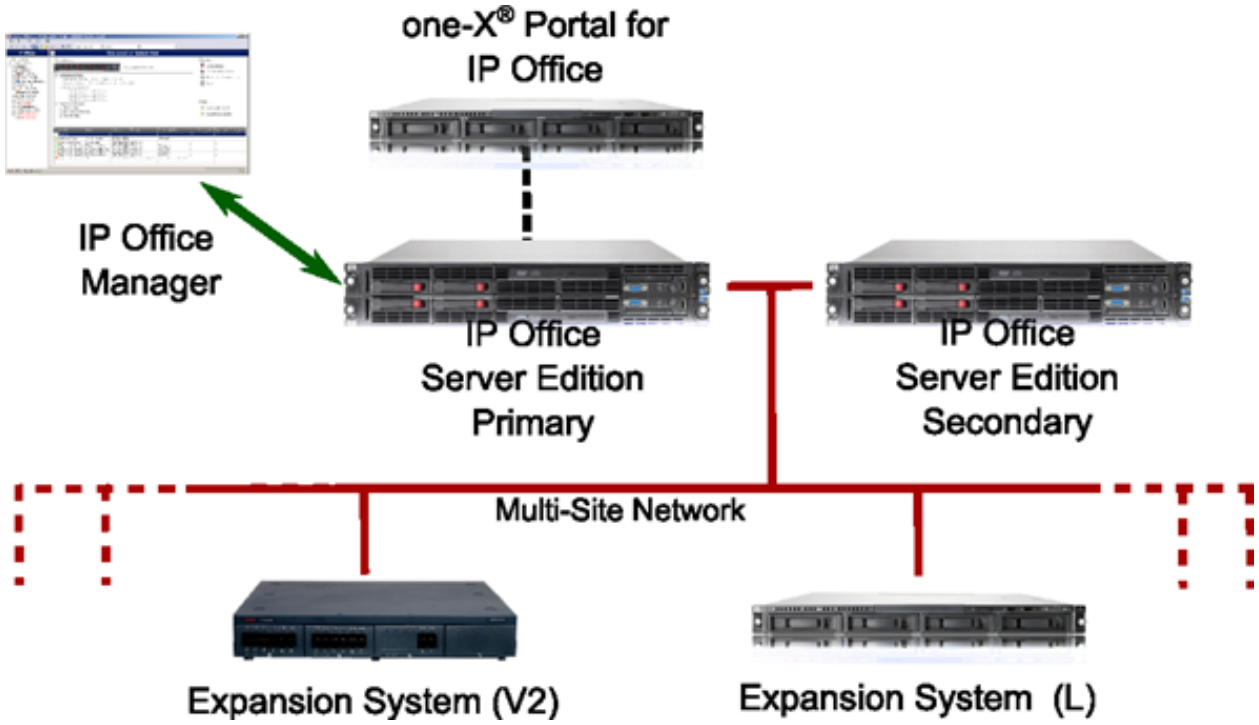


Figura 17: Topología de IP Office Server Edition

Modelos de implementación

Solo IP centralizada	Un servidor principal ubicado en la sede del cliente

IP analógica centralizada y digitales	Un servidor principal y un servidor de expansión ubicados en la sede del cliente
Solo IP distribuida	Un servidor principal ubicado en la sede del cliente y un servidor secundario ubicado en una ubicación remota
IP analógica distribuida y digitales	Un servidor primario y un sistema de expansión ubicado en la sede del cliente y un sistema de expansión ubicado en cada sitio remoto
virtualizado ambiente	Software y hardware proporcionados por el cliente Plataforma VMware vSphere con IP Office Server Edition y servidor de aplicaciones OVA activado como servidor principal, secundario, de expansión o de aplicaciones.

Componentes

Componente	Opciones del servidor	Descripción
Edición del servidor servidor principal	dell r630 dell r620 HP DL360G7 dell r220 dell r210 HP DL120G7	La distribución de software incluye: • Edición de servidor de IP Office • Correo de voz Pro • Avaya one-X®Portal para IP Office • Administrador de IP Office • Solicitud de estado del sistema (SSA) • SoftConsole
Edición del servidor servidor secundario	dell r630 dell r620 HP DL360G7 dell r220 dell r210 HP DL120G7	Componente opcional para soportar la resiliencia ya sea de forma centralizada o en un sitio remoto.
Edición del servidor Expansión Sistema	dell r630 dell r620 HP DL360G7 dell r220 dell r210 HP DL120G7	Componente opcional para admitir ubicaciones remotas. Hasta 148 sistemas de expansión brindan capacidad adicional, admiten interfaces analógicas o digitales y troncales locales en sitios remotos. Se puede configurar de forma centralizada o en un sitio remoto. **Nota:** En un entorno de nube, el sistema de expansión IP500 V2 brinda soporte para puntos finales analógicos y digitales.

La tabla continúa...

Componente	Opciones del servidor	Descripción
Edición del servidor Expansión Sistema	IP500 V2	Componente opcional para admitir ubicaciones remotas y como puerta de enlace. Puede ser un servidor IP500 V2 o IP Office Server Edition existente. Se puede configurar de forma centralizada o en un sitio remoto.
Avaya one-X® Portal de PI aplicación de oficina servidor	dell r630 dell r620 HP DL360G7 dell r220 dell r210 HP DL120G7	Componente opcional. Opcionalmente, puede configurar un servidor de aplicaciones separado dedicado a Avaya one-X®Portal para proporcionar más capacidad de usuarios avanzados por encima del máximo que admite Server Edition Primary.

Componentes del entorno virtualizado

Avaya proporciona un equivalente virtualizado de IP Office Server Edition y un servidor de aplicaciones empaquetado como un solo OVA listo para instalarse en hardware de host compatible con vSphere desde una PC. El OVA está disponible como descarga de Avaya o en un DVD que se puede pedir. Una vez implementado, puede activarse como servidor primario, secundario, de expansión o de aplicaciones.

Otras opciones de implementación

También puede implementar IP Office en:

- Un entorno de sucursal empresarial (sucursal de IP Office centralizada) o un entorno de sucursal distribuida).

  Puede implementar un sistema IP Office como una sucursal independiente o conectarlo a Avaya Aura® la red. También se admite un entorno de sucursal CS 1000.

- Un entorno Cloud con las ofertas Powered by Avaya.

Las opciones del centro de contacto también están disponibles.

Descripción general de IP Office como sucursal empresarial

Puede implementar IP Office como una sucursal empresarial para brindar una solución de comunicaciones adaptable para satisfacer las crecientes necesidades de una red de sucursal empresarial al mismo tiempo que brinda protección de la inversión en la plataforma de hardware y los teléfonos instalados. Puede implementar una sucursal empresarial de IP Office en un sistema de modo estándar, esencial o preferido de IP Office. El sistema IP Office puede instalarse como una sucursal independiente e independiente o conectarse a Avaya Aura®red y migró a una sucursal empresarial distribuida, centralizada o mixta para proporcionar características y aplicaciones específicas para satisfacer las necesidades de los empleados individuales en cada sucursal.

Además de los terminales SIP centralizados o los dispositivos analógicos centralizados configurados como ATA, IP Office puede admitir simultáneamente otros terminales IP y TDM para una comunidad de usuarios centralizados y usuarios de IP Office en la misma sucursal. Ideal para empresas que desean implementar aplicaciones en el cliente

Página623 de 3226.

centros de datos o en la sucursal, una sucursal de IP Office puede ofrecer de manera efectiva una variedad de herramientas de comunicación sin infraestructura ni administración complejas.

IP Office también es compatible con un entorno de sucursal de Avaya Communication Server 1000 (CS 1000). Solo se admite la opción de sucursal empresarial distribuida. IP Office se puede implementar como una nueva sucursal en una configuración CS 1000 existente con la adición de Avaya Aura®
Session Manager al que se conecta IP Office a través de la línea SM para la conectividad de la sucursal. Al brindar protección de la inversión telefónica, IP Office también se puede implementar como reemplazo de Business Communications Manager (BCM) o Norstar en una sucursal y conectarse a CS 1000 a través de Avaya Aura.®
Administrador de sesiones. IP Office no puede funcionar como una puerta de enlace recuperable para puntos finales CS 1000 de forma similar a la puerta de enlace remota recuperable (SRG).

Topología

La solución IP Office Branch brinda la flexibilidad para admitir sucursales independientes e independientes de IP Office, así como sucursales de IP Office conectadas a Avaya Aura.®sistema. La solución Branch también es compatible con la integración de CS 1000. Las siguientes opciones de implementación están disponibles para la arquitectura de la solución:

- **Opción de sucursal independiente de IP Office**: Los sistemas IP Office independientes se implementan dentro de la red. Estos sistemas IP Office no están conectados entre sí ni con ninguna otra cosa en la red. Con esta opción, las sucursales de IP Office no están conectadas a un Avaya Aura®
  sistema y los usuarios no pueden acceder a ningún Avaya Aura®servicios.
- **Opción de implementación de sucursales empresariales distribuidas**: Todos los usuarios de esta opción de implementación son usuarios de IP Office. Estos usuarios de IP Office obtienen servicios de telefonía de la IP Office local y no de Avaya Aura.®. Los sistemas IP Office en esta opción de implementación se pueden conectar a Avaya Aura®Session Manager y los administradores pueden obtener servicios de administración centralizados a través de Avaya Aura®Administrador de sistemas. La empresa puede optar por conectar a los usuarios de IP Office en esta opción de implementación a un sistema de correo de voz de IP Office, Embedded Voicemail o Voicemail Pro, o un sistema de correo de voz centralizado, como Avaya Aura.®
  Mensajería o Avaya Modular Messaging. Los usuarios de IP Office en esta implementación también tienen acceso a algunos Avaya Aura centralizados.®aplicaciones y servicios.

  Con la opción de implementación de sucursal distribuida, también puede conectar CS 1000 a IP Office en la sucursal a través de Avaya Aura®Administrador de sesiones. Los usuarios aún obtienen servicios de telefonía de IP Office local, pero pueden usar Avaya CallPilot®como su sistema de correo de voz. Cuando se conecta a CS 1000, IP Office y CS 1000 interoperan como pares a través de Avaya Aura®Administrador de sesiones.

- **Opción de implementación de sucursal empresarial centralizada**: Todos los usuarios de la empresa son usuarios centralizados.

  Registro centralizado de usuarios en Avaya Aura®Session Manager y obtener servicios de telefonía de Avaya Aura®Communication Manager Feature Server o Evolution Server en el núcleo empresarial. Si la conectividad WAN a Avaya Aura®Si se pierde Session Manager, el usuario obtiene automáticamente los servicios básicos de telefonía de la IP Office local. Las funciones de telefonía proporcionadas por IP Office en el modo de supervivencia son limitadas en comparación con las funciones que normalmente se brindan al teléfono centralizado.

  Los usuarios centralizados deben configurarse en Avaya Aura®Administrador de sesiones, administrador de comunicaciones e IP Office. Se debe configurar un usuario centralizado en Avaya Aura®Sesión

Gerente y Avaya Aura®Communication Manager como usuario SIP. En IP Office, el usuario centralizado debe tener una extensión SIP, una extensión analógica o un dispositivo de fax analógico.

- **Opción de implementación de sucursales empresariales mixtas**: una sucursal empresarial con usuarios centralizados y usuarios de IP Office. Los usuarios centralizados y los usuarios de IP Office obtienen los mismos servicios de telefonía descritos anteriormente. Todos los usuarios en esta opción de implementación deben usar un sistema de correo de voz centralizado: Avaya Aura®Mensajería o Avaya Modular Messaging.

Las opciones de implementación en la solución Branch le permiten comenzar con sistemas IP Office independientes y luego evolucionar lentamente la arquitectura de la solución hacia un entorno centralizado a medida que crece su empresa.

La siguiente imagen muestra la topología de la arquitectura de la solución con las opciones de implementación descritas anteriormente. Esta imagen no muestra CS 1000 en la implementación de sucursales distribuidas.

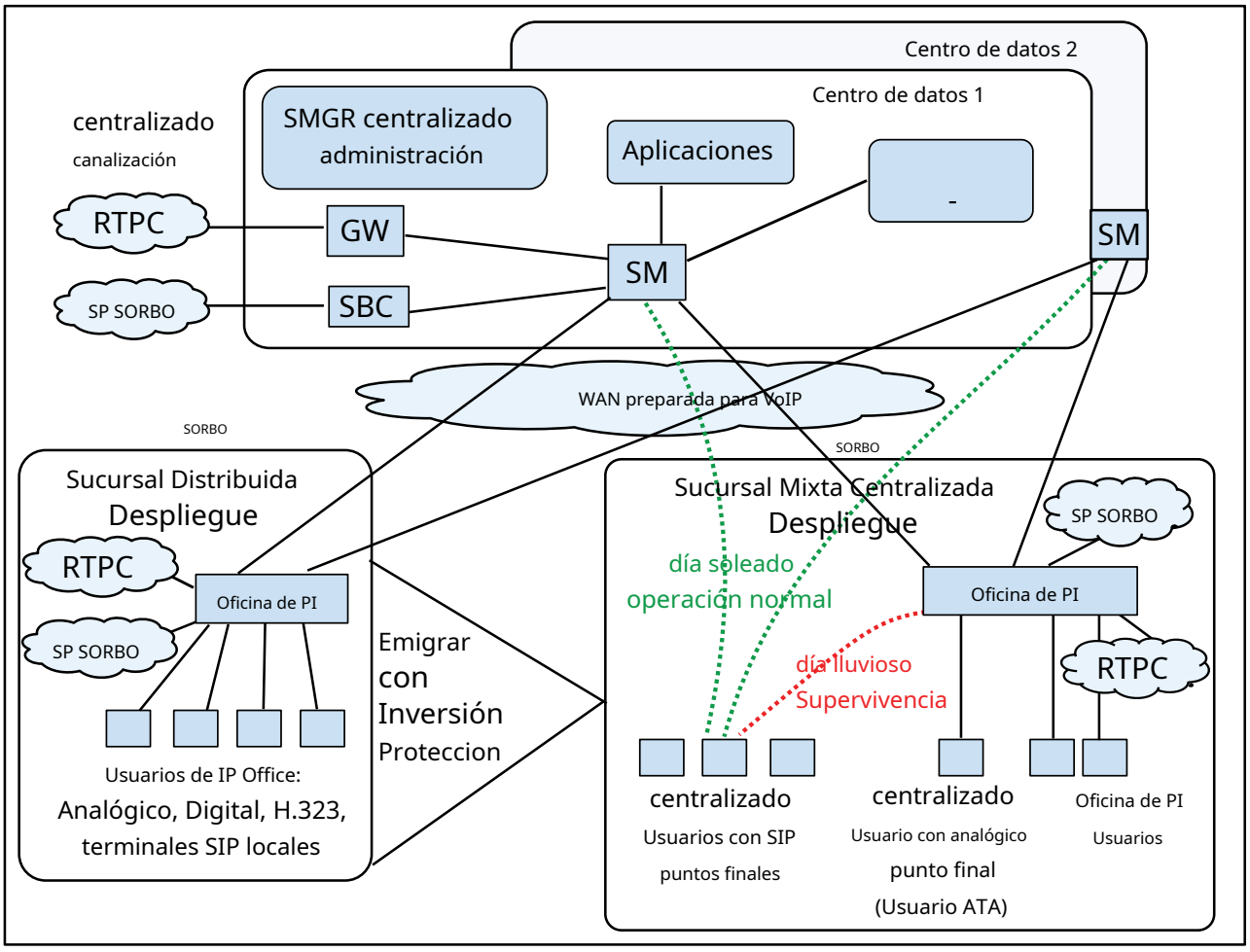


Figura 18: Topología de la arquitectura de la solución

Descripción general de Avaya Cloud

La solución Powered by Avaya Cloud le permite a usted, el BP o el proveedor, vender funciones principales de IP Office y, opcionalmente, IP Office Contact Center o Avaya Contact Center Select, a pequeñas y medianas empresas.

usuarios empresariales. Con Powered by Avaya, instala y aloja las instancias del producto en un centro de datos en la nube en su sitio.

La solución Powered by Avaya Cloud existente le permite a usted, el BP o el proveedor, vender funciones principales de IP Office y, opcionalmente, IP Office Contact Center o Avaya Contact Center Select, telefonía y comunicaciones unificadas (UC) a usuarios de pequeñas y medianas empresas. Con la nueva oferta de IP Office Cloud, los componentes opcionales de IP Office Contact Center y Avaya Contact Center Select no son compatibles. La funcionalidad de nube híbrida, Voicemail Pro y Media Manager tampoco son compatibles con la nueva oferta de IP Office Cloud. Esta oferta actualmente utiliza Embedded Voicemail como su sistema de correo de voz.

Con la oferta Powered by Avaya existente, instala y aloja las instancias del producto en un centro de datos en la nube. La nueva IP Office Cloud está alojada en un entorno de Google Cloud con un clúster de IP Office por proveedor.

Los beneficios clave de la solución en la nube incluyen lo siguiente:

- Reducción de los costos operativos para la empresa al reducir la complejidad de TI del mantenimiento del equipo.
- Reducción de costos de entrega de servicios para la BP a través de virtualización e infraestructura compartida.
- Interfaz programática para admitir instalaciones de licencias, configurar licencias centralizadas o eliminar un archivo de licencia.
- Facturación automatizada con Avaya One Source Cloud Services.
- Flexibilidad para cambiar su orden de Avaya One Source Cloud Services en cualquier momento. Puede agregar o eliminar usuarios en cualquier momento. Puede actualizar su pedido para agregar o eliminar los programas opcionales IP Office Contact Center y Avaya Contact Center Select, según sea necesario.
- Soporte para sistemas de expansión IP500 V2 en el sitio empresarial con Hybrid Cloud. Esto no se aplica a la nueva oferta de IP Office Cloud.
- Compatibilidad con resiliencia con alta disponibilidad (HA).

Desarrollado por la topología de Avaya

Desarrollado por Avaya es compatible con los siguientes modelos de implementación:

- Red pública: este modelo de implementación utiliza una conexión pública a través de Internet entre el centro de datos de la nube y las instalaciones de la empresa. Todos los usuarios que se conectan a través de la red pública se consideran trabajadores remotos.
- Red privada: este modelo de implementación requiere una conexión VPN de sitio a sitio o MPLS entre el centro de datos de la nube y las instalaciones de la empresa.

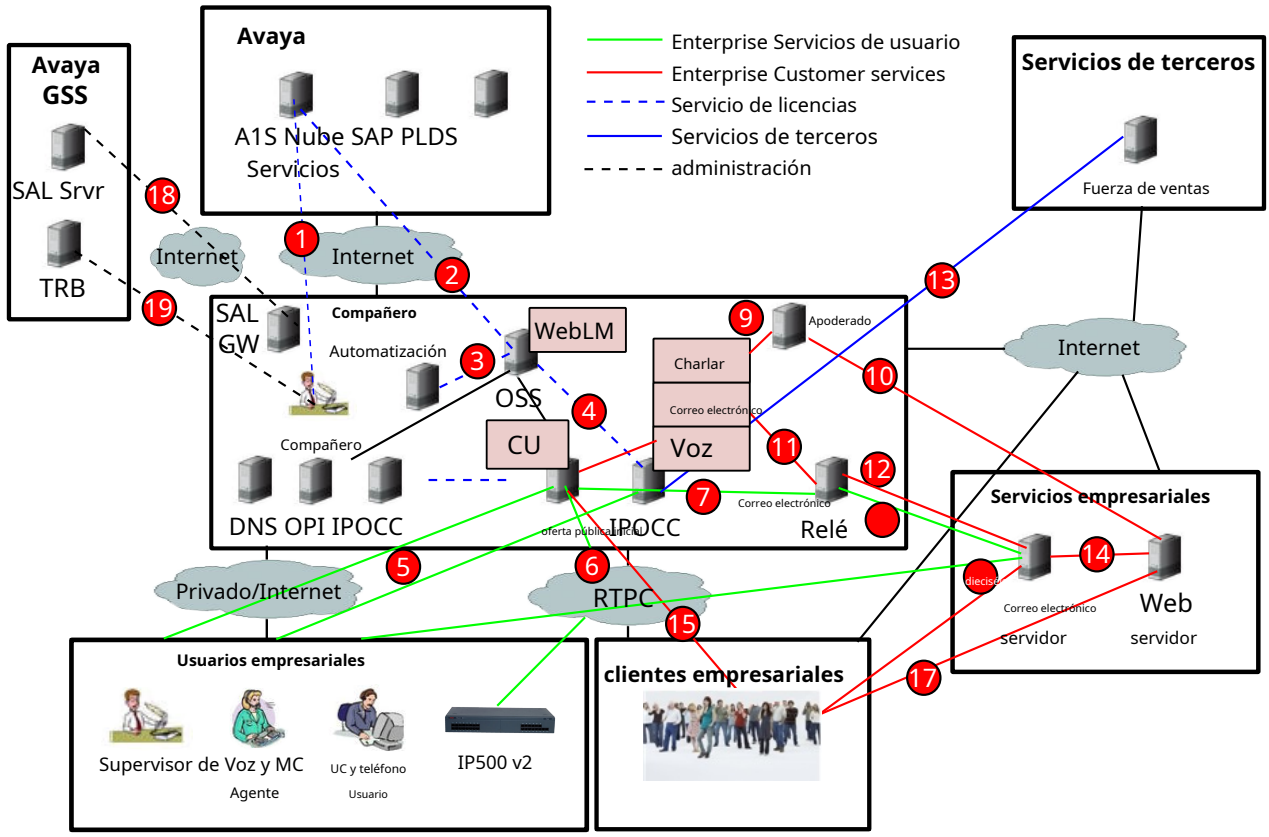


Figura 19: Topología Powered by Avaya

Configuraciones de referencia del centro de contacto

Opciones de implementación de IP Office Contact Center

IP Office Contact Center se puede implementar mediante las siguientes configuraciones y opciones de implementación:

Configuración	Opciones de implementación	Agentes y baúles
Centro de contacto de IP Office con IP500V2	IP500V2, servidor de IP Office Contact Center y un servidor de aplicaciones	Hasta 30 agentes en SIP y troncales digitales.
IP Office Contact Center con IP Office Server Edition	Servidor IP Office Server Edition y servidor IP Office Contact Center *y/o* un servidor de expansión Linux (opcional) *o* Alojado como un servicio en un entorno de nube	Hasta 250 agentes en troncales SIP. Solo se pueden implementar 125 agentes en cada Linux nodo de expansión.

La tabla continúa...

Configuración	Opciones de implementación	Agentes y baúles
IP Office Contact Center con IP Office Server Edition y Expansión IP500V2	Servidor IP Office Server Edition, servidor de expansión IP500V2 y servidor IP Office Contact Center	Hasta 250 agentes en SIP y troncales digitales. Solo se pueden implementar 30 agentes en cada nodo IP500V2.
IP Office Contact Center con IP Office Server Edition en un entorno distribuido	Servidor IP Office Server Edition, servidor de expansión IP500V2, servidor IP Office Contact Center y una expansión de Linux en un sistema distribuido ambiente	Hasta 250 agentes en SIP y troncales digitales. Se pueden implementar hasta 30 agentes en cada nodo IP500V2 y se pueden implementar hasta 125 agentes en cada nodo de expansión de Linux. Los agentes y troncales se distribuyen en cualquier servidor de expansión.

Las topologías detalladas de IP Office Contact Center se muestran en los siguientes documentos:

- *Avaya IP Office Contact Center Característica Descripción*
- *Configuración de referencia de Avaya IP Office Contact Center*

Configuraciones de referencia de Avaya Contact Center Select

Avaya Contact Center Select es una solución de centro de contacto rica en funciones que proporciona enrutamiento basado en habilidades para los contactos multimedia y de voz del cliente. Avaya Contact Center Select proporciona amplias herramientas para la gestión de agentes, informes históricos y en tiempo real, y herramientas gráficas para crear flujos de contacto y reglas de tratamiento. Proporciona administración de licencias, redes y servicios web de interfaces abiertas. Los clientes que integran Avaya Contact Center Select con la plataforma IP Office obtienen enrutamiento basado en habilidades, tratamientos de llamadas, informes, administración unificada de agentes y la utilidad gráfica Orchestration Designer.

En el momento de la implementación, Avaya Contact Center Select inicia automáticamente un asistente de configuración simple para implementar rápidamente una solución de centro de contacto funcional. Está precargado con usuarios de muestra, conjuntos de habilidades y parámetros del centro de contacto. Utilice estos datos de muestra para poner en marcha rápidamente la solución y realizar la primera llamada de cliente enrutada y contacto por correo electrónico.

Avaya Contact Center Select admite los siguientes tipos de contactos enrutados:

- Voz
- Correo electrónico
- Saliente
- Comunicaciones web (chat web)
- Mensajes de texto SMS
- Mensajes de fax
- Documentos escaneados
- Mensajes de correo de voz
- Redes sociales

Página628 de 3226.

Avaya Contact Center Select también es compatible con la mensajería instantánea punto a punto. Para admitir los tipos de contacto basados en correo electrónico, debe agregar un servidor de correo electrónico a su solución. Para admitir el tipo de contacto de comunicaciones web, debe agregar un servidor de comunicaciones web a su solución.

Avaya Contact Center Select proporciona una utilidad de administración de mensajes de voz simplificada. El supervisor del centro de contacto puede realizar un trabajo de administración rápido sin necesidad de acceso de administrador al servidor de Avaya Contact Center Select. Avaya Contact Center Select proporciona una serie de utilidades de monitoreo de estado para monitorear los puntos de integración con IP Office.

Contact Center Manager Administration es una interfaz de generación de informes y configuración basada en navegador para Avaya Contact Center Select. Los supervisores de Avaya Contact Center Select utilizan Contact Center Manager Administration para configurar recursos, agentes, conjuntos de habilidades, flujos de contacto, componentes y actividades del centro de contacto. Contact Center Manager Administration proporciona informes históricos y en tiempo real sobre el centro de contacto.

Sincronización de datos de usuario

Avaya Contact Center Select proporciona administración unificada para los agentes del centro de contacto y los usuarios de IP Office. Los usuarios (agentes y agentes-supervisores) que configura en Avaya Contact Center Select se duplican automáticamente en la IP Office conectada.

Cuando crea un agente en Avaya Contact Center Select, se crea una cuenta de usuario coincidente en IP Office. Cuando modifica los detalles del agente en Avaya Contact Center Select, los detalles del usuario de IP Office correspondiente se actualizan automáticamente. Sin embargo, si elimina un agente en Avaya Contact Center Select, el usuario de IP Office correspondiente no se elimina. La sincronización funciona en una dirección: desde Avaya Contact Center Select hasta IP Office. El administrador de IP Office puede forzar manualmente la sincronización de datos desde Avaya Contact Center Select.

Topología

En una solución de centro de contacto que utiliza Avaya Contact Center Select y un sistema telefónico IP Office, se aplican las siguientes consideraciones de topología de red y conectividad:

- El servidor Avaya Contact Center Select se admite en un grupo de trabajo o en un dominio de Windows.
- Cada Avaya Contact Center Select se conecta a un único servidor primario de IP Office Server Edition. De manera alternativa, cada Avaya Contact Center Select puede conectarse a un solo modo estándar de IP Office 500V2 con una licencia de edición avanzada.
- Una red comunitaria pequeña (SCN) es un sistema de sistemas IP Office en red que puede, entre otras funciones, compartir números de extensión y nombres de usuario. Cada IP Office SCN admite un solo Avaya Contact Center Select conectado. Avaya Contact Center Select se conecta al servidor primario de IP Office Server Edition del SCN. Para admitir una SCN de IP Office, Avaya Contact Center Select debe conectarse a un servidor primario de IP Office Server Edition en esa red SCN.
- El servidor Avaya Contact Center Select y el sistema telefónico IP Office conectado deben estar ubicados en la misma ubicación del campus.
- Cada computadora cliente supervisor se comunica con el servidor Avaya Contact Center Select. El supervisor utiliza la interfaz web de Contact Center Manager Administration para configurar agentes y ejecutar informes. El supervisor de agentes utiliza el software Avaya Agent Desktop para manejar llamadas de clientes, aceptar llamadas de emergencia o de supervisor de agentes y observar llamadas o contactos de comunicación web. Cada supervisor habilitado para voz con Agent Desktop requiere un teléfono IP Office asociado.

Página629 de 3226.

- Cada equipo cliente del agente se comunica con el servidor de Avaya Contact Center Select. El agente usa Agent Desktop para manejar los contactos multimedia y de voz del cliente. Cada agente habilitado para voz requiere un teléfono IP Office asociado.

Avaya Contact Center Select admite las siguientes opciones de implementación:

- DVD de Avaya Contact Center Select
- Avaya Contact Center Seleccione VMware
- Dispositivo de hardware Avaya Contact Center Select
- Avaya Contact Center Select Business Continuity

Para obtener más información sobre las opciones de implementación de Avaya Contact Center Select, consulte *Descripción de la solución Avaya Contact Center Select*.

Enlaces relacionados

Configuraciones de referencia en la página 67 DVD de Avaya Contact Center Select en la página 80 Avaya Contact Center Select y VMware en la página 81 Dispositivo de hardware Avaya Contact Center Select en la página 82 Continuidad comercial de Avaya Contact Center Select en la página 83

DVD de Avaya Contact Center Select

El DVD de Avaya Contact Center Select contiene el software de la aplicación del centro de contacto. La opción de implementación de DVD es compatible con Platform Vendor Independence (PVI). PVI brinda al cliente la flexibilidad de comprar un servidor que cumpla con los requisitos de servidor de Avaya Contact Center Select y se ajuste a los estándares corporativos propios del cliente.

Avaya Contact Center Select admite una variedad de especificaciones de servidor PVI, cada una de las cuales admite una capacidad máxima de agente y una tasa de llamadas especificadas. Esta gama de especificaciones de PVI brinda al cliente la flexibilidad de usar el hardware mínimo para cumplir con los requisitos de sus soluciones y permite futuras expansiones.

La opción de implementación de Avaya Contact Center Select DVD no requiere recursos ni infraestructura de VMware, lo que mantiene el costo total de propiedad (TCO) y la complejidad de la solución al mínimo.

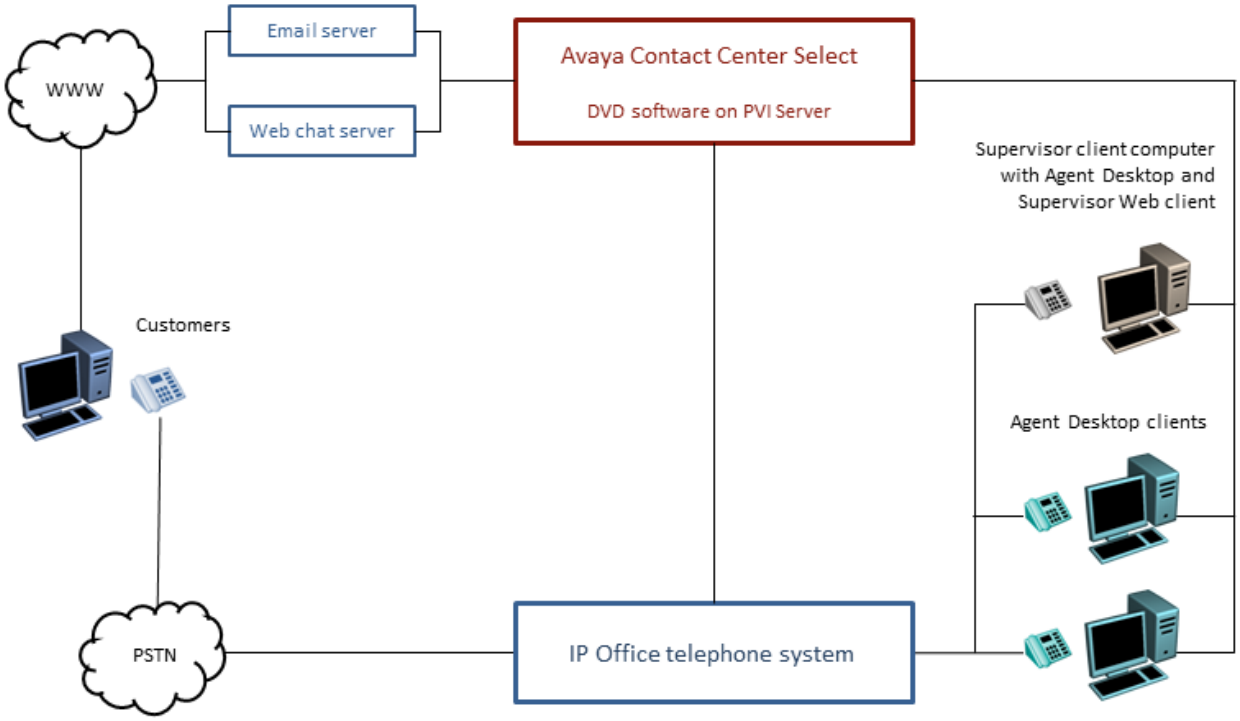


Figura 20: Implementación típica de Avaya Contact Center Select DVD

Para utilizar la opción de implementación de DVD de Avaya Contact Center Select, el cliente debe proporcionar lo siguiente:

- Hardware de servidor que cumple con una de las especificaciones PVI de Avaya Contact Center Select: nivel de entrada, gama media o gama alta.
- Licencia y sistema operativo Microsoft Windows 2012 R2 Standard o Datacenter Edition.

Para obtener más información sobre la opción DVD de Avaya Contact Center Select, consulte *Descripción de la solución Avaya Contact Center Select*.

Avaya Contact Center Select y VMware

Avaya Contact Center Select es compatible con la virtualización de VMware para aumentar la productividad, la flexibilidad y la eficiencia. Todas las opciones de implementación de Avaya Contact Center Select son compatibles con IP Office Server Edition OVA virtualizado en VMware.

Avaya Contact Center Select ofrece un paquete de dispositivo de software que consta de los siguientes componentes:

- Máquina virtual Avaya Contact Center Select
- Aura de Avaya®servidor de medios OVA
- Avaya WebLM OVA

Implemente estas máquinas virtuales e IP Office para crear una solución de centro de contacto escalable y virtualizada.

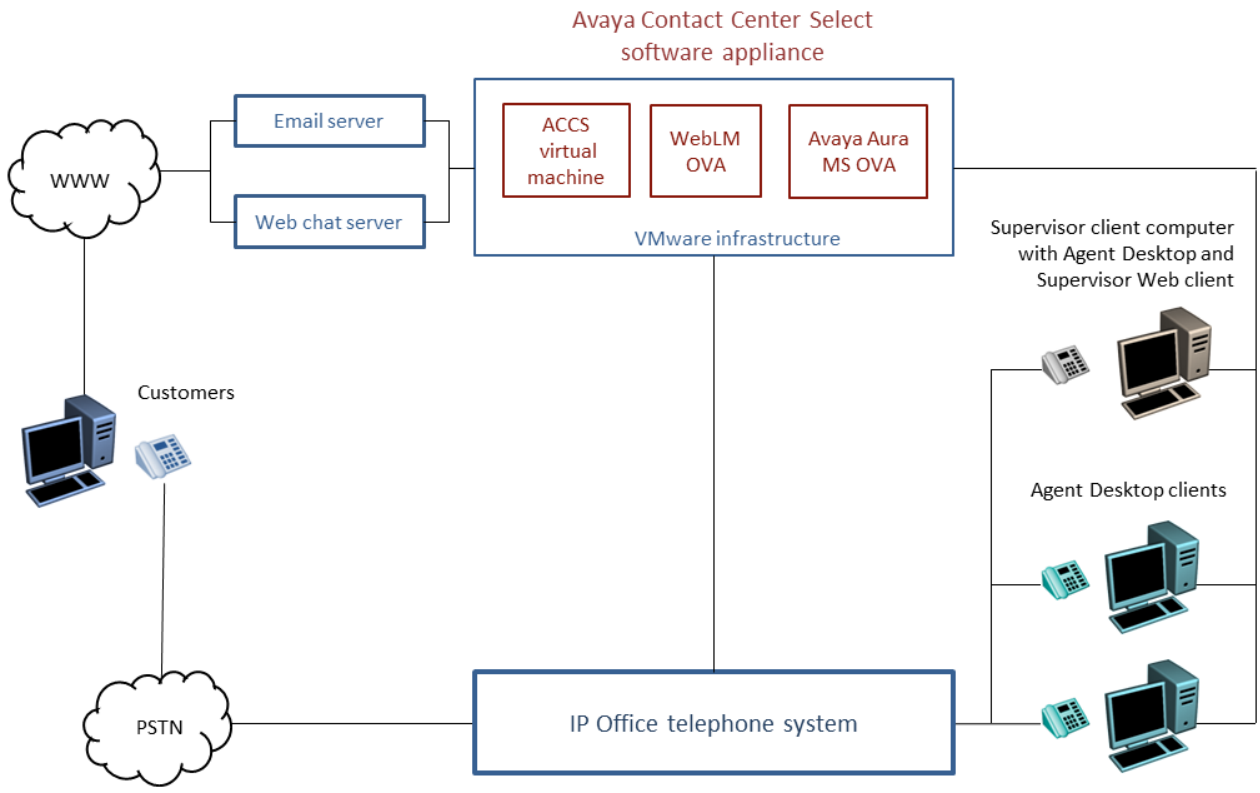


Figura 21: Solución típica de Avaya Contact Center Select y VMware

Avaya Contact Center Select es una colección de aplicaciones que brindan control de llamadas en tiempo real, manejo de multimedia e informes estadísticos. Implemente Avaya Contact Center Select en un entorno virtual VMware de nivel empresarial. Avaya recomienda que aplique la planificación, la ingeniería y la implementación de la virtualización con soporte organizacional completo para la virtualización en lugar de hacer crecer orgánicamente una infraestructura de virtualización.

Avaya Contact Center Select es compatible con VMware ESXi. No se requiere el software VMware vCenter; sin embargo, es compatible y es útil para Avaya Contact Center Select en entornos de centros de contacto de varios hosts.

Para obtener más información sobre Avaya Contact Center Select y VMware, consulte*Descripción de la solución Avaya Contact Center Select*.

Dispositivo de hardware Avaya Contact Center Select

El dispositivo de hardware Avaya Contact Center Select es un servidor físico de montaje en bastidor con el software de aplicación Avaya Contact Center Select ya cargado y parcialmente preconfigurado. Avaya proporciona el hardware del servidor y una licencia para el sistema operativo Microsoft Windows 2012 R2 Standard Edition.

El servidor de dispositivo de hardware de Avaya Contact Center Select ofrece una implementación de centro de contacto rápida y simplificada.

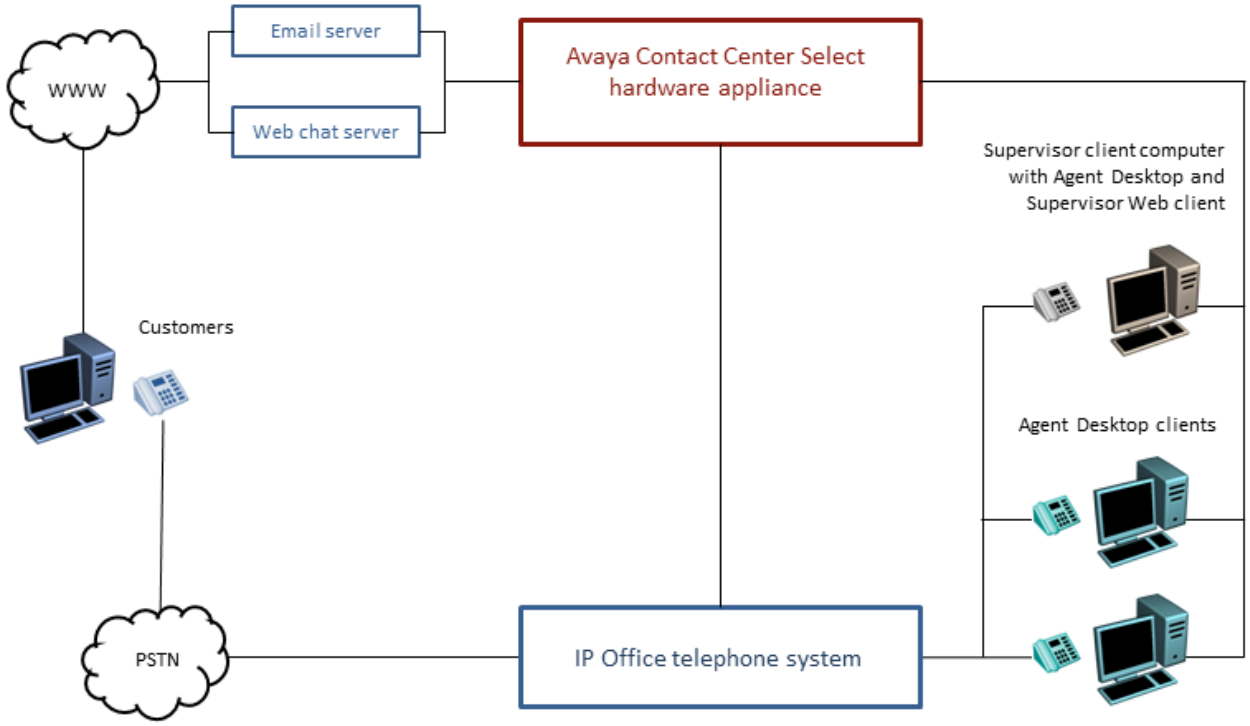


Figura 22: Solución típica de dispositivo de hardware de Avaya Contact Center Select

Después de que las funciones básicas de telefonía y correo electrónico estén funcionando, puede configurar más contactos multimedia, multiplicidad, avisos personalizados y otras funciones y funciones mejoradas para mejorar la experiencia de su cliente.

El servidor de dispositivos de hardware suministrado por Avaya está optimizado para proporcionar todos los recursos informáticos y de registro en tiempo real que requiere Avaya Contact Center Select. El dispositivo de hardware es compatible con la capacidad máxima de tasa de llamada y agente de Avaya Contact Center Select.

Avaya proporciona la clave de producto del sistema operativo Microsoft Windows para el dispositivo de hardware. La clave del producto se muestra en una etiqueta adherida a la parte superior del servidor del dispositivo de hardware de Avaya Contact Center Select.

Para obtener más información sobre el dispositivo de hardware Avaya Contact Center Select, consulte *Descripción de la solución Avaya Contact Center Select*.

Continuidad comercial de Avaya Contact Center Select

Business Continuity es una función con licencia de Avaya Contact Center Select. Las soluciones Avaya Contact Center Select que admiten Business Continuity tienen dos servidores Avaya Contact Center Select. Un servidor, denominado servidor activo, procesa los contactos de los clientes. El otro servidor, denominado standby o nodo geográfico remoto, oculta al servidor activo. Si el servidor activo falla, el otro servidor de Avaya Contact Center Select puede hacerse cargo del procesamiento de contactos. Esta función proporciona redundancia, resiliencia de datos y recuperación ante desastres de Avaya Contact Center Select.

Para respaldar la resiliencia de Business Continuity, los agentes de Avaya Contact Center Select deben tener cada uno una cuenta de usuario de dominio de Windows asociada en el mismo dominio de Windows que el agente activo.

Página633 de 3226.

y servidores de reserva. Los agentes de Avaya Contact Center Select también se admiten en dominios con una relación de confianza bidireccional con el dominio del servidor de Avaya Contact Center Select.

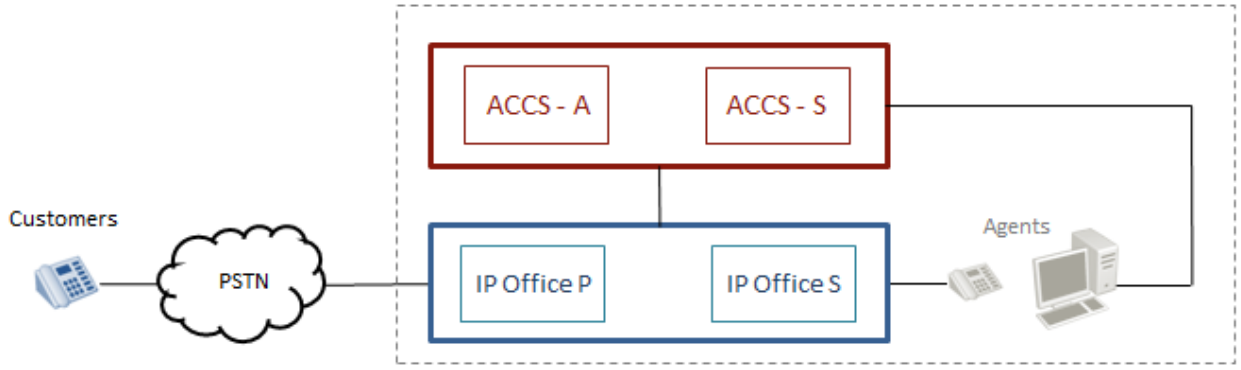


Figura 23: Avaya Contact Center Select Business Continuity con resiliencia de IP Office

Las soluciones IP Office Server Edition admiten la resistencia de la plataforma de voz cuando se agrega un servidor secundario de IP Office a la solución. Avaya Contact Center Select es compatible con esta función de resiliencia de IP Office.

Todas las opciones de implementación de Avaya Contact Center Select, DVD, VMware y Hardware Appliance son compatibles con Contact Center Business Continuity y resiliencia de IP Office. Avaya Contact Center Select Business Continuity agrega requisitos de recursos adicionales, topología, conectividad de red y consideraciones de diseño de dominio a la solución.

Para obtener más información, consulte *Continuidad comercial de Avaya Contact Center Select*.

Opciones de hardware y software

Opciones de hardware

Las opciones de hardware de servidor, tarjeta base, tarjeta troncal y módulo de expansión están disponibles según la edición requerida:

- Dell PowerEdge™R210 o R620
- Hewlett Packard ProLiant DL120 G7 o DL360 G7
- Avaya IP500 V2

Opciones de software

IP Office actúa como un servidor para una variedad de aplicaciones, que incluyen:

- Avaya Communicator for IP Office compatible con dispositivos Windows y iPad
- Avaya one-X®Móvil para IP Office
- Avaya one-X®Portal para IP Office

Página634 de 3226.

- Integración Lync para IP Office
- SoftConsole de IP Office
- Administrador de medios de IP Office
- Equinoccio de Avaya™cliente para IP Office
- Cliente web Avaya IP Office

IP Office también se puede implementar con otros componentes. Puede implementar IP Office con Radvision u otros terminales de video. También puede usar la oferta de la solución IP Office Branch para conectar las sucursales de IP Office a Avaya Aura.®infraestructura, lo que permite a los usuarios aprovechar el núcleo de Avaya Aura®
aplicaciones y servicios que incluyen planes de marcación centralizados, correo de voz, administración y licencias.

Enlaces relacionados

Acceso a las notas de la aplicación Avaya DevConnect en la página 134
interoperabilidad en la página 93

Especificaciones del servidor

Las siguientes tablas enumeran las especificaciones mínimas del servidor para IP Office Server Edition Solution:

opción de servidor	Servidor grande #1	Servidor grande #2	Servidor grande #3
Chasis	Dell R630 1U	Dell R620 1U	HP DL360G7 1U
Procesador	2 E5-2620v3, 2,4 GHz	2 E5-2630, 2,3 GHz	2 x E5620, 2,4 GHz
Memoria (RAM)	32GB	32GB	12 GB
Disco duro	2 de 600GB	2 de 600GB	2x 300GB, 10K
REDADA	Intercambio en caliente RAID 1	Intercambio en caliente RAID 1	Intercambio en caliente RAID 1
Controlador RAID	H730	H710	P410i
Fuentes de alimentación	2x 750W CA Intercambio en caliente	2x 495 W CA Intercambio en caliente	2x 460W CA Intercambio en caliente
NIC	dúplex completo de 6 GB	dúplex completo de 4 GB	4 puertos, placa base
Unidad óptica	1x DVD +/- RW	1x DVD +/- RW	1x DVD+/-RW, SATA, INTERNO
Tipo PCI	2 ranuras x8 Gen2 (PCIe)	2 ranuras x8 Gen2 (PCIe)	1-LP X8 PCIe y 1-FL/FH X16 PCIe elevador

opción de servidor	Pequeño servidor #1	Pequeño servidor #2	Pequeño servidor #3
Chasis	HP DL120G7 1U	Dell R210 1U	Dell R220 1U
Procesador	1 E3-1220, 3,1 GHz	1 E3-1220, 3,1 GHz	1 E3-1220, 3,1 GHz
Memoria (RAM)	12 GB	12 GB	16 GB
Disco duro	1x 250GB, 7.5K	1x 250GB, 7.5K	1x 500GB, 7.2K
REDADA	RAID 0 (ninguno)	RAID 0 (ninguno)	RAID 0 (ninguno)

La tabla continúa...

opción de servidor	Pequeño servidor #1	Pequeño servidor #2	Pequeño servidor #3
Controlador RAID	P212, 256 MB	A bordo	A bordo
Fuentes de alimentación	1 x 400 W CA	1 x 502 W CA	1 x 250 W CA
NIC	2 puertos, placa base	2 puertos, placa base	2 puertos, placa base
Unidad óptica	1x DVD+/-RW, SATA, INTERNO	1x DVD+/-RW, SATA, INTERNO	1x DVD+/-RW, SATA, INTERNO
Tipo PCI	1-HL/LP X8 PCIe y 1-FL/ FH X16 PCIe elevador	1 x16 ranuras Gen2 (PCIe)	1 x16 ranuras Gen2 (PCIe)

Nota:

En algunas zonas geográficas, donde 12 GB de RAM no son una opción estándar de Dell, use 16 GB de RAM.

Combinaciones y uso de servidores

- Server Edition Primary y Server Edition Secondary deben estar en la misma plataforma. Esta restricción se aplica igualmente a los servidores virtuales. Es posible mezclar servidores centrales nativos y virtuales, pero los recursos asignados al entorno virtual deben coincidir con el servidor nativo.
- Los servidores nativos y virtualizados se pueden combinar en la misma solución de Server Edition en cualquier rol, siempre que Server Edition Primary y Server Edition Secondary sean los mismos que se indicaron anteriormente.
- Es posible utilizar los servidores R210 / DL120 is / R220 de Unified Communication / Application Server ya que se trata del mismo hardware y software que los servidores Server Edition R210 / DL120 / R220. Si el servidor está instalado con el software Server Edition, será compatible con Avaya.
- No puede configurar un Sistema de expansión Server Edition (L) en el modo de funcionamiento estándar de IP Office en IP Office Server Edition Solution.
- No puede reaprovisionar un servidor Server Edition sin una reinstalación completa. Por ejemplo, no puede convertir un servidor principal en un sistema secundario o de expansión.
- No puede configurar un Sistema de expansión Server Edition (L) en el modo de operación estándar de IP Office en IP Office Server Edition Solution. No puede convertir un Sistema de expansión Server Edition (V2) en un servidor Server Edition Primario o Server Edition Secundario.
- No se admite el uso de ningún servidor Voicemail Pro externo (ya sea Linux o Windows).
- El uso de un Avaya one-X externo®El servidor de portal que no ejecuta el software Server Edition y no se ejecuta en un servidor compatible, no es compatible.

Nota:

Salesforce (SFDC) se eliminó de Avaya one-X®Portal.

Compatibilidad con sistema operativo y navegador

Sistema Operativo Windows

Tabla 7: Ediciones de Windows y Service Packs

Sistema operativo*	Paquete de servicio	Edición
ventanas 7	SP1	Profesional, Empresarial, Ultimate
Windows 8.1	N / A	Profesional, Empresa
ventanas 10	N / A	Profesional (PYME), Empresa
Servidor Windows 2012	N / A	Estándar
Servidor Windows 2012 R2	N / A	Estándar
Servidor Windows 2016	N / A	Estándar, Esenciales

*Windows Server 2008 R2 (64 bits) no es compatible con la versión 10.1.

Tabla 8: Compatibilidad con Windows: componentes del servidor

Servidor	ventanas 7		Windows 8.1*		ventanas 10		ventanas Servidor 2012, 2012 R2	ventanas Servidor 2016
	32 bits	64 bits	32 bits	64 bits	32 bits	64 bits	64 bits	64 bits
Edición preferida servidor (correo de voz Pro) Independiente	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Edición preferida servidor con UMS	No	No	No	No	No	No	Sí	Sí
Edición preferida servidor con Campañas	No	No	No	No	No	No	Sí	Sí
Edición preferida servidor con IMS	No	No	No	No	No	No	No	No
Edición preferida servidor con MAPI servicio de correo de voz Profesional en Linux	Sí	Sí	No	No	No	No	Sí	Sí
Avaya one-X®Portal para el servidor de IP Office	No	No	No	No	No	No	Sí	Sí
Primero de TAPI	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
TAPI de terceros	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

La tabla continúa...

Servidor	ventanas 7		Windows 8.1*		ventanas 10		ventanas Servidor 2012, 2012 R2	ventanas Servidor 2016
	32 bits	64 bits	32 bits	64 bits	32 bits	64 bits	64 bits	64 bits
TAPI WAV[2]	Sí	No	Sí	No	Sí	No	No	No

*Windows 8.1 es el paquete de servicio/reemplazo para Windows 8.0. Por lo tanto, ya no admitimos Windows 8.0.

Tabla 9: Soporte de Windows: aplicaciones de cliente pesado

Solicitud	ventanas 7		Windows 8.1*		ventanas 10		Ventana servidor 2012, 2012 R2	Ventana servidor 2016
	32 bits	64 bits	32 bits	64 bits	32 bits	64 bits	64 bits	64 bits
Edición preferida cliente	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Oficina de PI SoftConsole	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
Gerente de IP Office	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
monitor de sistema	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Estado del sistema Solicitud	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Primero de TAPI	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
TAPI WAV[3]	Sí	No	Sí	No	Sí	No	No	No
Equinoccio de Avaya™ para ventanas	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Avaya comunicador para ventanas	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Avaya one-X® Complemento del portal para Microsoft Outlook	Sí	Sí	Sí	Sí	Sí	Sí	No	No
asistente de llamadas	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Complemento para microsoft lync 2013/Skype para Negocio[4]	Sí	Sí	Sí	Sí	Sí	Sí	No	No

La tabla continúa...

[2] TAPI WAV no se recomienda para nuevos diseños y no es compatible con un sistema operativo de 64 bits. TAPI
[3] WAV no se recomienda para nuevos diseños y no es compatible con un sistema operativo de 64 bits. El
[4] complemento para Microsoft Lync 2010 no es compatible con la versión 10.1.

Solicitud	ventanas 7		Windows 8.1*		ventanas 10		Ventana servidor 2012, 2012 R2	Ventana servidor 2016
	32 bits	64 bits	32 bits	64 bits	32 bits	64 bits	64 bits	64 bits
Web conferencias[5]	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Web de IP Office Cliente	Sí	Sí	Sí	Sí	Sí	Sí	No	No

* Windows 8.1 es el paquete de servicio/reemplazo para Windows 8.0. Por lo tanto, ya no admitimos Windows 8.0.

Sistema operativo macOS

Tabla 10: Compatibilidad con macOS: aplicaciones de cliente grueso

Solicitud	mac OS 10.8 (Montaña León)	mac OS 10.9 (Inconformistas)	Mac OS 10.10 (Yosemite)	Mac OS 10.11 (El Capitán)	Mac OS 10.12 (Sierra)	Mac OS 10.13 (Alta Sierra)
Web conferencias[6]	Sí	Sí	Sí	Sí	Sí	
Avaya Equinoccio™por Mac	No	No	No	Sí	Sí	Sí

navegadores

Tabla 11: Navegadores compatibles

Solicitud	Internet Explorador 10*	Internet Explorador 11	Borde	Firefox	Cromo	Safari 8	Safari 9	Safari 10
Buzón de voz profesional Campañas	Sí	Sí	Sí	No	No	No	No	No
Buzón de voz profesional Correo Web UMS	Sí	Sí	Sí	No	No	No	No	No
Avaya one-X® Portal de PI cliente de oficina	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
Web conferencias[7]	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No

La tabla continúa...

[5] Incluye Adobe Flash y Java Applet para compartir.
[6] Incluye Adobe Flash y Java Applet para compartir.
[7] Incluye Adobe Flash y Java Applet para compartir.

Solicitud	Internet Explorador 10*	Internet Explorador 11	Borde	Firefox	Cromo	Safari 8	Safari 9	Safari 10
Administrador web y control web Página	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
DECT D100 Administración	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
IP DECT R4 Administración	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Avaya Comunicador para Internet	No	Sí	No	No	Sí	No	No	No
Medios de IP Office Gerente	Sí	Sí	Sí	Sí	Sí	No	No	No
Oficina IP de Avaya cliente web	No	No	No	No	Sí	No	No	No

* Solo en Windows Server 2012; sin embargo, Server 2012 R2 es compatible con Internet Explorer 11.

Otras aplicaciones

Tabla 12: Microsoft Exchange

Solicitud	Intercambio 2010	Intercambio 2013	Intercambio 2016
Correo de voz Pro UMS	Sí	Sí	Sí
Avaya one-X®Portal para IM y Presencia	Sí	Sí	Sí

Tabla 13: Microsoft Outlook

Solicitud	perspectiva 2010	Perspectivas 2013	Perspectivas 2016
Correo de voz Pro IMS	No	No	No
TAPI (para marcar)	Sí	Sí	Sí
Voicemail Pro UMS con IMAP	Sí	Sí	Sí
Avaya one-X®Complemento de Portal Outlook[8]	Sí	Sí	Sí

[8]Para Outlook 2013 y versiones posteriores, la función de pantalla emergente de contacto no es compatible.

Página640 de 3226.

virtualización

Tabla 14: Soporte de virtualización

hipervisor	Edición de servidor de IP Office	Hospedado por socios de IP Office
VMware ESXi 5.1	Sí	Sí
VMware ESXi 5.5 U2+	Sí	Sí
VMware ESXi 6.0	Sí	Sí
VMware ESXi 6.5	Sí	Sí
VMware ESXi 6.7	Sí	Sí
Microsoft HyperV en el servidor 2012 R2	Sí	Sí
Microsoft HyperV en el servidor 2016	Sí	Sí
KVM	No	Sí
AmazonAWS	Sí	Sí

Nota:

Google KVM es compatible con QEMU con CentOS versión 6 y 7 en el caso de la solución Powered by Avaya (alojada) y no es compatible con CPE. Para más información, ver *Guía de implementación impulsada por Avaya for Business Partners*.

Requisitos de PC proporcionados por el cliente

Los siguientes requisitos de PC proporcionados por el cliente para las aplicaciones son los mínimos requeridos.

Gerente de IP Office

IP Office Manager se utiliza para acceder a todas las partes de la configuración. Se pueden definir diferentes niveles de acceso para controlar qué partes de la configuración puede ver y modificar el usuario de IP Office Manager. IP Office Manager también se usa para actualizar los archivos de software en el sistema. IP Office Manager actúa como un servidor TFTP desde el cual algunos teléfonos Avaya pueden solicitar software nuevo.

RAM	Edición estándar: 4 GB Edición de servidor: 6 GB Edición de servidor seleccionada: 8 GB
Espacio libre en disco duro	1GB
Procesador	Edición estándar: Core i3 Edición de servidor: Core i5 Selección de edición de servidor: Core i5
Sistema operativo	Compatibilidad con sistema operativo y navegador en la página 88

Página641 de 3226.

software adicional	. NET Framework 4.0: Instalado con el software si aún no está instalado.

Monitor de sistema de IP Office

RAM	128 MB
Espacio libre en disco duro	10 GB
Procesador	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Sistema operativo	Compatibilidad con sistema operativo y navegador en la página 88

Aplicación de estado del sistema de IP Office

RAM	256 MB
Espacio libre en disco duro	1,4 GB
Procesador	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Sistema operativo	Compatibilidad con sistema operativo y navegador en la página 88
software adicional	Máquina virtual Sun Java Navegador web: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

TAPI

RAM	64 MB
Espacio libre en disco duro	50 MB
Procesador	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Sistema operativo	Compatibilidad con sistema operativo y navegador en la página 88
software adicional	Navegador web: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

Requisitos del entorno virtual

Asegúrese de tener lo siguiente:

- Software de cliente VMware vSphere para administración (software vSphere ESXi e instancias virtualizadas que se ejecutan en un único servidor host)

  Nota:

  No se requiere el software vCenter, sin embargo, puede ser útil para entornos de servidor de múltiples hosts.

- Host hardware compatible con los requisitos y especificaciones de recursos de VMware vSphere e IP Office Server Edition para satisfacer las necesidades de configuración.

Compatibilidad con VMware ESXi:

- IP Office Server Edition e IP Office Contact Center son compatibles con VMWare ESXi 5.1 y 5.5 U2.
- IP Office Contact Center es compatible con VMWare ESXi 6.0. IP Office Server Edition es compatible con VMWare ESXi 6.0 solo para las versiones 10.0 y posteriores.

  Para obtener más información sobre el soporte y las especificaciones de IP Office Contact Center, consulte *Configuración de referencia de Avaya IP Office Contact Center*.

Nota:

ESXi 4.x ya no es compatible.

Compatibilidad con hipervisor adicional: El

soporte de hipervisor ahora se extiende a:

- Microsoft Hyper-V
- AWS (para Amazon Web Services): se proporciona una AMI (imagen de máquina de Amazon) que puede realizar el encendido automático y la ICU en función de los datos de usuario establecidos en AWS. La AMI se comportará de manera similar a la imagen de Google Compute existente. Consulte los tipos de instancias que admite Amazon EC2 en el sitio web de Amazon AWS.

  En Amazon Dashboard, debe seleccionar Iniciar instancia en Crear instancia. Seleccione Community AMI y busque Avaya IP Office.

- KVM (para máquina virtual basada en kernel)

interoperabilidad

La interoperabilidad significa que dos sistemas pueden comunicarse con una interfaz en cada sistema para manejar la comunicación. Compatibilidad significa que dos componentes en el mismo entorno son compatibles entre sí si se ejecutan o residen en el entorno sin afectar negativamente el comportamiento del otro.

Para obtener información detallada sobre la interoperabilidad de IP Office y las versiones admitidas, consultehttps://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=IP+Office+Platform .

Interfaces de productos de Avaya

IP Office incluye una interfaz para los siguientes productos de Avaya:

- Aura de Avaya®
- Selección del centro de contacto de Avaya
- Aura de Avaya®Mensajería
- Avaya CallPilot®
- Fase de vídeo en la nube de Avaya
- Avaya Communicator para Windows
- Avaya Communicator para iPad
- Equinoccio de Avaya™
- Avaya one-X®Comunicador
- Controlador de borde de sesión de Avaya para empresas
- Gerente de comunicaciones comerciales de Avaya
- Servidor de comunicaciones Avaya 1000
- Mensajería modular de Avaya
- Avaya Scopia®
- Enlace de acceso seguro
- Aura de Avaya®Portal de experiencia

interfaces RDSI

Interfaces de la UE:

- BRI: tomas RJ45. Interfaces ETSI T-Bus y S-Bus a CTR3 para conexión paneuropea
- PRI E1: toma RJ45. Interfaz ETSI T-Bus a CTR4 para conexión paneuropea
- PRI T1/J1: enchufe RJ45: conexión FCC Parte 68/JATE

Interfaces de EE. UU.:

- Servicio PRI T1: Ground Start (GS) - Predeterminado, E&M, datos de 56 K para 5ESS, 56/64/64 restringido para 4ESS
- Compatibilidad con conmutador PRI ISDN: 4ESS, 5ESS, DMS-100, DMS-250 (incluye conformidad con ANSI T1.607 y Bellcore Special Report SR4287, 1992)
- Servicios PRI ISDN: AT&T Megacom 800, AT&T WATS (4ESS), AT&T SDS Accunet 56 Kbps y 64 Kbps (4ESS), AT&T Multiquest (4ESS)

Enlaces relacionados

Interoperabilidad telefónica en la página 95
Interoperabilidad de IP Office y Avaya Aura Communication Manager en la página 99
Interoperabilidad de BCM e IP Office en la página 100 Acceso a las notas de la aplicación Avaya DevConnect en la página 134 Compatibilidad del producto en la página 133 Opciones de hardware y software en la página 84

Interoperabilidad telefónica

La siguiente tabla resume la comparación de interoperabilidad de teléfonos por edición de IP Office.

Tabla 15: Teléfonos generalmente disponibles

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
Teléfonos de escritorio analógicos:			
OLLAS	Sí	Sí	No
Videoteléfonos Serie 1000:			
1010, 1020, 1030, 1040 (tamaño natural)	No	Sí	No
Serie 1400: Teléfonos DS Digital: IP Office y Communication Manager			
1403, 1408, 1416	Sí	Sí	No
DBM32	Sí	Sí	No
Serie 1600: Teléfonos IP (H.323): IP Office y Communication Manager			
1603, 1603SW, 1603SW–i, 1608, 1608–i, 1616, 1616–I	No	Sí	Sí
Serie 2400: Teléfonos DS Digital: IP Office y Communication Manager			
2402D, 2410D, 2420	Sí	Sí	No
UE24	Sí	Sí	No
Serie 3600: WiFi H.323 – IP Office y Communication Manager			
3641, 3645	No	Sí	Sí
Serie 3700:DECT: IP Office y administrador de comunicaciones			
3720, 3525, 3730, 3735, 3745, 3749	No	Sí	Sí
Serie 9500:DS digital: solo IP Office			
9504, 9508	Sí	Sí	No
BM12	Sí	Sí	No
Serie 9600:IP H.323: IP Office y Communication Manager			
9620L, 9620C, 9630, 9640G, 9650, 9650C	No	Sí	Sí
SBM24 con 96x0	No	Sí	Sí
9608, 9611, 9621, 9641, J169, J179	No	Sí	Sí
BM12	No	Sí	Sí
Teléfonos de conferencia de la serie B100:			
B149, B159	Sí	Sí	No

La tabla continúa...

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
B179 SORBO	No	Sí	Sí
Teléfonos DECT D100/D160:			
D160	Sí	Sí	Sí
Teléfonos IP de la serie E100:			
E129	No	Sí	Sí
E159	No	Sí	Sí
E169	No	Sí	Sí
Estaciones de colaboración de video de la serie H100:			
H175	No	Sí	Sí
Teléfonos IP de la serie J100 de Avaya:			
Teléfono IP Avaya J139	No	Sí	No
Teléfono IP Avaya J169	No	Sí	No
Teléfono IP Avaya J179	No	Sí	No
Softphone:			
Avaya Communicator Ventanas	No	Sí	Sí
Comunicador Avaya iPad	No	Sí	Sí
Equinoccio de Avaya™	No	Sí	Sí

Tabla 16: Teléfonos NORSTAR/BCM generalmente disponibles

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
Teléfonos SIP de la serie 1100: Migración BCM Unistim			
1120E, 1140E	No	Sí	Sí
BM LED y etiquetas de papel	No	Sí	Sí
BMLCD	No	Sí	Sí
Teléfonos SIP de la serie 1200: Migración BCM Unistim			
1220, 1230	No	Sí	Sí
papel BCM	No	Sí	Sí
BCMLCD	No	Sí	Sí
Teléfonos digitales NORSTAR/BCM:			

La tabla continúa...

Página646 de 3226.

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
T7000, T7100, T7208, T7316, T7316E	Sí	Sí	No
Módulo de llave T24	Sí	Sí	No
M7100(N), M7208(N), M7310(N), M7310BLF, M7324(N)[9]	Sí	Sí	No
Módulo clave CAP	Sí	Sí	No
Teléfono de conferencia digital NORSTAR/BCM	Sí	Sí	No
Teléfonos de movilidad digital de Nortel:			
T7406, T7406E	Sí	Sí	No
7420, 7430, 7434, 7439, 7440, 7449	Sí	Sí	No
4135, 4136, 4145, 4146, 4145EX, 4146EX	Sí	Sí	No

Avaya ha probado la interoperabilidad de los siguientes teléfonos con IP Office. Es posible que estos teléfonos no admitan todas las funciones. Si el teléfono ya pasó el Período de soporte del fabricante de Avaya, la resolución de problemas se limita a los que ya se solucionaron.

Tabla 17: Los teléfonos Avaya compatibles ya no están a la venta

Nota:

Compatible en este contexto significa que los teléfonos han sido probados por Avaya para la interoperabilidad con IP Office. Es posible que los modelos de teléfono más antiguos no admitan nuevas funciones si el modelo de teléfono está fuera del período de soporte del fabricante de Avaya. Si hay una actualización de software relacionada con la versión 11.0, no se proporcionará una corrección de software para los teléfonos que estén fuera del período de soporte de fabricación de Avaya. Los teléfonos que "ya no son compatibles" están fuera del período de soporte de fabricación de Avaya y no están cubiertos por las ofertas de mantenimiento de Avaya (soporte de fin de servicio y soporte de fin de mantenimiento)

1. OSX 10.9 Mavericks es la última versión del sistema operativo compatible con Video Softphone para MAC. Ese cliente ya no está disponible en el software 10.xo 11.0 por la misma razón. Avaya Communicator for Web, Avaya IP Office Web Client y Avaya Equinox™están disponibles para usuarios de Mac en la versión 11.0 de IP Office.

2. Los teléfonos digitales y analógicos son compatibles con Server Edition o Select, según se indica, utilizando IP500 V2 como módulo de expansión.

[9] Solo se admite la versión global de los teléfonos de la serie M7000. Las versiones no globales no son compatibles y pueden identificarse por los niveles de contraste; la versión global tiene 9 niveles de contraste y la versión no global tiene solo 4 niveles de contraste.

Teléfono	Edición básica	Esencial y Privilegiado Ediciones	Edición del servidor Seleccionar servidor Edición virtualizado
Teléfonos ETR: Teléfono con funciones analógicas, PARTNER e IP Office			
Display de 34, 18 y 6 botones “Refreshed”	Sí	No	No
Display “Euro” de 34 y 18 botones	Sí	No	No
Display “Euro” de 18 y 6 botones	Sí	No	No

Enlaces relacionados

interoperabilidad en la página 93

Disponibilidad de teléfono en la página 98

Acceso a las notas de la aplicación Avaya DevConnect en la página 134 Uso de la base de conocimientos de Avaya InSite en la página 134 Los telefonos en la página 38

Disponibilidad de teléfono

Teléfonos disponibles en todo el mundo

Los teléfonos de Avaya que se enumeran a continuación son los teléfonos recomendados para usar con IP Office. Estos teléfonos se venden en todo el mundo en todos los países donde está disponible IP Office.

Para obtener especificaciones detalladas, consulte la información específica del teléfono en el sitio de soporte de Avaya enhttp://soporte.avaya.com .

Modelos de teléfonos digitales	Modelos de teléfonos IP
1403	1603
1408	1608
1416	1616
9504	9608
9508	9611
	9621
	9641
	Teléfono IP Avaya J169
	Teléfono IP Avaya J179
	Teléfono IP Avaya J139

Teléfonos solo disponibles en ciertos países

Además de los teléfonos enumerados anteriormente, los siguientes teléfonos de Avaya están disponibles en ciertos países y regiones.

Teléfono digital/analógico modelos	Teléfonos IP
2402	9620L/9620C
2410	9630G/9640/9640G
2420	9650/9650C
3810 inalámbrico	Auricular inalámbrico 3720 DECT R4
Unidad DSS EU24/EU24BL	Auricular inalámbrico 3725 DECT R4
	Auricular inalámbrico 3730 DECT R4
	Auricular inalámbrico 3735 DECT R4
	Teléfono inalámbrico 3745 DECT R4
	Teléfono inalámbrico 3749 DECT R4
	3641 Teléfono inalámbrico (WiFi)
	Teléfono inalámbrico reforzado (WiFi) 3645
	D100

Enlaces relacionados

Interoperabilidad telefónica en la página 95

IP Office y Avaya Aura®Interoperabilidad de Communication Manager

IP Office usa el protocolo H.323 para troncales entre los nodos y Avaya Aura®Gerente de comunicación. El correo de voz centralizado para todos los sistemas IP Office en la red SCN y todos los teléfonos son compatibles con los servidores de llamadas individuales. Las funciones avanzadas de manejo de llamadas están disponibles entre los nodos de IP Office. Esta interfaz funciona en las ediciones Essential y Preferred.

Los teléfonos compatibles incluyen:

- Teléfonos IP de Avaya (H.323)
- Teléfonos digitales Avaya
- Teléfonos digitales de la serie BCM 7000
- Teléfonos IP de la serie BCM 1100/1200 (SIP)
- Teléfonos DECT R4
- Teléfonos analógicos

Estas funciones permiten necesidades de redes simples entre las sucursales remotas de IP Office a un Avaya Aura®Gerente de comunicación en el sitio principal.

Página649 de 3226.

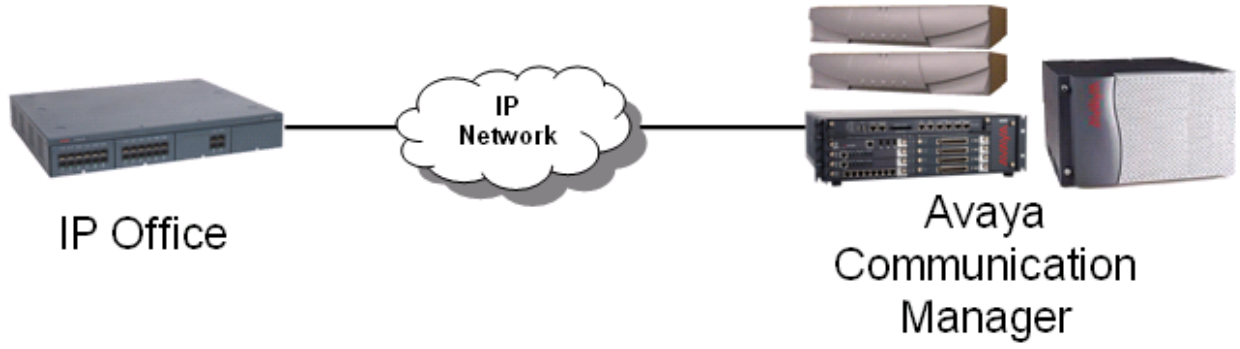


Figura 24: Red VoIP usando H.323

Q.SIG proporciona los siguientes servicios complementarios que también están disponibles entre IP Office y Avaya Aura®Communication Manager equipado con las licencias RFA pertinentes:

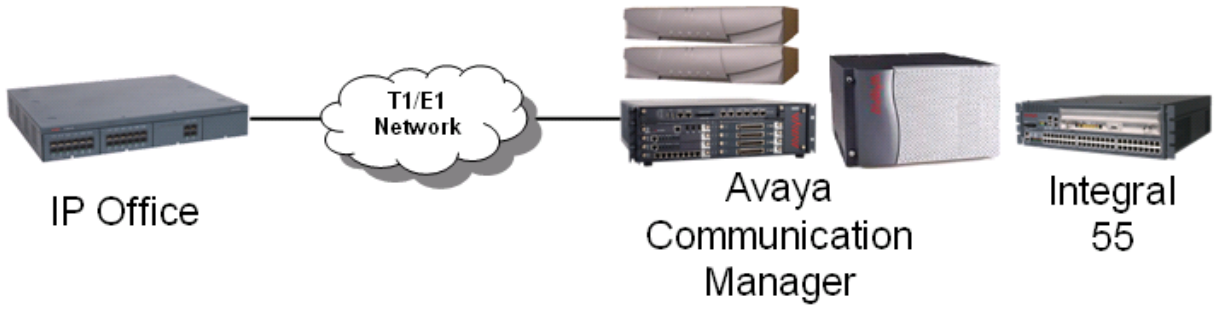


Figura 25: Redes Q.SIG utilizando enlaces T1/E1 (TDM)

Enlaces relacionados

interoperabilidad en la página 93

Interoperabilidad de BCM e IP Office

El soporte de interoperabilidad SIP entre IP Office y BCM50/450 permite a los clientes migrar una red de BCM, paso a paso, a una red IP Office SCN o Server Edition.

Soporte de protocolo	IP Office a BCM: SIP BCM a BCM: SIP o SIP/MCDN IP Office a IP Office H.323: SCN o SIP
	Nota: No es posible conectar IP Office y BCM a través del protocolo MCDN o SCN directamente.
plataforma IP Office requisitos	Versión 8.1 o superior, ediciones Essential, Preferred o Server

plataforma BCM requisitos	BCM50 o BCM450 6.0
centralizado mensaje de voz	IP Office con un sistema Voicemail Pro centralizado en la red SCN BCM con un correo de voz centralizado dentro de la red BCM MCDN. **Nota:** No se admite el correo de voz centralizado en los sistemas IP Office y BCM.
Los telefonos	Todos los teléfonos son compatibles con los servidores de llamadas individuales y las versiones, incluido el teléfono IP de Avaya (H.323), los teléfonos digitales de Avaya, los teléfonos digitales de la serie BCM 7000, los teléfonos IP de la serie BCM1100/1200 (SIP), DECT R4 y los teléfonos analógicos.
Características	Conjunto de funciones avanzadas de IP Office SCN disponible entre IP Office y BCM. Las funciones de MCDN también están disponibles entre IP Office y BCM. Se admiten las funciones SIP estándar.

Enlaces relacionados

interoperabilidad en la página 93

Especificación de seguridad

El Equipo de soporte de seguridad de productos de Avaya (PSST) responde a las vulnerabilidades de seguridad en curso para todos los productos de Avaya. Para más información, ver *Política de respuesta a vulnerabilidades de seguridad de productos de Avaya* y *Clasificación de vulnerabilidades de seguridad de Avaya* en el sitio web de soporte de Avaya en https://support.avaya.com/security .

Seguridad predeterminada

El motor de seguridad del software IP Office es suministrado por Mocana Corporation. Para más información, ver https://www.mocana.com .

Las funciones de seguridad están integradas en la plataforma de software. Estas características consisten en:

- Cortafuegos integrado para evitar ataques de denegación de servicio (DoS)
- Conexiones seguras para asegurar la privacidad e integridad de la información transmitida, incluyendo:
  - TSL en las interfaces de administración
  - Cliente HTTPS
  - Servidor HTTPS
  - IPSec
  - SIP-TLS

Página651 de 3226.

-SSL/VPN

- Integración VMPro/Exchange MAPI (TLS)

Para obtener información detallada sobre el acceso remoto SSL/VPN, consulte*Implementación de IP Office de Avaya™ Plataforma SSL VPN Servicios*y*Oficina IP de Avaya™Matriz de puertos de plataforma*en el sitio web de soporte de Avaya.

Seguridad configurable

Los ajustes de seguridad configurables incluyen las siguientes funciones:

- Cifrado y autenticación de mensajes
- Configuración de los ajustes del cortafuegos integrado
- Certificados digitales
- Prevención del fraude de herramientas mediante la restricción de los privilegios de los usuarios y el uso de la configuración de políticas de seguridad para administrar las credenciales de la cuenta y el control de acceso

Ver*Oficina IP de Avaya™Directrices de seguridad de la plataforma*para más información.

Seguridad de la red

La seguridad de la red aprovecha los recursos como VLAN y firewalls disponibles en la red empresarial e incluye:

- Configuración de cortafuegos externo
- Separación de la funcionalidad de la red mediante la creación de grupos de VLAN y zonas de seguridad independientes
- Fortalecimiento de la capa 2 (capa de enlace de datos) y la capa 3 (capa de red) mediante la configuración de destinos de trampas SNMP, entradas de syslog y una VPN IPSec.
- Acceso remoto SSL/VPN

Seguridad operativa

La seguridad operativa continua para mantener un sistema seguro incluye:

- Aplicación de parches
- Registro y monitoreo
- Protección de virus

Enlaces relacionados

Detalles de seguridad de la plataforma y la aplicación en la página 102

Detalles de seguridad de la plataforma y la aplicación

Para obtener información adicional sobre seguridad, consulte*Oficina IP de Avaya™Directrices de seguridad de la plataforma*

Plataforma

- El sistema operativo IP Office para Linux se basa en Red Hat Enterprise Linux, que se fortalece aún más para los valores predeterminados, los paquetes y los usuarios.
- El sistema operativo de Server Edition Expansion System (L) está desarrollado para IP Office. El sistema operativo es simple, estable y confiable.

Página652 de 3226.

- El sistema operativo de Server Edition Expansion System (V2) está desarrollado para IP Office. El sistema operativo es simple, estable y confiable.
- Componentes que son seguros:
  - Motor de seguridad de software para todos los componentes.
  - Motor de seguridad de hardware para Office Server Edition Expansion System (V2).
  - Políticas del motor de control de acceso interno para solicitudes de servicios externos y aplicaciones internas.

Gerente

- Transport Layer Security (TLS) asegura las comunicaciones entre IP Office Manager e IP Office y los cifrados inseguros están deshabilitados.
- Proporciona control de acceso de usuarios basado en funciones (RBAC).
- Proporciona controles completos de cuentas de usuario y contraseñas.
- Puede habilitar un dominio de confianza de PKI.
- El sistema genera mensajes de advertencia si las contraseñas administrativas están configuradas como predeterminadas. El sistema envía alarmas o falla de inicio de sesión.
- El sistema registra todos los accesos en el registro de auditoría.
- Puede deshabilitar servicios y puertos no utilizados, como HTTP.

Cuentas de usuario de administración

Las cuentas de usuario de administración se pueden controlar para:

- Complejidad de la contraseña
- Historial de contraseñas anteriores (solo cuentas administrativas)
- Cambiar contraseña en el próximo inicio de sesión
- Bloqueo inactivo y bloqueo por falla de inicio de sesión
- Hora y fecha de vencimiento de la cuenta (solo cuentas administrativas)

Inicio de sesión único (SSO)

- Las credenciales de administración para iniciar sesión en la configuración de la plataforma Linux se transfieren de forma segura al cliente Manager, SSA, Voicemail Pro.
- Todos los inicios de sesión administrativos en todos los componentes de IP Office, incluidos Voicemail Pro y Avaya one-X®Portal para IP Office utiliza la configuración de seguridad de IP Office.
- La función de administración de usuarios del servidor en Web Manager sincroniza las credenciales de los usuarios administrativos con todos los componentes de IP Office, incluidos Voicemail Pro y Avaya one-X.®Portal para IP Office en IP Office Server Edition Solution.

Pista de auditoría

- Cada sistema IP Office mantiene un registro de auditoría de acceso y cambio de configuración.
- La configuración de la plataforma Linux también mantiene un registro de auditoría.
- El sistema IP Office muestra la pista de auditoría en IP Office Server Edition Manager y SSA.
-

Infraestructura de clave pública (PKI)

- IP Office admite certificados X.509
- El servidor Primario de Server Edition y el servidor de aplicaciones admiten una Autoridad de certificación (CA) integrada
- El almacén de certificados de confianza se puede configurar y el certificado de identidad está disponible.
- El sistema realiza una Solicitud de firma de certificado (CSR) a través del Protocolo de inscripción de certificado simple (SCEP).
- El sistema crea un certificado de identidad autofirmado que se puede copiar a todas las interfaces HTTPS/TLS.
- Controles flexibles para hacer cumplir el dominio de confianza en servicios específicos. Controles de confianza extendidos para PKI.
- Consola de administración web, Voicemail Pro y Avaya one-X®Portal para IP Office en Linux admite certificados X.509, pero no PKI.

LAN

- Los servidores y los sistemas de expansión se someten a pruebas exhaustivas de resistencia a la denegación de servicio y otros ataques.
- El sistema de expansión Server Edition (V2) es compatible con un cortafuegos configurable
- Perfiles de tiempo en Server Edition Expansion System (V2) únicamente
- NAT estático y NAPT en el sistema de expansión Server Edition (V2)
- Filtrado ICMP
- L2TP/PPP VPN en Sistema de expansión Server Edition (V2) únicamente
- Intercambio de contraseñas PAP o CHAP
- Tiempo de espera inactivo o de cuota
- IPSec VPN en Server Edition Expansion System (V2) solamente

Puntos finales

- El nombre de usuario y el PIN, la contraseña o el código de inicio de sesión se encuentran en la configuración de IP Office y puede administrarlos a través de IP Office Server Edition Manager.
- Puede usar HTTP o HTTPS para configuraciones y actualizaciones de firmware
- No puede hacer llamadas a menos que haya iniciado sesión

Bloqueo de llamadas

- Puede configurar controles de restricción de llamadas flexibles utilizando el nombre de inicio de sesión o el código de cuenta para permitir llamadas internas, locales, nacionales o internacionales en función de cada usuario y sistema.
- No puede usar marcaciones rápidas, transferencias, reenvíos y conferencias para omitir los controles.
- Puede habilitar llamadas de troncal a troncal mediante IP Office Server Edition Manager. Las llamadas de troncal a troncal están deshabilitadas de manera predeterminada.
- La configuración del troncal SIP para las llamadas entrantes debe coincidir con los URI.
- Puede utilizar SMDR (CDR) para crear un registro de todas las llamadas.

Cliente Voicemail Pro

- Puede forzar el inicio de sesión del usuario con un número de identificación personal (PIN) y configurar la complejidad del PIN.
- Puede forzar el cambio de PIN cuando el usuario inicia sesión por primera vez.
- Tiempo de inactividad.

Enlaces relacionados

Especificación de seguridad en la página 101

Asignaciones de puertos

Los detalles del rango de puertos utilizados por IP Office y las aplicaciones de IP Office se encuentran enhttps://support.avaya.com/products/ .

puerto DTE	Conector tipo D hembra de 9 vías tipo D: V.24/V.28
Puertos troncales analógicos	Tomas RJ45: Loop Start/Ground Start (según la región)
Puertos de falla de energía	Tomas RJ45: 2 tomas para ATM16 y 1 toma para ATM4
Tarifas de datos RDSI	BRI: canal B 64 Kbps o 56 Kbps, canal D 16 Kbps
Puertos de teléfono analógico	• Tomas RJ45 • REN: 2. (Sirena externa vía puerto POT: REN = 1) • Corriente descolgada: 25 mA. • Voltaje de timbre: 40 V (nominal) RMS.
LAN	Tomas RJ45. Ethernet 10/100 BaseT de negociación automática (10/100 Mbps)
Audio	• Toma jack estéreo de 3,5 mm. Impedancia de entrada 10 K/canal. • Señal de CA máxima: 200 mV rms.
Puerto de salida externo	• Toma jack estéreo de 3,5 mm. Capacidad de conmutación 0,7 A. • Voltaje Máximo - 55V DC. Sobre la resistencia del estado 0.7. • Corriente de cortocircuito 1 A. Capacidad de corriente de circuito inverso 1,4 A.
Voz integrada memoria	IP500V2: tarjeta de memoria flash compacta (SD) de 512 MB para correo de voz

Rutas de actualización típicas

Actualización de plataformas IP500 V2

Los clientes pueden migrar a la última versión mediante la compra de una licencia de actualización o según los términos de su contrato de soporte de servicios de soporte de IP Office, según corresponda. Los clientes que migren a la última versión deberán tener una unidad de control IP500 V2 o servidores compatibles con Server Edition. Las tarjetas base IP500, las tarjetas de troncales y los módulos de expansión son compatibles con la unidad de control IP500 V2 y pueden migrar a la unidad de control V2. Las licencias requerirán un intercambio de dongle para pasar de la tarjeta llave IP500 a la tarjeta SD IP500 V2.

Para los sistemas que utilizan IP500 V2 con cualquier versión de software anterior a 8.1.1.0, se requiere un proceso de actualización de dos etapas para hacer frente al aumento de tamaño del archivo binario 9.1. Actualice a 8.1.1.0 o cualquier versión 9.0 antes de intentar actualizar a 9.1.

Asegúrese de que los sistemas no contengan hardware no compatible. Actualícelos si es necesario antes de actualizar el software. Instale licencias de actualización antes de la actualización.

Utilice el asistente de actualización de Manager para mostrar el software actualmente presente en la tarjeta SD y las nuevas versiones disponibles para la actualización.

Ya no se admitirá el hardware IP400, incluidas las tarjetas internas de la serie IP400, los módulos de expansión y las tarjetas troncales que se enumeran a continuación:

Tarjetas VCM IP400	VCM4 VCM8 VCM16 VCM24 VCM30
Módulos IP400 y tarjetas de estación	Digital Station V1: variantes de 16 y 30 puertos Teléfono V1: variantes de 8, 16 y 30 puertos So8: compatibilidad con ETSI BRI SO
Tarjetas IP400	Tarjeta de troncales analógicas Uni (ATM4U) Tarjetas de troncales analógicas (ATM4) Tarjetas troncales BRI Tarjetas de troncales PRI T1 Tarjetas de troncales PRI E1 Tarjetas de troncales PRI E1R2

Los siguientes módulos de estación y troncal IP400 seguirán siendo compatibles con la versión actual.

Módulos de expansión IP400	Troncal analógico 16 Digital Station V2: variantes de 16 y 30 puertos

Phone V2: variantes de 16 y 30 puertos

Actualización de la edición del servidor

Actualice los sistemas primario, secundario y de expansión de Server Edition utilizando la imagen iso grabada en un DVD o USB. Instale licencias de actualización antes de actualizar. Hay dos opciones disponibles:

Actualización a IP Office Select

Las licencias de Server Edition existentes deben migrarse mediante la compra de un nuevo conjunto de licencias Select PLDS.

Actualización del servidor de aplicaciones

El proceso de actualización para Application Server es el mismo que para IP Office Server Edition.

Actualización de UCM

Actualice UCM utilizando una llave de memoria USB2 con software nuevo o el proceso de actualización ISO de Web Manager.

Actualización de aplicaciones de servidor de Windows

Descargue las últimas aplicaciones de Windows y cópielas en el servidor o grábelas en un DVD.

Actualización de sistemas en red

En versiones anteriores, la red se lograba mediante líneas H.323 configuradas con servicios complementarios establecidos en SCN. A partir de la versión 9.1 y posterior, estas líneas se migrarán a Líneas de IP Office.

Reemplazo del reportero de llamadas de clientes

Advanced Edition y Customer Call Reporter (CCR) ya no están disponibles para la venta. Además, los clientes existentes de Advanced Edition deberán migrar su CCR a IP Office Contact Center mediante la compra de la solución IP Office Contact Center antes de la actualización. Sin embargo, CCR seguirá vendiéndose y recibiendo soporte en la versión anterior de acuerdo con la política de soporte del ciclo de vida de Avaya.

Avaya brindará a los clientes de CCR un camino claro para migrar a IP Office Contact Center. Además, como resultado de este cambio, Preferred Edition ahora vendrá con la base de datos Voicemail Pro y Visual Basic Scripting (anteriormente formaban parte de Advanced Edition).

Proceso de pedido

Los socios de Avaya pueden pedir las aplicaciones de software a su distribuidor autorizado de Avaya. Los socios de Avaya deben comunicarse directamente con sus respectivos distribuidores para comprar todas las aplicaciones de software de IP Office. Cada distribuidor implementa un proceso personalizado de compra y distribución de software IP Office para su red de socios de Avaya. Estos procesos internos específicos del distribuidor no están cubiertos por este documento.

Migración de BCM con CS1000 a IP Office

Esta configuración permite migrar una red de BCM y CS1000 a IP Office paso a paso al agregarle sistemas IP Office.

Soporte de protocolo	IP Office a BCM: SIP

	IP Office a CS1000: SIP IP Office a IP Office: SIP o H323 - SCN Networking BCM a BCM: SIP o SIP/MCDN BCM a CS1000: SIP o SIP/MCDN **Nota:** Solo se admitirá UDP y no TCP. IP Office a CS1000 mediante troncales H.323 o PRI no es compatible.
plataforma IP Office requisitos	Versión 8.1 o superior, ediciones Essential, Preferred o Server
plataforma BCM requisitos	BCM50 o BCM450 6.0
plataforma CS1000 requisitos	CS1000 7.5 con NRS
centralizado mensaje de voz	Correo de voz centralizado para todos los sistemas IP Office en la red SCN. Los sistemas BCM pueden usar el correo de voz centralizado del CS1000. Los sistemas IP Office no pueden usar el correo de voz centralizado de CS1000.
Los telefonos	Todos los teléfonos son compatibles con los servidores de llamadas individuales y las versiones, incluidos Avaya IP Phone (H.323), teléfonos Avaya Digital, teléfonos digitales de la serie BCM 7000, teléfonos IP (SIP) de la serie BCM1100/1200, teléfonos DECT R4 y teléfonos analógicos.

Migración de sucursales de IP Office

Hoja de ruta de migración y limitaciones

Puede actualizar desde un B5800 Branch Gateway a la versión actual de IP Office, o desde una versión anterior de IP Office a la versión actual de IP Office. El proceso de actualización para la solución IP Office Branch varía según cómo se implemente la arquitectura.

Si la versión de B5800 Branch Gateway o IP Office desde la que está actualizando está conectada a Avaya Aura®infraestructura y usos Avaya Aura®System Manager para administración centralizada, use Avaya Aura®System Manager para actualizar el firmware y el software del sistema.

Si la arquitectura se implementa en un entorno de sucursal independiente de IP Office sin centralización ni conexión a Avaya Aura®red, debe usar IP Office Manager para las actualizaciones. Desde IP Office Manager, puede realizar una actualización mediante el asistente de actualización o la tarjeta SD del sistema.

Para conocer los procedimientos sobre cómo realizar actualizaciones de System Manager o IP Office Manager para su solución de sucursal, consulte*Migración de IP Office o B5800 Branch Gateway a IP Office Enterprise Branch*.

Licencias

Muchas soluciones, aplicaciones y funciones de los sistemas IP Office tienen licencia y solo funcionan cuando se detecta una licencia válida. Esto incluye funciones dentro de las aplicaciones de IP Office conectadas al sistema IP Office.

Esta sección describe los requisitos de licencia para las funciones de IP Office. Para obtener información y procedimientos sobre la gestión de licencias, consulte "Solicitud de licencias" en los siguientes documentos:

- *Administración de IP Office de Avaya™Plataforma con Gerente*
- *Administración de IP Office de Avaya™Plataforma con Web Manager*

Puertos, canales y usuarios

Algunas licencias permiten varios puertos, canales o usuarios. Dependiendo de la licencia en particular, cada instancia admitida se puede consumir cuando está configurada para su uso o cuando realmente se está utilizando. Cuando no hay más instancias de una licencia disponibles, no se permite el uso posterior de la función con licencia.

Se pueden agregar varias licencias para brindar una mayor cantidad de puertos, canales o usuarios admitidos. Sin embargo, las licencias por encima de la capacidad admitida por la unidad de control de IP Office en particular no funcionarán.

Licencias PLDS

IP Office utiliza el Sistema de entrega y licencias de productos (PLDS) de Avaya para administrar las licencias. PLDS es una herramienta en línea basada en la web para administrar los derechos de licencia y la entrega electrónica de software y archivos de licencia relacionados. PLDS brinda a los clientes, socios de Avaya, distribuidores y asociados de Avaya herramientas fáciles de usar para administrar los derechos de licencia y la entrega electrónica de software y archivos de licencia relacionados. Con PLDS, puede realizar operaciones como activaciones de licencias, actualizaciones de licencias, movimientos de licencias y descargas de software. Puede acceder a PLDS desdehttp://plds.avaya.com/ .

Archivos de licencia PLDS

Las licencias se entregan desde PLDS con archivos de licencia. Se genera un archivo de licencia PLDS para instalar en una máquina específica. Hay dos opciones de implementación:

- Los archivos de licencia de PLDS Nodal se generan e instalan en nodos particulares de IP Office.
- Los archivos de licencia PLDS WebLM se generan e instalan en un servidor WebLM que puede otorgar licencias a varios nodos de IP Office.

Las licencias centralizadas de WebLM se admiten en IP Office Server Edition y en las implementaciones de IP Office Branch, pero no en las implementaciones que no son de sucursal del modo estándar de IP Office.

Página659 de 3226.

Id. de host PLDS

Cada archivo de licencia PLDS debe crearse con el ID de host PLDS del sistema donde se cargará el archivo de licencia. Los archivos de licencia de PLDS Nodal son específicos de la máquina y debe especificar el ID de host en el**Id. de host PLDS**campo en IP Office Manager o Web Manager.

Sistemas IP500 V2: Puede encontrar el ID de host de PLDS en el**Licencia**pestaña de IP Office Manager y Web Manager. La ID de host PLDS consta de dos dígitos "11", seguidos del número de serie de la clave de función de 10 dígitos impreso en la tarjeta SD de IP Office. Si se cambia la tarjeta SD, la ID de host PLDS también cambiará.

Servidores IP Office Linux: El ID de host de PLDS se puede encontrar en la etiqueta del servidor, la etiqueta del paquete del servidor y la pantalla de inicio de sesión de encendido del sistema. El ID de host de PLDS se deriva del ID del sistema. Si la ID del sistema cambia, la ID del host PLDS también cambiará.

WebLM: El ID de host de WebLM es la dirección Mac del servidor WebLM. En un entorno virtual, la ID de host de WebLM es una dirección Mac virtual que comienza con la letra "V". La ID de host de WebLM se debe usar al generar un archivo de licencia PLDS para el servidor WebLM a fin de implementar un esquema de licencia centralizado para múltiples sistemas IP Office. El ID de host de WebLM se puede encontrar en la etiqueta del servidor, la etiqueta del paquete del servidor, la pantalla de inicio de sesión del sistema y a través de la interfaz de administración de WebLM.

Administrador de licencias web (WebLM)

Web License Manager (WebLM) es una aplicación basada en web para administrar licencias. Si usa el servidor WebLM que se ejecuta en el servidor IP Office, puede usar IP Office Web Manager para iniciar sesión en el servidor WebLM seleccionando**Aplicaciones**>**Administrador de licencias web**. Las credenciales de WebLM se administran por separado de las contraseñas del sistema de IP Office y no forman parte del inicio de sesión único (SSO).

Nota:

- La administración de licencias de WebLM es compatible con las implementaciones de Server Edition y para las implementaciones de Enterprise Branch mediante el servidor WebLM de System Manager. No es compatible con los sistemas de modo estándar.
- Al actualizar desde una versión anterior, todos los sistemas deben ejecutar el mismo nivel de software. IP Office Server Edition no admite versiones mixtas.

Para obtener más información sobre WebLM, consulte*Administración de Avaya WebLM independiente*.

Migración de licencias ADI

Las licencias ADI ya no se admiten a partir de la versión 10.0. Las nuevas licencias deben obtenerse de PLDS.

Con One Source Configurator (OSC), todas las licencias ADI de versiones anteriores se actualizan a PLDS. los **Migración de licencia**La opción en IP Office Manager se puede usar para extraer información de licencia sobre el sistema, y esta información se puede cargar luego en OSC. Después de extraer la información, IP Office Manager firma el archivo para que no se pueda modificar.

Creación de licencia PLDS

La licencia PLDS debe crearse con la ID de host PLDS del sistema donde se cargará la licencia. Si las licencias se cargan localmente en IP Office, la ID de host PLDS está disponible en IP Office Manager o Web Manager. Para IP500 V2, también es el número de clave de función en la tarjeta SD, que comienza con "11". Si el archivo PLDS se carga en un servidor WebLM, la ID de host está disponible en la interfaz WebLM en **Propiedades del servidor**.

Para obtener más información sobre la migración de licencias de IP Office a PLDS, consulte*Administración de IP Office de Avaya™Plataforma con Gerente*o*Administración de IP Office de Avaya™Plataforma con Web Manager*.

Licencias virtuales

Como parte del proceso de migración, las siguientes licencias virtuales se proporcionan como licencias PLDS reales solo a través del proceso de migración XML:

- Edición esencial virtual
- Virtual Preferred Edition para sistemas con módulo UCMv1
- Terminales IP virtuales de Avaya para sistemas con:
  - Módulos VCM32/64 v1 que proporcionaron 12 terminales IP de Avaya
  - Licencias de migración de canal de VCM heredadas
- Puertos Voicemail Pro virtuales adicionales para Server Edition

  El sistema de licencias PLDS agrega dos puertos de Voicemail Pro a cualquier licencia de Server Edition o Server Edition Select.

Los clientes con sistemas más antiguos (IP500 V1 / IP406 V2 / IP412 en la versión 6.0 o posterior) pueden actualizar a través de la carga de BOM del configurador A1S y el proceso de validación de licencia ADI. Las licencias virtualizadas en estos sistemas más antiguos no se transferirán y se deben comprar como nuevas.

Nota:

El teléfono basado en software heredado de Windows no es compatible con la versión 11.0 de IP Office y no funcionará. Las licencias virtuales anteriores proporcionadas al actualizar ya no se proporcionan en la versión 11.0. Equinoccio de Avaya™para Windows es el reemplazo. La licencia Teleworker permite el uso de Avaya Equinox™para ventanas. En versiones anteriores, esto solo estaba disponible con Office Worker y Power User.

Licenciamiento centralizado y nodal de Server Edition

Antes de la versión 10, las implementaciones de Server Edition usaban licencias nodales. Este tipo de licencia aún se puede usar en la versión 10 y posteriores. Sin embargo, se espera que la mayoría de las implementaciones prefieran centralizar la administración de licencias mediante el servidor Avaya Web License Management (WebLM). El servidor WebLM se instala automáticamente en el servidor Primario de Server Edition. Para los sistemas recién instalados, la licencia centralizada es la configuración predeterminada.

Todos los sistemas de la solución Server Edition deben utilizar el mismo**Fuente de licencia**.

Licencias nodales

Con la licencia de nodo, los archivos de licencia deben instalarse en cada nodo del sistema. Para algunas funciones con licencia, la licencia requerida se puede instalar en el servidor Primario de Server Edition y

utilizado por todos los nodos del sistema. Sin embargo, para otras funciones con licencia, la licencia requerida debe instalarse en el nodo donde se usa la función.

Licencias centralizadas

A partir de la versión 10, puede usar el servidor WebLM que se ejecuta en el servidor Primario de Server Edition para centralizar completamente la administración de licencias. Con la gestión de licencias centralizada, todas las licencias están contenidas en un solo archivo PLDS cargado en WebLM. Todos los nodos de la solución obtienen sus licencias de WebLM.

El servidor secundario de IP Office y los sistemas de expansión se pueden configurar para solicitar licencias directamente desde el servidor WebLM o para usar una opción de proxy. Cuando se configura para usar la opción de proxy, las solicitudes de licencia se envían a través del servidor primario de IP Office, que envía las solicitudes al servidor WebLM. El servidor primario no asigna licencias, solo actúa como proxy.

Los sistemas que usan licencias nodales se pueden convertir para usar licencias centralizadas. Dado que los archivos de licencia PLDS se generan utilizando la ID de host del servidor donde residen, debe volver a generar el archivo de licencia utilizando la ID de host del servidor WebLM que alojará el archivo de licencia.

Distribución centralizada de licencias

Cuando el origen de la licencia es WebLM, el**Licencias reservadas**los campos de solo lectura indican las licencias que se requieren para las funciones configuradas actualmente. Los campos editables se pueden utilizar para:

- Solicitar licencias adicionales del servidor WebLM.
- Eliminar licencias del nodo de IP Office para aplicarlas en otro lugar.

Importante:

Al reasignar licencias, siempre reduzca el número en el nodo de IP Office donde se aplican actualmente antes de aplicarlas en otro nodo. Si supera el número de licencias disponibles, recibirá un mensaje de error.

Distribución después de la conversión de licencias nodales a centralizadas

- Si el nodo de IP Office necesita alguna de las siguientes licencias, debe configurar manualmente la respectiva**Licencias reservadas**campos editables. Esto permitirá que el nodo de IP Office solicite las licencias del servidor WebLM.
  - **Administradores de grabaciones de VMPro**
  - **VMPro TTS profesional**
  - **Enlace CTI Pro**

Configuración de licencia reservada de extensión: Cuando la fuente de la licencia es**Local**, el ajuste **Extensión**> **VoIP**>**Licencia de reserva**se establece en**Ninguna**. Cambiar la fuente de licencia a WebLM cambia la configuración a**Reservar la licencia de endpoint IP de Avaya**. Si es necesario, debe cambiar manualmente esta configuración a**Reservar licencia de terminal de terceros**o**Ambas cosas**.

Asignación de licencias en WebLM

Puede utilizar WebLM para ver las licencias utilizadas por cada nodo en IP Office Server Edition. En el panel de navegación de WebLM a la izquierda, haga clic en**Productos con licencia**. La tabla Licencias adquiridas muestra información sobre las licencias adquiridas para cada ID de cliente. En IP Office, la ID de cliente de WebLM para cada nodo se muestra en la página del servidor remoto de la licencia.

Distribución de licencias nodales

Cuando el**Fuente de licencia**es**Local**, la**Licencias reservadas**los campos de solo lectura indican las licencias que se requieren para las funciones configuradas actualmente.

La licencia nodal para una solución Server Edition se basa en una combinación de licencias realizadas a través del servidor Primario de Server Edition más algunas licencias específicas del servidor. Todas las licencias específicas del usuario y del sistema se pueden administrar desde el servidor primario de Server Edition que también actúa como un servidor de licencias. Las licencias se ingresan en la configuración del servidor Primario de Server Edition y se basan en la ID del sistema de ese servidor.

Cuando se usa una licencia para habilitar funciones, como canales SIP Trunk, en otros sistemas, el servidor Primario de Server Edition solo asigna esas licencias a otros sistemas después de haber satisfecho sus propias necesidades de licencia.

Cuando otro sistema pierde la conexión con el servidor Primario de Server Edition, cualquier requisito de licencia basado en las licencias ingresadas en la configuración del servidor Primario de Server Edition se admite durante un período de gracia de 30 días.

Otras licencias específicas del servidor se ingresan en la configuración del servidor que requiere la función y se basan en el ID del sistema de ese sistema.

Licencia	servidor principal	Específico del servidor
Edición del servidor	Sí	No
Terminales IP de Avaya	Sí	No
Puntos finales de IP de terceros	Sí	No
Canales troncales SIP	Sí	No
Canales PRI universales IP500	No	Sí
Puertos de correo de voz adicionales [3]	Sí	No
Colaboración web	No	Sí
Servicios Web UMS [1]	No	Sí
Empleado de oficina	Sí	No
Usuario de poder	Sí	No
Actualización de Office Worker a Power User	Sí	No
Recepcionista	No	Sí
Enlace CTI Pro	No	Sí
Mensajería TTS Pro [3]	Sí	No
Administrador de grabaciones de Voicemail Pro [2] [3]	Sí	No
Usuario WAV	No	Sí
tunelización IPSec	No	Sí

1. Las licencias del servicio web UMS son solo para grupos de búsqueda.
2. La licencia de administrador de grabación de Voicemail Pro hace referencia a Contact Store. Solo se requiere una licencia para una red Server Edition.

3. Para implementaciones con dos servidores Voicemail Pro, Messaging TTS Pro, Voicemail Pro Recording Administrator y las licencias de puertos de correo de voz adicionales deben estar en el servidor secundario.

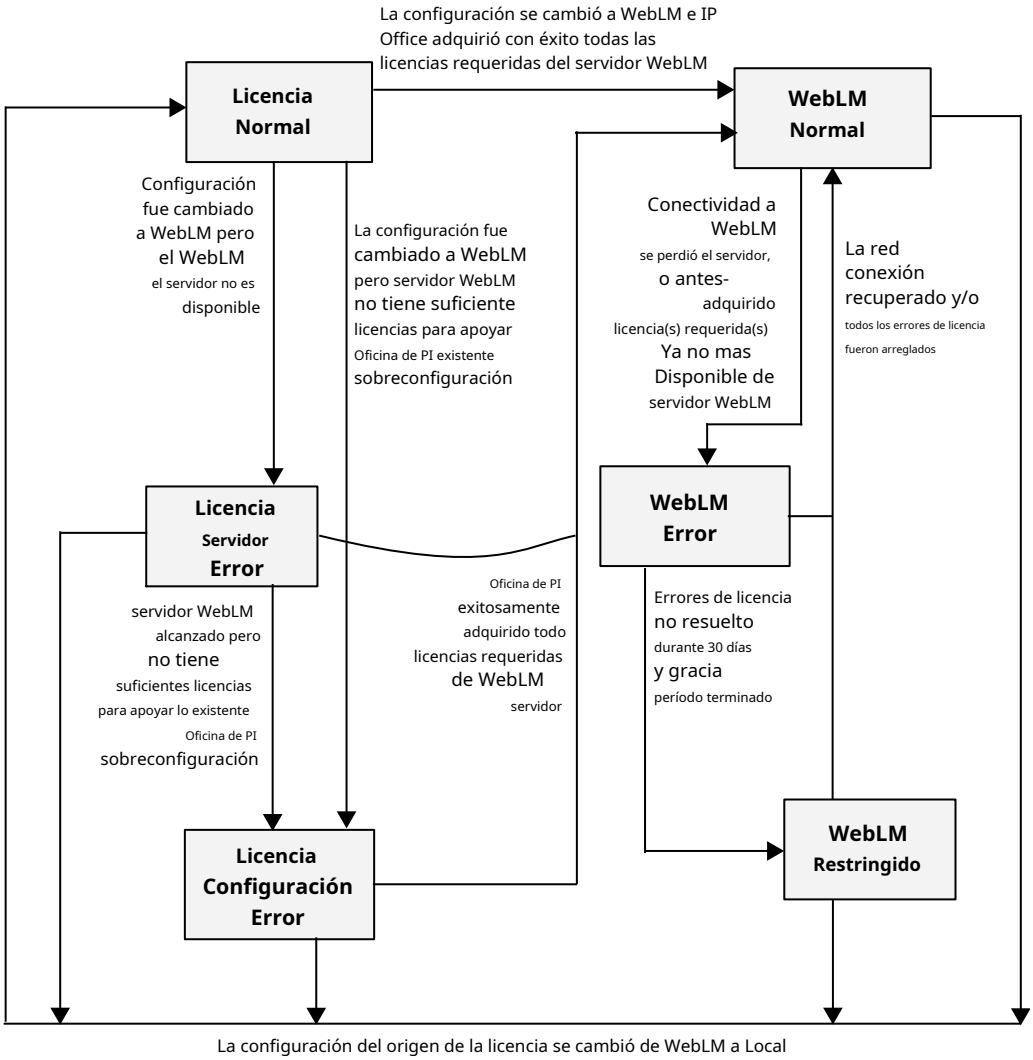
Licencias WebLM

Modos de licencia

Los siguientes son los modos de licencia de IP Office cuando utiliza licencias WebLM. El modo de licencia se muestra en IP Office Manager, Web Manager y System Status Application (SSA).

Modo	Descripción
Licencia Normal	La licencia de WebLM no está configurada. Licenciamiento Nodal Tradicional. Sin período de gracia. Se permite la sobreconfiguración.
Servidor de licencias Error	La configuración se cambió a WebLM, pero el servidor WebLM no está disponible. Sin período de gracia. Hasta que se resuelva el problema, IP Office no tiene licencia y no se puede usar de manera similar a las licencias tradicionales de Nodal si no se instalan licencias.
Licencia Configuración Error	La configuración se cambió a WebLM y el servidor WebLM está disponible, pero no tiene suficientes licencias para admitir la configuración de IP Office existente. Sin período de gracia. Hasta que se resuelva el problema, IP Office no tiene licencia y no se puede usar de manera similar a las licencias tradicionales de Nodal si no se instalan licencias. Las licencias se deben agregar al archivo de licencia de WebLM o se debe modificar la configuración de IP Office para corregir la sobreconfiguración.
WebLM normal	IP Office está configurado para licencias WebLM, el servidor WebLM está disponible e IP Office adquirió con éxito todas las licencias necesarias para admitir todas sus funciones configuradas. Se adquieren nuevas licencias para funciones recién configuradas y se evita la sobreconfiguración de funciones con licencia si no se pueden adquirir licencias. IP Office renueva periódicamente sus licencias adquiridas. Si no se renueva, se activará el modo de error de WebLM con un período de gracia.
Error de WebLM	IP Office está configurado para licencias de WebLM y anteriormente estaba en el modo normal de WebLM. Pero IP Office ahora no puede renovar ni volver a adquirir todas las licencias requeridas para admitir todas sus funciones configuradas. Se evita la sobreconfiguración de las funciones con licencia si no se pueden adquirir las licencias. IP Office sigue funcionando durante un período de gracia de 30 días según su configuración existente (las licencias perdidas se reemplazan con licencias de gracia virtuales).
WebLM Restringido	IP Office estaba en el modo de error de WebLM, pero el período de gracia de 30 días venció y los problemas de este error no se resolvieron. Las funciones sin licencia dejarán de funcionar (se eliminarán las licencias virtuales de gracia). No se permite ninguna configuración de IP Office, excepto los cambios de configuración que reducen los errores de licencia.

Transiciones de estado del modo de licencia



Configuración de licencias de WebLM

En las licencias de WebLM, las licencias deben ser totalmente compatibles con la configuración de IP Office. No se permite la sobreconfiguración. IP Office, según su configuración, solicita las licencias requeridas del servidor WebLM.

Para algunos tipos de licencias, como para usuarios, extensiones, recepcionistas y colaboración web, el tipo y la cantidad de licencias requeridas está determinado por la configuración de los elementos respectivos. Por ejemplo, los registros de Usuario y Extensión en la configuración de IP Office. Estas cantidades se muestran en campos de solo lectura en la lista 'Licencias reservadas' en la pestaña Licencia de configuración de IP Office > Servidor remoto.

Para otros tipos de licencias, como sesiones de troncales SIP y puertos Voicemail Pro, la cantidad de licencias requeridas debe configurarse explícitamente. Estas cantidades deben configurarse en campos editables en la lista de Licencias reservadas en la pestaña Licencia de configuración de IP Office > Servidor remoto.

Advertencias y alarmas de configuración de licencias

Modo de error de configuración de licencia

- IP Office entra en el modo de error de configuración de licencia cuando cambia el origen de la licencia de IP Office de "Local" a "WebLM" y tiene una licencia insuficiente o una configuración excesiva.

  En este modo, IP Office no tiene licencia y no se puede utilizar. Este modo es un estado de error de transición y no se admite como estado estable. Intente evitar entrar en este modo y, si sucede, corrija los errores de inmediato.
- Los sistemas instalados con licencias tradicionales pueden tener una licencia insuficiente o una configuración excesiva. Si se actualizan a la versión 10.0 y se migran mediante licencias WebLM sin adquirir las licencias adicionales necesarias o eliminar la sobreconfiguración, los sistemas instalados entran en el modo Error de configuración de licencia después de la migración.

  Para ayudar a evitar este problema, la herramienta de migración de licencias de IP Office Manager emite advertencias. Si IP Office tiene una configuración excesiva en relación con sus licencias antiguas existentes, la herramienta de migración de licencias muestra una advertencia y también incluye información de advertencia detallada en el archivo de información de migración de licencias.
- Si IP Office se encuentra en el modo Error de configuración de licencia, la página de alarmas de Systems Status Application (SSA) muestra alarmas que indican la causa del problema.

  Si encuentra este modo, revise los errores de alarma de SSA y resuélvalos adquiriendo las licencias requeridas que faltan o modificando la configuración de IP Office para que no requiera estas licencias.

Otras advertencias

Cuando el administrador establece el Origen de la licencia en “WebLM”, IP Office Manager e IP Office Web Manager muestran una advertencia que le indica al administrador que revise y verifique que haya suficientes licencias disponibles en el servidor WebLM.

Licencias de usuario WebLM y punto final de IP

Licencias de terminales de IP

Cuando IP Office utiliza licencias WebLM, cada extensión H.323 o SIP configurada requiere una licencia e IP Office solicita las licencias requeridas del servidor WebLM. Se requieren licencias suficientes para todas las extensiones H.323 y SIP configuradas y no solo para el número máximo de extensiones registradas simultáneamente. Esto es coherente con las licencias de WebLM para usuarios y recepcionistas.

Nota:

Con las licencias de WebLM, IP Office no admite la configuración de una gran cantidad de extensiones con una pequeña cantidad de licencias para cubrir solo un subconjunto de las extensiones que se registran al mismo tiempo. Por ejemplo, configurar tres extensiones con una licencia de terminal de IP para cubrir solo una de las tres extensiones que se registran al mismo tiempo. Sin embargo, si desea compatibilidad con este comportamiento, puede utilizar un archivo de licencia PLDS local en lugar de una licencia WebLM centralizada y establecer el **Licencia de reserva**campo para las extensiones aNinguna.

Para cada extensión H.323 o SIP configurada, IP Office solicita al servidor WebLM una licencia de terminal IP de Avaya o de un tercero, según el**Licencia de reserva**campo del registro de extensión configurado. Cuando IP Office utiliza licencias WebLM, el**Licencia de reserva**El campo para cada extensión H. 323 y SIP configurada se establece de forma predeterminada en la licencia de terminal IP de Avaya. Este campo es editable y el

el administrador puede cambiarla a una licencia de terminal IP de terceros o a Avaya y terminales IP de terceros.

Nota:

Para el**Licencia de reserva**campo, el valorNingunano está disponible con licencias WebLM porque IP Office debe solicitar una licencia del servidor WebLM.

Licencias de usuario

Cuando IP Office utiliza licencias WebLM, se requieren suficientes licencias de usuario según la configuración de usuarios de IP Office y no solo para la cantidad máxima de usuarios registrados simultáneamente. Esto es coherente con las licencias de WebLM para recepcionistas y terminales de IP. IP Office solicita del servidor WebLM las licencias de usuario requeridas (por ejemplo, licencias de usuario avanzado) según el perfil de usuario de todos los usuarios configurados.

Nota:

Con las licencias de WebLM, IP Office no admite la configuración de una gran cantidad de usuarios con una pequeña cantidad de licencias para cubrir solo un subconjunto de usuarios que se registran al mismo tiempo. Por ejemplo, configurar tres usuarios con una licencia de usuario para cubrir solo uno de los tres usuarios que se registran al mismo tiempo. Sin embargo, si desea compatibilidad con este comportamiento, puede utilizar un archivo de licencia PLDS local en lugar de una licencia WebLM centralizada.

Licencias de recepcionista

Cuando IP Office usa licencias de WebLM, se requieren licencias de recepcionista para todos los usuarios que están configurados como recepcionista y no solo para la cantidad máxima de usuarios que ejecutarían su aplicación IP Office SoftConsole simultáneamente. Esto es coherente con las licencias de WebLM para puntos finales y usuarios de IP. Con WebLM, se requieren licencias de acuerdo con los objetos configurados, y no se permite la sobreconfiguración ni la sublicencia.

Nota:

Con las licencias de WebLM, IP Office no admite la configuración de una gran cantidad de usuarios Receptionist con una pequeña cantidad de licencias para cubrir solo un subconjunto de usuarios que se conectan al mismo tiempo mediante IP Office SoftConsole. Por ejemplo, configurar tres usuarios de recepcionista con una licencia de recepcionista para cubrir solo uno de los tres usuarios que se conectan al mismo tiempo mediante IP Office SoftConsole. Sin embargo, si desea compatibilidad con este comportamiento, puede utilizar un archivo de licencia PLDS local en lugar de una licencia WebLM centralizada.

Soporte de creación automática para usuarios y extensiones

Cuando IP Office utiliza licencias WebLM, no puede crear automáticamente usuarios y extensiones, ya que no es compatible. El administrador debe configurar manualmente los usuarios y las extensiones. Para extensiones DECT, se debe utilizar el método “Preconfigurado”.

Sin embargo, se admite la creación automática de usuarios y extensiones si utiliza un archivo de licencia PLDS local en lugar de una licencia WebLM centralizada.

Licencia Basic Edition para nuevos sistemas

Para actualizar a la versión 11.0, la nueva licencia de tiempo de ejecución de actualización PLDS R11.0 se utiliza en combinación con el software R11.0. La actualización a IP Office R11.0 desde versiones anteriores a la R10.0 implica una transición completa a las licencias PLDS. Para actualizar los sistemas IP Office existentes a IP Office R11.0, se requieren licencias de actualización o migración pagadas o transaccionales o autorizadas de la Edición R11.0.

Código material	Licencia	Descripción
396490	ACTUALIZACIÓN DE MIG DE LA EDICIÓN BÁSICA DE IP OFFICE R11 plds	R11 Edición básica a partir de PLDS
369472	MIGRACIÓN DE LA EDICIÓN BÁSICA DE IP OFFICE R11 MEJORA	Actualización de ADI o PLDS a R11 Edición básica

Los clientes también deben comprar tarjetas SD, que están configuradas, de manera predeterminada, con la Edición básica.

Los clientes deben obtener este código de material, que es comercializable y no tiene que configurarse, antes de solicitar los servicios de soporte de IP Office. Esto es especialmente importante para los clientes que ya tienen la Edición básica o para compras de servicios de soporte de IP Office posventa, incluidos los clientes que primero configuran la Edición básica sin los servicios de soporte de IP Office, pero luego eligen obtener los servicios de soporte de IP Office. Estos clientes deben realizar un pedido de mercadería para este código de material primero y luego realizar su compra posventa de servicios de soporte de IP Office y registrar su equipo para servicio.

Nota:

La Edición Básica no es un requisito previo para la Edición Esencial o la Edición Preferida, y no se apila bajo la Edición Esencial.

Licencias Essential Edition y Preferred Edition

Una licencia de Essential Edition es un requisito previo en los sistemas IP500 V2 e incluye hermanamiento móvil para todos los usuarios y cuatro trabajadores remotos.

Una licencia de Preferred Edition es un requisito previo para cualquier licencia de perfil de usuario. En una red multisitio, la licencia Preferred Edition del sistema central se comparte automáticamente con otros sistemas en la red, lo que permite licencias de perfil de usuario en esos otros sistemas. Sin embargo, cada sistema que admita un servidor de Voicemail Pro aún requiere su propia licencia Preferred Edition para el funcionamiento de Voicemail Pro. Para un sistema IP500 V2 equipado con un módulo de comunicaciones unificadas (UCM V2), la tarjeta requiere una licencia Preferred Edition separada.

La licencia Preferred Edition incluye soporte para 4 puertos de mensajería. El número total de puertos de mensajería admitidos se puede aumentar agregando licencias de puertos de mensajería adicionales, en el momento de la compra o posteriormente, hasta el máximo admitido por la unidad de control en particular.

Código de orden	Licencia	Descripción
396491	ACTUALIZACIÓN DE IP OFFICE R11 ESSENTIAL EDITION PLDS LIC:DS	Edición esencial (actualizaciones de PLDS)
396474	IP OFFICE R11 ESSENTIAL EDITION MIG UPG LICENCIA:DS	Migraciones de ADI a PLDS y actualizaciones a R11.0 Essential Edition
396492	IP OFFICE R11 PREFERENCIAL VOICEMAIL PRO ACTUALIZAR PLDS LIC:DS	Edición preferida (actualizaciones de PLDS)
396476	IP OFFICE R11 PREFERIDO VOICEMAIL PRO MIG UPG LIC:DS	Migraciones de ADI a PLDS y actualizaciones a R11.0 Preferred Edition

Licencias de edición de servidor

Una licencia de Server Edition incluye:

- Características de la Edición Esencial
- Características de la edición preferida
- Voicemail Pro centralizado
- Dos puertos de Voicemail Pro
- Canales ilimitados de redes multisitio (líneas de IP Office)

Una licencia de Server Edition permite:

- Conferencia Meet-Me
- Mensajería avanzada
- Asistente automático
- Grabacion de llamada
- Enrutamiento de llamadas condicional
- Anuncios de cola
- Hermanamiento móvil
- Control de llamadas
- Llamar de vuelta

Se requiere una licencia de Server Edition para el servidor principal, el servidor secundario y para cada sistema de expansión Linux o IP500 V2. Las licencias permiten redes de voz entre sistemas en la red de Server Edition.

Código de orden	Licencia	Descripción
Actualizaciones de PLDS (a partir de PLDS)		
396493	IPO R11 SE/VRTLZD UPG PLDS LIC	Código de actualización pagado
Migraciones de ADI a PLDS y actualización a R11.0		
396480	IP Office R11 SE ADI MIG UPG LIC	Código de actualización pagado
396478	IPO R11 VRTLZD SE Migración ADI UPG LIC	Código de actualización pagado
Actualizaciones de PLDS de IP Office		
396519	IPO-SL 11 SE/VRTLZD UPG PLDS LIC	Código de actualización pagado

Licencias de sucursales

La siguiente tabla describe las licencias clave de IP Office que son de particular interés para las implementaciones de sucursales.

Nombre para mostrar	Descripción
Modelo WebLM de Avaya	Esta licencia es requerida por IP Office en implementaciones de sucursales para poder conectarse al servidor WebLM y usar licencias centralizadas de WebLM.
Sistema de Sucursales	Esta licencia es necesaria para IP Office en implementaciones de sucursales. Se utiliza únicamente con fines de seguimiento.
Licencia de terminales centralizados de IP Office	Se requiere una licencia para cada usuario centralizado configurado en IP Office con una extensión SIP o una extensión analógica. **Importante:** Además de esta licencia de IP Office, cada usuario centralizado también requiere una licencia en Avaya Aura central.®sistema.
Canal troncal SM	Se requiere esta licencia con la cantidad suficiente para permitir que se habilite en el sistema la cantidad máxima de llamadas de línea SM simultáneas. La cantidad total de requisitos de licencias de canal troncal SM depende de los patrones de tráfico esperados en la implementación en particular. **Nota:** IP Office también admite conexiones de línea SM a Avaya Aura® Session Manager en otras implementaciones de IP Office Server Edition. Estas conexiones no se limitan a implementaciones de sucursales.

Licencias de red comunitaria pequeña

En una red comunitaria pequeña (SCN), debe haber al menos una edición preferida de IP Office. Se requieren dos con resiliencia.

Los diferentes tipos de usuarios en un SCN tienen la misma funcionalidad, independientemente de dónde esté instalado IP Office Preferred Edition.

En una red multisitio, si uno o más sistemas IP Office Preferred Edition están instalados, todos los sistemas IP Office en la red multisitio tendrán automáticamente licencias Preferidas como requisitos previos para los siguientes tipos de usuarios:

- Usuarios avanzados
- Teletrabajadores
- Trabajadores móviles
- Trabajadores de oficina

Licencias troncales

Las tablas de esta sección incluyen todos los códigos de material de licencia de software IP Office PLDS nuevos y actualizados. Los códigos de material con indicación de R10+ se conocen como códigos "CUALQUIERA" y se pueden usar para implementaciones de sistemas de la versión 10.0 y posteriores. Las descripciones de SAP se han modificado para mostrar 10+ para este cambio, mientras que el código de material sigue siendo el mismo. Otros códigos son específicos de la versión R11.0 y contienen R11.0 en la descripción.

Sesiones de troncales SIP

Estas licencias se utilizan para permitir sesiones en troncales SIP y líneas SM agregadas al sistema. Se pueden combinar varias licencias para el número total de canales necesarios.

Código de orden	Licencia	Descripción
383085	IPO R10+ SIP TRNK 1 LIC	Troncal SIP 1 sesión
307332	IIPO-SL R10+ SIP TRNK 1 LIC	Sesión de troncal SIP 1: seleccione
383120	IPO R10+ SM LÍNEA SIP TRNK LIC	Sesión de línea SM
382917	IPO-SL R10+ LÍNEA SM SIP TRK LIC	Sesión de línea IP Office Select SM

Canales adicionales IP500 Universal PRI

La tarjeta troncal universal (UTC) IP500 PRI está disponible en variantes de 1 o 2 puertos, cada puerto admite una única conexión de circuito PRI. Los puertos se pueden cambiar entre los tipos de línea compatibles E1, E1R2 o T1 según sea necesario para el enlace troncal que se está conectando. Cada puerto admite 8 canales B ("Portador") que no necesitan licencia. Si se requieren canales B adicionales, se deben licenciar mediante la adición de las licencias a continuación. Se pueden agregar varias licencias para lograr el número total de canales necesarios. Los canales D no están sujetos a licencia. Las licencias son consumidas por esos canales, que están configurados como*en servicio*, en el orden de las tarjetas IP500 PRI-U instaladas.

IP500 Universal PRI canales E1 adicionales

Estas licencias se utilizan para habilitar canales B E1 adicionales para tarjetas IP500 PRI-U configuradas para operación E1. Cada puerto puede admitir hasta 30 canales B en este modo.

Código de orden	Licencia	Descripción
383092	IPO R10+ IP500 E1 AGREGAR LICENCIA DE 2 CANALES	2 canales E1
383093	IPO R10+ IP500 E1 AGREGAR LICENCIA DE 8 CANALES	8 canales E1
383094	IPO R10+ IP500 E1 AGREGAR LICENCIA DE 22 CANALES	22 canales E1
307337	IPO-SL R10+ IP500 E1 AGREGAR LICENCIA DE 2 CANALES	2 canales E1 – Seleccionar
307338	IPO-SL R10+ IP500 E1 AGREGAR LICENCIA DE 8 CANALES	8 canales E1 – Seleccione
307339	IPO-SL R10+ IP500 E1 LICENCIA DE 22 CANALES	22 canales E1 – Seleccionar

IP500 Universal PRI canales adicionales E1R2

Estas licencias se utilizan para habilitar canales B E1R2 adicionales para tarjetas IP500 PRI-U configuradas para la operación E1R2. Cada puerto puede admitir hasta 30 canales B en este modo.

Página671 de 3226.

Código de orden	Licencia	Descripción
275637	IPO R10 IP500 E1R2 AGREGAR 2CH PLDS LIC	2 canales E1R2
383096	IPO R10+ IP500 E1R2 AGREGAR LICENCIA DE 8 CANALES	8 canales E1R2
383097	IPO R10+ IP500 E1R2 AGREGAR LICENCIA DE 22 CANALES	22 canales E1R2
307340	IPO-SL R10+ IP500 E1R2 2CH LIC	2 canales E1R2 – Seleccionar
307341	IPO-SL R10+ IP500 E1R2 8CH LIC	8 canales E1R2 – Seleccione
307342	IPO-SL R10+ IP500 E1R2 LICENCIA DE 22 CANALES	22 canales E1R2 – Seleccionar

IP500 V2 Universal PRI canales T1 adicionales

Estas licencias se utilizan para habilitar canales T1 B adicionales para tarjetas IP500 PRI-U configuradas para operación T1 PRI o T1 con bits robados. Cada puerto puede admitir hasta 23 canales B (T1 PRI) o 24 canales B (bit T1 robado) en este modo.

Código de orden	Licencia	Descripción
383091	IPO R10+ IP500 T1 AGREGAR LICENCIA DE 2 CANALES	2 canales T1
307336	IPO-SL R10+ IP500 T1 AGREGAR LICENCIA DE 2 CANALES	2 canales T1 – Seleccione

Redes de voz IP500 V2

El uso de troncales de redes de voz privadas entre unidades de control IP500 V2 y otros sistemas requiere licencias de canales de redes de voz dentro de IP500 V2. Esto se aplica a las troncales IP H.323 configuradas en IP500 V2, incluidas las troncales IP que se utilizan para una red comunitaria pequeña (SCN) de IP Office. También se requiere una licencia de redes de voz para el uso de troncales configuradas para operación Q.SIG. En un troncal IP H.323, se consume una instancia de licencia para cada llamada saliente simultánea. En un troncal Q.SIG, la cantidad de llamadas está limitada por el tipo de troncal en lugar de las licencias disponibles.

Se pueden agregar licencias adicionales para lograr la cantidad de canales de red de voz necesarios.

Código de orden	Licencia	Descripción
383087	IPO R10+ IP500 VCE NTWK 4 LIC	4 canales de red de voz, incluidas las funciones de red avanzada (grupos distribuidos y escritorio compartido en Small Community Network)

Licencias de usuario

Un perfil controla si los usuarios pueden configurarse para una serie de funciones. Todos los usuarios del sistema, excepto los usuarios con perfil de usuario básico y los usuarios sin licencia, requieren uno de los tipos de licencia de usuario.

La siguiente tabla enumera los diferentes perfiles de usuario y las funciones a las que puede acceder cada perfil. Establecer un usuario en un perfil particular habilita esas funciones de forma predeterminada, pero se pueden deshabilitar manualmente si es necesario. El número de usuarios que se pueden configurar para cada perfil está controlado por las licencias de usuario presentes en la configuración.

Excepto para un usuario básico, una licencia del sistema Preferred Edition es un requisito previo para cualquier licencia de perfil de usuario. En una red de sitios múltiples, la licencia de Preferred Edition para el sistema central se comparte automáticamente con otros sistemas en la red, lo que permite licencias de perfil de usuario en esos otros sistemas. Sin embargo, cada sistema que admita un servidor de Voicemail Pro aún requiere su propia licencia Preferred Edition para el funcionamiento de Voicemail Pro.

Rasgo		Modo estandar					Edición del servidor		
	No- con licencia Usuario [1]	Básico Usuario	Oficina Trabajador	teletrabajo ker	Móvil Trabajador	Energía Usuario	Básico Usuario	Oficina Trabajador	Energía Usuario
una-X Portal Servicios	–	–	Sí	Sí	–	Sí	–	Sí	Sí
telecomunicaciones útero opciones	–	–	–	Sí	–	Sí	–	–	Sí
Web de la UMS Servicios	–	–	Sí	Sí	–	Sí	–	Sí	Sí
TTS para Correo electrónico Lectura	–	–	–	–	Sí	Sí	–	–	Sí
Remoto trabajador [2]	–	–	–	Sí	–	Sí	Sí	Sí	Sí
Avaya comun gato [3]	–	–	Sí	Sí	–	Sí	Sí	Sí	Sí
WebRTC	–	–	Sí	–	–	Sí	–	Sí	Sí
Avaya Equinoccio™	–	–	Sí	Sí	–	Sí	–	Sí	Sí

Notas de perfil de usuario:

1. Se pueden crear usuarios sin licencia en los sistemas Standard Mode y Server Edition.
2. El sistema admite usuarios que utilizan extensiones remotas H.323 o SIP. En los sistemas que no son Server Edition, se admiten hasta 4 usuarios como extensiones remotas sin necesidad de configurarlos ni obtener una licencia para un perfil de usuario. Se admiten usuarios remotos adicionales si tienen licencia y están configurados para un **teletrabajador**o**Usuario de poder**perfil del usuario. En los sistemas Server Edition, el trabajador remoto es compatible con todos los perfiles de usuario.
3. Compatible con el uso avanzado de Avaya Communicator para IP Office si también están instaladas las aplicaciones one-X Portal y Voicemail Pro. De lo contrario, solo se admite el uso básico de Avaya Communicator para IP Office.
4. Equinoccio de Avaya™se puede utilizar con una licencia de usuario básico o de trabajador móvil junto con una licencia de IP Softphone, pero solo en modo estándar. En tales casos, el modo simultáneo, la función de control compartido y el soporte de presencia no estarán disponibles.

Usuario sin licencia

Un usuario sin licencia:

- Se permite acceso telefónico y paginación.
- Se puede utilizar como puerto de buscapersonas analógico o de música en espera.
- Se puede autenticar para permitir el acceso remoto para la administración remota.
- Puede realizar llamadas internas y de emergencia como NoUser.
- Puede reenviar al buzón de correo de voz para usuarios de buzón de correo de voz únicamente.
- Se puede utilizar para hermanamiento interno.

Usuarios básicos

Los nuevos usuarios se crean como usuarios básicos de forma predeterminada. Los usuarios básicos pueden realizar hot-desking, realizar y recibir llamadas, desviar llamadas y realizar hermanamiento móvil.

Las licencias de usuario básicas ya no se proporcionan. Tanto para los sistemas nuevos como para las actualizaciones, el**Usuarios básicos**el campo está atenuado.

Se requieren licencias de usuario básicas solo en el entorno de la nube.

licencias de oficinista

Esta opción está dirigida a usuarios que trabajan en la oficina. Junto con un teléfono Avaya con cable o inalámbrico, estos usuarios cuentan con funciones para controlar su comunicación con una PC. Por ejemplo, estos usuarios pueden controlar conferencias de audio o administrar el correo de voz con un cliente de correo electrónico (requiere una licencia Preferred Edition).

Una licencia de Office Worker habilita Avaya Communicator, Avaya Equinox™para Windows y Mac, y Avaya Communicator for Web. La licencia de Office Worker permite a un usuario utilizar el Servicio de mensajería unificada (UMS) y Avaya one-X®Portal para IP Office sin funcionalidad Telecommuter. Las instancias de licencia se consumen para cada usuario que se configura.

Código de orden	Licencia	Descripción
383105	IPO R10+ TRABAJADOR MÓVIL 5 TRL LIC	5 licencias para trabajadores móviles
383107	IPO R10+ TRABAJADOR DE OFICINA 5 TRL LIC	5 licencias para oficinistas
307347	IPO-SL R10+ OFICINA TRABAJADOR 5 TRL LIC	5 usuarios – Seleccionar

Licencias de teletrabajador

Esta opción está dirigida a usuarios que trabajan desde casa o en otro lugar con conexión a Internet a la oficina. Se les proporciona la capacidad de aprovechar el PLDS o ISDN usando el modo Telecommuter, sin incurrir en cargos telefónicos remotos. Como alternativa, se puede usar el nuevo IP Office Video Softphone si la calidad del servicio de la conexión a Internet local es adecuada.

Teleworker incluye la capacidad de trabajador remoto con el paquete. Una licencia de Essential Edition proporciona 4 puestos de trabajo remoto. Los clientes que requieran asientos adicionales deberán comprar la solución Teleworker.

La licencia Teleworker permite a un usuario utilizar Avaya Communicator, Avaya Equinox™para Windows y Mac, y Avaya one-X® Portal de IP Office. La funcionalidad UMS para correo de voz o integración de correo electrónico también está habilitada, proporcionando sincronización con cualquier cliente de correo electrónico IMAP. Las instancias de licencia se consumen para cada usuario que se configura.

Código de orden	Licencia	Descripción
383103	Licencia IPO R10+ TELEWORKER 5 TRL	5 usuarios

Licencias de trabajadores móviles

Esta opción está dirigida a usuarios con dispositivos móviles. Por ejemplo, el personal de servicio y ventas de campo que a menudo está de viaje. Estos usuarios cuentan con funciones, como acceso a un número y control de llamadas como si estuvieran en la oficina, lo que les permite no perder nunca una llamada. La licencia de Mobile Worker permite el uso del cliente one-X Mobile Preferred en modo de devolución de llamada (pero no en modo VoIP).

Licencias de usuario avanzado

Esta opción está dirigida a trabajadores clave del conocimiento que necesitan la funcionalidad de trabajador móvil y teletrabajador. Una licencia de usuario avanzado habilita Avaya Communicator, Avaya Equinox™ (escritorio y móvil), Avaya Communicator for Web y modo VoIP en one-X Mobile Preferred.

La licencia de usuario avanzado le permite a un usuario usar Avaya one-X®Portal para IP Office, todas las funciones de movilidad y UMS. Se requiere una licencia de usuario avanzado para habilitar la programación de conferencias en Avaya one-X®Portal de IP Office.

Las instancias de licencia se consumen para cada usuario que se configura.

Código de orden	Licencia	Descripción
396319	IP Office R11 OFICINA DE TRABAJADOR PARA USUARIO POTENCIAL 1 UPLIFT LIC	Actualización de Office Worker a Power User: 1 usuario
396505	IP OFFICE: SELECCIONE R11 OFFICE WORKER PARA EL USUARIO ENERGÉTICO 1 UPLIFT LIC	Actualizar de Office Worker a Power User – 1 usuario – Seleccione
396318	IP Office R11 MOBILE TO POWER USER 1 UPLIFT LIC	Actualización de trabajador móvil a usuario avanzado: 1 usuario
396316	LICENCIA DE USUARIO 1 DE IP Office R11	1 usuario
396503	IP Office-Select R11 POWER USER 1 LIC	1 usuario – Seleccionar

Licencias de recepcionista

Esta opción está dirigida a operadores o recepcionistas y proporciona una interfaz de computadora visual para el manejo y administración de llamadas para múltiples sitios. Se admiten hasta 10 usuarios recepcionistas en cada nodo. Server Edition admite hasta 32 usuarios Receptionist y Server Edition Select admite hasta 50.

La licencia de recepcionista también permite que un usuario use IP Office SoftConsole, una aplicación de Windows diseñada para recepcionistas y operadores. Se pueden ejecutar hasta 4 clientes IP Office SoftConsole al mismo tiempo y tener licencia en un solo sistema IP Office. Se pueden agregar licencias adicionales.

Código de orden	Licencia	Descripción
307318	IPO-SL R10+ RECEPTA 1 LIC	1 usuario
382687	IPO R10+ RECEPCIONISTA 1 LICENCIA	1 usuario

Licencia de usuario centralizada

En implementaciones de sucursales de IP Office, donde IP Office se implementa como una sucursal de un Avaya Aura central® sistema, los usuarios con una extensión SIP o analógica se pueden configurar como usuarios centralizados. Cada usuario centralizado requiere una licencia de punto final centralizado.

Licencias de colaboración web

Código de orden	Licencia	Descripción
383122	IPO R10+ WEB COLLAB USUARIO 1 LICENCIA	1 usuario
382918	IPO-SL 10+ WEB COLLAB USR 1 LIC	1 usuario – Seleccionar

Licencias de terminales de IP

Todos los puntos finales de IP, Avaya y de terceros, requieren una licencia de punto final.

Licencias de terminales IP de Avaya

Todos los teléfonos IP de Avaya, incluidos los teléfonos DECT y Wi-Fi, requieren una licencia de terminal IP de Avaya y consumirán una instancia de esa licencia. Esto no se aplica a Avaya Softphone o Avaya Communicator. Los teléfonos IP de Avaya sin licencia aún podrán registrarse, pero se limitarán a realizar llamadas de emergencia únicamente. El teléfono mostraráNo hay licencia disponibleySolo llamadas de emergencia.Si una licencia está disponible, se asignará primero a cualquier teléfono DECT sin licencia y luego a cualquier otro teléfono IP de Avaya sin licencia en el orden en que se registraron los teléfonos.

Código de orden	Licencia	Descripción
307350	IPO-SL R10+ AV IP PTO FINAL 1 LIC	1 punto final: seleccione
383110	IPO R10+ AV IP PTO FINAL 1 LIC	1 punto final

Licencias de terminales de IP de terceros

Los teléfonos IP que no son de Avaya, incluidos los dispositivos SIP o H.323, requieren una licencia de terminal IP de terceros para registrarse en IP Office y consumirán una instancia de esa licencia.

Código de orden	Licencia	Descripción
307323	IPO-SL R10+ 3ER PTY IP EXTREMO 1 LIC	1 punto final: seleccione
383072	IPO R10+ 3ER PTY IP ENDPT 1 LIC	1 punto final

Licencias de prueba

Código de orden	Licencia	Descripción
396446	LICENCIA DE PRUEBA DE IP OFFICE R11 ESSENTIAL EDITION	Edición esencial
396448	LICENCIA DE PRUEBA DE IP OFFICE R11 PREFERED VOICEMAIL PRO	Edición preferida

La tabla continúa...

Código de orden	Licencia	Descripción
383123	IPO R10+ WEB COLLAB 5 TRL LIC	5 licencias de colaboración web
382919	IPO-SL R10+ WEB COLLAB 5 TRL LIC	5 licencias de colaboración web: seleccione
396504	IP OFFICE-SELECT R11 POWER USER 5 LICENCIA DE PRUEBA	5Licencia de usuario avanzado: seleccione
396317	IP OFFICE R11 POWER USER 5 LICENCIA DE PRUEBA	5 licencias de usuario avanzado
383103	Licencia IPO R10+ TELEWORKER 5 TRL	5 licencias de teletrabajador
383105	IPO R10+ TRABAJADOR MÓVIL 5 TRL LIC	5 licencias de trabajador móvil
307347	IPO-SL R10+ OFICINA TRABAJADOR 5 TRL LIC	5 licencias para trabajadores de oficina: seleccione
383107	IPO R10+ TRABAJADOR DE OFICINA 5 TRL LIC	5 licencias de oficinista
307319	IPO-SL R10+ RECEPTA 5 TRL LIC	5 Licencias de recepcionista — Seleccionar
382688	IPO R10+ RECEPCIONISTA 5 TRL LIC	5 licencias de recepcionista
307324	IPO-SL 10 3ER PTY IP 5 TRL LIC	Licencia de prueba de punto final de IP de terceros: seleccione
383073	IPO R10 3RDPTY IPENDPT 5 TRL LIC	Licencia de prueba de punto final de IP de terceros
382913	IPO-SL R10+ AV IP ENDPT 5 TRL LIC	5 Licencias para terminales IP de Avaya: seleccione
383111	IPO R10+ AV IP ENDPT 5 TRL LIC	5 licencias de terminal IP de Avaya
383090	IPO R10+ VMPRO UMS 5 TRL LIC	5 licencias Voicemail Pro UMS
307335	IPO-SL R10+ VMPRO UMS 5 TRL LIC	5 licencias Voicemail Pro UMS: seleccione
383078	IPO R10+ 3ER PTY TTS TRL LIC	Licencia TTS de Voicemail Pro de terceros
383076	IPO R10+ TTS WNDWS TRL LIC	Licencia Voicemail Pro Windows TTS
307327	IPO-SL R10+ TTS PROLINUX TRL LIC	Licencia Voicemail Pro Linux TTS: seleccione
383080	Licencia IPO R10+ TTS PRO LINUX TRL	Licencia Voicemail Pro Linux TTS
307329	IPO-SL R10+ IPSEC VPN TRL LIC	Tunelización IPSec — Seleccionar
383082	IPO R10+ IPSEC VPN TRL LIC	Tunelización IPSec
307333	IPO-SL R10+ SIP TRNK 5 TRL LIC	Sesiones de troncales SIP — Seleccionar
383086	IPO R10+ SIP TRNK 5 TRL LIC	Sesiones de troncales SIP
383088	IPO R10+ IP500 VCE NTWK 4	Redes de voz IP500
307321	IPO-SL R10+ CTI TRL LIC	CIT Link Pro — Seleccionar
383070	IPO R10+ CTI TRL LIC	Enlace CIT Pro

Licencias de actualización

Para actualizar los sistemas existentes a la versión más reciente, se requieren licencias de actualización. Las licencias de actualización se venden por separado. Los clientes solo pueden actualizar al último equivalente de su edición existente.

Nota:

La actualización de una versión anterior de Basic Edition a la última versión de Essential Edition no es una ruta de actualización válida.

Código de orden	Licencia	Descripción
383738	IPO-SL R10+ RECEPTA 1 UPG PLDS LIC	Seleccione la actualización de recepcionista
383696	IPO R10+ RECEPCIONISTA 1 UPG PLDS LIC	Actualización de recepcionista
383739	IPO-SL 10+ CTI UPG PLDS LIC	Seleccione la actualización de CTI
383697	IPO R10+ TI UPG PLDS LICENCIA	actualización CTI
383740	IPO-SL 10+ MPRO 1 UPG PLDS LIC	Seleccione la actualización de Voicemail Pro
383698	IPO R10+ VM PRO 1 UPG PLDS LIC	Actualización de Voicemail Pro
383741	IPO-SL 10+ 3RDPTY IPEND1 UPG PLDS LIC	Seleccione la actualización de punto final de IP de terceros
383699	IPO R10+ 3RDPTY IPENDPT1 UPG PLDS LIC	Actualización de punto final de IP de terceros
383742	IPO-SL 10+ TAPI WAV 1 UPG PLDS LIC	Seleccione la actualización TAPI WAV
383700	IPO R10+ TAPI WAV 1 UPG PLDS LIC	Actualización TAPI WAV
383702	IPO R10+ 3ER PTY TTS UPG PLDS LIC	Actualización de TTS de terceros
383744	IPO-SL 10+ IPSEC VPN UPG PLDS LIC	Seleccione la actualización de VPN IPSec
383704	IPO R10+ IPSEC VPN UPG PLDS LIC	Actualización de VPN IPSec
383747	IPO-SL 10+ VMPRO UMS 1 UPG PLDS LIC	Seleccione la actualización del servidor de mensajería unificada de Voicemail Pro
383708	IPO R10+ VM PRO UMS 1 UPG PLDS LIC	Actualización del servidor de mensajería unificada de Voicemail Pro
383748	IPO-SL 10+ IP500 T1 CH1 UPG PLDS LIC	Seleccione la actualización de canal adicional IP500
383709	IPO R10+ IP500 T1 CH1 UPG PLDS LIC	Actualización de canal adicional IP500
383749	IPO-SL 10+ IP500 E1 CH1 UPG PLDS LIC	Seleccione la actualización de canal adicional IP500
383710	IPO R10+ IP500 E1 CH1 UPG PLDS LIC	Actualización de canal adicional IP500
383752	IPO-SL 10+ IP500 E1R2 CH1 UPG PLDS LIC	Seleccione la actualización de canal adicional IP500
383713	IPO R10+ IP500 E1R2 CH1 UPG PLDS LIC	Actualización de canal adicional IP500

La tabla continúa...

Código de orden	Licencia	Descripción
383707	IPO R10+ IP500 VCE NTWK1 UPG PLDS LIC	Actualización de red de voz IP500
383757	IPO-SL 10+ AV IP ENDPT 1 UPG PLDS LIC	Seleccione la actualización de punto final IP de Avaya
383722	IPO R10+ SFTPH 1 PLDS UPG LIC	Actualización de teléfono suave
383760	IPO-SL 10+ SMLINE SIPTRK UPG PLDS LIC	Seleccione la actualización del troncal SIP de la línea SM
383726	IPO R10+ SM LINE SIPTRNK UPG PLDS LIC	Actualización del troncal SIP de la línea SM
383706	IPO R10+ SIP TRNK 1 UPG PLDS LIC	Actualización de troncales SIP
383761	IPO-SL 10+ WEBCOLLB USR1 UPG PLDS LIC	Seleccione la actualización de usuario de Web Collaboration
383728	IPO R10+ WEBCOLLAB USER1 UPG PLDS LIC	Actualización de usuario de Web Collaboration
383730	IPO R10 ESS ED EVM 1CH UPG PLDS LIC	Actualización del canal de correo de voz incorporado Essential Edition

Capítulo 4: Recursos

Documentación

Consulte los siguientes documentos relacionados en el sitio web de soporte de Avaya ensoporte.avaya.com y la base de conocimientos de IP Office enherramientas de marketing.avaya.com/knowledgebase .

Documento número	Título	Utilice este documento para:	Audiencia
Visión general			
16–604278	*Oficina IP de Avaya™Plataforma Comience aquí primero*	Vea una lista de todos los documentos relacionados con la solución.	Todo el mundo
no numerado	*Oficina IP de Avaya™Característica de la plataforma Descripción*	Comprender las características de la solución a un alto nivel.	Todo el mundo
no numerado	*Avaya IP Office Contact Center Característica Descripción*	Comprender las funciones y capacidades de IP Office Contact Center.	Todo el mundo
Planificación			
15–604135	*Oficina IP de Avaya™ Configuración de referencia de Platform Server Edition*	Comprender las especificaciones técnicas y planificar la implementación de IP Office Server Edition.	Ingenieros de Ventas Implementación Ingenieros
15–604253	*Oficina IP de Avaya™Plataforma en un entorno de sucursal Configuración de referencia*	Comprender las especificaciones técnicas y planificar IP Office en la implementación de un entorno de sucursal.	Ingenieros de Ventas Implementación Ingenieros
no numerado	*en Avaya™y con la tecnología de referencia de Avaya Configuración para socios comerciales*	Comprenda las especificaciones técnicas de ambas soluciones IP Office Cloud y planifique la implementación.	Ingenieros de Ventas Implementación Ingenieros
no numerado	*Oficina IP de Avaya™Directrices de seguridad de la plataforma*	Comprender y seguir pautas de seguridad recomendadas.	Ingenieros de Ventas Implementación Ingenieros
no numerado	*Referencia de Avaya IP Office Contact Center Configuración*	Comprender las especificaciones técnicas de IP Office Contact Center y planificar la implementación.	Ingenieros de Ventas Implementación Ingenieros

Búsqueda de documentos en el sitio web de soporte de Avaya

Acerca de esta tarea

Utilice este procedimiento para buscar la documentación del producto en el sitio web de soporte de Avaya.

Procedimiento

1. Use un navegador para navegar al sitio web de soporte de Avaya enhttp://soporte.avaya.com/ .
2. En la parte superior de la pantalla, ingrese su nombre de usuario y contraseña y haga clic en**Acceso**.
3. Coloque el cursor sobre**Soporte por producto**.
4. Haga clic en**Documentos**.
5. En el**Ingrese su producto aquí**cuadro de búsqueda, escriba el nombre del producto y luego seleccione el producto de la lista desplegable.
6. Si hay más de un lanzamiento, seleccione el número de lanzamiento apropiado de la**Elija Liberar**la lista desplegable.
7. Usa el**Tipo de contenido**filtro a la izquierda para seleccionar el tipo de documento que está buscando, o haga clic en **Seleccionar todo**para ver una lista de todos los documentos disponibles.

   Por ejemplo, si está buscando guías de usuario, seleccione**Guías de usuario**en el**Tipo de contenido** filtrar. Solo los documentos de la categoría seleccionada aparecerán en la lista de documentos.
8. Haga clic en**Ingresar**.

Capacitación

La capacitación y las credenciales de Avaya están diseñadas para garantizar que nuestros Business Partners tengan las capacidades y habilidades para vender, implementar y respaldar con éxito las soluciones de Avaya y superar las expectativas de los clientes. Las siguientes credenciales están disponibles:

- Especialista en ventas certificado de Avaya (APSS)
- Especialista profesional en implementación de Avaya (AIPS)
- Especialista en soporte certificado de Avaya (ACSS)

Los mapas de credenciales están disponibles en el sitio web de Avaya Learning enhttp://avaya-learning.com/ .

Los siguientes cursos también están disponibles en el sitio web de Avaya Learning. Después de iniciar sesión en el sitio web, ingrese el código del curso o el título del curso en el**Búsqueda**campo.

Código del curso	Título del curso
2S00012W	APSS – Comunicaciones de mercado pequeño y mediano – IP Office™Descripción general de la plataforma y selección

La tabla continúa...

Código del curso	Título del curso
4601W	Oficina IP de Avaya™Plataforma — Componentes
4602W	Oficina IP de Avaya™Plataforma — Ediciones
2S00015O	Comunicaciones para pequeñas y medianas empresas — IP Office — Endpoints
10S00005E	Acceso al conocimiento: IP Office de Avaya™Implementación de la plataforma
5S00004E	Acceso al conocimiento: IP Office de Avaya™Soporte de plataforma

Incluido en todas las ofertas de Knowledge Collection Access anteriores hay un área separada llamada IP Office Supplemental Knowledge. Este piso en el Campus Virtual contiene objetos de aprendizaje autodirigidos, que cubren la información delta de IP Office. Este material puede ser consumido por técnicos con experiencia en IP Office.

Visualización de videos de mentores de Avaya

Los videos de orientación de Avaya brindan contenido técnico sobre cómo instalar, configurar y solucionar problemas de los productos de Avaya.

Acerca de esta tarea

Los videos están disponibles en el sitio web de soporte de Avaya, enumerados bajo el tipo de documento de video y en el canal administrado por Avaya en YouTube.

Procedimiento

- Para encontrar videos en el sitio web de soporte de Avaya, vaya ahttp://soporte.avaya.com y realice una de las siguientes acciones:
  - En**Búsqueda**, escribeVídeos de orientación de Avayapara ver una lista de los videos disponibles.
  - En**Búsqueda**, escriba el nombre del producto. En la página Resultados de la búsqueda, seleccione**Video**en el **Tipo de contenido**columna de la izquierda.
- Para encontrar los videos de Avaya Mentor en YouTube, vaya awww.youtube.com/AvayaMentor y realice una de las siguientes acciones:
  - Ingrese una palabra clave o palabras clave en el**Canal de búsqueda**para buscar un producto o tema específico.
  - Desplácese hacia abajo en Listas de reproducción y haga clic en el nombre de un tema para ver la lista disponible de videos publicados en el sitio web.

Nota:

Los videos no están disponibles para todos los productos.

Recursos adicionales de IP Office

Puede encontrar información en los siguientes sitios web de recursos adicionales.

Avaya

http://www.avaya.com es el sitio web oficial de Avaya. La página principal también brinda acceso a sitios web individuales de Avaya para diferentes países.

Portal de socios y ventas de Avaya

http://ventas.avaya.com es el sitio web oficial de todos los Business Partners de Avaya. El sitio requiere el registro de un nombre de usuario y contraseña. Una vez accedido, el portal se puede personalizar para productos específicos y tipos de información que desea ver y recibir notificaciones por correo electrónico.

Base de conocimientos de IP Office de Avaya

http://herramientas de marketing.avaya.com/knowledgebase proporciona acceso a una versión en línea actualizada periódicamente de la base de conocimientos de IP Office.

Información de mantenimiento, ciclo de vida y garantía de Avaya

Los servicios de soporte de Avaya complementan las políticas estándar de mantenimiento, ciclo de vida y garantía de Avaya que se publican enhttp://soporte.avaya.com . Para obtener más información, envíe un correo electrónico a support@avaya.com .

Grupo internacional de usuarios de Avaya

http://www.iaug.org es el foro de discusión oficial para los usuarios de productos de Avaya.

Compatibilidad del producto

Para obtener la información de compatibilidad más reciente y precisa, vaya ahttps://support.avaya.com/CompatibilityMatrix/Index.aspx .

Enlaces relacionados

Acceso a las notas de la aplicación Avaya DevConnect en la página 134
interoperabilidad en la página 93

Apoyo

Vaya al sitio web de soporte de Avaya enhttp://soporte.avaya.com para obtener la documentación, los avisos de productos y los artículos de conocimiento más actualizados. También puede buscar notas de la versión, descargas y resoluciones de problemas. Utilice el sistema de solicitud de servicio en línea para crear una solicitud de servicio. Chatea con agentes en vivo para obtener respuestas a tus preguntas o solicita a un agente que te conecte con un equipo de soporte si un problema requiere experiencia adicional.

Uso de la base de conocimientos de Avaya InSite

Avaya InSite Knowledge Base es un motor de búsqueda basado en la web que proporciona:

- Procedimientos de resolución de problemas y consejos técnicos actualizados
- Información sobre paquetes de servicios
- Acceso a la documentación técnica y del cliente
- Información sobre programas de capacitación y certificación
- Enlaces a otra información pertinente

Si es un socio autorizado de Avaya o un cliente actual de Avaya con un contrato de soporte, puede acceder a la base de conocimiento sin costo adicional. Debe tener una cuenta de inicio de sesión y un número de cliente válido.

Utilice la base de conocimientos de Avaya InSite para buscar posibles soluciones a los problemas.

1. Ir ahttp://www.avaya.com/support .
2. Inicie sesión en el sitio web de Avaya con una ID de usuario y una contraseña válidas de Avaya. Aparece la página de soporte.
3. Bajo**Soporte por producto**, haga clic**Soporte específico del producto**.
4. Introduce el producto en**Introduzca el nombre del producto**cuadro de texto y presione Entrar.
5. Seleccione el producto de la lista desplegable y elija la versión correspondiente.
6. Seleccione el**Soluciones Técnicas**pestaña para ver artículos.
7. Seleccione artículos relevantes.

Enlaces relacionados

Los telefonos en la página 38

Interoperabilidad telefónica en la página 95

Acceso a las notas de la aplicación Avaya DevConnect

El programa Avaya DevConnect realiza pruebas con proveedores de servicios para establecer la compatibilidad con los productos de Avaya.

Procedimiento

1. Ir ahttp://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp .
2. Inicie sesión o regístrese.
3. Haga clic en un período de tiempo para buscar dentro.

   Aparece una lista de todas las notas de la aplicación para ese período de tiempo.

4. En el**Búsqueda**Tipo de campoOficina de PIy presiona**Ingresar**.

   Aparece una lista de notas de aplicación relevantes.

Enlaces relacionados

Los telefonos en la página 38

Interoperabilidad telefónica en la página 95 Compatibilidad del producto en la página 133 Opciones de hardware y software en la página 84 interoperabilidad en la página 93

lista del glosario

Ruta Automática Selección	Característica de algunos sistemas telefónicos en la que el sistema elige automáticamente la forma más rentable de enviar una llamada interurbana.
Llamada en hora pico Terminaciones	Una medida de llamadas de tráfico dinámico que se pueden completar en una hora pico promedio.
Comunicación Gerente	Un componente clave de Avaya Aura®. Ofrece capacidades ricas de voz y video y proporciona una red distribuida resistente para puertas de enlace de medios y dispositivos de comunicación analógicos, digitales y basados en IP. Incluye funciones de movilidad avanzadas, conferencias telefónicas integradas, aplicaciones de centros de contacto y capacidades E911.
Soportado por computadora telecomunicaciones Solicitud (CSTA)	Una interfaz estándar para aplicaciones de integración de telefonía informática (CTI), como correo de voz y operadora automática, para interactuar con equipos de telefonía.
Digital Comunicaciones Protocolo	Un protocolo propietario que se utiliza para transmitir tanto voz digitalizada como datos digitalizados a través del mismo enlace de comunicaciones. Un enlace de Protocolo de comunicaciones digitales (DCP) consta de dos canales de información (I) de 64 kbps y un canal de señalización (S) de 8 kbps. El protocolo DCP admite dos canales portadores de información y dos teléfonos o módulos de datos.
Directorio habilitado administración	Una interfaz que utiliza Avaya Directory Server para facilitar la administración de Modular Messaging desde una ubicación centralizada.
Repartido Comunicaciones Sistema	Un protocolo de interconexión de redes patentado de Avaya con el que puede configurar dos o más redes de comunicación privadas basadas en Avaya para que funcionen como una gran red.
Nombre de dominio Sistema (DNS)	Un estándar del Grupo de trabajo de ingeniería de Internet (IETF) para cadenas ASCII para representar direcciones IP. El DNS es un servicio de directorio interno distribuido que se utiliza principalmente para traducir entre nombres de dominio y direcciones IP. Los teléfonos IP de la serie 9600 de Avaya pueden usar DNS para convertir nombres en direcciones IP. En los archivos DHCP, TFTP y HTTP, los nombres DNS se pueden usar siempre que haya direcciones IP disponibles, siempre que se identifique primero un servidor DNS válido.

Datos dinámicos Intercambio (DDE)	Un método de comunicación entre procesos (IPC).
Anfitrión dinámico Configuración Protocolo (DHCP)	Un protocolo del Grupo de trabajo de ingeniería de Internet (IETF) que se utiliza para automatizar la asignación y administración de direcciones IP.
Enrutamiento Ethernet Interruptor (ERS)	El sistema de chasis apilable de Avaya que proporciona conectividad de conmutación Ethernet de alto rendimiento, preparada para la convergencia, segura y resistente.
Interfaz de expansión	Paquete de circuitos de puertos en una red de puertos (PN) que proporciona la interfaz entre un bus de multiplexación por división de tiempo (TDM) o un bus de paquetes en la PN y un enlace de fibra óptica. La interfaz de expansión (EI) transporta datos de conmutación de circuitos, datos de conmutación de paquetes, control de red, control de temporización y control de señal digital 1 (DS1). EI en una red de puertos de expansión (EPN) también se comunica con la tarjeta de mantenimiento maestra para proporcionar el estado ambiental y el estado de alarma de la EPN al elemento de procesamiento del conmutador (SPE).
Puerto de expansión la red	En las configuraciones de Intuity Audix Server, una red de puertos (PN) que está conectada al bus de multiplexación por división de tiempo (TDM) y al bus de paquetes de una red de puertos de procesador (PPN). El control se logra mediante la conexión indirecta de la EPN a la PPN a través de un enlace de red de puerto (PNL).
Extensión a Celular número de acceso	El número de teléfono marcado para conectarse al servidor de Avaya que ejecuta Communication Manager. El número de acceso de Extension to Cellular inicia el proceso de habilitar o deshabilitar Extension to Cellular o cambiar el código de seguridad de la estación.
Federal Comunicaciones Comisión (FCC)	Una agencia federal de los Estados Unidos que regula las comunicaciones, como las comunicaciones por cable e Internet.
técnico mundial Servicios	Un equipo de Avaya que responde a las llamadas de los clientes sobre productos en Avaya Integrated Management.
protocolo de Internet	Un protocolo sin conexión que opera en la capa 3 del modelo de interconexión de sistemas abiertos (OSI). El Protocolo de Internet (IP) se utiliza para el direccionamiento de Internet y el enrutamiento de paquetes a través de múltiples redes hasta un destino final. IP funciona junto con el Protocolo de control de transmisión (TCP) y se identifica como TCP/IP.
Superviviente local Procesador	Una configuración del servidor de medios S8300 en la que el servidor actúa como servidor alternativo o controlador de acceso para entidades IP como teléfonos IP y puertas de enlace de medios G700. Estas entidades de IP utilizan el Procesador recuperable local (LSP) cuando las entidades de IP pierden la conectividad con el servidor principal.

Pasarela de medios

Un elemento de hardware habilitador de aplicaciones que forma parte de una familia de dichos elementos. Esta familia incluye conectividad dentro del switch, interfaces de control, interfaces de puerto y gabinetes. Los gateways de medios de Avaya admiten tráfico portador y tráfico de señalización que se enruta entre redes de conmutación de paquetes y redes de conmutación de circuitos para brindar capacidades de datos, voz, fax y mensajería. Los gateways de medios brindan conversión de protocolo, como IP a ATM a TDM, conferencias, presencia, como colgado o descolgado, conectividad a redes privadas y redes públicas, como IP, ATM, TDM y redes, como QSIG. , DCS, RDSI. Los gateways de medios admiten factores de forma opcionales.

Dirección de red
Traducción de puertos

Una técnica de enrutamiento de red. La traducción de puertos de direcciones de red (NAPT) se utiliza para acceder a los sistemas en la misma subred que IP Office.

Enrutamiento de red
Política

Una aplicación para gestionar de forma centralizada el enrutamiento SIP para las instancias de Session Manager. Una política de enrutamiento describe cómo se enruta una llamada: de dónde viene, hacia dónde se dirige, cuál es su patrón de marcación, a qué hora del día se enruta y su costo para una ruta en particular.

novela®directorio electrónico™

Un producto de software de servicio de directorio compatible con X.500 lanzado inicialmente en 1993 por Novell®para administrar de forma centralizada el acceso a los recursos en múltiples servidores y computadoras dentro de una red determinada. novela®directorio electrónico™ antes conocido como Novell®Directorio de Servicios. A veces se denomina Servicios de directorio de Netware. novela®directorio electrónico™es una base de datos jerárquica orientada a objetos que se utiliza para representar ciertos activos en una organización en un árbol lógico, que incluye personas, puestos, servidores, estaciones de trabajo, aplicaciones, impresoras, servicios y grupos.

OFCOM

La Oficina de Comunicaciones del Reino Unido para la regulación de las telecomunicaciones.

COMPAÑERO®Contacto
Adjunto de cierre

Un dispositivo que está conectado al chasis de un portal de medios y proporciona cierres de contactos. El complemento de cierre de contacto (CCA) cierra un relé en respuesta a un comando de acceso telefónico desde el portal de medios para operar una puerta o realizar una acción similar.

Información del Producto
Sistema de presentación

Los informes del Sistema de presentación de información del producto (PIPS) proporcionan datos del Experto en información del producto (PIE), una herramienta de minería de datos que extrae la información de configuración adjunta y del interruptor del cliente de Avaya y la almacena en una base de datos.

Licencias de productos
y sistema de entrega
(PLDS)

El sitio web y el sistema de administración de licencias y descargas de Avaya. Los socios comerciales y los clientes de Avaya utilizan este sitio para obtener archivos de imágenes ISO y otras descargas de software.

Conmutado público
Red Telefónica
(RTPC)

Una red telefónica que incluye muchas tecnologías de comunicación, como transmisión de microondas, satélites y cables submarinos.

Función remota Activación	Una aplicación de Avaya basada en la web para activar funciones de forma remota y aumentar las capacidades en el sistema de un cliente mediante la entrega de un nuevo archivo de licencia.
Administrador de sistemas	Un marco de gestión común para Avaya Aura®que proporciona funciones de gestión centralizadas para el aprovisionamiento y la administración para reducir la complejidad de la gestión.
Estado del sistema Solicitud	Una aplicación de IP Office que muestra el estado de cosas como las llamadas salientes.
teletrabajador	La configuración en la que Communication Manager establece la conexión de voz a un teléfono con conmutación de circuitos. Requiere dos conexiones: una conexión TCP/IP para control de señalización y una conexión de conmutación de circuitos para voz.
Telefonía Programa de aplicación Interfaz (TAPI)	un microsoft®API de Windows que permite que las computadoras que ejecutan Windows usen servicios de telefonía. TAPI se utiliza para comunicaciones de datos, FAX y voz. Las aplicaciones pueden usar TAPI para controlar las funciones de telefonía, como marcar, contestar y colgar.
Servicio de Telefonía Interfaz de proveedor (TSPI)	Una interfaz definida por Microsoft para el proveedor de servicios de telefonía (TSP). microsoft®Windows viene con un TSP H.323, un TSP de conferencia IP, un TSP de controlador de dispositivo en modo kernel y un TSP unimodem.

Índice

A

a-ley PCM 31
notas de aplicación 134
Soporte de aplicaciones 87
arquitectura 71
soporte de creación automática para usuarios y extensiones en WebLM... 117 Comunicador Avaya 45
ipad 46
Ventanas 47
Selección del centro de contacto de Avaya
Continuidad del negocio 83
opciones de implementación 80
–83 DVD 80
dispositivo de hardware 82
visión general ..... sesenta y cinco
configuraciones de referencia 78
topología ..... 78 ,80 –83
sincronización de datos de usuario 78
Vmware 81
Reunión en línea de Avaya Equinox 55
Descripción general de Avaya Spaces 55

B

cartas base 31
Edición básica 67
Migración de BCM ..... 100 ,107 compatibilidad con navegadores 87

C

CA 61
Acceso Centro 61
gerente de operaciones en la nube 63
visión general de la nube 75
componentes 72
Integración de telefonía informática 27
llamadas de conferencia 51
configuración de licencias WebLM 115
avisos y alarmas 116
centro de contacto 64
unidad de control 29
TIC 27
requisitos de PC proporcionados por el cliente 91

D

red de datos 18
opciones de implementación 67
Selección del centro de contacto de Avaya ..... 78 ,80 –83 DVD ..... 80 ,83
opciones de implementación *(continuado)*
dispositivo de hardware 82
Vmware 81
DevConnect 134
DMM 64
cambios en el documento 7

mi

Correo de voz integrado 50
puntos finales 126
aplicaciones de usuario final 40
Equinoccio para IP Office
Equinoccio
Equinoccio de Avaya 42
Edición Esencial 69
módulos de expansión externos ..... ,35

F

teclas de función 31
caracteristicas 13
Descripción de las características 54

GRAMO

porteros 22
puertas de enlace 22
pautas
WebRTC 38

H

H.323 22
opciones de hardware 84

yo

Base de conocimientos de InSite 134
interfaces 105
interoperabilidad ..... 93 ,99
IP500 V2 29
ipad 46
Licencias de terminales de IP 126
Licencias de terminales de IP para WebLM 116
aplicaciones de IP Office
aplicaciones de centros de contacto 64
Aplicaciones de instalación y administración 55
aplicaciones de usuario 40
Centro de contacto de IP Office
opciones de implementación 77
topología 77

ediciones de ip office 10
Telefonía IP 19

L

Migración de licencias
IDA 110
licencias 109
Edición básica 118
Rama 120
Edición Esencial 118
Puntos finales IP 126
Edición preferida 118
ESCN 120
Edición del servidor 119
pequeña red comunitaria 120
Modo estandar 118
juicios 126
baúles 121
actualizaciones ..... 106 ,127
usuarios 122

METRO

Gerente 55
MCU 22
Administrador de medios
visión general 58
Conferencia Meet-Me 52
Migración
Hoja de ruta y limitaciones 108
Unidades de Conexión Multipunto 22

norte

nuevas características 11

O

Preferido de one-X Mobile 40
Portal one-X para IP Office 41
soporte del sistema operativo 87
opciones
despliegue 73
visión general ..... 10 ,64 ,75
Selección del centro de contacto de Avaya ..... sesenta y cinco
Reunión en línea de Avaya Equinox 55
Espacios de Avaya 55
sucursal de la empresa 73
oficina de PI 73

PAGS

Redes de voz y datos basadas en paquetes 18
PCM 31
Los telefonos 38
Los telefonos *(continuado)*
compatibilidad 95
disponibilidad del país 98
remoto 39
Licencias PLDS 109
puertos 105
Edición preferida 70
red privada de voz conmutada por circuito 14
Compatibilidad del producto 133
Redes de voz pública 15
modulación de código de pulso 31

R

Radvisión 53
licencias de recepcionista para WebLM 117
configuración de referencia
Centro de contacto de IP Office 77
configuraciones de referencia ..... 67 ,73
documentos relacionados 130
telefonos remotos 39
sitios web de recursos 133

S

Licencias SCN 120
Escopia 53
tarjetas SD 31
seguridad ..... 101 ,102
Edición del servidor 70
Licenciamiento centralizado 111
licencias 119
Licencias nodales 111
Administrador de la edición del servidor 56
Protocolo de Iniciacion de Sesion 23
SORBO ..... 23,25 Agentes de usuario de punto final SIP 26
SMA 61
Consola de administración SNMP 61
Consola suave 49
Administración de SoftConsole 61
opciones de software 84
Aplicación de gestión de soluciones 61
especificación de la solución 85
especificaciones
interfaces de puerto 105
SSA 62
Modo estandar 118
apoyo 133
Monitor de sistema 63

T

telefonos 38
topología ..... 14 ,71 ,74
Selección del centro de contacto de Avaya ..... 78 ,80 –83

Página691 de 3226.

topología*(continuado)*
Alojado por BP 76
Continuidad del negocio 83
DVD 80
dispositivo de hardware 82
Impulsado por socios 76
Vmware 81
capacitación 131
juicios 126
tarjetas de troncales 33
bañador
licencias 121

tu

licencias de actualización 127
actualizaciones 106
licencias de usuario 122
licencias de usuario para WebLM 117

V

VCM 22
Solución de videocolaboración 53
videoconferencia 53
vídeos 132
ambiente virtual 93
licencias virtuales 111
Módulos de compresión de voz 22
Correo de voz Pro 50
red de voz ..... 14 , 15 , 18

W

cliente web
cliente web oficina ip
webrtc 44
Administrador de licencias web 110
WebLM 110
Modos de licencia de WebLM 114
Transiciones de estado del modo de licencia de WebLM 115
Licencias WebLM
creación automática de soporte para usuarios y extensiones 117
configuración 115
advertencias y alarmas de configuración 116
Licencias de terminales de IP 116
modos de licencia 114
transiciones de estado del modo de licencia 115
licencias de recepcionista 117
licencias de usuario 117
Administrador web 58
WebRTC 38

Traducido del inglés al español - www.onlinedoctranslator.com

AVAYA

Resumen y especificaciones de Avaya Session Border Controller para empresas

Versión 7.2.2.2

Número 8

abril 2019

©2017-2019, Avaya Inc. Todos
los derechos reservados.

Aviso

Si bien se han realizado esfuerzos razonables para garantizar que la información de este documento sea completa y precisa en el momento de la impresión, Avaya no asume ninguna responsabilidad por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información de este documento sin la obligación de notificar a ninguna persona u organización sobre dichos cambios.

Descargo de responsabilidad de la documentación

"Documentación" se refiere a la información publicada en diversos medios que pueden incluir información sobre el producto, instrucciones de funcionamiento y especificaciones de rendimiento que generalmente se ponen a disposición de los usuarios de los productos. La documentación no incluye materiales de marketing. Avaya no será responsable de ninguna modificación, adición o eliminación de la versión original publicada de la Documentación, a menos que dichas modificaciones, adiciones o eliminaciones hayan sido realizadas por Avaya o en su nombre expreso. El usuario final acepta indemnizar y eximir de responsabilidad a Avaya, a los agentes, servidores y empleados de Avaya frente a todos los reclamos, juicios, demandas y juicios que surjan de, o en relación con, modificaciones, adiciones o eliminaciones posteriores a esta documentación, en la medida en que lo haga End Usuario.

Descargo de responsabilidad del enlace

Avaya no es responsable del contenido o la confiabilidad de los sitios web vinculados a los que se hace referencia en este sitio o la documentación proporcionada por Avaya. Avaya no es responsable de la precisión de la información, declaración o contenido proporcionado en estos sitios y no respalda necesariamente los productos, servicios o información descritos u ofrecidos en ellos. Avaya no garantiza que estos enlaces funcionen todo el tiempo y no tiene control sobre la disponibilidad de las páginas enlazadas.

Garantía

Avaya proporciona una garantía limitada para el hardware y el software de Avaya. Consulte su contrato de venta para establecer los términos de la garantía limitada. Además, el lenguaje de la garantía estándar de Avaya, así como la información sobre el soporte para este producto mientras está bajo garantía, está disponible para los clientes de Avaya y otras partes a través del sitio web de Soporte de Avaya:https://support.avaya.com/helpcenter/ getGenericDetails?detailId=C20091120112456651010 bajo el enlace "Garantía y ciclo de vida del producto" o el sitio sucesor designado por Avaya. Tenga en cuenta que si adquirió los productos de un socio de canal autorizado de Avaya fuera de los Estados Unidos y Canadá, dicho socio de canal de Avaya le proporciona la garantía y no Avaya.

"Servicio alojado" hace referencia a una suscripción de servicio alojado de Avaya que adquiere de Avaya o de un socio de canal autorizado de Avaya (según corresponda) y que se describe con más detalle en SAS alojado u otra documentación de descripción del servicio con respecto al servicio alojado aplicable. Si compra una suscripción al Servicio alojado, es posible que la garantía limitada anterior no se aplique, pero puede tener derecho a servicios de soporte en relación con el Servicio alojado, como se describe más adelante en los documentos de descripción del servicio para el Servicio alojado correspondiente. Comuníquese con Avaya o con el socio de canal de Avaya (según corresponda) para obtener más información.

Servicio alojado

LO SIGUIENTE SE APLICA ÚNICAMENTE SI COMPRA UNA SUSCRIPCIÓN AL SERVICIO ALOJADO DE AVAYA DE AVAYA O DE UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA), LOS TÉRMINOS DE USO PARA LOS SERVICIOS ALOJADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA,HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO BAJO EL ENLACE "Términos de uso de Avaya para servicios alojados" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, Y SON APLICABLES A CUALQUIER PERSONA QUE ACCEDA O UTILICE EL SERVICIO ALOJADO. AL ACCEDER O UTILIZAR EL SERVICIO ALOJADO, O AL AUTORIZAR A OTROS A HACERLO, USTED, EN NOMBRE DE USTED Y DE LA ENTIDAD PARA LA QUE LO ESTÁ HACIENDO (EN ADELANTE DENOMINADO INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA LOS TÉRMINOS DE USO. SI USTED ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR DICHA ENTIDAD A ESTOS TÉRMINOS DE USO. SI USTED NO TIENE DICHA AUTORIDAD, O SI USTED NO DESEA ACEPTAR ESTOS TÉRMINOS DE USO, NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO.

Licencias

LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA,HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, BAJO EL ENLACE "TÉRMINOS DE LICENCIA DE SOFTWARE DE AVAYA (Productos de Avaya)" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, SON APLICABLES A CUALQUIER PERSONA QUE DESCARGUE, UTILICE Y/O INSTALE SOFTWARE DE AVAYA, COMPRADO DE AVAYA INC., CUALQUIER AFILIADO DE AVAYA O UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA) BAJO UN ACUERDO COMERCIAL CON AVAYA O UN SOCIO DE CANAL DE AVAYA. A MENOS QUE AVAYA ACORDE LO CONTRARIO POR ESCRITO, AVAYA NO EXTENDERÁ ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE CUALQUIER PERSONA QUE NO SEA AVAYA, UNA AFILIADA DE AVAYA O UN SOCIO DE CANAL DE AVAYA; AVAYA SE RESERVA EL DERECHO DE TOMAR ACCIONES LEGALES CONTRA USTED Y CUALQUIER OTRA PERSONA QUE UTILICE O VENDA EL SOFTWARE SIN LICENCIA. AL INSTALAR, DESCARGAR O UTILIZAR EL SOFTWARE, O AUTORIZAR A OTROS A HACERLO, USTED, EN SU NOMBRE Y EN EL DE LA ENTIDAD PARA LA QUE ESTÁ INSTALANDO, INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA ESTOS TÉRMINOS Y CONDICIONES Y CREA UN CONTRATO VINCULANTE ENTRE USTED Y AVAYA INC. O LA AFILIADA DE AVAYA CORRESPONDIENTE ("AVAYA").

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el cual el alcance de la licencia se detalla a continuación. Cuando la documentación del pedido no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de Sistema Designado como se establece a continuación en la sección Licencia de Sistema(s) Designado(s) (DS) según corresponda. El número aplicable de licencias y unidades de capacidad para las que se otorga la licencia será uno (1), a menos que se especifique un número diferente de licencias o unidades de capacidad en la documentación u otros materiales disponibles para Usted. "Software" hace referencia a los programas informáticos en código objeto, proporcionados por Avaya o un socio de canal de Avaya, ya sea como productos independientes, preinstalados en productos de hardware y cualquier mejora, actualización, parche, corrección de errores, o versiones modificadas de los mismos. "Procesador designado" significa un único dispositivo informático independiente. "Servidor" hace referencia a un conjunto de Procesadores designados que aloja (física o virtualmente) una aplicación de software a la que acceden varios usuarios. "Instancia" significa una única copia del Software que se ejecuta en un momento determinado: (i) en una máquina física; o (ii) en una máquina virtual de software implementada ("VM") o implementación similar.

Tipos de licencia

Licencia de sistema(s) designado(s) (DS). El Usuario final puede instalar y utilizar cada copia o una Instancia del Software únicamente: 1) en una cantidad de Procesadores designados hasta la cantidad indicada en el pedido; o 2) hasta el número de Instancias del Software que se indique en el pedido, la Documentación o que Avaya autorice por escrito. Avaya puede solicitar que los Procesadores designados se identifiquen en el pedido por tipo, número de serie, clave de función, Instancia, ubicación u otra designación específica, o que el Usuario final los proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este objetivo.

Licencia de Usuario Concurrente (CU). El Usuario final puede instalar y utilizar el Software en varios Procesadores designados o en uno o más Servidores, siempre que solo el número de Unidades con licencia acceda y utilice el Software en un momento dado. Una "Unidad" hace referencia a la unidad en la que Avaya, a su exclusivo criterio, basa el precio de sus licencias y puede ser, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o correo de voz a nombre de una persona. o función corporativa (por ejemplo, webmaster o servicio de asistencia), o una entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software. Las Unidades pueden vincularse a un Servidor específico e identificado oa una Instancia del Software.

Software de la herencia de Nortel

"Software Heritage Nortel" significa el software que fue adquirido por Avaya como parte de su compra de Nortel Enterprise Solutions Business en diciembre de 2009. El software Heritage Nortel es el

software incluido en la lista de productos de Heritage Nortel ubicada enhttps://support.avaya.com/LicenseInfo bajo el enlace "Productos de Heritage Nortel" o el sitio sucesor designado por Avaya. Para el software Heritage Nortel, Avaya le otorga al Cliente una licencia para usar el software Heritage Nortel proporcionado en virtud del presente únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la Documentación, y únicamente como integrado, para ejecución en, o para comunicación con equipos Avaya. Los cargos por el software Heritage Nortel pueden basarse en el grado de activación o uso autorizado según se especifica en un pedido o factura.

Derechos de autor

Salvo que se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, la documentación, el software, el servicio alojado o el hardware proporcionado por Avaya. Todo el contenido de este sitio, la documentación, el Servicio alojado y el producto proporcionado por Avaya, incluida la selección, disposición y diseño del contenido, es propiedad de Avaya o de sus otorgantes de licencias y está protegido por derechos de autor y otras leyes de propiedad intelectual, incluida la ley sui generis. derechos relativos a la protección de las bases de datos. No puede modificar, copiar, reproducir, volver a publicar, cargar, publicar, transmitir o distribuir de ninguna manera ningún contenido, en su totalidad o en parte, incluido cualquier código y software, a menos que Avaya lo autorice expresamente. La reproducción, transmisión, difusión, almacenamiento o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede ser un delito,

virtualización

Lo siguiente se aplica si el producto se implementa en una máquina virtual. Cada producto tiene su propio código de pedido y tipos de licencia. Tenga en cuenta, a menos que se indique lo contrario, que cada Instancia de un producto debe solicitarse y solicitarse por separado. Por ejemplo, si el cliente usuario final o el socio de canal de Avaya desea instalar dos instancias del mismo tipo de productos, entonces se deben pedir dos productos de ese tipo.

Componentes de terceros

"Componentes de terceros" significa que ciertos programas de software o partes de los mismos incluidos en el Software o el Servicio alojado pueden contener software (incluido el software de código abierto) distribuido bajo acuerdos de terceros ("Componentes de terceros"), que contienen términos relacionados con los derechos de uso de ciertos partes del Software ("Términos de terceros"). Según sea necesario, la información sobre el código fuente del sistema operativo Linux distribuido (para aquellos productos que tienen el código fuente del sistema operativo Linux distribuido) y la identificación de los titulares de derechos de autor de los componentes de terceros y los términos de terceros que se aplican está disponible en los productos, la documentación o en el sitio web de Avaya. a:https://support.avaya.com/Copyright o el sitio sucesor designado por Avaya. Los términos de la licencia de software de código abierto proporcionados como Términos de terceros son consistentes con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del software de código abierto. Los Términos de terceros prevalecerán sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables en la medida en que estos Términos de licencia de software le impongan mayores restricciones que los Términos de terceros aplicables.

Lo siguiente se aplica solo si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO TIENE LICENCIA BAJO LA LICENCIA DE CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS POR LOS QUE NO RECIBE REMUNERACIÓN PARA (i) CODIFICAR VÍDEO EN CUMPLIMIENTO CON EL ESTÁNDAR AVC (“AVC VIDEO”) Y/O (ii) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL DE MPEG LA, LLC VERHTTP://WWW.MPEGLA.COM .

Proveedor de servicio

LO SIGUIENTE SE APLICA AL ALOJAMIENTO DE PRODUCTOS O SERVICIOS DE AVAYA POR PARTE DEL SOCIOS DE CANAL DE AVAYA. EL PRODUCTO O EL SERVICIO ALOJADO PUEDE UTILIZAR COMPONENTES DE TERCEROS SUJETOS A TÉRMINOS DE TERCEROS Y REQUIERE QUE UN PROVEEDOR DE SERVICIOS TENGA UNA LICENCIA INDEPENDIENTE DIRECTAMENTE DEL PROVEEDOR DE TERCEROS. EL ALOJAMIENTO DE PRODUCTOS AVAYA POR PARTE DE UN SOCIOS DE CANAL DE AVAYA DEBE ESTAR AUTORIZADO EN POR ESCRITO DE AVAYA Y SI DICHOS PRODUCTOS ALOJADOS UTILIZAN O INTEGRAN DETERMINADO SOFTWARE DE TERCEROS, INCLUYENDO, ENTRE OTROS, SOFTWARE O CÓDECS DE MICROSOFT, EL SOCIO DE CANAL DE AVAYA DEBE OBTENER DE FORMA INDEPENDIENTE CUALQUIER ACUERDO DE LICENCIA CORRESPONDIENTE, POR CUENTA DEL SOCIO DE CANAL DE AVAYA, DIRECTAMENTE DEL PROVEEDOR TERCERO APLICABLE.

CON RESPECTO A LOS CÓDECS, SI EL SOCIO DE CANAL DE AVAYA ALOJA CUALQUIER PRODUCTO QUE UTILICE O INTEGRA EL CÓDEC G.729, EL CÓDEC H.264 O EL CÓDEC H.265, EL SOCIO DE CANAL DE AVAYA RECONOCE Y ACEPTA QUE EL SOCIO DE CANAL DE AVAYA ES RESPONSABLE DE CUALQUIER Y TODAS LAS TARIFAS Y/O REGALÍAS RELACIONADAS. EL CÓDEC G.729 TIENE LICENCIA DE SIPRO LAB TELECOM INC. VER WWW.SIPRO.COM/CONTACTO.HTML . EL CÓDEC H.264 (AVC) TIENE LICENCIA BAJO LA LICENCIA DE LA CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS EN LOS QUE NO RECIBE REMUNERACIÓN PARA: (I) CODIFICAR VÍDEO DE CONFORMIDAD CON EL ESTÁNDAR AVC (“AVC VIDEO ”) Y/O (II) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO CON LICENCIA PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL PARA LOS CÓDECS H.264 (AVC) Y H.265 (HEVC) DE MPEG LA, LLC VERHTTP:// WWW.MPEGLA.COM .

De acuerdo con las leyes

Usted reconoce y acepta que es su responsabilidad cumplir con las leyes y reglamentaciones aplicables, incluidas, entre otras, las leyes y reglamentaciones relacionadas con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude y los derechos de interpretación musical, en el país o territorio donde se utiliza el producto Avaya.

Prevención del fraude de llamadas

El "fraude interurbano" es el uso no autorizado de su sistema de telecomunicaciones por parte de una parte no autorizada (por ejemplo, una persona que no es un empleado corporativo, agente, subcontratista o que no trabaja en nombre de su empresa). Tenga en cuenta que puede haber un riesgo de fraude de llamadas asociado con su sistema y que, si ocurre, puede resultar en cargos adicionales sustanciales para sus servicios de telecomunicaciones.

Intervención de fraude de llamadas de Avaya

Si sospecha que está siendo víctima de fraude de llamadas y necesita asistencia o soporte técnico, llame a la línea directa de intervención de fraude de llamadas del Centro de Servicio Técnico al +1-800-643-2353 para los Estados Unidos y Canadá. Para obtener números de teléfono de soporte adicionales, consulte el sitio web de soporte de Avaya:https://soporte.avaya.como el sitio sucesor designado por Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de soporte de seguridad de Avaya en la sección Políticas de seguridad y soporte dehttps://support.avaya.com/security.

Las sospechas de vulnerabilidades de seguridad de productos de Avaya se manejan según el Flujo de soporte de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Descarga de documentación

Para obtener las versiones más recientes de la documentación, consulte el sitio web de soporte de Avaya:https://soporte.avaya.com, o el sitio sucesor designado por Avaya.

Comuníquese con el soporte de Avaya

Consulte el sitio web de soporte de Avaya:https://soporte.avaya.compara avisos y artículos sobre productos o Servicios alojados, o para informar un problema con su producto o Servicio alojado de Avaya. Para obtener una lista de números de teléfono y direcciones de contacto de soporte, vaya al sitio web de Soporte de Avaya:https://soporte.avaya.com(o el sitio sucesor designado por Avaya), desplácese hasta la parte inferior de la página y seleccione Contactar con el soporte de Avaya.

Marcas registradas

Las marcas comerciales, los logotipos y las marcas de servicio ("Marcas") que se muestran en este sitio, la Documentación, los Servicios alojados y los productos proporcionados

por Avaya son las Marcas registradas o no registradas de Avaya, sus afiliados, sus licenciantes, sus proveedores u otros terceros. Los usuarios no pueden usar dichas Marcas sin el consentimiento previo por escrito de Avaya o de un tercero que pueda ser propietario de la Marca. Nada de lo contenido en este sitio, la Documentación, los Servicios alojados y los productos debe interpretarse como una concesión, por implicación, impedimento legal o de otro modo, de cualquier licencia o derecho sobre las Marcas sin el permiso expreso por escrito de Avaya o el tercero aplicable.

Avaya es una marca registrada de Avaya Inc.

Todas las marcas comerciales que no son de Avaya son propiedad de sus respectivos dueños. linux®es la marca registrada de Linus Torvalds en los EE. UU. y otros países.

Contenido

Capítulo 1 Introducción..... 8
Objetivo..... 8
Cambia la historia..... 8
Garantía..... 9
Capítulo 2: Descripción general de Avaya Session Border Controller for Enterprise..... 10
Servicios estándar..... 10
Servicios Avanzados..... 11
Entidades funcionales..... 12
Elemento de señalización..... 12
Elemento mediático..... 13
Aprovisionamiento de elementos y gestión..... 13
Implementación de Avaya SBCE..... 14
Modelos de despliegue..... 14
Modos de despliegue..... 14
Plataformas de implementación admitidas para SBCE..... dieciséis
Despliegue de seguridad de red adicional..... 19
Políticas de contraseñas..... 20
Nuevas características para la versión 7.2.1..... .21
Nuevas funciones para la versión 7.2.2..... .21
Nuevas funciones para la versión 7.2.2.2..... 22
Descripción de la función..... 22
Anclaje de medios..... 22
Desanclaje de medios..... 22
Configuración de trabajadores remotos..... 22
Servicios de gestión remota..... 23
Manipulación de la señalización..... ... 23
Enlace troncal SIP..... 24
UCID..... 25
Compatibilidad con SRTP de vídeo..... ... 26
CONSULTAR Manipulación..... 27
Acceso a varios dispositivos..... 29
Gestión de reinvitaciones..... 30
Supervisión de RTCP..... 30
Generación de informes de monitoreo de RTCP..... 35
Proxy inverso..... 36
Control de la cámara del extremo lejano..... .. 37
Protocolo de Control de Piso Binario..... 38
Corrección de errores de reenvío..... 42
Registro de usuario..... 43
Estado del servidor SIP en tiempo real..... 43

Requisitos de licencia 43
Inicio de sesión único y motor de identidad 44
Múltiples implementaciones de Avaya SBCE 44
Gestión de llamadas habilitada para WebRTC 45
Visión general de la arquitectura de virtualización 46
Descripción general de SRTP 47
Múltiples subredes y múltiples interfaces 48
herramienta traceSBC 54
Compatibilidad con Avaya SBCE para Serviceability Agent 55
Multi Alquiler 56
Compatibilidad con troncales de IP Office desde una dirección IP dinámica 59
Reutilización de la conexión establecida por IP Office para la entrega de llamadas 59
Proxy de servicios de habilitación de cliente seguro 60
Compatibilidad con la tarjeta de acceso remoto Dell integrada y Lights-Out integrado 60
Solución de grabación basada en SIPREC 61
Indicación segura de extremo a extremo 64
Cifrado de medios usando AES-256 ..... sesenta y cinco
Transcodificación ..... sesenta y cinco
Compatibilidad con direcciones IPv6 66
Servidor perimetral para la solución de conferencia convergente 67
Soporte ENUM 70
Preservación de llamadas 71
Compatibilidad con el adaptador de aplicaciones inteligente TILEncore-Gx36 72
Capítulo 3: Interoperabilidad ..... .76
Compatibilidad del producto 76
Servidores compatibles con Avaya SBCE 76
Productos de Avaya 77
Requisitos de productos de terceros 77
Compatibilidad del sistema operativo 77
Capítulo 4: Especificaciones de rendimiento 78
Capacidad admitida 78
Redundancia y alta disponibilidad 79
Alta disponibilidad de Avaya SBCE 80
Réplica de EMS 81
Capítulo 5: Requisitos ambientales 82
Requisitos de altitud 82
Dimensiones de los herrajes 82
Requerimientos de temperatura y humedad 83
Requerimientos de energía 83
Requisitos de protección del sistema físico 84
Normas reglamentarias 84
Capítulo 6: Seguridad 86
Especificación de seguridad 86

Protección contra intrusiones de comunicaciones unificadas..... 86
Protección contra ataques 87
Fortalecimiento de Avaya SBCE 88
Protección contra inundaciones de capa 3 y capa 4 y escaneos de puertos..... 88
Características de seguridad de DoS 89
Depurador de protocolos 90
Ocultación de topología..... 90
Reglas de cortafuegos..... 90
Especificación de utilización del puerto 94
Restricciones del puerto de la interfaz de administración 94
Paquetes TCP..... 95
Puerto SSH 95
Asignaciones de puertos adicionales..... 95
Capítulo 7: Requisitos de licencia..... 97
Características de la licencia SBCE de Avaya..... 97
Detalles del servidor WebLM..... 98
Capítulo 8: Recursos..... 100
Documentación..... 100
Búsqueda de documentos en el sitio web de soporte de Avaya..... 101
Capacitación..... 101
Visualización de videos de orientación de Avaya..... 101
Apoyo..... 102
Glosario..... 103

Capítulo 1 Introducción

Objetivo

Este documento describe las características y capacidades probadas de Avaya Session Border Controller for Enterprise (Avaya SBCE), incluidas descripciones de funciones, interoperabilidad, especificaciones de rendimiento, seguridad y requisitos de licencia.

Este documento está destinado a personas que desean obtener una comprensión de alto nivel de las características, funciones, capacidades y limitaciones de Avaya SBCE.

Cambia la historia

Tema	Fecha	Resumen de Cambios
1	junio 2017	Documento de la versión 7.2.
2	junio 2017	Se actualizó la tabla de especificaciones de capacidad y escalabilidad.
3	septiembre 2017	Se agregó el soporte de Dell 330 en el tema Redundancia y alta disponibilidad.
4	noviembre 2017	Se actualizó el documento para los siguientes cambios de la versión 7.2.1: • Se agregó el soporte de SHA2 en túneles de medios • Se agregó el soporte de ESXi 6.5 para VMware • Se agregó compatibilidad con Nutanix para la implementación de KVM • Se agregó una nueva función de generación de informes de monitoreo de RTCP • NAT simétrica añadida y compatibilidad con múltiples direcciones IP para navegador habilitado para WebRTC • Se actualizó la tabla de especificaciones de capacidad y escalabilidad para Nutanix.
5	diciembre 2017	Se actualizó el tema de compatibilidad con Vmware ESXi para todas las versiones del software ESXi.

La tabla continúa...

Tema	Fecha	Resumen de Cambios
6	abril 2018	Se agregó la introducción de las siguientes funciones nuevas para la versión 7.2.2: • Licencias centralizadas • Reglas de carga • Mejora de WebRTC Se agregó un nuevo tema de plataformas de implementación admitidas para Avaya SBCE.
7	junio 2018	• Se agregó una nota en el tema de Capacitación. • Se agregó un nuevo tema de Políticas de contraseñas. • Se actualizó la tabla de especificaciones de capacidad y escalabilidad.
8	abril 2019	• Se agregó un nuevo tema Nuevas funciones para la versión 7.2.2.2. • Se actualizó el tema de Funciones para la grabación de sesiones para Release 7.2.2.2. • Se actualizó el tema de los servidores compatibles con Avaya SBCE para la versión 7.2.2.2. • Se actualizó el tema Capacidad admitida para la versión 7.2.2.2.

Garantía

Avaya ofrece una garantía limitada de un año para el hardware Avaya SBCE y de 90 días para el software Avaya SBCE. Para comprender los términos de la garantía limitada, consulte el acuerdo de venta u otra documentación aplicable. Además, la garantía estándar de Avaya y los detalles de soporte para Avaya SBCE en el período de garantía están disponibles en el sitio web de soporte de Avaya.http://soporte.avaya.com/ por debajo**Ayuda y Políticas**>**Políticas y Legales**>**Garantía y ciclo de vida del producto**. Ver también**Ayuda y Políticas**>**Políticas y Legales**>**Términos de licencia**.

Capítulo 2: Borde de sesión de Avaya

Descripción general de Controller para empresas

Avaya SBCE brinda seguridad a las redes de comunicaciones unificadas (UC) basadas en SIP. Avaya SBCE está disponible en dos versiones: Servicios avanzados y Servicios estándar. Cualquiera de las versiones puede residir en servidores compatibles. Para obtener información sobre los servidores compatibles, consulte la sección Servidores compatibles con Avaya SBCE.

Avaya SBCE tiene dos componentes principales: el controlador de borde de sesión (Avaya SBCE) y un sistema de gestión llamado Element Management System (EMS). Según el tamaño de la red y los requisitos del servicio, puede implementar Avaya SBCE en una de las siguientes configuraciones:

- Configuración independiente

  En la configuración independiente, Avaya SBCE y EMS residen en el mismo servidor físico.

- Configuración de múltiples servidores

  En la configuración de múltiples servidores, EMS y Avaya SBCE se implementan en servidores físicos separados.

- Configuración de alta disponibilidad (HA)

  En la configuración de alta disponibilidad o HA, los servidores SBCE de Avaya se implementan en pares. Cada par tiene un servidor SBCE de Avaya que actúa como principal mientras que el otro es secundario. Ambos servidores están controlados por un solo dispositivo Avaya Element Management System (EMS) o un par de EMS replicado.

Enlaces relacionados

Servidores compatibles con Avaya SBCE en la página 76

Servicios estándar

Los servicios estándar de SBCE de Avaya proporcionan un subconjunto de la funcionalidad de la oferta de servicios avanzados. Los servicios estándar tienen la funcionalidad requerida para que una empresa termine los troncales SIP sin la complejidad y el precio más alto asociado con un controlador de borde de sesión (SBC) típico.

Página702 de 3226.

Avaya SBCE Standard Services es un verdadero SBC empresarial, no un SBC de operador reempaquetado. Este producto proporciona una alternativa de menor costo a los SBC de Carrier más costosos. Los servicios estándar también brindan un SBC empresarial que es asequible, altamente escalable y fácil de instalar y administrar. Standard Services es una solución Plug and Play para empresas y pequeñas y medianas empresas.

Con este producto, los clientes pueden beneficiarse de la amplia experiencia de Avaya en la implementación de troncales SIP y en la compatibilidad con un gran número de usuarios empresariales. Avaya SBCE Standard Services presenta el exclusivo módulo Signaling Manipulation (módulo SigMa), que simplifica drásticamente la implementación de troncales SIP. El módulo Sigma agiliza la integración de troncales SIP en miles de variaciones de entornos de telefonía SIP empresarial, lo que reduce en gran medida el tiempo de implementación. Como resultado, la implementación de troncales SIP en muchas configuraciones estándar puede ocurrir en 2 horas o menos.

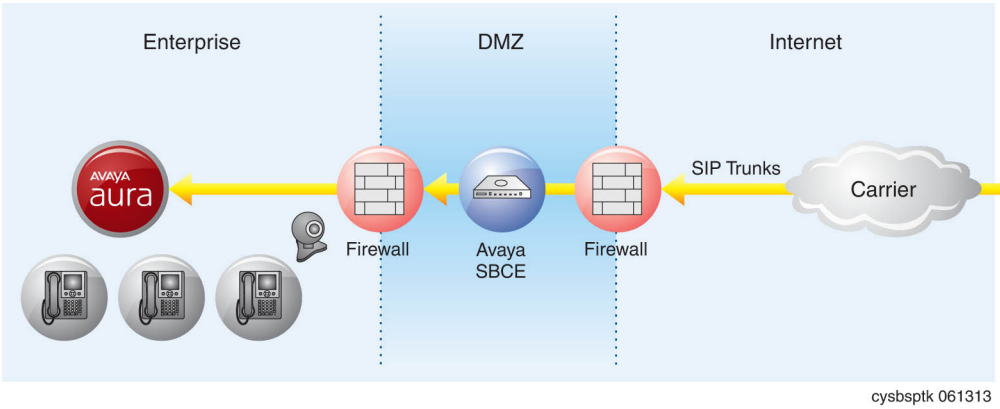


Figura 1: Enlace troncal SIP

Servicios Avanzados

Advanced Services es un producto de seguridad especializado en comunicaciones unificadas (UC). Los servicios avanzados protegen todas las aplicaciones multimedia en tiempo real basadas en IP, los terminales y la infraestructura de red de ataques y usos indebidos potencialmente catastróficos. Este producto brinda la flexibilidad en tiempo real para armonizar y normalizar el tráfico de comunicaciones empresariales para mantener los niveles más altos de eficiencia y seguridad de la red.

Los servicios avanzados brindan las funciones de seguridad requeridas por el mercado de UC en constante cambio y expansión. Los servicios avanzados protegen a cualquier empresa o proveedor de servicios de línea fija o inalámbrica que haya implementado UC, de ataques maliciosos. Estos ataques pueden originarse desde cualquier parte del mundo en cualquier momento. Advanced Services es la única solución de seguridad específica de UC que incorpora todos los enfoques de manera eficaz y sin inconvenientes en un solo sistema integral.

Avaya SBCE Advanced Services incorpora las mejores prácticas de todas las fases de seguridad de datos para garantizar que las nuevas amenazas de UC se reconozcan, detecten y eliminen de inmediato. Advanced Services incorpora técnicas de seguridad que incluyen detección y filtrado de anomalías del protocolo UC,

y detección de anomalías basadas en el aprendizaje del comportamiento. Juntas, estas técnicas monitorean, detectan y protegen cualquier red UC de vulnerabilidades de seguridad conocidas al:

- Validación y soporte de usuarios remotos para la extensión de Avaya Aura®servicios de la UC.
- Usar servicios de encriptación como SRTP.

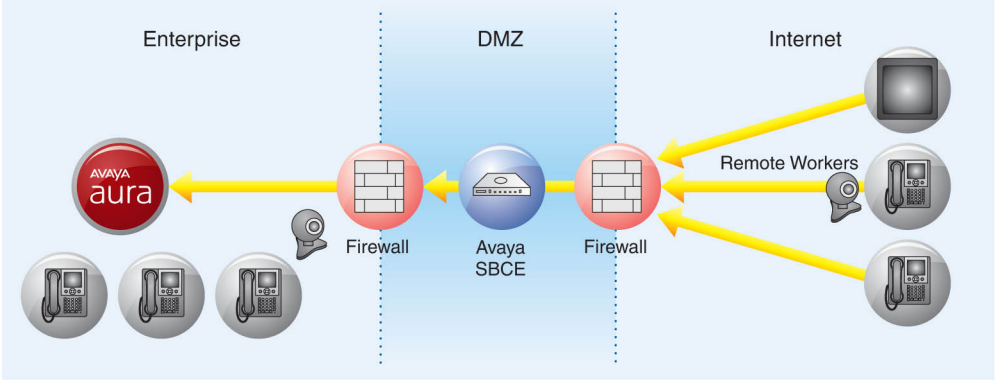


Figura 2: Solución de servicios avanzados

entidades funcionales

Los productos de seguridad SBCE de Avaya realizan funciones de seguridad utilizando tres entidades funcionales interrelacionadas y complementarias: señalización, medios e inteligencia.

Elemento de señalización

El elemento de señalización es el subsistema primario de protección de señalización de llamadas. El elemento de señalización generalmente se implementa en el borde de la red, en la DMZ. Al funcionar como un proxy, el elemento de señalización representa menos de 2 ms del presupuesto de latencia de extremo a extremo.

El elemento de señalización proporciona las siguientes características:

- Descifrado de señalización en línea y administración segura de claves a través de soporte TCP y TLS
- Validación de SIP mejorada a través de la limitación de fuentes, aplicación de políticas y detección de DDoS
  - Travesía NAT/FW
  - Protección de red SIP
  - Tronco SIP y protección de extranet de voz encriptada
  - Detección y prevención de anomalías de protocolo
  - Limitación de fuente SIP
  - Detección y prevención de ataques DoS y DDoS

- Detección y prevención de anomalías en la secuencia de mensajes

- Aprendizaje continuo del comportamiento del usuario

- Omisión de todo el tráfico que no sea SIP, incluidos ARP, DNS, ICMP, STUN y TURN

- Filtrado de políticas basado en dominios basado en criterios de origen y destino de llamadas definibles por el usuario

- Detección de anomalías de comportamiento

• Suplantación de identidad y detección de llamadas generadas por máquinas (MCD)

• Generación de alarmas y reporte de incidentes al elemento funcional de inteligencia Avaya SBCE

Esta entidad también proporciona la información de configuración a los puntos finales remotos. El elemento de señalización utiliza http o https para enviar la información del Administrador de perfil personal (PPM) al teléfono.

---

elemento multimedia

El elemento Media es el subsistema principal de protección de medios RTP. Un elemento de medios se despliega en la red con el elemento de señalización.

El elemento multimedia proporciona las siguientes funciones:

• Cumplimiento de la política de medios

• Detección de anomalías RTP

• Validación de tiempo y ancho de banda

• Inteligencia de detección de tonos de módem y FAX

Aprovisionamiento de elementos y gestión

El aprovisionamiento de elementos y administración es el principal subsistema de administración de información de seguridad de UC de la solución Avaya SBCE. El aprovisionamiento de elementos y gestión recibe los informes de eventos y alarmas con distintos formatos de los diferentes componentes de seguridad de la red. Luego, este sistema almacena, normaliza, agrega y correlaciona la información en un formato completo que permite detectar y mitigar eficazmente los ataques distribuidos.

El aprovisionamiento de elementos y administración proporciona las siguientes funciones:

• Recopila registros de eventos

• Difunde instrucciones al Ente de Señalización para acciones preventivas

• Propaga alarmas a los sistemas de gestión de red

• Mantiene las puntuaciones de confianza de las personas que llaman, las listas blancas y las listas negras

• Proporciona un repositorio de almacenamiento maestro para llamantes y dominios

• Mantiene modelos de comportamiento por usuario, por persona que llama y por elemento de red sobre una base ToD y DoW

Implementación de Avaya SBCE

Modelos de implementación

Según el tamaño de la red y los requisitos del servicio, puede implementar Avaya SBCE en una de las siguientes configuraciones:

- **Configuración independiente**: En la configuración independiente, Avaya SBCE y EMS residen en el mismo servidor físico. En esta implementación, los teléfonos mantienen dos conexiones de socket separadas a Avaya SBCE, en dos direcciones IP diferentes alojadas por Avaya SBCE.
- **Configuración multiservidor**Nota: una configuración de varios servidores requiere que EMS y Avaya SBCE se implementen en diferentes servidores.
- **Configuración de alta disponibilidad (HA)**: una configuración de alta disponibilidad (HA) requiere un servidor EMS independiente. Los pares Avaya SBCE HA se pueden implementar en una empresa en una configuración de modo paralelo. En la configuración en paralelo, los paquetes de señalización se enrutan solo al Avaya SBCE principal o activo, que realiza todo el procesamiento de datos. Los puertos de interfaz en el Avaya SBCE en espera no procesan ningún tráfico. Las interfaces de administración en los dispositivos Avaya SBCE tienen diferentes direcciones IP, pero las interfaces de señalización o de medios tienen la misma dirección IP. Tras la conmutación por error, el SBCE de Avaya en espera anuncia su nueva MAC como la dirección L2 para la dirección IP común. Los dispositivos Avaya SBCE se sincronizan a través del latido en las interfaces dedicadas, y ambos dispositivos Avaya SBCE están en comunicación continua con Avaya EMS.

Estas configuraciones también están disponibles con implementación en el entorno virtualizado.

Avaya SBCE está empaquetado como un dispositivo virtual (OVA) listo para implementarse en hardware certificado por VMware para ejecutarse en un entorno de VMware. A partir de la versión 6.3, Avaya SBCE también se entrega en formato vAppliance (OVA) para implementaciones basadas en VMware. A partir de la versión 7.0, Avaya SBCE tiene un solo archivo OVA para EMS, SBCE+EMS y solo implementación de Avaya SBCE. El archivo .ova está disponible en PLDS. Esta configuración es compatible con funciones de VMware, como vMotion, alta disponibilidad en centros de datos y configuración de hardware mixta.

Para obtener más información acerca de la virtualización, consulte*Implementación de Avaya Session Border Controller para empresas en un entorno virtualizado*.

Modos de implementación

Los dispositivos SBCE de Avaya se pueden implementar con o sin seguridad de la capa de transporte (TLS) o cifrado de protocolo de transporte seguro en tiempo real (SRTP).

Independientemente del escenario de implementación, Avaya SBCE ofrece una flexibilidad total y una configuración intuitiva. Estos productos no requieren ninguna gestión en los terminales además de lo necesario para habilitar TLS, SRTP y autenticación implícita.

Despliegue de dos hilos

La topología de dos hilos, también conocida como en línea, es la implementación más simple y básica. Avaya SBCE está ubicado en el borde de la red en la DMZ. Avaya SBCE está directamente en línea con los servidores de llamadas y protege la red empresarial contra todas las intrusiones y ataques involuntarios y maliciosos.

En esta configuración, Avaya SBCE realiza funciones de control de acceso fronterizo, como firewall interno y externo o traducción de direcciones de red (FW/NAT), administración y control de acceso transversales. Estas funciones se basan en políticas de dominio que el usuario puede configurar y funcionalidad de intrusión para proteger contra DoS, suplantación de identidad, ataques sigilosos y SPAM de voz.

La implementación de Avaya SBCE de dos hilos permite el cifrado TLS del tráfico de señalización y el cifrado SRTP del tráfico de medios.

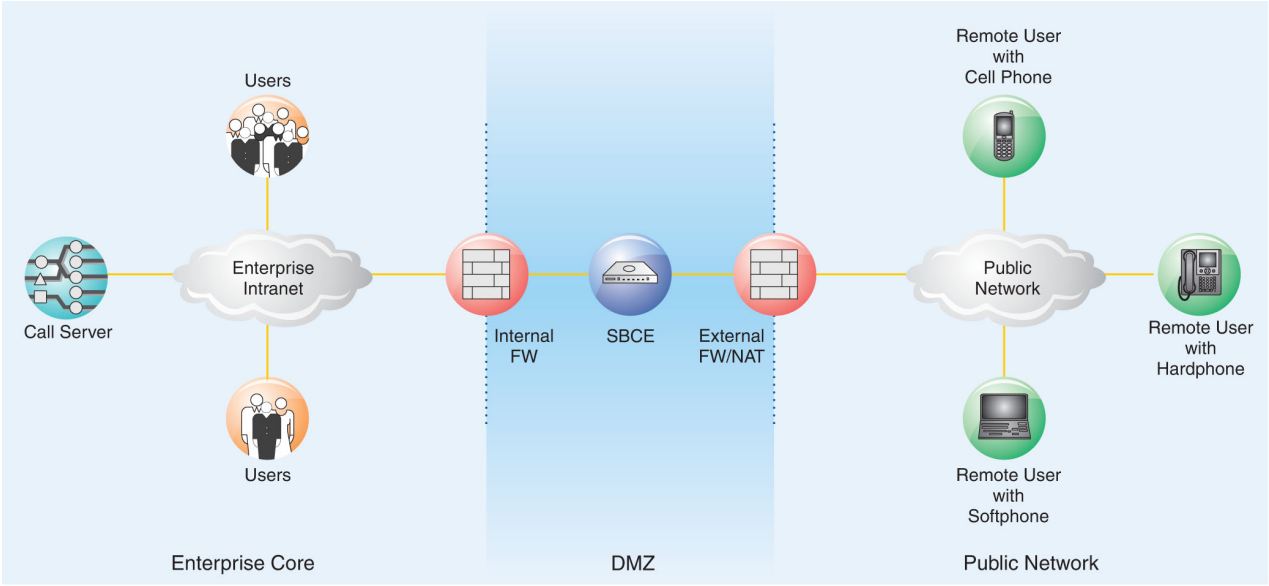


Figura 3: Implementación de Avaya SBCE: dos hilos

Implementación de un solo cable

Con la implementación de un solo cable, también conocida como subred filtrada, Avaya SBCE se implementa en la DMZ de la empresa, pero no directamente en línea con los servidores de llamadas de la empresa. Avaya SBCE se encuentra en la ruta de señalización directa, utiliza una única interfaz Ethernet y es el siguiente salto para el tráfico SIP.

Avaya SBCE en una implementación de un solo cable proporciona un alto nivel de funcionalidad de seguridad característica de la implementación en línea. Esta implementación no agrega ninguna latencia a las aplicaciones multimedia de tiempo crítico, como videoconferencias o música a pedido, en comparación con una implementación de dos hilos.

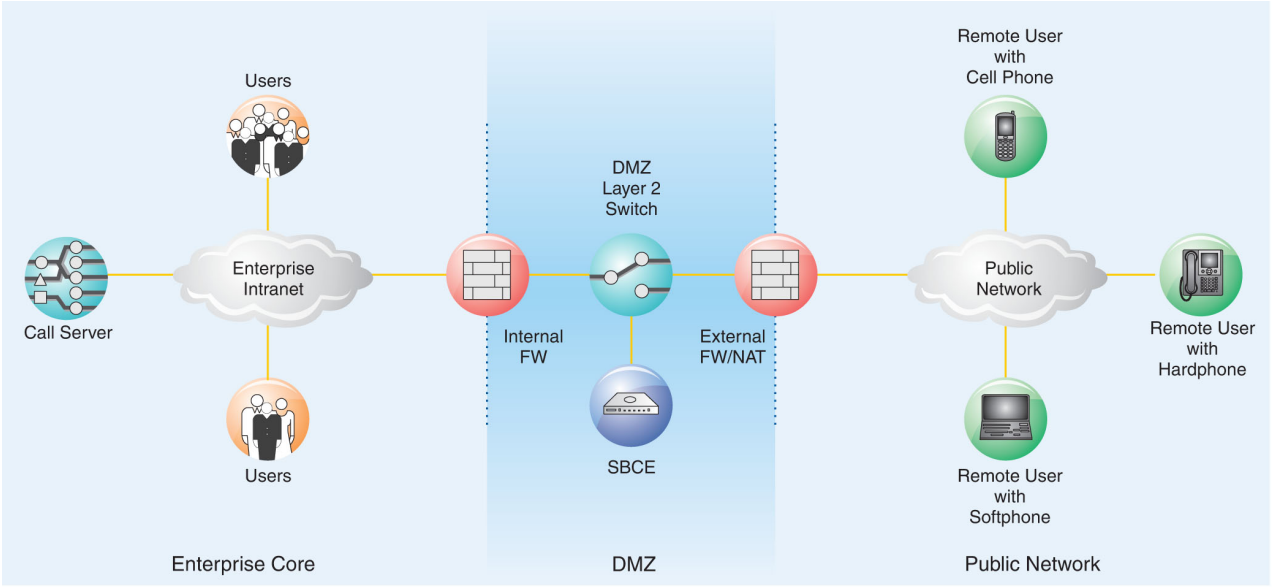


Figura 4: Implementación de Avaya SBCE: One-Wire

Plataformas de implementación admitidas para SBCE

Descripción general de la arquitectura de virtualización

Para la implementación en hardware certificado por VMware, Avaya SBCE se empaqueta como vAppliance Ready (OVA) para ejecutarse en el entorno virtualizado. Por lo tanto, a partir de la versión 6.3, Avaya SBCE también está disponible para implementaciones basadas en VMware.

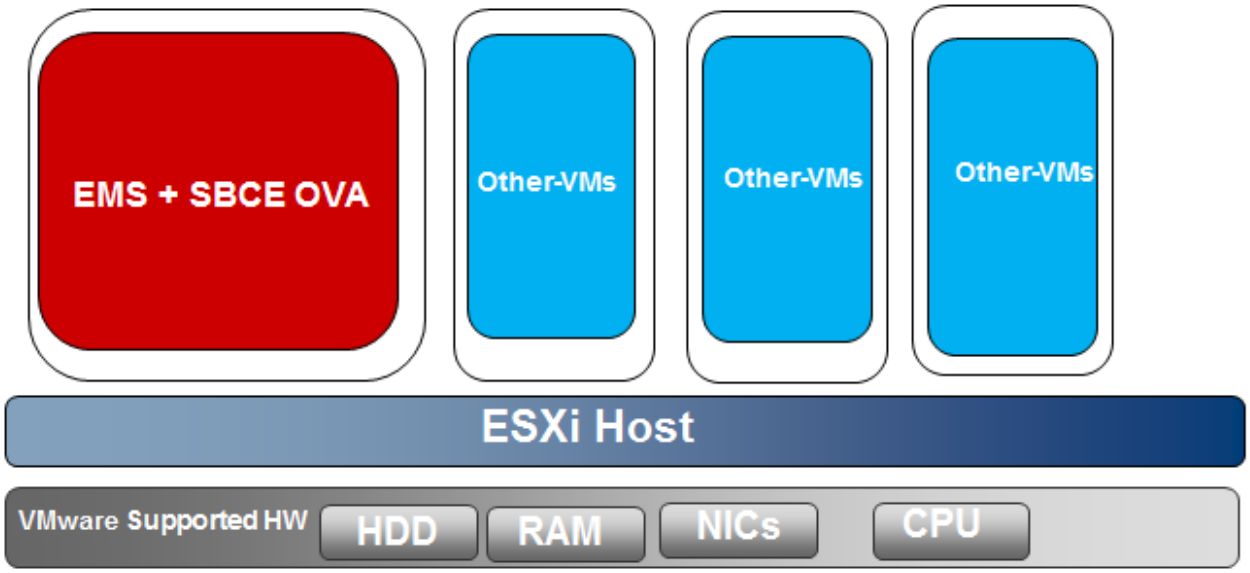
A partir de la versión 7.0, un solo archivo OVA está disponible para implementar EMS y Avaya SBCE.

Avaya SBCE es compatible con las funciones de VMware, como vMotion, HA en los centros de datos y configuraciones de hardware mixtas.

Los archivos Avaya SBCE OVA se ofrecen como vAppliance para configuraciones de EMS y Avaya SBCE. El archivo .ova está disponible en el Sistema de entrega y licencia de productos (PLDS).

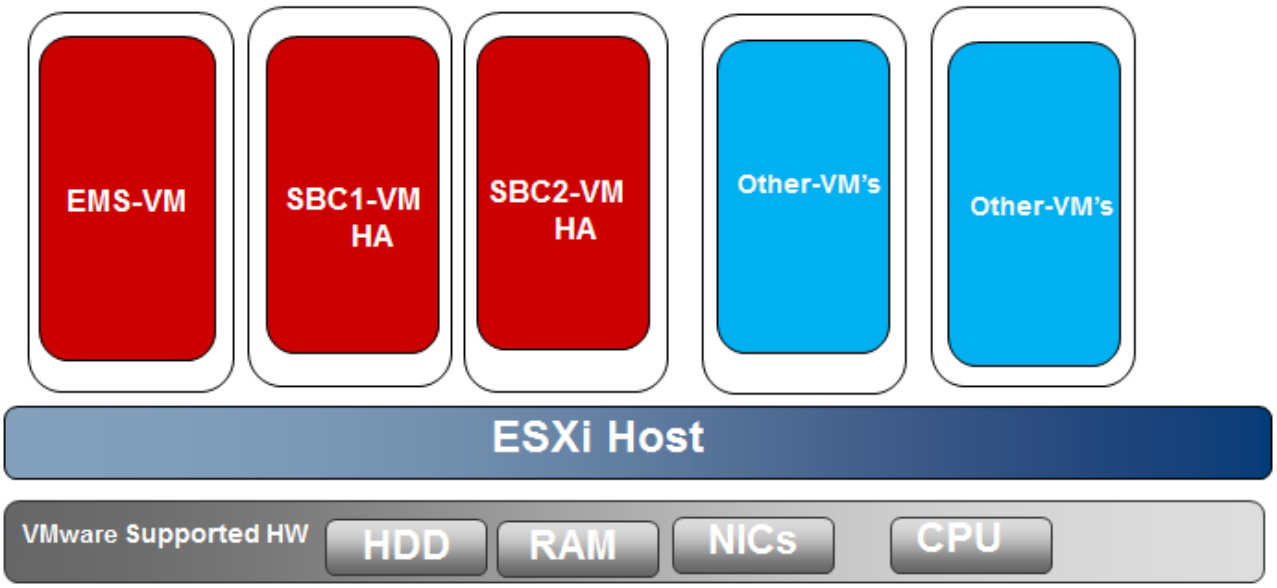
Modo independiente Avaya SBCE

Si selecciona una implementación independiente, el archivo OVA instala configuraciones para Avaya SBCE y EMS.



EMS y SBC en modo de alta disponibilidad (HA)

Para el modo HA, implemente el archivo OVA por separado para EMS y Avaya SBCE. Desde la versión 7.0, un solo archivo OVA está disponible para implementar EMS y Avaya SBCE. Por lo tanto, puede usar el mismo archivo OVA, pero elegir diferentes configuraciones para implementar EMS y Avaya SBCE.



Para más información, ver *Implementación de Avaya Session Border Controller para empresas en un entorno virtualizado*.

Aura de Avaya®en la descripción general de Amazon Web Services

Amazon Web Services (AWS) es una plataforma de servicios en la nube que permite a las empresas ejecutar aplicaciones de forma segura en la nube virtual. Los componentes clave de AWS son Amazon Elastic Compute Cloud (EC2) y Amazon Simple Storage Service (S3).

La compatibilidad con las aplicaciones de Avaya en la plataforma de infraestructura como servicio (IaaS) de AWS brinda los siguientes beneficios:

- Minimiza el gasto de capital (CAPEX) en infraestructura. Los clientes pueden pasar de CAPEX a gastos operativos (OPEX).
- Reduce el costo de mantenimiento de operar los centros de datos.
- Proporciona una plataforma común para implementar las aplicaciones.
- Proporciona un entorno flexible para adaptarse a los cambiantes requisitos comerciales de los clientes.

Puede implementar los siguientes Avaya Aura®aplicaciones en Amazon Web Services:

- Aura de Avaya®Administrador de sistemas
- Aura de Avaya®Administrador de sesión
- Aura de Avaya®Gerente de Comunicación
- Aura de Avaya®Servicios de utilidad
- Avaya WebLM
- Servicios de presencia con Avaya Breeze™
- Controlador de borde de sesión de Avaya para empresas
- Aura de Avaya®Servicios de dispositivos
- Aura de Avaya®Servicios de habilitación de aplicaciones (solo software)
- Aura de Avaya®Servidor multimedia (solo software)
- Servidor de diagnóstico de Avaya (solo software)

Avaya Aura compatible®Las aplicaciones de AWS también se pueden implementar en las instalaciones.

Puede conectar las siguientes aplicaciones a Avaya Aura®Instancias de AWS desde las instalaciones del cliente:

- Aura de Avaya®Conferencia versión 8.0 y posteriores
- Aura de Avaya®Mensajería versión 6.3 y posteriores
- G430 Branch Gateway, G450 Branch Gateway y G650 Media Gateway

Para más información, ver*Implementación de Avaya Session Border Controller para empresas en Amazon Web Services*

Descripción general de la máquina virtual basada en kernel

La máquina virtual basada en kernel (KVM) es una infraestructura de virtualización para el kernel de Linux que convierte el kernel de Linux en un hipervisor. Puede acceder de forma remota al hipervisor para implementar aplicaciones en el host KVM.

La solución de virtualización KVM es:

- Rentable para los clientes.
- Seguro ya que utiliza las características de seguridad avanzadas de SELinux.
- Rendimiento confiable y altamente escalable.
- Software de código abierto que se puede personalizar según los requisitos comerciales cambiantes de los clientes.

También puede implementar KVM con Nutanix.

Para más información, ver *Implementación de Avaya Session Border Controller para empresas en un entorno virtualizado*.

Despliegue de seguridad de red adicional

Esta implementación brinda protección a la infraestructura central de UC al tiempo que permite el acceso a los servicios entregados a través del núcleo Aura.®infraestructura de aplicaciones. El siguiente diagrama muestra esta implementación.

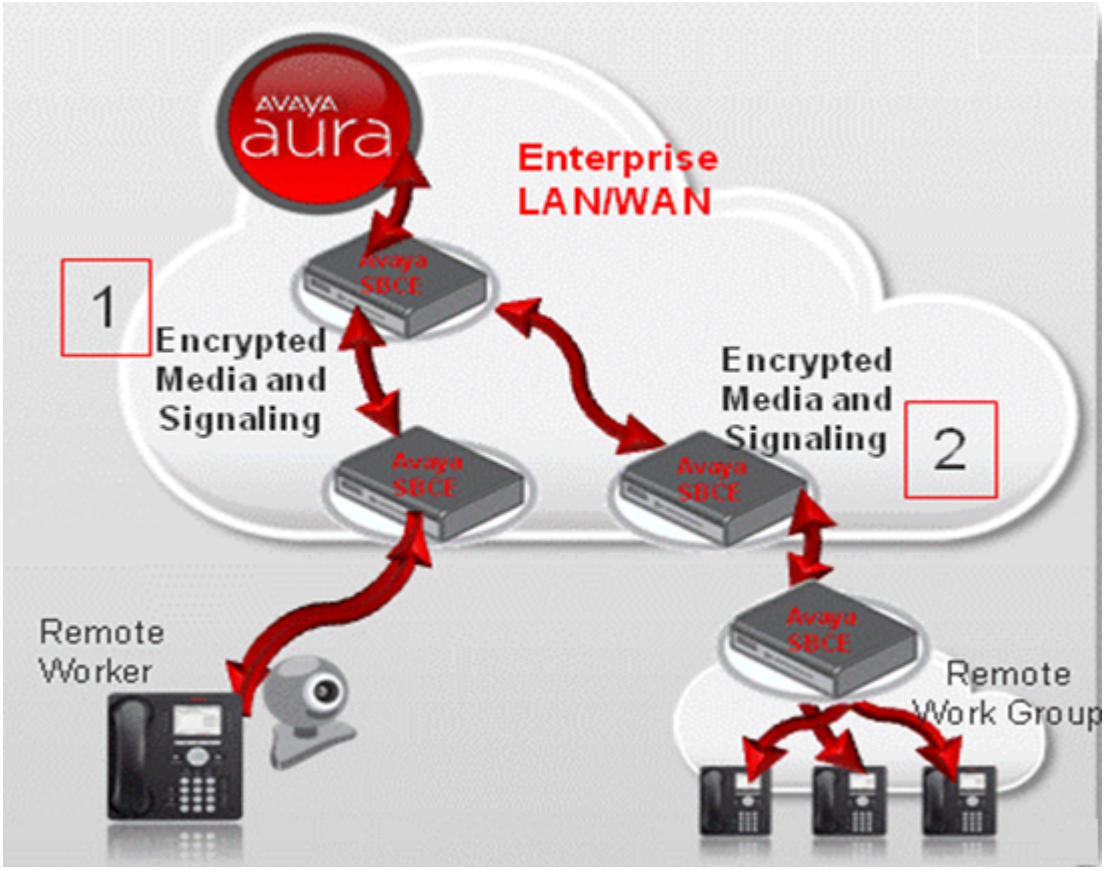


Figura 5: Implementación de seguridad de red adicional

En el diagrama, se representan dos casos de uso. La primera configuración muestra un escenario consecutivo en el que el núcleo de Aura está protegido internamente por Avaya SBCE y los trabajadores remotos se conectan al núcleo a través de un Avaya SBCE diferente. Avaya SBCE mantiene la seguridad y los enlaces NAT y el cifrado de extremo a extremo en este escenario de back-to-back (B2B). El segundo escenario representa un grupo de trabajo remoto que utiliza un SBCE de Avaya en el borde local del grupo, creando un escenario de espalda con espalda (B2B2B). Esta configuración permite el tratamiento del grupo de trabajo como Remoto tanto desde la red principal como desde el núcleo Aura y admite el cifrado de señalización y medios de los clientes a Avaya SBCE y luego al núcleo si se desea. Esta configuración es compatible con los clientes SIP Avaya 96x1.

Políticas de contraseña

Las contraseñas raíz e ipcs se determinan y configuran durante la instalación del producto. La GUI de EMS tiene una contraseña separada. Cuando inicia sesión por primera vez después de la instalación, el sistema le solicita que cree una nueva contraseña para acceder a la GUI de EMS. El ID de usuario y la contraseña predeterminados son ucsec.

Las restricciones de contraseña se imponen en elucsecy cuentas ipcs. La nueva contraseña debe cumplir con los criterios de contraseña de un mínimo de 8 caracteres, incluidos:

- Una letra mayúscula, una letra minúscula y un número.
- Un carácter especial del guión (-), guión bajo (_), arroba (@), asterisco (*) y signo de exclamación (!). No debe usar el signo de número (#), el signo de dólar ($) , y ampersand (&).

Nota:

El administrador de la red del cliente determina las contraseñas raíz e ipcs de la CLI de SBCE de Avaya durante el procedimiento de instalación. Dos pasos de instalación solicitan al instalador que ingrese una contraseña elegida.

Nuevas funciones para la versión 7.2.1

Avaya Session Border Controller for Enterprise versión 7.2.1 es compatible con las siguientes funciones y mejoras nuevas:

- Compatibilidad con VMWare ESXi 6.0 y ESXi 6.5
- Compatibilidad con la implementación de KVM mediante Nutanix
- Generación de informes de monitoreo de RTCP
- Recopilación de registros
- Compatibilidad con SHA2 para tunelización de medios
- Compatibilidad con NAT simétrica y varias direcciones IP para navegadores habilitados para WebRTC

Nuevas funciones para la versión 7.2.2

Avaya Session Border Controller for Enterprise versión 7.2.2 es compatible con las siguientes funciones y mejoras nuevas:

- Licenciamiento centralizado.
- Función DNS-SRV agregando soporte de registro para configurar el perfil del servidor SIP
- Normas de tarificación.
- Compatibilidad con la configuración del EMS secundario al estado predeterminado de fábrica.
- Compatibilidad con TURN utilizando indicación SEND y DATA y señalización TURN en TCP, TLS y UDP.
- Soporte para configurar el servicio de retransmisión TURN para llamadas WebRTC
- Se agregó el soporte del intervalo de monitoreo en ausencia del informe RTCP para la generación de informes de monitoreo RTCP

Página713 de 3226.

Nuevas funciones para la versión 7.2.2.2

Avaya Session Border Controller for Enterprise versión 7.2.2 2 admite las siguientes funciones y mejoras nuevas:

- Se agregó el soporte de la opción KDDI en el campo Extensión del perfil Interworking
- Cálculo de RTT con la ayuda de flujos RTCP de Avaya SBCE
- Identificación del troncal o del agente de usuario con la ayuda de flujo de medios
- Se agregó la compatibilidad con el servidor de la serie Avaya Converged Platform 100 con perfil 3
- Se agregó la compatibilidad con el servidor de la serie Avaya Converged Platform 100 con perfil 5

Descripción de la función

Anclaje de medios

Avaya SBCE ancla los flujos de medios de todos los medios que pasan por Avaya SBCE. Con el anclaje de medios, Avaya SBCE puede realizar la terminación SRTP, donde Avaya SBCE descifra o encripta el tráfico RTP según las políticas de seguridad y NAT transversal. Todas las configuraciones admitidas requieren anclaje de medios.

Desanclaje de medios

Para mejorar el uso del ancho de banda para puntos finales dentro de la misma subred y para permitir que los medios directos fluyan entre estos puntos finales, anule los medios para las sesiones. Utilice esta función para mejorar el uso del ancho de banda cuando se conecte a una red MPLS administrada o una red en la nube.

A partir de la versión 7.1, Avaya SBCE es compatible con el desanclaje de medios para todas las llamadas sin horquilla, incluidas las de troncal a empresa, de empresa a troncal, remota a empresa y de empresa a remota. Avaya SBCE admite el desanclaje de medios para llamadas de audio, video y multimedia.

Configuración de trabajadores remotos

La configuración del trabajador remoto brinda a los usuarios de SIP ubicados de forma remota acceso a la red interna de comunicaciones unificadas (UC) de la empresa mediante la implementación de funciones de seguridad integrales de UC. Estas características incluyen cruce sofisticado de cortafuegos/NAT, encriptación, autenticación de usuarios y aplicación de políticas de llamadas de puntos finales y sesiones.

La configuración de trabajadores remotos está disponible para implementaciones SIP. Esta configuración utiliza la autenticación para verificar la legitimidad del usuario remoto y descifra la señalización cifrada con TLS.

Tráfico SIP en tiempo real. Cuando se completa el descifrado, Avaya SBCE analiza el tráfico en busca de comportamientos anómalos, ataques e intrusiones, y aplica las políticas de UC definidas por el usuario.

La llamada puede originarse desde una configuración de trabajador remoto ubicada de forma remota, fuera de la red empresarial, a un usuario interno dentro de la red empresarial central. Luego, Avaya SBCE en la DMZ empresarial descifra los medios SRTP que llegan a la empresa desde la red IP externa o Internet. Avaya SBCE realiza cualquier traducción de direcciones de red (NAT) requerida, analiza el tráfico en busca de comportamientos anómalos y aplica las políticas de medios de UC relevantes. Avaya SBCE en la DMZ pasa el flujo RTP al destinatario previsto.

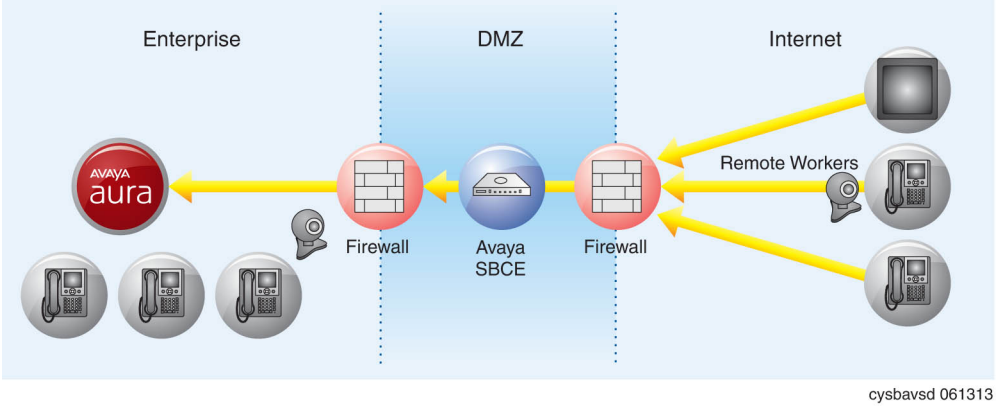


Figura 6: Trabajador remoto

Servicios de gestión remota

Un servicio de red privada virtual (VPN) de capa de sockets seguros (SSL) de IP Office proporciona un túnel seguro entre un sitio de soporte o servicios de Avaya y un SBCE de Avaya que está instalado en el sitio de un cliente. Con el túnel seguro, los proveedores de servicios de Avaya pueden ofrecer servicios de administración remota, como administración, monitoreo y administración de fallas a los clientes de IP Office.

Avaya SBCE también admite el acceso remoto a través de la puerta de enlace SAL.

Los servicios de administración remota brindan a los agentes de atención al cliente de Avaya un fácil acceso a la interfaz gráfica de usuario del controlador de borde de sesión o SSH.

Manipulación de señalización

Con la manipulación de encabezados de señalización SIP de Avaya, los usuarios pueden agregar, cambiar y eliminar los encabezados y otra información en un mensaje SIP. La manipulación de la señalización se puede configurar en cada nivel de flujo utilizando un lenguaje de secuencias de comandos patentado.

enlace troncal SIP

SIP Trunking permite a las empresas habilitadas para SIP Trunk asegurar completamente la conectividad SIP a través de Internet a través de los servicios de SIP Trunking obtenidos de un proveedor de servicios de telefonía por Internet (ITSP).

El enlace troncal SIP garantiza la privacidad de todas las llamadas que atraviesan la red empresarial, al mismo tiempo que mantiene un punto de demarcación bien definido entre el núcleo y la red de acceso. Además, la función de enlace troncal SIP permite que una empresa mantenga un control granular a través de políticas de dominio bien definidas que protegen las implementaciones SIP o los servidores de los clientes de las vulnerabilidades SIP y multimedia conocidas.

Debido a que Avaya SBCE se implementa en la DMZ empresarial como un host confiable, todo el tráfico de señalización SIP destinado a la empresa es recibido por el firewall externo y enviado a Avaya SBCE para su procesamiento.

Si el tráfico de señalización está cifrado, Avaya SBCE descifra todo el tráfico cifrado con TLS y busca un comportamiento anómalo antes de reenviar los paquetes a través del firewall interno a la IP PBX adecuada en el núcleo de la empresa para establecer la sesión de llamada solicitada.

Cuando se ha configurado una sesión de llamada válida, los paquetes de medios del Protocolo de transporte en tiempo real (RTP) o del Protocolo de transporte seguro en tiempo real (SRTP) pueden fluir a través del firewall externo al Avaya SBCE en la DMZ. Luego, el SBC busca un comportamiento anómalo en los medios antes de pasar el flujo RTP/SRTP al punto final deseado.

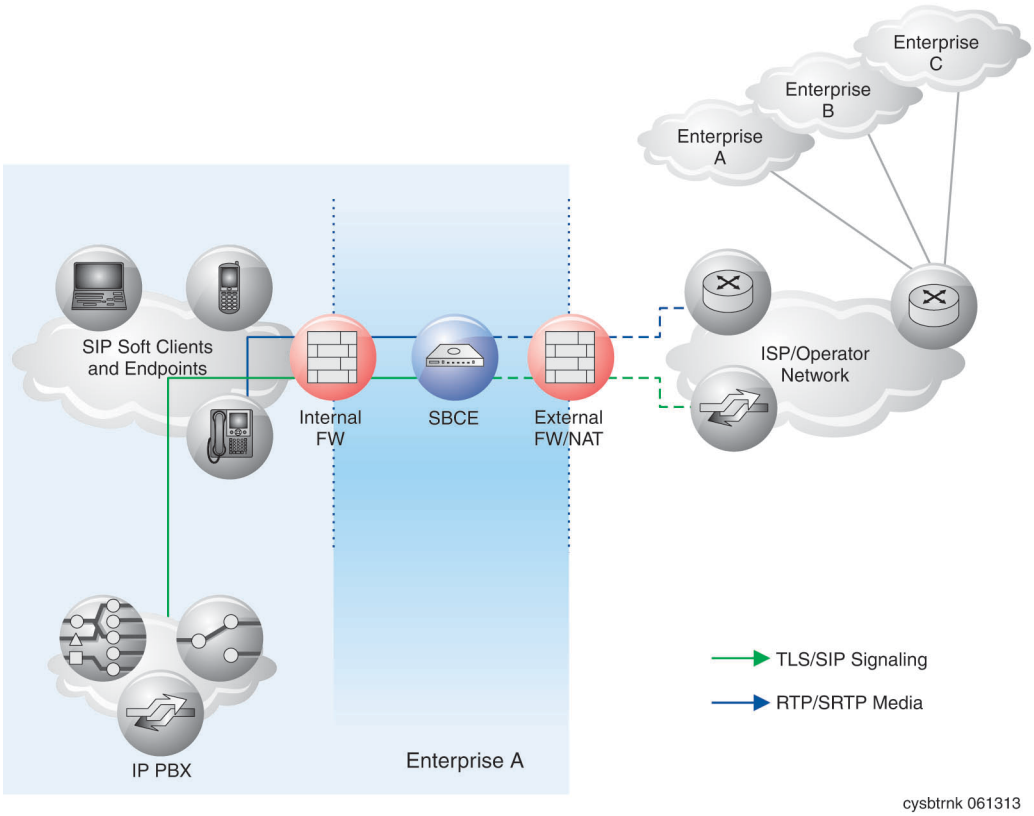


Figura 7: Enlace troncal SIP

UCID

El Universal Call ID (UCID) es un identificador de llamadas de propiedad de Avaya que se utiliza en las aplicaciones del centro de contacto. UCID se utiliza para monitorear, controlar y grabar llamadas en interfaces no SIP de CTI. También se puede usar para rastrear el historial de llamadas.

AACC

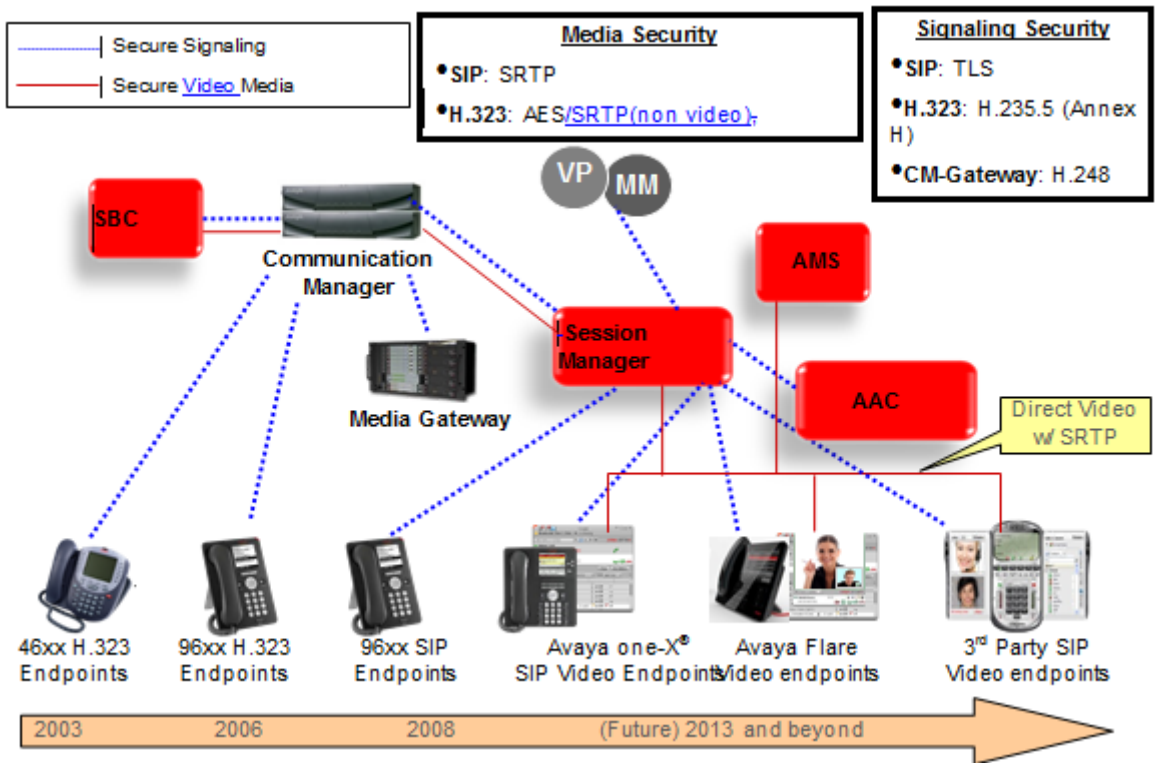
Se requiere la generación de UCID por parte de Avaya SBCE en Avaya Aura®Entorno Contact Center 7.0. Se asigna un UCID a cualquier llamada entrante en la frontera Avaya SBCE para que AACC tenga un identificador único para cada llamada. Por ejemplo, AACC luego monitorea o controla cualquier aplicación, incluida la grabadora de llamadas, utilizando la interfaz CTI y el UCID para la llamada.

CC Élite

La generación de UCID por parte de Avaya SBCE no afecta a Avaya Aura®Centro de llamadas de élite. En este escenario, la aplicación del centro de contacto recibe un identificador único de la llamada de Avaya Aura® Gerente de comunicación. Avaya SBCE genera un UCID para todas las llamadas SIP entrantes y ACM reutiliza el mismo UCID. No se produce ningún conflicto de UCID entre las aplicaciones ACM, Avaya SBCE y Contact Center. En funciones como la retención de llamadas, ACM mantiene una asociación entre el nuevo UCID y el UCID principal.

Soporte para video SRTP

Communication Manager admite SRTP para video cuando se habilitan las configuraciones adecuadas en la tabla de funciones de parámetros del sistema. La habilitación de SRTP para video en una llamada de SIP a SIP se basa en la política establecida en la tabla de conjunto de códecs IP. El filtrado de cryptosuite basado en las reglas del conjunto de códecs IP no se aplica a la transmisión de medios de video. Las reglas del conjunto de códecs IP habilitan la política SRTP para la transmisión de medios de video.



Casos de usuario admitidos

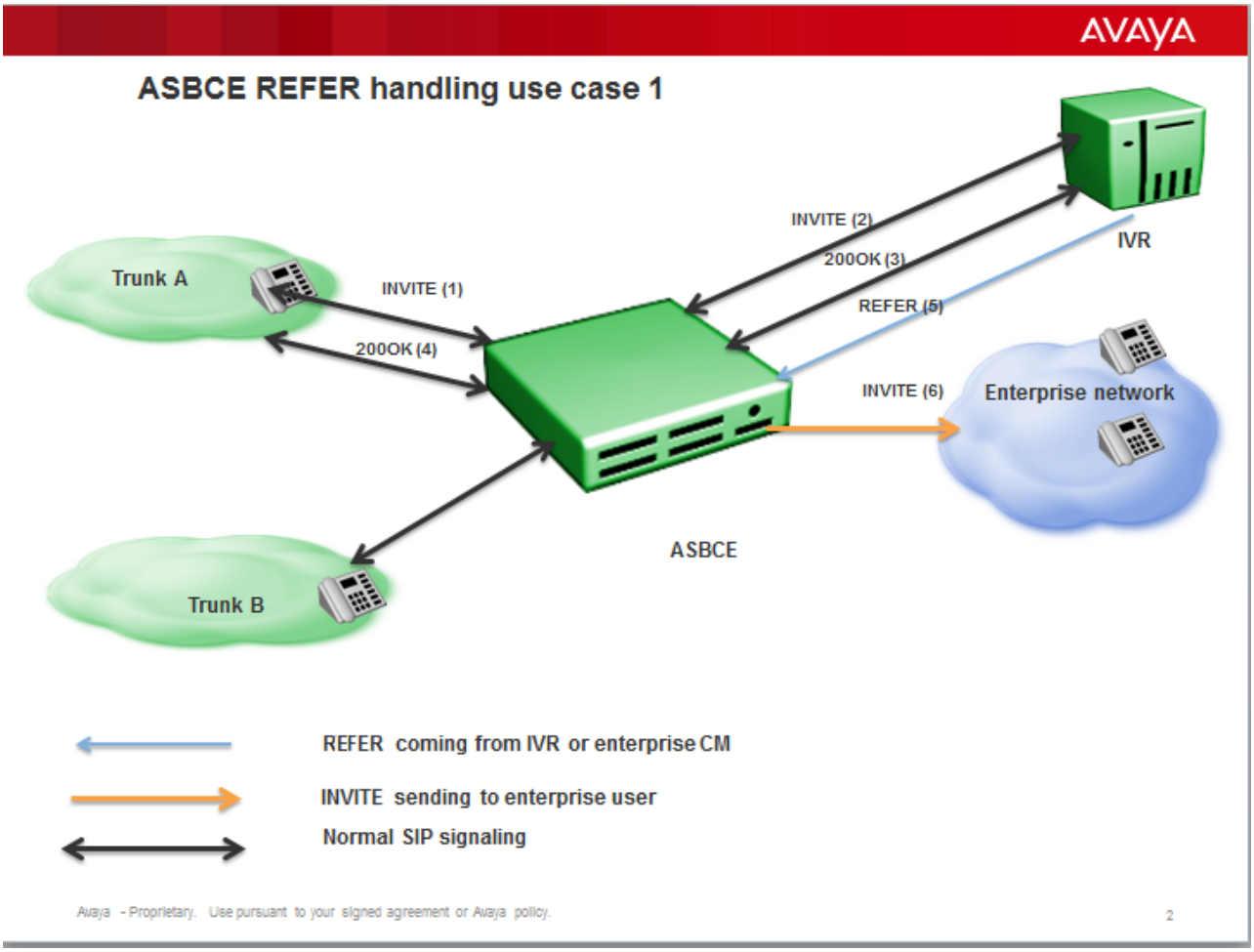
- Usuarios de escritorio: Extremo de video SIP de Avaya, como videollamada SIP cifrada 1XC a 1XC SRTP: habilitación de videollamadas entre dos extremos SIP de operador de IntereXchange habilitados para video.
  Se pueden usar todas las funciones estándar de telefonía y video, como silenciar, transferir y retener.
- Mixto: videollamada SIP SRTP entre 1XC y un punto final de video de terceros (SIP): los dispositivos de terceros se pueden registrar en URE como con 1XC. Sin embargo, la configuración de PPM, el perfil de usuario o de estación no está disponible para esos dispositivos. Los terminales SIP de terceros pueden incluir hardware de videoconferencia. Estos terminales también incluyen terminales de video compatibles con SRTP que llaman a terminales de video que no son SRTP y viceversa.
- Tercero: videollamada SIP entre terminales de video de terceros (SIP).

REFERIR Manipulación

Cuando el manejo de REFERENCIA está habilitado, Avaya SBCE traduce la solicitud SIP REFER entrante a una solicitud SIP INVITE. El mensaje REFER proviene de la empresa, como Communication Manager o IVR, y Avaya SBCE maneja ese REFER que va hacia el servidor troncal en función de la configuración del perfil de interconexión del servidor troncal. Los siguientes son tres casos de uso para el manejo de REFERENCIA.

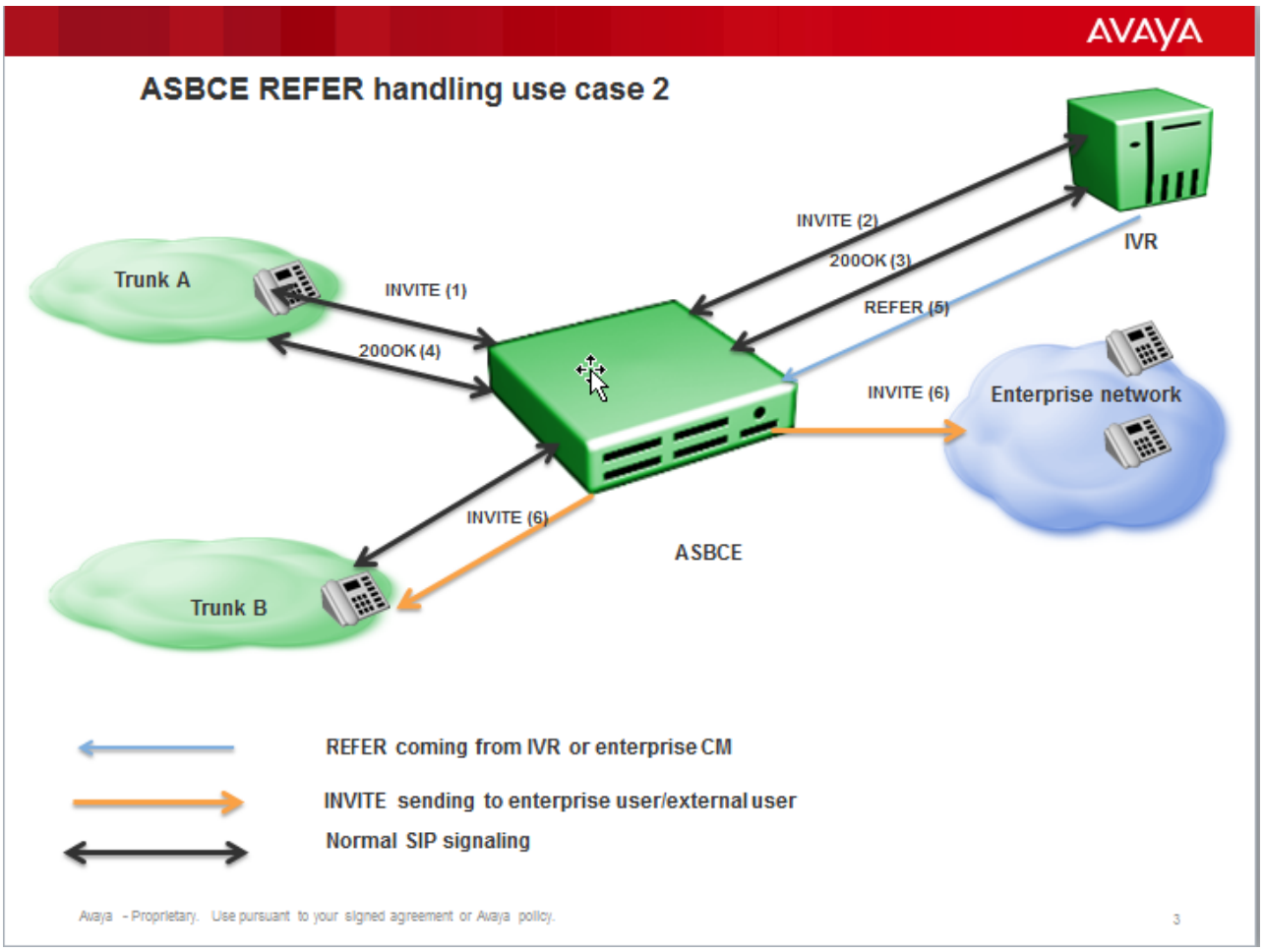
Caso de uso 1

Avaya SBCE utiliza el mensaje REFER y envía una INVITACIÓN de enrutamiento hacia el usuario empresarial.



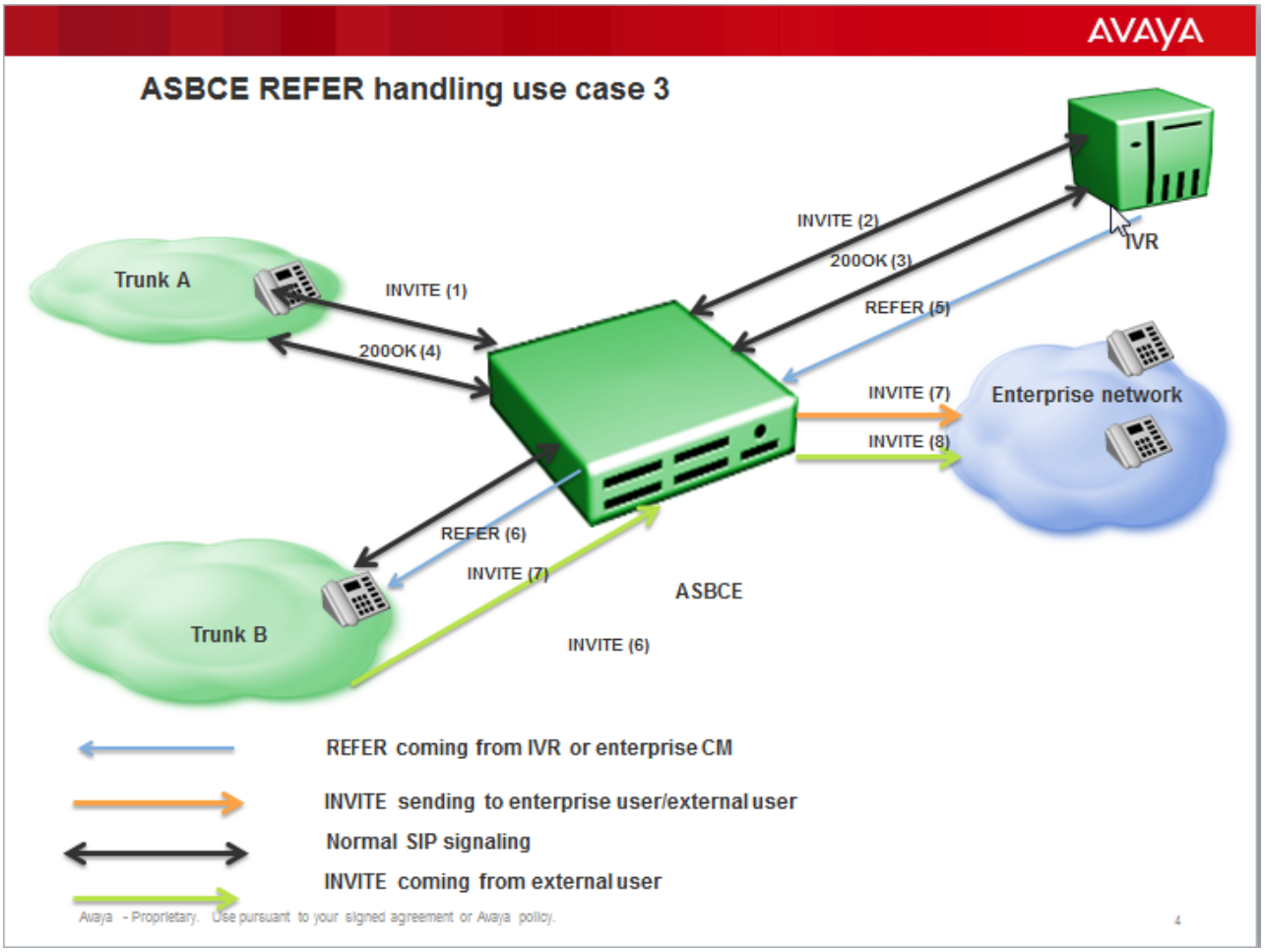
caso de uso 2

Avaya SBCE usa el mensaje REFER para enviar una INVITACIÓN hacia el usuario de troncal o el usuario empresarial en función de los perfiles de enrutamiento creados para enrutar la nueva INVITACIÓN. INVITE creado a partir de REFER se enruta utilizando el enrutamiento basado en URI. Las entradas de enrutamiento deben crearse en el perfil de enrutamiento del servidor troncal para enrutar la solicitud al troncal externo. De forma predeterminada, la solicitud se enruta de nuevo al servidor empresarial. En el modo de transferencia Aura AST2, Avaya SBCE siempre debe enrutar el nuevo INVITE hacia el servidor empresarial, ya que Avaya SBCE no puede encontrar el cuadro de diálogo para reemplazar.



caso de uso 3

Según la configuración del grupo URI en la configuración de manejo de referencias, Avaya SBCE usa algunos mensajes REFER. Dependiendo de la configuración del grupo URI, los mensajes REFER se retransmiten al troncal externo. Los troncales externos generan un nuevo mensaje de INVITACIÓN para los usuarios de destino.



Acceso a múltiples dispositivos

Con la función Acceso a múltiples dispositivos (MDA), un usuario puede acceder a llamadas en múltiples dispositivos de varias capacidades, pero usando el mismo número. Todos los dispositivos del usuario sonarán para una llamada entrante y el usuario puede responder con el dispositivo elegido o un dispositivo móvil emparejado. Una vez que se responde la llamada, los dispositivos restantes dejan de sonar. Si el usuario quiere usar un dispositivo con mejor capacidad, el usuario puede unirse a la llamada existente usando ese dispositivo. Por lo tanto, se crea una conferencia en ACM y el usuario puede desconectar manualmente el dispositivo anterior. Este procedimiento se conoce como traspaso. En el caso de una conferencia alojada en AAC, el último dispositivo MDA que se unió a la llamada permanece activo y todos los dispositivos anteriores se desconectan.

La función de acceso a múltiples dispositivos consiste en que el mismo usuario y la misma extensión usen el mismo AOR para registrar múltiples dispositivos en el Administrador de sesiones. Todos los dispositivos registrados suenan simultáneamente y el dispositivo en el que el usuario toma la llamada se convierte en un dispositivo con la llamada activa. Otros dispositivos MDA emparejados reciben notificación de la llamada activa e información de diálogo. Los dispositivos MDA emparejados pueden unirse a la llamada usando esta información de diálogo. La pantalla muestra una llamada bipartita y no una conferencia. Solo se mantiene una llamada MDA activa para una llamada que involucre AAC.

Manejo de reinvitaciones

Algunos clientes y proveedores de servicios no desean que los mensajes de reinvitación se transmitan al troncal SIP. Avaya SBCE bloquea los mensajes de reinvitación que llegan sin cambios en el Protocolo de descripción de sesión, conocido como Invitaciones de actualización de sesión. La misma regla se aplica a las invitaciones en espera o reanudar sin cambios en SDP, excepto los atributos de puerto, IP y SDP. Los atributos SDP incluyen enviar recepción, enviar solo y solo recibir.

Monitoreo RTCP

La función de monitoreo de RTCP en Avaya SBCE actualiza el paquete de RTCP con la dirección IP del terminal y la información de salto correspondientes. Los terminales están configurados para enviar mensajes RTCPMON al SBCE de Avaya en el que está registrado el terminal. Un único SBCE de Avaya se designa como SBCE central de Avaya y se envía a Prognosis. Avaya SBCE mantiene la asignación de puertos RTCP y actualiza esta asignación por llamada como parte de la señalización SIP. Avaya SBCE implementa una nueva función en la aplicación que tiene la capacidad de rastrear múltiples destinos simultáneamente.

- Se proporcionan API para que la aplicación SIP obtenga la información de ruta de seguimiento para su reutilización posterior al modificar los mensajes RTCPMON.
- La implementación de la función tracerouting de Avaya SBCE reutiliza las API de tracerouting basadas en Linux.
- Los modos de configuración ICMP/UDP/TCP Avaya SBCE pueden usar tracerouting y pueden administrarse desde la GUI.

Al recibir el mensaje RTCPMON para Prognosis, Avaya SBCE realiza una búsqueda en la asignación de puertos RTCP. Luego, Avaya SBCE modifica la dirección IP remota y el puerto RTCP en el mensaje rtcp Subtipo 4 de Avaya, según la asignación. Luego, Avaya SBCE agrega la información de salto de seguimiento del siguiente nodo de red donde los paquetes RTP se reenvían en Avaya Subtipo 5. Si este Avaya SBCE es el núcleo designado de Avaya SBCE, realice pasos adicionales antes de reenviar los paquetes a Prognosis. Determine el campo SSRC de los paquetes de monitoreo RTCP desde el punto final, por ejemplo, SSRC1. Avaya SBCE también determina el SSRC del flujo RTP entrante desde la puerta de enlace de medios o la persona que llama, por ejemplo, SSRC2. Avaya SBCE crea una clave de asignación mediante SSRC1 y SSRC2, si la asignación no existe. La clave de asignación contiene la siguiente información:

- Puerto o dirección IP de origen de medios para SSRC1: se completa a partir del mensaje RTCPMON Subtipo 4.
- Puerto o dirección IP de origen de medios para SSRC2: se completa a partir del mensaje RTCPMON Subtipo 4.
- Información de seguimiento de ruta para todos los saltos desde el extremo [llamador] hasta el Core Avaya SBCE
  - Llenado del mensaje RTCPMON subtipo 5.
- Información de Traceroute para todos los saltos desde el punto final [Callee] hasta el Core Avaya SBCE
  - Llenado del mensaje RTCPMON subtipo 5.

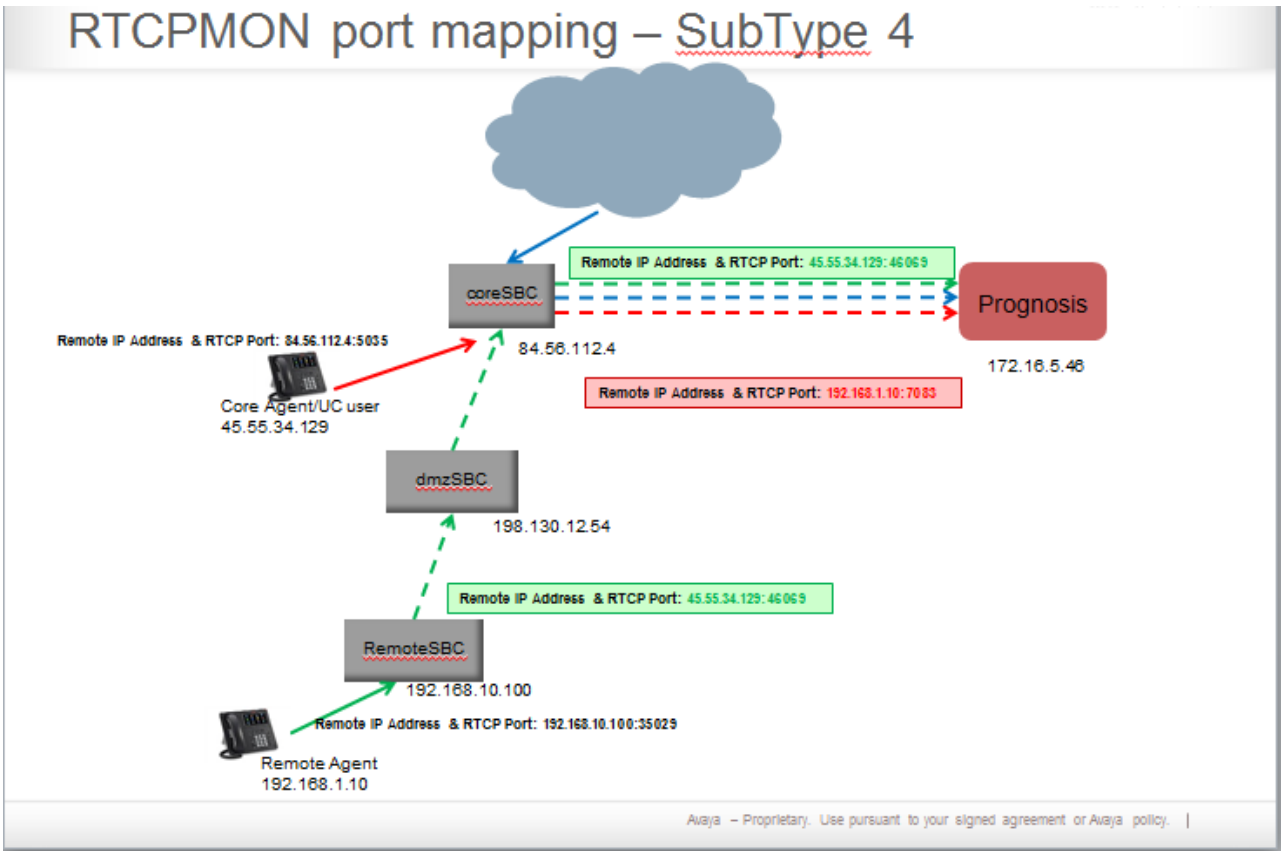
Si existe una asignación en Avaya SBCE para SSRC1 y SSRC2, entonces Avaya SBCE usa la información de asignación para reescribir lo siguiente en los paquetes RTCPMON que se enviarán a Prognosis:

- Subtipo 4 RTCPMON.
- La dirección IP remota/puerto de SSRC1 se establecerá en la dirección IP de origen de medios/puerto de SSRC2 desde la asignación.
- La dirección IP remota/puerto de SSRC2 se establecerá en la dirección IP de origen de medios/puerto de SSRC1 desde la asignación.
- Subtipo 5
- La información de salto de rastreo para SSRC1 incluirá la información de salto de rastreo actual recibida en el paquete RTCPMON más la información de salto de rastreo guardada para SSRC2.
- La información de salto de rastreo para SSRC2 incluirá la información de salto de rastreo actual recibida en el paquete RTCPMON más la información de salto de rastreo guardada para SSRC1.

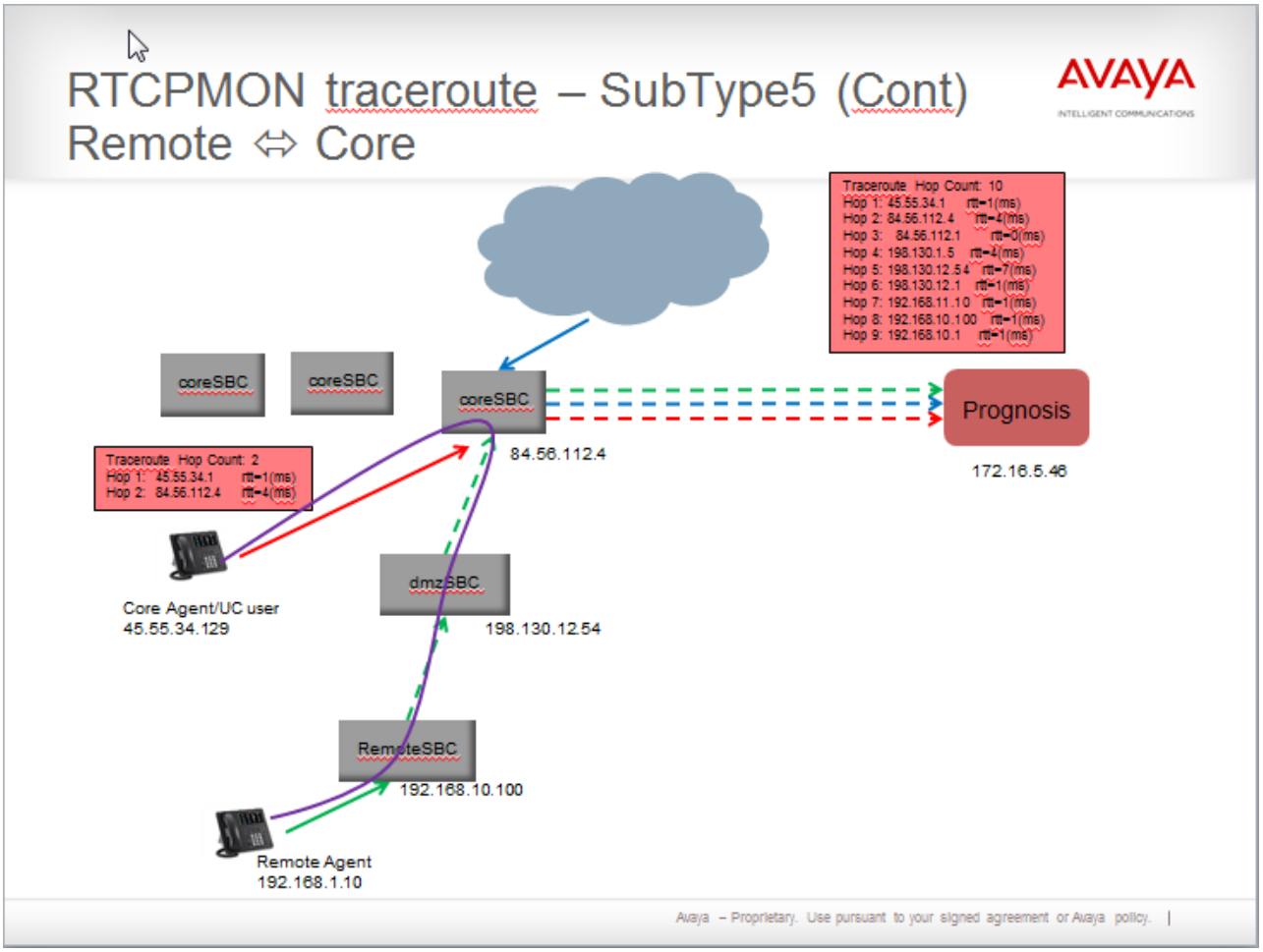
Los paquetes RTCPMON procesados ahora se enviarán a Prognosis según la información completada por Avaya SBCE.

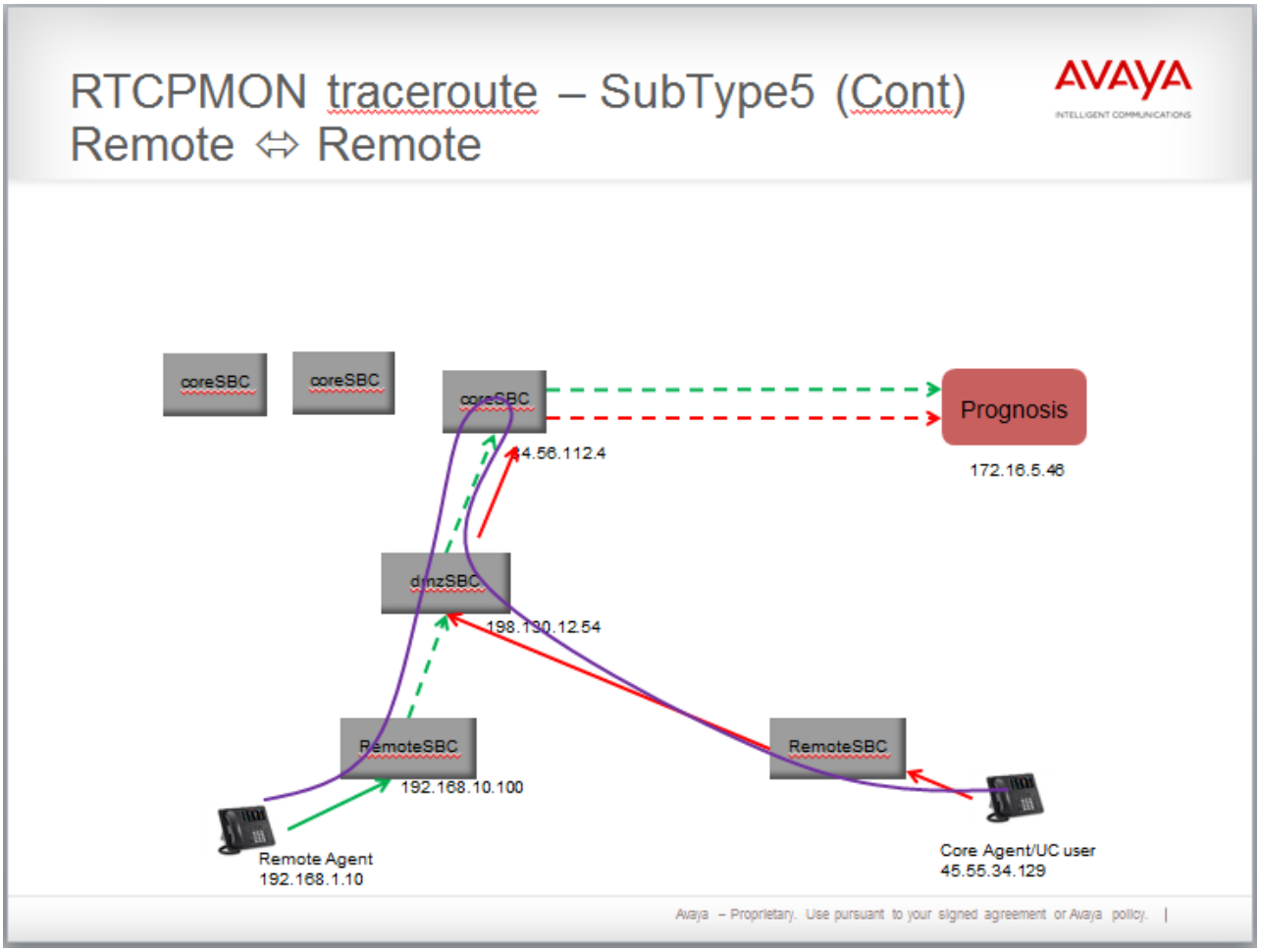
Modos de configuración

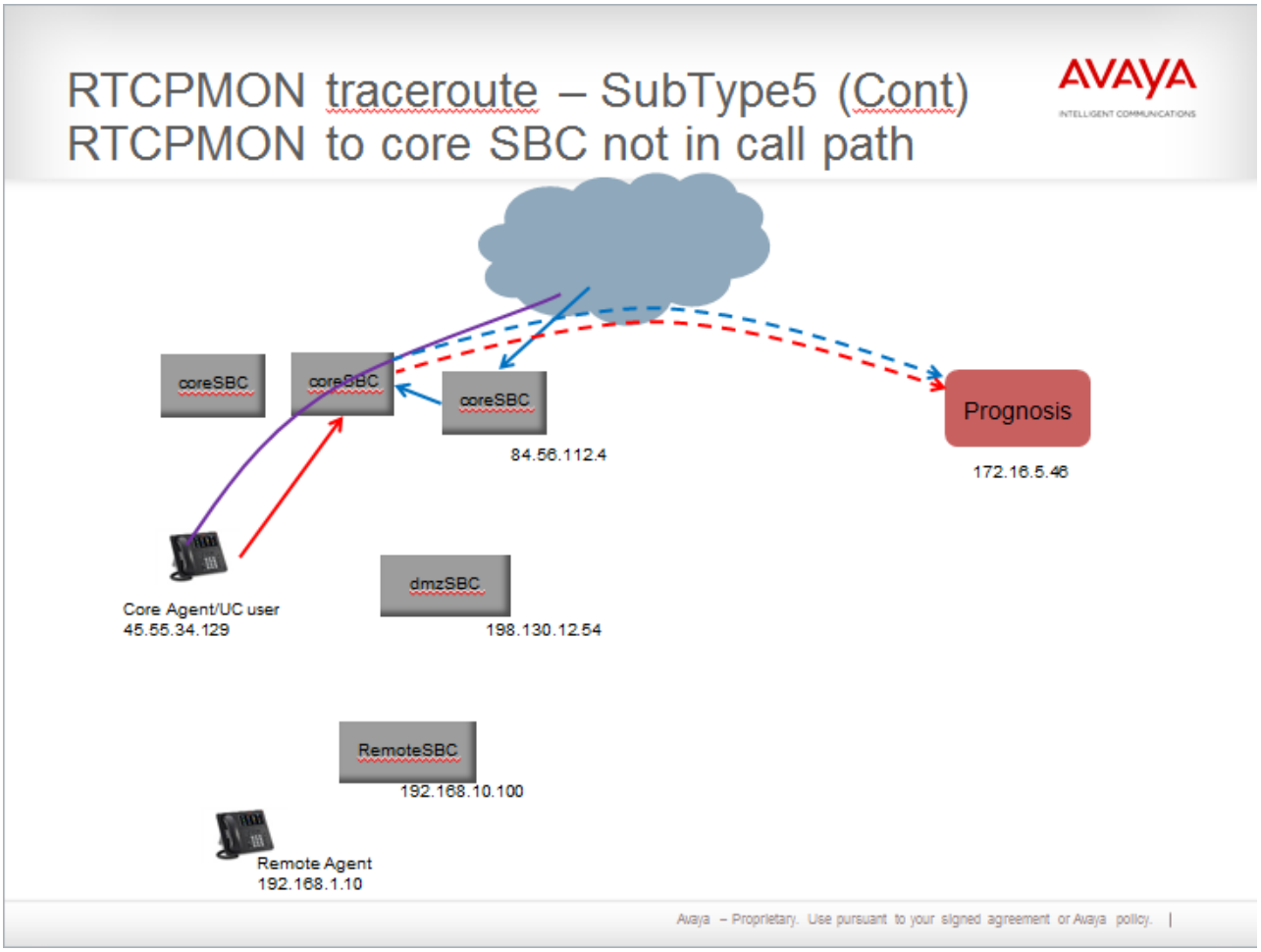
- **Reescritura END-end:**Avaya SBCE actualiza el paquete RTCP subtipo 4 desde el extremo de terminación de medios. En el subtipo 4, Avaya SBCE vuelve a escribir el campo Dirección IP remota con la dirección del extremo remoto que es el destinatario de los paquetes RTCP. La reescritura de extremo a extremo debe configurarse en todos los dispositivos SBCE de Avaya que tienen extremos de terminación de medios conectados directamente. No existe ningún otro dispositivo SBCE de Avaya entre ese dispositivo SBCE de Avaya en particular y los terminales de terminación de medios.



- **Ruta de rastreo Hop-by-Hop:**Avaya SBCE actualiza el paquete RTCP subtipo 5 con la información de la ruta de seguimiento. En el paquete de subtipo 5, Avaya SBCE agrega la ruta de seguimiento hacia la entidad a la que Avaya SBCE reenvía el paquete RTP. Avaya SBCE envía la ruta de rastreo hacia la entidad desde la cual Avaya SBCE recibió el paquete RTP. Debe configurar la ruta de rastreo salto por salto para todos los dispositivos SBCE de Avaya.


RTCPMON traceroute – SubType5 (Cont)
Remote ⇔ Core
AVAYA
INTELLIGENT COMMUNICATIONS
Traceroute Hop Count: 10
Hop 1: 45.55.34.1 rtt=1(ms)
Hop 2: 84.56.112.4 rtt=4(ms)
Hop 3: 84.56.112.1 rtt=0(ms)
Hop 4: 198.130.1.5 rtt=4(ms)
Hop 5: 198.130.12.54 rtt=7(ms)
Hop 6: 198.130.12.1 rtt=1(ms)
Hop 7: 192.168.11.10 rtt=1(ms)
Hop 8: 192.168.10.100 rtt=1(ms)
Hop 9: 192.168.10.1 rtt=1(ms)
coreSBC
coreSBC
coreSBC
84.56.112.4
Prognosis
172.16.5.46
Traceroute Hop Count: 2
Hop 1: 45.55.34.1 rtt=1(ms)
Hop 2: 84.56.112.4 rtt=4(ms)
Core Agent/UC user
45.55.34.129
dmzSBC
198.130.12.54
RemoteSBC
192.168.10.100
Remote Agent
192.168.1.10
Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy.


RTCPMON traceroute – SubType5 (Cont)
Remote ⇔ Remote
AVAYA
INTELLIGENT COMMUNICATIONS
coreSBC
coreSBC
coreSBC
Prognosis
172.16.5.48
4.56.112.4
dmzSBC
198.190.12.54
RemoteSBC
192.168.10.100
RemoteSBC
Remote Agent
192.168.1.10
Core Agent/UC user
45.55.34.129
Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy.



- **Puente:**Avaya SBCE elimina las rutas de rastreo inversas agregadas por la ruta de rastreo Hop-by-Hop y agrega estos datos al paquete RTCP subtipo 5 que proviene del lado opuesto.
  El puente debe configurarse solo en dispositivos CORE Avaya SBCE.

Nota:

Si una solución incluye solo un SBCE de Avaya, se requieren todas estas configuraciones.

Generación de informes de monitoreo de RTCP

A partir de la versión 7.2.1 y posteriores, Avaya SBCE es compatible con la función de generación de informes de monitoreo de RTCP.

Avaya SBCE recibe flujos RTCP de un enlace troncal que no tiene ninguna información de control específica de Avaya como la presente en los terminales de Avaya

Avaya SBCE genera un informe de monitoreo de RTCP que utiliza esta función. Debe configurar Avaya SBCE con la dirección IP del servidor de monitoreo RTCP para enviar los datos generados

Esta característica es aplicable solo para troncales SIP.

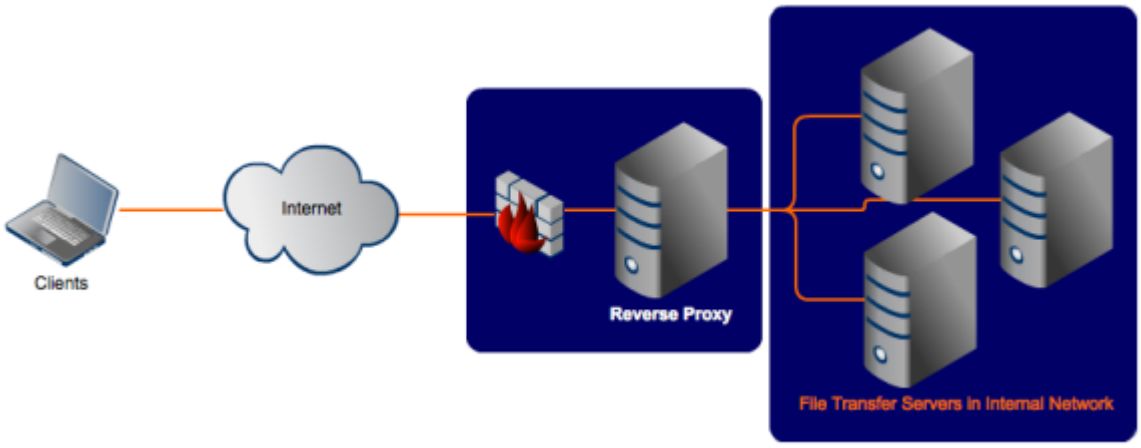
proxy inverso

Un proxy inverso es un servidor web que finaliza las conexiones con los clientes y realiza nuevas conexiones a los servidores back-end en su nombre.

Un servidor backend se define como un servidor al que el proxy inverso establece una conexión para cumplir con la solicitud del cliente. Estos servidores back-end pueden tomar varias formas y el proxy inverso se puede configurar de manera diferente para manejar cada uno de ellos.

Un proxy inverso también se conoce como proxy de entrada, porque el servidor recibe solicitudes de Internet y las reenvía o las envía a un pequeño conjunto de servidores. Los servidores suelen estar ubicados en una red interna y no se puede acceder a ellos directamente desde el exterior. Este proxy es inverso, porque un proxy tradicional o de salida recibe solicitudes de un pequeño conjunto de clientes en una red interna y las reenvía a Internet.

El siguiente diagrama ilustra la configuración típica del proxy inverso para servidores de transferencia de archivos.



Ventajas de los proxy inversos

• Seguridad:

Un proxy inverso puede ocultar la topología y las características de los servidores backend al eliminar la necesidad de acceso directo a Internet a ellos. Puede colocar su proxy inverso en una DMZ orientada a Internet, pero ocultar sus servidores web dentro de una subred no pública.

• Almacenamiento en caché:

El proxy inverso también puede actuar como caché. Puede tener un caché tonto que caduque después de un período determinado, o mejor aún, un caché que respete los encabezados Cache-Control y Expires. Esto puede reducir considerablemente la carga en los servidores backend.

• Compresión:

Para reducir el ancho de banda necesario para las solicitudes individuales, el proxy inverso puede descomprimir las solicitudes entrantes y comprimir las salientes. Esto reduce la carga en los servidores backend que, de otro modo, tendrían que comprimir las solicitudes salientes. El proxy inverso facilita la depuración de solicitudes y respuestas de los servidores backend.

• Simplifica las tareas de control de acceso:

Los clientes solo tienen un único punto de acceso, puede concentrar el control de acceso en ese único punto.

• Agregar varios sitios web en el mismo espacio de URL:

En una arquitectura distribuida, diferentes piezas de funcionalidad pueden ser atendidas por componentes aislados. Un proxy inverso puede enrutar diferentes ramas de un solo espacio de direcciones URL a diferentes servidores web internos.

• URL de solicitud de reescritura:

A veces, el esquema de URL que presenta una aplicación heredada no es ideal para el descubrimiento o la optimización de motores de búsqueda. Un proxy inverso puede reescribir las URL antes de pasarlas a sus servidores backend.

• Autenticación:

El proxy inverso puede usar certificados de cliente para verificar la identidad del cliente.

• Lista blanca de usuarios:

La lista blanca se puede usar para bloquear o permitir que un conjunto específico de direcciones IP de usuario use el servicio de proxy inverso. Por ejemplo, si agrega una dirección IP de usuario incluida en la lista blanca, se deniega el acceso a todas las direcciones IP que no sean la IP incluida en la lista blanca para usar el servicio de proxy inverso.

• Terminación SSL:

El proxy inverso maneja las conexiones HTTPS entrantes, descifra las solicitudes y pasa las solicitudes sin cifrar a los servidores web. Esto tiene varios beneficios:

- Elimina la necesidad de instalar certificados en muchos servidores web back-end.

- Proporciona un único punto de configuración y gestión para SSL/TLS.

- Quita la carga de procesamiento de cifrar o descifrar el tráfico HTTPS de los servidores web.

- Facilita la prueba e interceptación de solicitudes HTTP a servidores web individuales.

Control de cámara del extremo lejano

Avaya SBCE es compatible con Oferta y respuesta de FECC en SDP. Avaya SBCE verifica si la línea de la aplicación de medios usa el códec H.224. Cualquier otra línea de aplicación de medios sin un tipo de códec H.224 se ignora.

Avaya SBCE no negocia el SDP de oferta y respuesta para la línea de aplicación de medios Far End Camera Control (FECC). El intercambio y la negociación de oferta y respuesta se realiza de extremo a extremo entre el remitente y el receptor. Avaya SBCE no admite el cifrado mixto porque FECC está vinculado a las reglas de medios. Por lo tanto, FECC está encriptado si el video principal está encriptado. De manera similar, FECC está en RTP si el video principal está en RTP. Si no se negocia FECC en oferta y respuesta de extremo a extremo, el canal de video principal funciona sin FECC.

Avaya SBCE aplica el cifrado de acuerdo con la política SDP Capability Negotiation y SDES by Avaya SBCE.

Protocolo de control de piso binario

Para proporcionar una presencia continua durante las videoconferencias, las aplicaciones utilizan la técnica de video conmutado o de video mixto y conmutado.

Aura de Avaya®Las conferencias utilizan la técnica de video conmutado para proporcionar una presencia continua. Los flujos de video se transmiten a todos los participantes para que cada participante reciba los flujos de video múltiples correspondientes desde los extremos remotos. Avaya Scopia®utiliza la técnica de video mixto donde se mezcla un solo flujo de medios de video para todos los usuarios participantes.

A través del canal de video, uno de los flujos de presencia continua brinda información sobre la presentación además del video principal. El canal de presentación es a través de la web y no a través de un canal de vídeo. Los flujos de video conmutados usan solo un canal de video de presentación para múltiples flujos de medios de video principales para cada participante. Los dispositivos de video mixto usan un flujo de medios de video para la presentación. El flujo de medios de video principal muestra a los participantes en un cuadro. El control de palabra de este canal de video de presentación es mediante mensajes del Protocolo de control de palabra binaria (BFCP).

Los mensajes BFCP controlan cómo varias transmisiones de video acceden y usan el canal de video compartido.

Descripción detallada del protocolo de control de piso binario

En una conferencia, algunas aplicaciones controlan el acceso a un conjunto compartido de recursos. Con BFCP, estas aplicaciones brindan a los usuarios acceso coordinado a los recursos.

Terminologías

Para comprender cómo funciona BFCP, debe estar familiarizado con los siguientes términos:

- **Piso**: un permiso temporal para acceder a un recurso compartido específico o a un conjunto de recursos.
- **Silla de piso**: Una entidad lógica que administra un piso.
- **control de piso**: Un mecanismo que permite que las aplicaciones o los usuarios obtengan acceso compartido o exclusivo al recurso.
- **Servidor de control de piso**: Una entidad lógica que mantiene el estado del piso, incluidos detalles como qué pisos existen y quién tiene un piso.
- **participante de piso**: Una entidad lógica que solicita pisos e información relacionada de un servidor de control de piso. En conferencias controladas por el piso, un participante del piso puede estar ubicado junto con un participante de los medios.

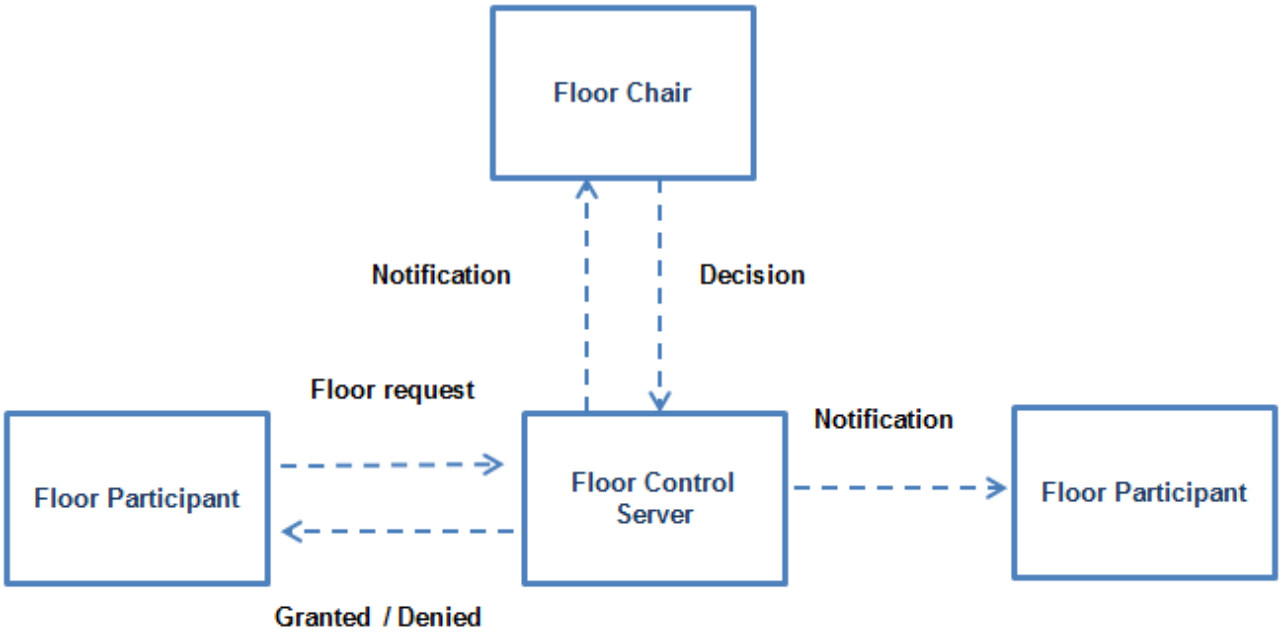


Figura 8: componentes de BFCP

Funcionamiento de BFCP

Con BFCP, los participantes de la sala pueden enviar solicitudes de sala a los servidores de control de la sala y los servidores de control de la sala pueden conceder o denegar el acceso al recurso solicitado. Además, los servidores de control de piso pueden mantener informados a los participantes y presidentes de piso sobre el estado de un piso determinado o una solicitud de piso determinada.

Avaya SBCE transmite mensajes de control BFCP para controlar el canal de presentación. Avaya SBCE admite BFCP solo para dos canales de video, uno de los cuales es un canal de presentación de video.

En esta versión, Avaya SBCE admite TCP y UDP para la aplicación BFCP.

Avaya SBCE negocia con Avaya Scopia®MCU o Avaya Scopia®clientes XT y obtiene el valor del atributo setup como pasivo. Luego, el otro extremo inicia la conexión TCP para la aplicación BFCP. Si Avaya SBCE no puede negociar el atributo de configuración, Avaya SBCE inicia la conexión TCP. Sin embargo, si la conexión no se establece debido a las restricciones del cortafuegos, el otro extremo establece la conexión TCP. Todos los atributos conocidos, como control de piso, id de confianza, id de usuario e id de piso, también se transmiten en SDP.

Reglas de intercambio de oferta y respuesta de SDP

Los participantes y el servidor de control de la sala utilizan las reglas de intercambio de oferta y respuesta de SDP para establecer y autenticar la conexión BFCP. Avaya SBCE no juega ningún papel en el establecimiento o restablecimiento de la conexión y la autenticación.

Avaya SBCE negocia la oferta y responde SDP para BFCP según las siguientes reglas:

- Avaya SBCE recibe una oferta en el tramo entrante con el atributo de configuración como actpass o activo. Avaya SBCE responde con el atributo de configuración como pasivo con un parámetro de puerto válido en la línea de la aplicación BFCP.

- Avaya SBCE envía una oferta con el atributo de configuración como pasivo en el tramo saliente. La entidad remota responde con el atributo de configuración como activo con el parámetro de puerto descartado en la línea de aplicación BFCP.
- Avaya SBCE recibe una oferta en el tramo entrante con el atributo de configuración como pasivo. Avaya SBCE responde con el atributo de configuración como activo con un parámetro de puerto válido en la línea de aplicación BFCP. Avaya SBCE intenta iniciar la conexión TCP según lo indica el atributo de configuración como activo. La entidad del extremo lejano inicia la conexión TCP en la misma conexión después del tiempo de espera.
- Avaya SBCE recibe una oferta con el atributo de conexión como nuevo. Avaya SBCE responde con un atributo de conexión como nuevo.
- Avaya SBCE recibe una oferta con el atributo de conexión como existente. Avaya SBCE responde con un atributo de conexión como existente.
- Avaya SBCE inicia una oferta en el tramo saliente con el atributo de conexión como nuevo para todos los casos.

Avaya SBCE transmite otros atributos de la aplicación BFCP, como floor-ctrl, label, floorid, confid e userid. Avaya SBCE negocia estos parámetros de atributo para la conexión de extremo a extremo.

Arquitectura del protocolo de control de piso binario

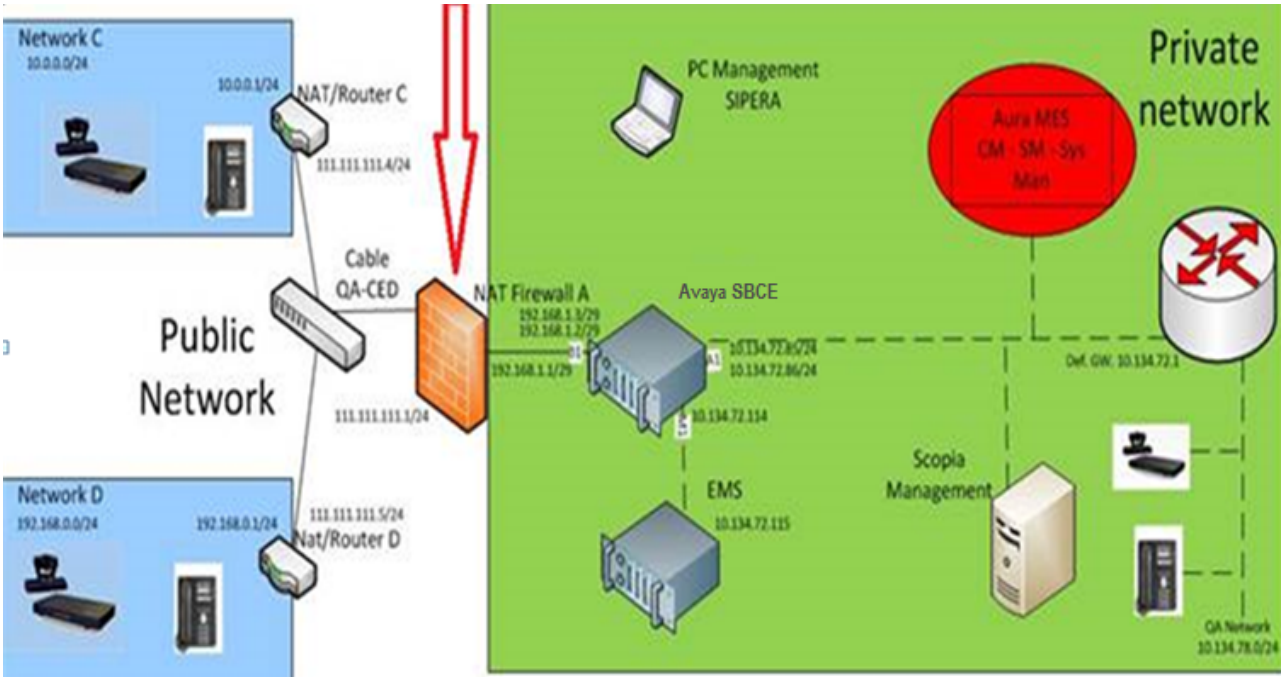


Figura 9: arquitectura BFCP

Existe un firewall interno en la mayoría de las instalaciones en la interfaz A1, que es la interfaz privada hacia la empresa. El diagrama muestra un cortafuegos externo en la interfaz B1.

Escenarios de protocolo de control de piso binario

Ejemplos de escenarios en los que se utiliza BFCP y los mensajes de oferta y respuesta para cada escenario.

Remote Worker XT-cliente llama XT-MCU

No Señor	Remitente	Floor-ctrl	Atributo de configuración	Conexión	BFCP línea de aplicación
1	Trabajador remoto cliente XT	solo c	actuar pasar	nuevo	Conexión válida y puerto
2	Avaya SBCE	solo c	pasivo	nuevo	Conexión válida y puerto
3	XT-MCU	s-solo	activo	nuevo	Puerto descartado. por ejemplo, 9
4	Avaya SBCE (responde a Trabajador remoto cliente XT)	s-solo	pasivo	nuevo	Conexión válida y puerto

Los mismos parámetros se intercambian cuando un cliente de Remote Worker XT llama a Elite-MCU.

Remote Worker XT-MCU llama al cliente XT interno

No Señor	Remitente	piso-ctrl	atributo de configuración	conexión	BFCP solicitud línea
1	Trabajador remoto XT-MCU	cs	actuar pasar	nuevo	Válido conexión y Puerto
2	Avaya SBCE	cs	pasivo	nuevo	Válido conexión y Puerto
3	cliente XT	solo c	activo	nuevo	Puerto descartado
4	Avaya SBCE	solo c	pasivo	nuevo	Válido conexión y Puerto

XT-MCU interno a la empresa marca y llama al cliente XT, que es un trabajador remoto

No Señor	Remitente	piso-ctrl	atributo de configuración	conexión	BFCP solicitud línea
1	XT-MCU	cs	actuar pasar	nuevo	Válido conexión y Puerto
2	Avaya SBCE	solo c	pasivo	nuevo	Válido conexión y Puerto
3	trabajador remoto cliente XT	solo c	activo	nuevo	Puerto descartado

La tabla continúa...

No Señor	Remitente	piso-ctrl	atributo de configuración	conexión	BFCP solicitud línea
4	Avaya SBCE responde a XT-UCM	solo c	pasivo	nuevo	Válido conexión y Puerto

Elite-MCU versión 8.3 interno a la empresa marca y llama a XT-Client, que es un trabajador remoto

No Señor.	Remitente	piso-ctrl	atributo de configuración	conexión	BFCP solicitud línea
1	Élite-MCU	s-solo	pasivo	nuevo	Válido conexión y Puerto
2	Avaya SBCE	s-solo	pasivo	nuevo	Válido conexión y Puerto
3	trabajador remoto cliente XT	solo c	activo	nuevo	Puerto descartado
4	Avaya SBCE responde a UCM de élite	solo c	activo	nuevo	Válido conexión y Puerto

Después de que Avaya SBCE responde a Elite MCU, Avaya SBCE no inicia ninguna conexión TCP hacia Elite MCU 8.3. Elite MCU 8.3 agota el tiempo de espera e intenta establecer una conexión TCP.

Conmutación por error o interrupción de la red

En una conmutación por error o interrupción de la red, una entidad intenta restablecer una conexión TCP en la conexión existente. Si la entidad falla, Avaya Scopia®no vuelve a establecer la conexión.

Corrección de errores de reenvío

El video sobre IP requiere un alto ancho de banda. La transmisión de datos de video a través de canales de comunicación no confiables puede provocar la pérdida de paquetes y errores. La corrección de errores de reenvío (FEC) es un mecanismo para controlar la pérdida de paquetes y los errores en la transmisión de datos a través de la red IP. El remitente codifica los mensajes de forma redundante utilizando el código de corrección de errores. La función de redundancia permite que el receptor detecte errores y corrija los errores sin retransmisión. Este mecanismo es útil cuando la comunicación es unidireccional y tiene múltiples receptores.

El mecanismo FEC utiliza los esquemas FEC definidos en RFC 5445, el componente básico FEC definido en RFC 5052 y la señalización SDP definida en RFC 5109. Avaya Scopia®utiliza la señalización SDP patentada y los bloques y esquemas de construcción FEC, que no son compatibles con el estándar IETF.

FEC detecta errores y protege el video principal pero no protege los datos de los canales de audio. FEC también se aplica a los códecs de video H264/SVC.

Registro de usuario

Desde Avaya SBCE versión 6.3, puede ver la lista de usuarios que están registrados a través de Avaya SBCE en la**Registros Estado**columna en la página Registros de usuarios. También puede ingresar criterios de búsqueda personalizados para los campos que se muestran en el sistema.

Estado del servidor SIP en tiempo real

Avaya SBCE versión 6.3 en adelante, puede ver el estado actual de los servidores SIP configurados. El sistema muestra el estado de conectividad de los servidores troncales y los servidores de llamadas empresariales. Puedes usar el**El estado del servidor**opción de la**Estado**barra de herramientas para ver el estado de la conexión. La pantalla Estado del servidor muestra la lista de servidores según la configuración de la pantalla Configuración del servidor.

Para que los servidores aparezcan en la ventana Estado, debe configurar el latido del servidor en Configuración del servidor.

Requisitos de licencia

Avaya SBCE usa WebLM para los requisitos de licencia. Puede instalar el archivo de licencia SBCE de Avaya en el Sistema de administración de elementos (EMS) mediante la página Administración del sistema. Asegúrese de que el archivo de licencia del servidor WebLM muestre el código de producto Session Border Controller E AE. Antes de configurar el archivo de licencia, puede ver el**Estado de la licencia**,**Estado del período de gracia**, y **Fecha de vencimiento del período de gracia**campos en la página Panel. Para instalar un archivo de licencia en un EMS recién instalado o actualizado, tiene un período de gracia de 30 días desde el día de la instalación o actualización.

El archivo de licencia contiene la siguiente información:

- Nombre del producto
- Versión de software compatible
- Fecha de caducidad
- Identificación del anfitrión

  El ID de host principal de WebLM se usa para crear el archivo de licencia.
- Funciones con licencia
- Capacidad con licencia

Todos los dispositivos de hardware Avaya SBCE pueden usar un servidor WebLM local para las licencias. Sin embargo, para entornos de implementación mixtos con EMS en VMware y Avaya SBCE en hardware, use un servidor WebLM instalado en VMware o System Manager WebLM.

Avaya SBCE admite licencias agrupadas. A diferencia de la asignación de licencias estáticas, Avaya SBCE reserva y anula la reserva de forma dinámica de licencias agrupadas cuando es necesario. Por ejemplo, los clientes con varios dispositivos SBCE de Avaya pueden usar un conjunto de licencias dinámicamente en los dispositivos según sea necesario.

Inicio de sesión único y motor de identidad

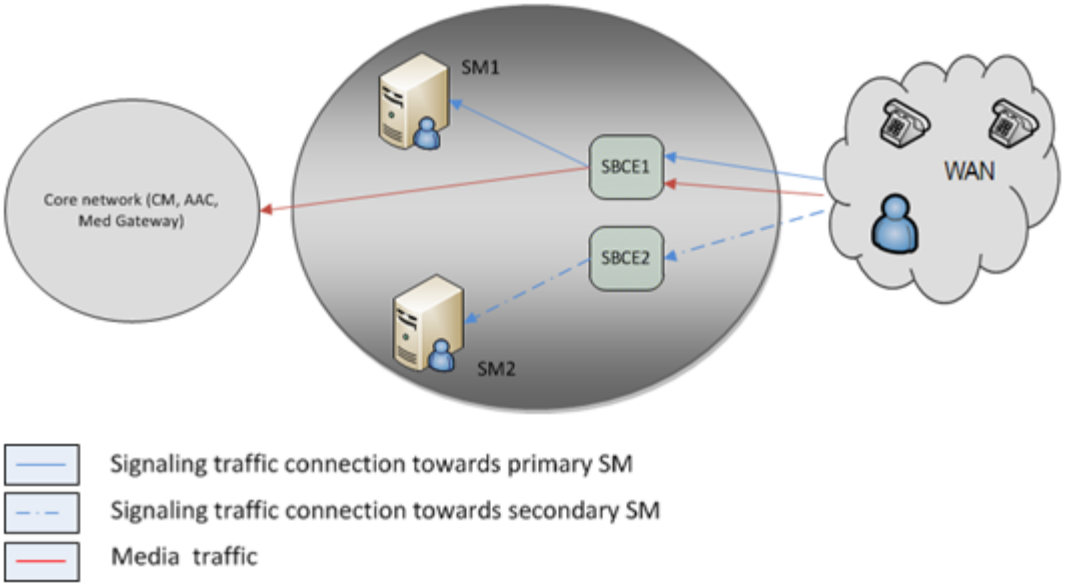
Avaya SBCE utiliza DNS dividido para la función Single Sign-On y Identity Engine. En una infraestructura DNS dividida, los hosts internos se dirigen a un servidor de nombres de dominio interno para la resolución de nombres. Los hosts internos resuelven el dominio IDE en una dirección de servidor IDE. Los hosts externos se dirigen a un servidor de nombres de dominio externo para la resolución de nombres. Los hosts externos resuelven el dominio IDE en una dirección externa de Avaya SBCE.

Implementación múltiple de Avaya SBCE

En una implementación con redundancia geográfica, puede implementar dos dispositivos Avaya SBCE diferentes en dos centros de datos diferentes. Puede implementar los dispositivos como dispositivos Avaya SBCE individuales o dispositivos administrados por su propio EMS. Puede implementar estos dispositivos SBCE de Avaya en un modo de alta disponibilidad o en un modo que no sea de alta disponibilidad.

Implementación múltiple de Avaya SBCE en el modo no HA

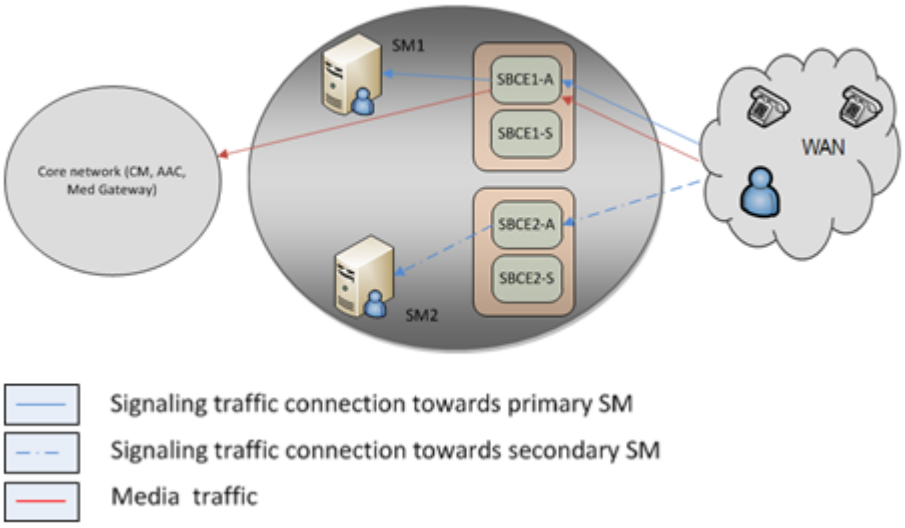
En el siguiente diagrama, SBCE1 y SBCE2 son dos dispositivos físicos diferentes implementados en diferentes centros de datos. Los puntos finales tienen una conexión con SBCE1 correspondiente al Administrador de sesión principal, SM1. La segunda conexión con SBCE2 corresponde al Session Manager secundario, SM2.



Implementación múltiple de Avaya SBCE en el modo HA

En el siguiente diagrama, SBCE1 y SBCE2 son dos dispositivos físicos diferentes que se implementan en modo HA en diferentes centros de datos. Los puntos finales tienen una conexión con SBCE1-A, que es SBCE activo correspondiente al administrador de sesión principal, SM1. La segunda conexión es con SBCE2-A, SBCE Activo correspondiente al Administrador de Sesión secundario, SM2.

Durante una conmutación por error de SBCE1-A, SBCE1-S, que es el SBCE de Avaya en espera, maneja los medios de las llamadas activas. Durante una conmutación por error de SBCE2-A, SBCE2-S, que es el SBCE de Avaya en espera, maneja los medios de las llamadas activas.



Gestión de llamadas habilitada para WebRTC

Avaya SBCE admite llamadas entrantes desde navegadores web habilitados para WebRTC a un Avaya Aura interno®red con SIP en el núcleo. Por ejemplo, un consumidor puede llamar a un Avaya Aura®red mediante el uso de un navegador habilitado para WebRTC desde una red externa. Esta llamada WebRTC es posible si la organización divulga el sitio web de la organización para llamadas multimedia en tiempo real y habilita el navegador con API para la comunicación multimedia en tiempo real. La señalización y los medios atraviesan el límite de la red empresarial que contiene el firewall y Avaya SBCE en DMZ. En este escenario, Avaya SBCE, Avaya Breeze™y Avaya Aura®Media Server juntos funcionan como la puerta de enlace WebRTC-SIP. La señalización y los medios deben atravesar el límite de la red empresarial. Avaya SBCE retransmite la señalización HTTP mediante la función de proxy inverso y la retransmisión de medios mediante la funcionalidad de retransmisión del servidor TURN. Además, para una llamada WebRTC, se requieren enlaces STUN, descubrimiento reflexivo de direcciones STUN y comprobaciones de conectividad ICE. Todos estos aspectos se implementan dentro de la funcionalidad del servidor TURN/STUN integrada en Avaya SBCE.

A partir de la versión 7.2.1 y posteriores, un navegador habilitado para WebRTC admite NAT simétrica y varias direcciones IP.

A partir de la versión 7.2.2 y posteriores, Avaya SBCE admite TURN mediante la indicación SEND o DATA y la señalización TURN en TCP, TLS y UDP.

Para obtener información sobre el rendimiento y la capacidad de WebRTC, consulte*Referencia del complemento WebRTC de Avaya*.

Descripción general de la arquitectura de virtualización

Para la implementación en hardware certificado por VMware, Avaya SBCE se empaqueta como vAppliance Ready (OVA) para ejecutarse en el entorno virtualizado. Por lo tanto, a partir de la versión 6.3, Avaya SBCE también está disponible para implementaciones basadas en VMware.

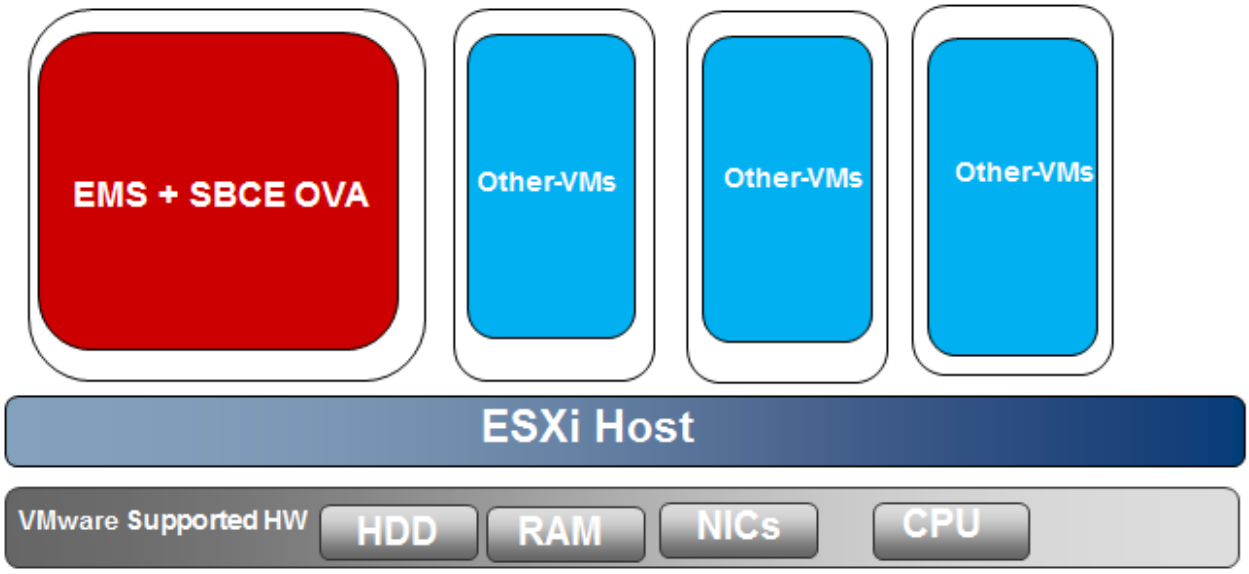
A partir de la versión 7.0, un solo archivo OVA está disponible para implementar EMS y Avaya SBCE.

Avaya SBCE es compatible con las funciones de VMware, como vMotion, HA en los centros de datos y configuraciones de hardware mixtas.

Los archivos Avaya SBCE OVA se ofrecen como vAppliance para configuraciones de EMS y Avaya SBCE. El archivo .ova está disponible en el Sistema de entrega y licencia de productos (PLDS).

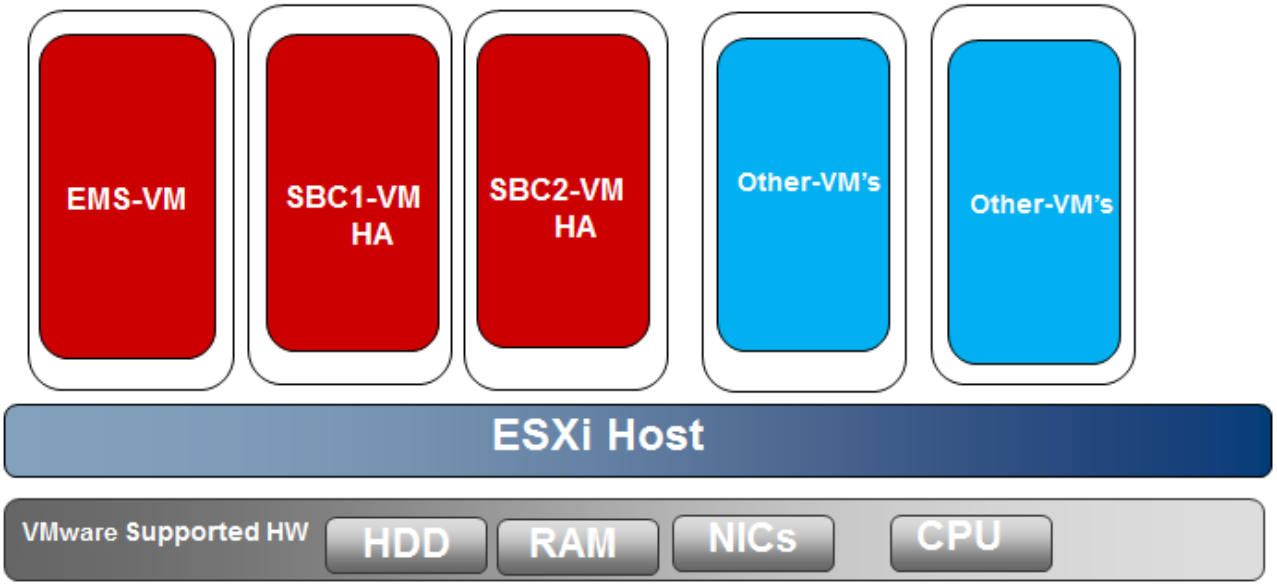
Modo independiente Avaya SBCE

Si selecciona una implementación independiente, el archivo OVA instala configuraciones para Avaya SBCE y EMS.



EMS y SBC en modo de alta disponibilidad (HA)

Para el modo HA, implemente el archivo OVA por separado para EMS y Avaya SBCE. Desde la versión 7.0, un solo archivo OVA está disponible para implementar EMS y Avaya SBCE. Por lo tanto, puede usar el mismo archivo OVA, pero elegir diferentes configuraciones para implementar EMS y Avaya SBCE.



Para más información, ver *Implementación de Avaya Session Border Controller para empresas en un entorno virtualizado*.

LAN virtuales

Una red de área local virtual (VLAN) es un grupo lógico de elementos de red, como estaciones de trabajo, servidores y dispositivos de red que abarcan varias redes físicas. Una VLAN superpone una red virtual de capa 2 sobre una red física de capa 2 insertando una etiqueta VLAN en el encabezado de capa 2 de un paquete. Los dispositivos de red compatibles con VLAN, como los conmutadores, pueden enviar paquetes a través de la superposición de VLAN.

Etiquete una VLAN para identificar claramente la VLAN como parte de una red de capa 2 lógicamente diferente.

El primer paso para el etiquetado de VLAN es crear una interfaz de VLAN. Los paquetes que salen y entran de Avaya SBCE en una VLAN usan un enlace físico conectado a una interfaz física.

El segundo paso es configurar todas las redes a las que se conecta Avaya SBCE. Cada red a la que se conecta Avaya SBCE está definida y conectada a una interfaz.

Nota:

Se admite una VLAN en la interfaz de datos y señalización.

Descripción general de SRTP

Avaya SBCE admite audio encriptado y múltiples medios de video, como video principal, presentación de video y Control de cámara del extremo lejano (FECC) basado en la negociación de capacidad SDP.

Si la entidad del extremo lejano no admite el cifrado SRTP, Avaya SBCE convierte un tramo de la llamada como RTP y el otro tramo como SRTP mediante la negociación SDP. La conversión entre los tramos de origen y destino depende de la política de cifrado administrada en Avaya SBCE.

Avaya SBCE no utiliza Master Key Index (MKI) ni RTCP encriptado para Avaya Scopia® interoperabilidad Avaya SBCE negocia la sesión SDP mediante RTCP sin cifrar.

Nota:

Avaya SBCE admite llamadas SRTP a través de SIP, pero Avaya Aura®admite llamadas SRTP solo cuando la llamada utiliza el protocolo TLS.

Consideraciones de SRTP

Avaya SBCE admite:

1. Retroceso de SRTP a RTP debido a una limitación de ancho de banda o un cambio en la topología de la llamada, como un servidor de medios que no admite SRTP y la aplicación de música en espera.
2. Actualice de RTP a SRTP.
3. Conversión de RTP a SRTP entre los tramos de origen y destino después de la conmutación por error.
4. Modificación de claves mediante REINVITE.
5. Retroceso de RTP a SRTP después de la conmutación por error.

Múltiples subredes y múltiples interfaces

Múltiples subredes

Con Avaya SBCE, los clientes pueden conectarse a múltiples subredes desde una sola interfaz. Avaya SBCE admite varias direcciones IP para cada subred y una puerta de enlace de siguiente salto única para cada dirección IP. Por lo tanto, puede tener varias subredes en la misma interfaz. La interfaz puede ser una interfaz física o VLAN.

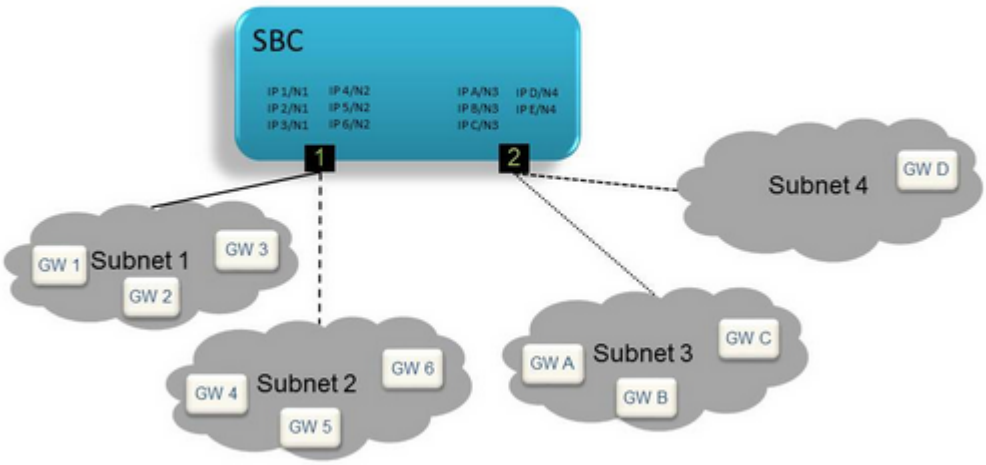


Figura 10: Conectividad a varias subredes en una sola interfaz de datos

EnFigura 10: Conectividad a varias subredes en una sola interfaz de datos en la página 49, se puede acceder a las subredes 1 y 2 a través de la interfaz 1, mientras que a las subredes 3 y 4 se puede acceder a través de la interfaz 2.

Espacios de direcciones superpuestos

Puede usar varias subredes para configurar implementaciones basadas en la nube y multiusuario. En tales configuraciones, Avaya SBCE se conecta a dos o más redes físicamente distintas que comparten parte o todo el espacio de direcciones IP. Cuando configura espacios de direcciones superpuestos, varios terminales con la misma dirección IP pueden conectarse simultáneamente a Avaya SBCE. Sin embargo, Avaya SBCE puede distinguir entre las conexiones. Aunque varios puntos finales usan la misma dirección IP, las redes en las que residen los puntos finales son físicamente distintas. Avaya SBCE se conecta a las redes físicamente distintas mediante el uso de direcciones IP únicas en cada espacio de direcciones superpuestas.

Soporte de VLAN

Con la capacidad de LAN virtual (VLAN), una red virtual de capa 2 puede superponerse en una red física de capa 2 insertando una etiqueta VLAN en el encabezado de capa 2 del paquete. Los dispositivos de red compatibles pueden cambiar dichos paquetes a través de la superposición de VLAN. En esta versión, Avaya SBCE admite VLAN solo en las interfaces de datos.

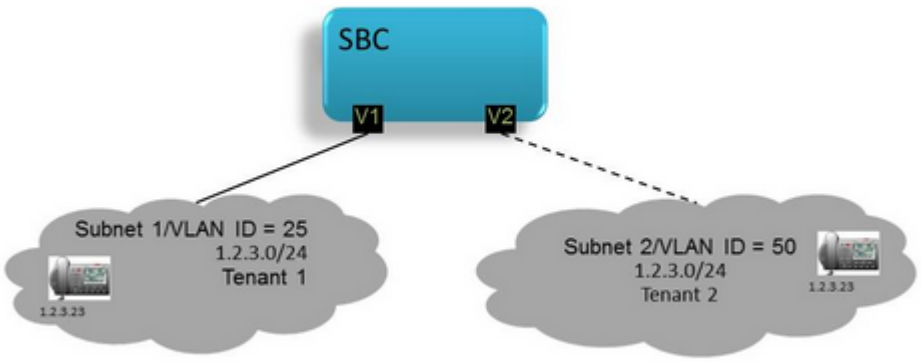


Figura 11: compatibilidad con VLAN

Ejemplos de implementación

Avaya SBCE conectado a múltiples subredes en una sola interfaz

En este escenario, Avaya SBCE se conecta a varias subredes en la misma interfaz de datos.

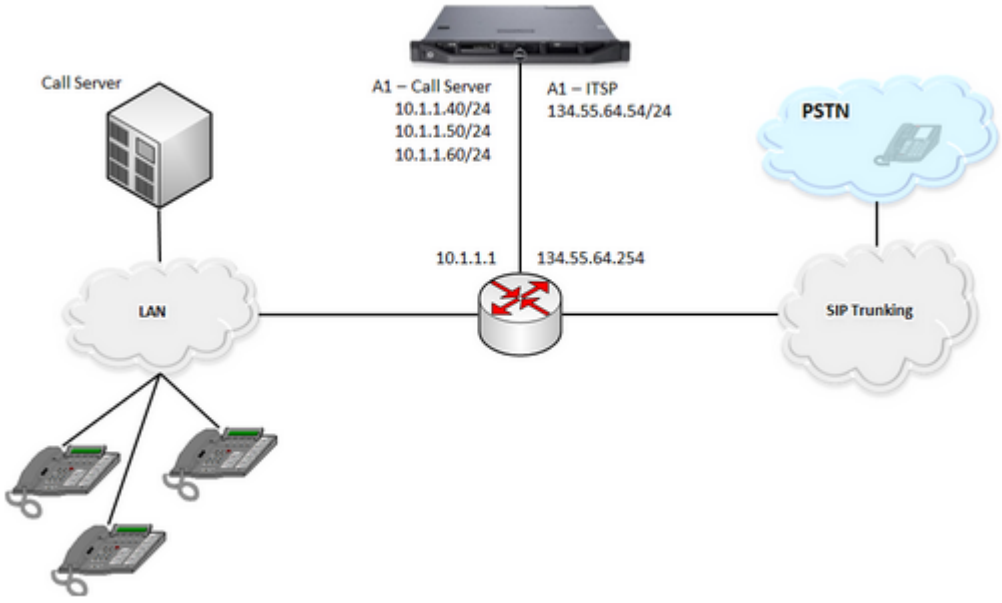


Figura 12: Avaya SBCE conectado a múltiples subredes en una sola interfaz

Detalles de configuración

- **Interfaces y propósitos**: esta configuración utiliza solo la interfaz de datos A1 Avaya SBCE. Con la ayuda del enrutador de siguiente salto, esta interfaz de datos brinda conectividad a dos

redes: la red del servidor de llamadas y la red ITSP. Esta configuración utiliza tres direcciones IP Avaya SBCE: dos para la red del servidor de llamadas y una para la red ITSP.

- **Equipo de red circundante**: esta configuración utiliza el enrutador de siguiente salto para admitir varias direcciones de puerta de enlace en la misma conexión de red física.
- **Interfaces de red**: En este escenario, A1 está habilitado. A2, B1 y B2 permanecen desactivados. Habilite solo una interfaz de datos.
- **Redes conectadas a Avaya SBCE**: En esta configuración, se agregan dos redes a la misma interfaz Avaya SBCE. Utilizar el**Configuración específica del dispositivo**>**Administración de redes**> **Redes** pestaña. Defina primero la red del servidor de llamadas y luego defina la red ITSP. Por lo tanto, para configurar varias redes en la misma interfaz de datos Avaya SBCE, agregue las redes a la misma interfaz cuando defina las redes.

Avaya SBCE conectado a múltiples subredes en dos interfaces

En este escenario, Avaya SBCE se conecta a un servidor de llamadas en una interfaz y a un servidor troncal en otra.

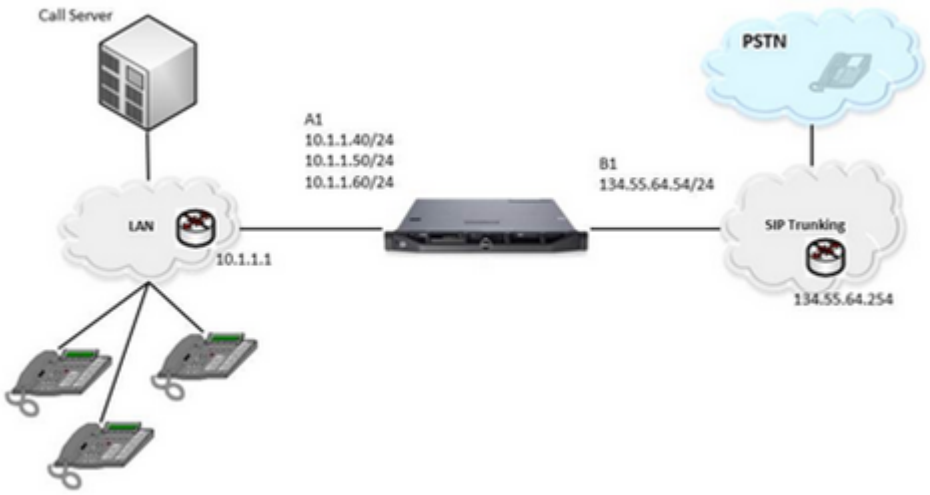


Figura 13: Avaya SBCE conectado a múltiples subredes en dos interfaces de datos

Detalles de configuración

- **Interfaces Avaya SBCE**: Esta configuración utiliza cuatro direcciones IP: tres en la interfaz A1 y una en la interfaz B1.
- **Equipo de red circundante**: Los enrutadores de siguiente salto en ambas interfaces de datos no necesitan admitir múltiples subredes Avaya SBCE o etiquetado VLAN.
- **Interfaces de red Avaya SBCE**: este escenario utiliza las interfaces A1 y B1. Asegúrese de configurar las interfaces requeridas.
- **Redes conectadas a Avaya SBCE**: En este ejemplo, Avaya SBCE se conecta a dos redes de datos a través de las interfaces A1 y B1. Cada dirección IP configurada puede usar un enrutador de siguiente salto único, si es necesario, o la puerta de enlace predeterminada. Defina cada red que se conecta a Avaya SBCE. Utilizar el**Administración de redes**ficha en**Configuración específica del dispositivo**para definir la red.

- **Otra configuración de Avaya SBCE**: para configurar interfaces de medios y señalización, flujos y perfiles de enrutamiento, consulte las secciones relacionadas.

Avaya SBCE conectado a varias subredes mediante una sola VLAN

En este escenario, Avaya SBCE se conecta a una combinación de redes VLAN y no VLAN mediante una sola interfaz de datos.

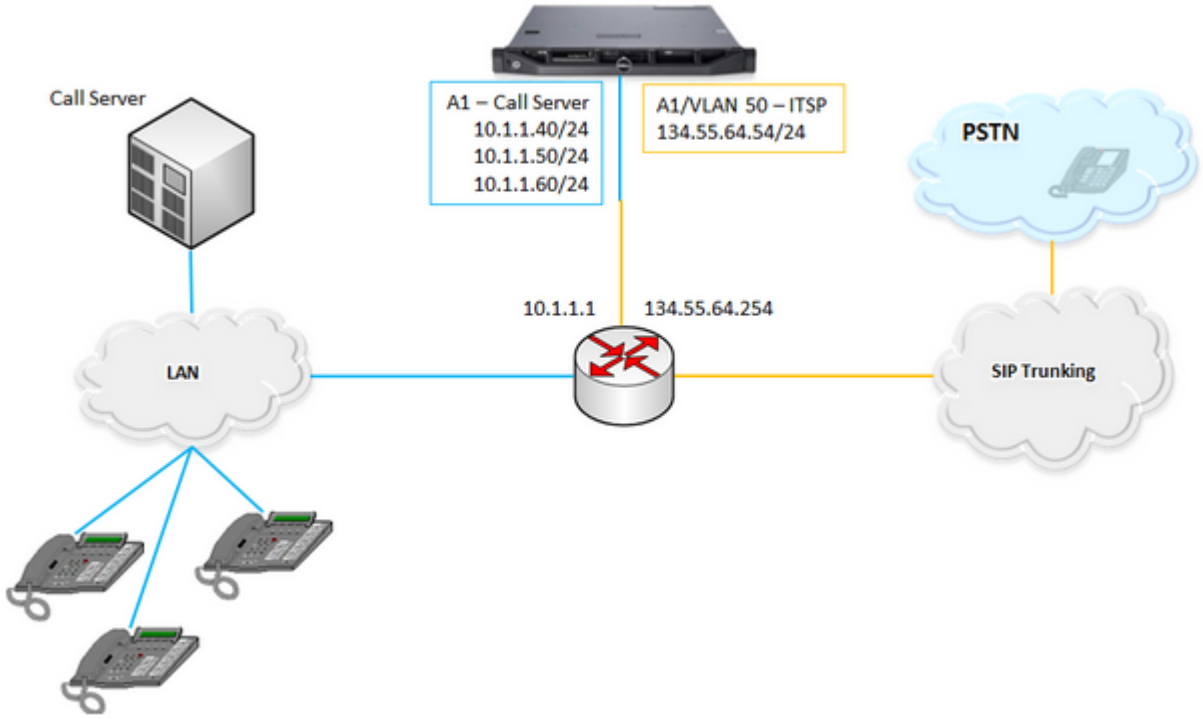


Figura 14: Avaya SBCE conectado a múltiples subredes, usando una sola VLAN y una sola interfaz de datos

Detalles de configuración

- **Interfaces y propósitos**: En este escenario, solo se utiliza la interfaz de datos A1 Avaya SBCE. Esta interfaz de datos proporciona conectividad a dos redes diferentes con la ayuda del enrutador nexthop: la red del servidor de llamadas y la red ITSP. Además, una de las redes, la red ITSP, está en una VLAN. Se requieren tres direcciones IP SBCE de Avaya para la red del servidor de llamadas, una interfaz VLAN en la interfaz física A1 y una dirección IP SBCE de Avaya en la red ITSP.
- **Equipo de red circundante**: En este ejemplo, el enrutador de siguiente salto está configurado para admitir dos direcciones IP de puerta de enlace y una VLAN en el mismo puerto físico.
- **Interfaces de red**: La red ITSP requiere etiquetado VLAN. La red ITSP usa la ID de VLAN (VID) 50. Los paquetes que salen de Avaya SBCE en la red ITSP deben contener un VID de 50. Para habilitar el etiquetado de VLAN, cree una interfaz VLAN. Las interfaces VLAN en Avaya SBCE utilizan las instalaciones subyacentes de una interfaz física A1, A2, B1 o B2. Los paquetes que salen y entran de Avaya SBCE en VLAN usan el enlace físico conectado a la interfaz física asociada. Defina la interfaz VLAN para conectar Avaya SBCE a la red ITSP. Utilizar el**Agregar VLAN**botón ubicado en el **Configuración específica del dispositivo**>**Administración de redes**>**Interfaces**

Página744 de 3226.

pestaña. Inicialmente, mantenga la interfaz VLAN deshabilitada. Luego habilite las interfaces VLAN A1 e ITSP mientras otras interfaces permanecen deshabilitadas.

- **Redes conectadas a Avaya SBCE**: En este ejemplo, la red ITSP se conecta a la interfaz VLAN sobre la interfaz física A1. Defina la red del servidor de llamadas de la misma manera que en otros escenarios de varias subredes. Defina la red ITSP y use la nueva interfaz VLAN.

Múltiples puertas de enlace en la misma red

Esta configuración incluye dos enrutadores de puerta de enlace y dos servidores de llamadas conectados a la red del servidor de llamadas. En esta configuración, solo la segunda puerta de enlace puede enrutar llamadas al segundo servidor de llamadas.

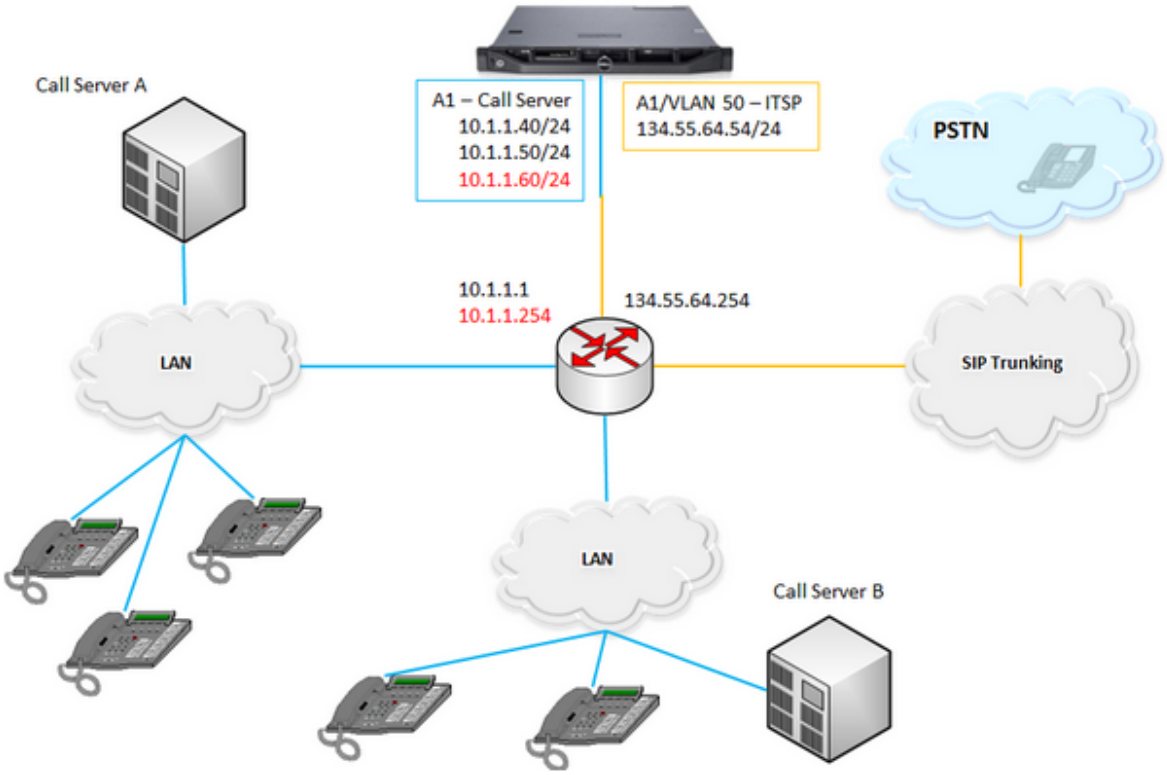


Figura 15: Varias puertas de enlace en la misma red

Detalles de configuración

- **Interfaces y propósitos**: solo una interfaz SBCE de Avaya se conecta tanto al servidor de llamadas como a las redes ITSP. Debido a que la red del servidor de llamadas tiene varios enrutadores de puerta de enlace, una de las direcciones IP de Avaya SBCE en esa red proporciona capacidades de enrutamiento de llamadas al servidor de llamadas B.

- **Equipo de red circundante**: El enrutador de siguiente salto admite tres direcciones IP de puerta de enlace y una VLAN en el mismo puerto físico. Dos direcciones IP de puerta de enlace están en la red del servidor de llamadas y una está en la red ITSP. La dirección de puerta de enlace 10.1.1.1 es la puerta de enlace predeterminada en la red del servidor de llamadas. Además, Avaya SBCE utiliza el 10.1.1.254

puerta de enlace para comunicarse con el servidor de llamadas B, ya que la puerta de enlace predeterminada en este ejemplo no puede comunicarse con la red.

- **Interfaces de red SBC**: La configuración del servidor de llamadas y las interfaces de red del ITSP es la misma que en los escenarios anteriores.
- **Redes conectadas a Avaya SBCE**: La configuración de la red ITSP es la misma que en los ejemplos anteriores. Para cada red adjunta, defina un enrutador de puerta de enlace predeterminado. Cada dirección IP de Avaya SBCE en la red puede anular la dirección IP de la puerta de enlace predeterminada, si es necesario. Por ejemplo, Avaya SBCE usa 10.1.1.254 como enrutador de siguiente salto en lugar de 10.1.1.1.

---

herramienta traceSBC

La herramienta tcpdump es la principal herramienta de solución de problemas de Avaya SBCE, que puede capturar el tráfico de la red. El uso de tcpdump es una forma confiable de analizar la información que llega y se envía desde Avaya SBCE. Sin embargo, tcpdump tiene sus propias limitaciones, lo que puede dificultar la resolución de problemas y llevar mucho tiempo. Esta herramienta tradicional no es útil para manejar el tráfico cifrado y la resolución de problemas en tiempo real.

El tráfico SIP y PPM está encriptado, especialmente en configuraciones de trabajo remoto. Verificar el tráfico encriptado con una captura de red es difícil y requiere mucho tiempo. El retraso ocurre porque se necesita la clave privada no cifrada de Avaya SBCE para descifrar el tráfico TLS y HTTPS.

La herramienta traceSBC ofrece soluciones para ambos problemas. traceSBC es un script de Perl que analiza los archivos de registro de Avaya SBCE y muestra mensajes SIP y PPM en un diagrama de escalera. Debido a que los registros contienen los mensajes descifrados, puede usar la herramienta fácilmente incluso en el caso de TLS y HTTPS. traceSBC puede analizar los archivos de registro descargados de Avaya SBCE. traceSBC también puede procesar archivos de registro en tiempo real en Avaya SBCE, para que pueda verificar el tráfico SIP y PPM durante las llamadas en vivo. La herramienta también puede funcionar en el modo no interactivo, lo cual es útil para la automatización.

Administración de registros SIP y PPM

A partir de la versión 6.3, el registro SIP siempre está habilitado de forma predeterminada. Puede habilitar el registro de PPM, STUN, TLS y AMS, si es necesario.

Archivos de registro

Avaya SBCE puede registrar mensajes SIP según lo procesan diferentes subsistemas y también registrar mensajes PPM. La utilidad traceSBC puede procesar los archivos de registro en tiempo real al abrir los archivos de registro más recientes en los directorios proporcionados. traceSBC también comprueba periódicamente si se genera un nuevo archivo, en cuyo caso se cierra el anterior y se continúa procesando con el nuevo. Se genera un nuevo archivo de registro cada vez que se reinician los procesos relevantes o cuando el tamaño alcanza el límite de ~10 M.

Ubicaciones de registro:

Los mensajes SIP se encuentran en /archivo/registro/tracesbc/tracesbc_sip/y los mensajes PPM se pueden encontrar en /archivo/registro/tracesbc/tracesbc_ppm/.

Los archivos activos tienen el siguiente formato:

- rw-rw---- 1 raíz raíz 112445 21 de agosto 10:12 tracesbc_sip_1408631651

Los archivos inactivos o cerrados tienen el siguiente formato:

- rw-rw---- 1 raíz raíz 175236 21 de agosto 06:33 tracesbc_sip_1408617250_1408620820_1o

- rw-rw---- 1 raíz raíz 31706 10 de julio 13:34 tracesbc_sip_1436549674_1436553270_1.gz

Ventajas

Memoria

Después de 10000 mensajes capturados, traceSBC deja de procesar los archivos de registro para evitar que se agote la memoria. Esta verificación se realiza durante la captura cuando la herramienta está analizando los archivos de registro. La herramienta cuenta la cantidad de mensajes SIP y PPM en los registros. Este número no es el número de mensajes enviados o recibidos en las interfaces. Este contador es un resumen de los mensajes de todos los registros, no de cada registro. Tenga en cuenta que esta protección está presente solo para el modo en tiempo real. Cuando la herramienta se usa en modo de tiempo no real, este contador no deja de procesar los registros especificados en la línea de comando. El contador continúa procesando los registros especificados en la línea de comando para poder procesar más archivos o mensajes en modo fuera de línea.

Procesador

Un mecanismo integrado está disponible para evitar un uso elevado de la CPU. La limitación no está ligada al nivel de la CPU. En la implementación actual, la limitación se realiza liberando la CPU durante un breve período después de que se procese cada línea del archivo. El resultado es que la ocupación de la CPU es baja en un sistema inactivo cuando la herramienta procesa activamente archivos de registro de gran tamaño. Puede deshabilitar la limitación mediante el parámetro de línea de comando –dt, que puede ser útil cuando se procesan archivos de registro grandes sin conexión. Sin embargo, en este caso, la ocupación de la CPU puede llegar al 100 %, por lo que no debe utilizar esta opción en un sistema activo.

Soporte de Avaya SBCE para Serviceability Agent

Avaya SBCE contiene Serviceability Agent que monitorea fallas en el sistema. Serviceability Agent envía notificaciones SNMPv2c y SNMPv3 a destinos configurados a través del agente maestro net-SNMP.

Con la compatibilidad con Serviceability Agent, puede usar Avaya SBCE para:

- Administrar usuarios de SNMPv3.
- Administrar destinos de trampas SNMP.
- Crear, editar y ver perfiles de trampas SNMP.

Para una seguridad óptima, habilite solo SNMP v3 con modos de autenticación y privacidad. Los clientes que hayan actualizado desde una versión anterior a la 7.1 pueden habilitar las versiones v1 y v2c de SNMP, si es necesario. Sin embargo, los clientes son responsables de los riesgos de seguridad relacionados con el uso de las versiones v1 y v2c de SNMP. A partir de la versión 7.1, para las nuevas instalaciones de Avaya SBCE, la configuración de SNMP v1/v2 no está disponible.

Para asegurarse de poder ver las alarmas SBCE de Avaya en System Manager, debe cargar el archivo de definiciones de alarmas comunes (cadf) en System Manager. Para obtener más información sobre cómo cargar el archivo cadf, consulte*Administración de Avaya Session Border Controller para empresas*.

Multi Alquiler

Avaya SBCE logra la tenencia múltiple utilizando múltiples inquilinos, servidores de llamadas e interfaces de Avaya SBCE.

Este escenario utiliza las cuatro interfaces de datos de Avaya SBCE. Avaya SBCE se conecta a dos redes de inquilinos, cada una con un conjunto único de trabajadores remotos. Avaya SBCE también se conecta a otras tres redes, cada una con un servidor de llamadas. Se llega a cada servidor de llamadas a través de una interfaz física separada, que proporciona una medida de redundancia cuando uno o más servidores de llamadas dejan de responder.

Ejemplo de configuración 1: multiusuario con múltiples usuarios, servidores de llamadas e interfaces SBCE de Avaya

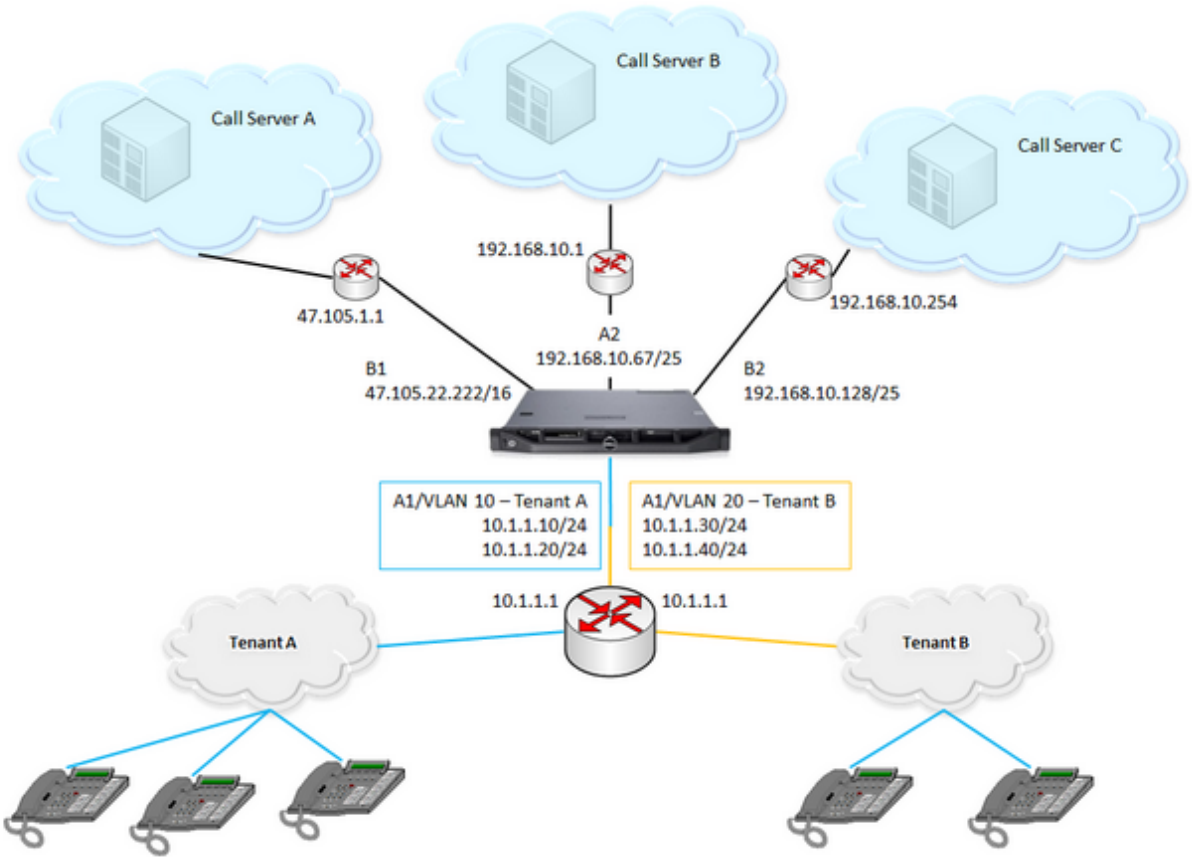


Figura 16: Múltiples inquilinos, servidores de llamadas e interfaces Avaya SBCE

- **Interfaces y propósitos**: La interfaz A1 de Avaya SBCE brinda conectividad a subredes de inquilinos. Cada subred usa una etiqueta de VLAN única: el inquilino A (en azul) está en la VLAN 10, mientras que el inquilino B (en naranja) usa la VLAN 20. El enrutador de puerta de enlace en la interfaz A1 proporciona conectividad a ambas VLAN de inquilino.

  La interfaz B1 proporciona conectividad al servidor de llamadas A, A2 conecta Avaya SBCE al servidor de llamadas B y B2 conecta la red que contiene el servidor de llamadas C.

Nota:

Puede adjuntar inquilinos a la interfaz B1 y conectar el servidor de llamadas A a través de la interfaz A1. Los puertos físicos conservan sus nombres históricos: A1, A2, B1 y B2.

- **Equipo de red circundante**: esta configuración admite la asignación correspondiente entre las NIC del SBC y las NIC del servidor físico. Configure la puerta de enlace en la interfaz A1 para admitir VLAN 10 y VLAN 20, y las direcciones IP de puerta de enlace asociadas. No necesita configurar las otras tres puertas de enlace en A2, B1 o B2 por separado. Si Avaya SBCE se ejecuta en una máquina virtual, configure VMWare vSwitch y las interfaces físicas en el servidor. Si cada interfaz física en Avaya SBCE usa un vSwitch independiente y cada vSwitch se conecta a una interfaz física independiente en el servidor, conecte el vSwitch a una configuración de puerto físico. Configure hasta cuatro vSwitches.

- **Interfaces de red Avaya SBCE**: Cuando configura VLAN en Avaya SBCE, el primer paso siempre es crear las interfaces de VLAN. En este ejemplo, se crean dos interfaces VLAN para admitir las dos redes de inquilinos. Primero, la VLAN para el arrendatario A en la interfaz A1. Luego, la VLAN para el inquilino B en A1. Las redes restantes usan interfaces físicas en Avaya SBCE. Finalmente, habilite todas las interfaces: las dos VLAN, así como A2, B1 y B2.
- **Redes conectadas a Avaya SBCE**: En este ejemplo, Avaya SBCE está conectado a cinco redes. Para cada red adjunta, defina un enrutador de puerta de enlace predeterminado, comenzando con el inquilino A, seguido por el inquilino B, llame al servidor A, llame al servidor B y finalmente llame al servidor C.

Ejemplo de configuración 2: Tenencia múltiple usando la misma dirección IP

Avaya SBCE admite el uso de la misma dirección IP en múltiples interfaces de datos en Avaya SBCE. Los clientes a menudo comparten el mismo espacio de direcciones y la misma dirección IP de servicio mientras usan las funciones de multiinquilino y en la nube. Con soporte para usar la misma dirección IP más de una vez, más de un cliente puede usar la misma dirección IP para conectarse a Avaya SBCE.

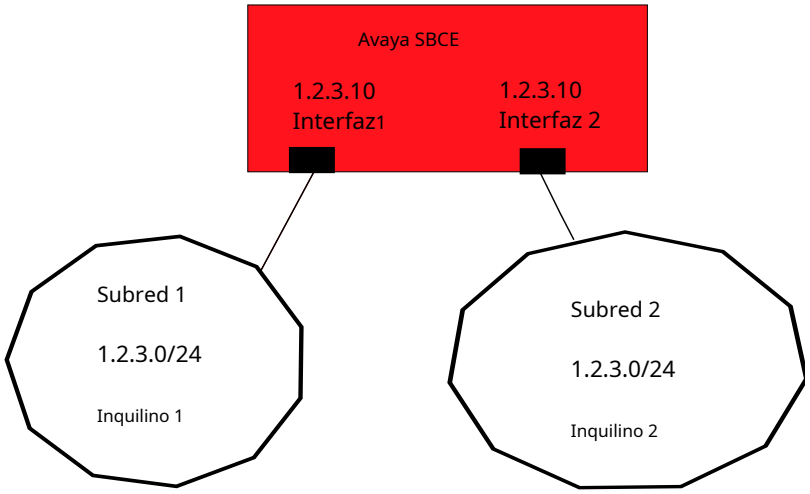


Figura 17: Misma dirección IP utilizada en diferentes interfaces

Para permitir el uso de múltiples instancias de la misma IP, las instancias deben existir en interfaces de red separadas, interfaces de red virtual o ambas. Avaya SBCE separa la definición de interfaz de la definición de red de la siguiente manera:

- Una interfaz es una combinación de un puerto físico, como A1, A2, B1 y B2, y una ID de vlan. Una ID de vlan puede ser**sin VLAN**.

Página749 de 3226.

- Una red vincula un conjunto de IP y puertas de enlace de Avaya SBCE con una interfaz.

Por lo tanto, para dos instancias de 1.2.3.0 en Avaya SBCE, debe definir dos interfaces y dos redes, de modo que 1.2.3.0 ocurra exactamente una vez dentro de cada red.

En este escenario, Avaya SBCE se conecta a dos redes de inquilinos, cada una con un conjunto único de trabajadores remotos. Sin embargo, se asigna la misma dirección IP en Avaya SBCE en ambas redes de inquilinos.

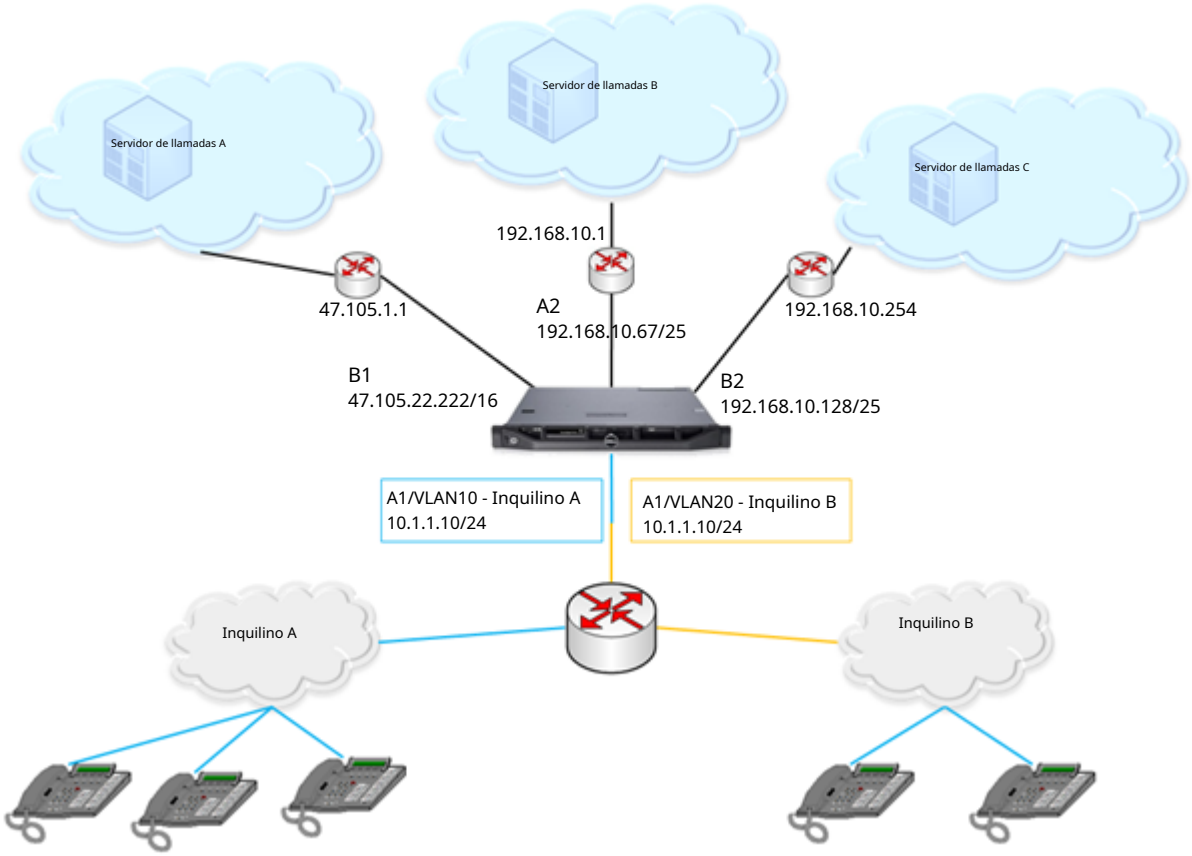


Figura 18: Múltiples inquilinos usando la misma dirección IP

Las siguientes secciones describen los detalles de configuración para este ejemplo de implementación.

Interfaces y propósitos:

La interfaz A1 de Avaya SBCE proporciona conectividad a las subredes de inquilinos. Cada subred usa una etiqueta de VLAN única: el inquilino A, resaltado en azul, está en la VLAN 10, mientras que el inquilino B, resaltado en naranja, usa la VLAN 20. El enrutador de puerta de enlace en la interfaz A1 proporciona conectividad a ambas VLAN de inquilino.

La interfaz B1 proporciona conectividad al servidor de llamadas A, A2 conecta Avaya SBCE al servidor de llamadas B y B2 conecta la red que contiene el servidor de llamadas C.

Equipo de red circundante:

Configure la puerta de enlace en la interfaz A1 para admitir VLAN 10 y VLAN 20, y las direcciones IP de puerta de enlace asociadas. Como la dirección SBCE de Avaya en ambos inquilinos es la misma, la puerta de enlace debe poder distinguir entre las direcciones de las redes de ambos inquilinos.

Página750 de 3226.

Interfaces de red:

Para usar la misma dirección IP en Avaya SBCE varias veces, seleccione la**Permitir direcciones IP no únicas para redes complejas**campo en la página Opciones de red. Para configurar VLAN en Avaya SBCE, cree interfaces de VLAN. En este ejemplo, se crean dos interfaces VLAN para admitir las dos redes de inquilinos:

- La VLAN para el arrendatario A en la interfaz A1
- La VLAN para el inquilino B en A1

Las redes restantes usan interfaces físicas en Avaya SBCE. Finalmente, habilite todas las interfaces: las dos VLAN, así como A2, B1 y B2.

En este ejemplo, Avaya SBCE está conectado a cinco redes. Para cada red adjunta, defina un enrutador de puerta de enlace predeterminado y direcciones IP de Avaya SBCE. Comience con el inquilino A, seguido del inquilino B, llame al servidor A, llame al servidor B y finalmente llame al servidor C.

Compatibilidad con troncales de IP Office desde una dirección IP dinámica

Avaya SBCE admite un enlace troncal de IP Office que se origina en direcciones IP dinámicas. La dirección externa del enrutador ISP o firewall en el sitio remoto se basa en el Protocolo de configuración dinámica de host (DHCP). Por lo tanto, una dirección IP externa estática no está disponible para configuración o instalación.

En su lugar, en la configuración del servidor para servidores de sucursales remotas, puede administrar un FQDN que apunte a un registro de DNS dinámico. Si se interrumpe la conexión TLS de la sucursal remota, Avaya SBCE resuelve la entrada FQDN nuevamente para todos los servidores de la sucursal remota. Si el valor TTL del registro DNS caduca, Avaya SBCE consulta el DNS para todas las entradas FQDN en la configuración del servidor.

Nota:

Si falla una búsqueda de DNS, Avaya SBCE intenta la búsqueda de DNS cada 30 segundos para las primeras 10 fallas y luego cada 3000 segundos.

Reutilización de la conexión establecida por IP Office para entregar llamadas

Avaya SBCE reutiliza la conexión TLS de IP Office para la señalización SIP hacia IP Office. El perfil de enrutamiento hacia la sucursal remota debe usar una entrada de enrutamiento que coincida con la configuración del servidor para la sucursal remota. Para entradas de enrutamiento de sucursales remotas, el transporte debe ser TLS y el**Puerto**el campo debe estar vacío.

Avaya SBCE rechaza la conexión TLS entrante de IP Office si:

- El certificado de cliente TLS requerido no está configurado en IP Office.
- IP Office presenta el certificado autofirmado durante el protocolo de enlace TLS.
- La verificación de pares falla en Avaya SBCE con el certificado de cliente TLS presentado por IP Office.

Si se interrumpe la conexión TLS de la sucursal remota, Avaya SBCE rechaza las llamadas que se originan en la empresa hasta que se restablece la conexión. Mientras tanto, Avaya SBCE muestra un mensaje de error interno del servidor 500.

Nota:

Puede proporcionar entradas de ruta personalizadas con el puerto de escucha de IP Office si administra reglas DNAT en el Firewall o el enrutador NAT.

Proxy de servicios de habilitación de cliente seguro

Client Enablement Services (CES) brinda acceso a muchas capacidades de Comunicaciones Unificadas (UC) de Avaya, incluidas telefonía, movilidad, mensajería, conferencias y Presence Services a través de una sola aplicación. Avaya one-X®El móvil se comunica con el servidor CES mediante el protocolo CES. Para proporcionar servicios CES a Avaya one-X®Clientes móviles fuera de la red empresarial, Avaya SBCE proporciona un proxy seguro que debe implementarse en la DMZ empresarial. Avaya SBCE verifica todo el tráfico de Avaya one-X®Clientes móviles fuera de la red empresarial al servidor CES.

Cuando se establece una nueva conexión desde Avaya one-X®Móvil fuera de la red empresarial:

- Avaya SBCE comprueba si el primer mensaje de Avaya one-X®El dispositivo móvil es una solicitud de inicio de sesión y reenvía el mensaje al servidor CES. Avaya SBCE elimina todos los mensajes recibidos de Avaya one-X®Dispositivo móvil antes de la solicitud de inicio de sesión.
- El servidor CES autentica Avaya one-X®Mobile o envía un mensaje de error a Avaya SBCE. Después de una falla de autenticación, Avaya SBCE rechaza todos los mensajes subsiguientes de Avaya one-X®Móvil.
- Después de la autenticación, Avaya SBCE reenvía todos los mensajes de Avaya one-X®Móvil al servidor CES.

Avaya SBCE mantiene estadísticas de todos los intentos de inicio de sesión. Avaya SBCE admite al menos 10 000 Avaya one-X®Clientes móviles en Dell R630 y HP DL360 G9.

Compatibilidad con la tarjeta de acceso remoto de Dell integrada y Lights-Out integrado

Dell Remote Access Controller (DRAC) y HP Integrated Lights-Out (iLO) son herramientas de administración. Estas herramientas brindan potentes funciones de administración de servidores remotos, incluido el control para encender o apagar un servidor de forma remota. Puede utilizar las funciones de DRAC para solucionar y diagnosticar problemas durante el reinicio de un servidor remoto. Desde la versión 7.0 en adelante, Avaya SBCE es compatible con las siguientes funciones de la tarjeta iDRAC Express:

- Aprovisionamiento del sistema: puede instalar Avaya SBCE ISO mediante las funciones de aprovisionamiento de iDRAC.
- Supervisión y gestión del sistema: puede supervisar el estado del servidor mediante las funciones de iDRAC.

Traducido del inglés al español - www.onlinedoctranslator.com

Puede comprar la tarjeta iDRAC con o sin el servidor. Para servidores Dell posteriores a la serie 600, la tarjeta iDRAC Express es parte de la configuración básica. Para estos servidores, no es necesario que instale, respalde ni administre otra licencia para la tarjeta iDRAC express. Sin embargo, para actualizar de la versión express a la versión empresarial, debe comprar otra licencia directamente de Dell. De manera similar, para actualizar de iLO 3 a iLO 4, debe comprar otra licencia de HP.

Para obtener más información sobre la instalación y el uso de iDRAC, vaya a http://www.support.dell.com/ y ver *Guía del usuario del controlador de acceso remoto integrado de Dell*.

Plataformas de hardware compatibles

Avaya SBCE es compatible con Dell iDRAC y HP iLO en las siguientes plataformas:

Plataforma	Compatibilidad con iDRAC e iLO
Portwell MXN 0208	No es compatible con iDRAC e iLO.
Dell R210 II y R210 II XL	No es compatible con iDRAC.
dell r320	No es compatible con iDRAC.
dell r620	No es compatible con iDRAC.
dell r630	Admite iDRAC 8 expreso.
HP DL360 G8	No es compatible con iLO.
HP DL360 G9	Compatible con iLO 4.

Importante:

Los servidores Dell R210 II y Dell R320 no son compatibles con las interfaces de iDRAC, por lo tanto, estos servidores no son compatibles con iDRAC.

Los servidores de la generación anterior tienen vulnerabilidades de cifrado 0. Por lo tanto, no use iDRAC e iLO cuando iDRAC e iLO no estén incluidos con la plataforma.

Solución de grabación basada en SIPREC

Avaya SBCE admite una solución de grabación de medios basada en SIP (SIPREC) con los siguientes componentes:

- Avaya SBCE como cliente de grabación SIP (SRC)
- Avaya Contact Recorder como servidor de grabación SIP (SRS)
- Servicios de habilitación de aplicaciones para la integración de CTI
- Servidores de aplicaciones de Contact Center como Avaya Aura®Contact Center y Call Center Elite
- Puntos de anclaje multimedia como Avaya Aura®Media Server o Communication Manager Media Gateway

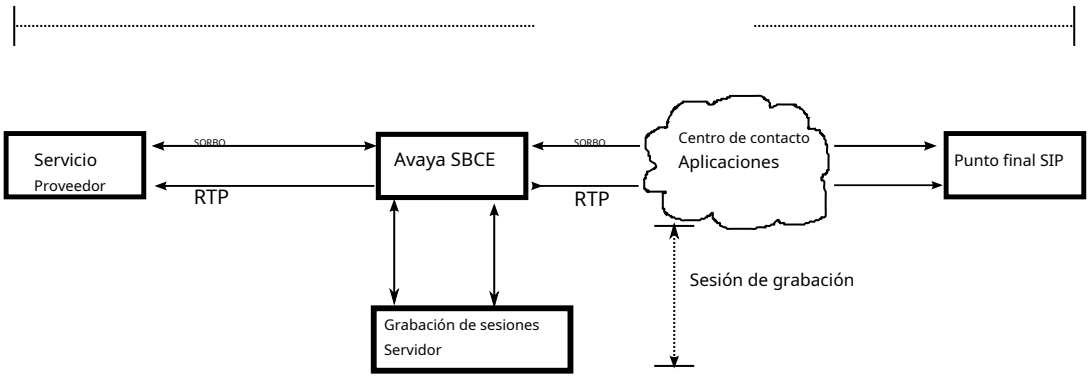


Figura 19: Arquitectura de solución de grabación basada en SIPREC

Con la solución de grabación basada en SIPREC, Avaya SBCE admite la grabación de sesiones a tiempo completo, la grabación selectiva y la grabación continua. Con la grabación de sesiones de tiempo completo, se graban todas las sesiones de comunicación conectadas mediante Avaya SBCE.

Los servidores de grabación se pueden colocar con Avaya SBCE o distribuirse en diferentes ubicaciones. Si el SRS y Avaya SBCE están en diferentes ubicaciones, asegúrese de que la red no requiera la traducción de direcciones de red entre el SRS y los dispositivos Avaya SBCE. Debe implementar Avaya SBCE y Recording Server en una red confiable y segura para la privacidad y seguridad de los medios grabados.

Debe tener un troncal SIP en Avaya SBCE para garantizar que SIPREC funcione correctamente.

Funciones para la grabación de sesiones

Las siguientes funciones de Avaya SBCE son compatibles con la solución de grabación:

- Inicio, modificación y finalización de la sesión de grabación desde el servidor de grabación SIP (SRS) durante la sesión de grabación.
- Prevención temprana de recortes de medios durante la configuración de la sesión.
- Archivo Wave reproducido para indicar que la sesión se está grabando.
- Enrutamiento alternativo para sesiones de grabación con equilibrio de carga Round Robin.

  Cuando comienza una sesión de grabación, Avaya SBCE inicia un temporizador. Cuando el temporizador expira, Avaya SBCE activa mecanismos de enrutamiento alternativos. Avaya SBCE también usa mecanismos de enrutamiento alternativo después de recibir los siguientes mensajes del servidor de grabación: 408,480,486,488, 500 y 503.
- Alta disponibilidad para el flujo de medios de la grabadora y los metadatos enviados a los servidores de grabación.
- Enrutamiento del servidor de grabación.

  Avaya SBCE se comunica con un grupo de servidores de grabación. Debe administrar una URL para cada servidor de grabación en el clúster. Avaya SBCE envía un mensaje de INVITACIÓN al servidor de grabación. Cuando Avaya SBCE envía el URI de contacto con la etiqueta de función +sip.src en el mensaje INVITE al SRS, el SRS identifica una sesión de grabación.
- Elementos de metadatos para identificar flujos de medios de SRC y SRS.

  Avaya SBCE proporciona los siguientes elementos de metadatos:

Elemento de metadatos	parámetro de apoyo
Identificador de llamada	UCID
Identificador de sesión	id de sesión sdp
Identificador de participante	PAI
Identificador de flujo	Etiqueta en el flujo de medios
dirección de la corriente	enviar, recibir e inactivo
Marca de tiempo para la resincronización	N / A

- Sin controles desde el lado del maletero de las sesiones de grabación.

  Avaya SBCE usa solo los controles especificados desde Avaya SBCE y en el servidor de grabación.

- Etiquetas únicas que son las etiquetas de medios para flujos de medios para identificar el flujo de medios para los participantes en la sesión de grabación. Las etiquetas de medios solo se aplican a la grabación de audio.

  A partir de la versión 7.2.2.2, para identificar el enlace troncal y la empresa, el valor del flujo de medios de un enlace troncal debe ser menor que el valor del flujo de medios proveniente de una empresa.

- Opciones de seguridad.

  Avaya SBCE admite un perfil SAVP para sesiones SRTP y un perfil AVP para sesiones RTP. Avaya SBCE es compatible con la conexión TLS y TCP. ACR admite la conexión TCP con el esquema SIP uri utilizando el perfil RTP/AVP y SAVP.

  Nota:

  Para SIPREC, Avaya SBCE admite SRTP solo con hmac80, ya que ACR no admite ningún otro algoritmo criptográfico.

- Manejo y redirección de REFER admitidos en escenarios de grabación.
- Grabación SIP en modo traductor. Avaya SBCE recibe flujos de medios y los retransmite al servidor de grabación. Avaya SBCE no cambia ningún dato en los flujos de medios.

Además, a partir de la versión 7.1, Avaya SBCE ofrece las siguientes funciones:

- Compatibilidad con grabación continua, selectiva y de tiempo completo.
- Soporte para terminación de llamadas en caso de falla de grabación.

  Cuando Avaya SBCE inicia una sesión hacia cada servidor de grabación configurado, puede haber situaciones en las que ninguno de los servidores responda. En tales escenarios, Avaya SBCE puede finalizar la sesión que se inició o está en curso hacia la parte llamante o llamada. La terminación de llamadas en caso de falla de grabación no es compatible con llamadas de trabajadores remotos.

- Soporte para grabar una llamada de trabajador remoto a trabajador remoto.
- Soporte para grabación en caso de bifurcación aguas abajo.

  Si Avaya SBCE recibió varios diálogos bifurcados, se registra el primer diálogo recibido con los primeros medios. Los primeros medios subsiguientes en diálogos bifurcados no se registran. Para la respuesta final, se graba el flujo de medios entre la persona que llama y la parte que responde al final.

Grabación selectiva

A partir de la versión 7.1, Avaya SBCE admite la grabación selectiva. Para la grabación selectiva, los medios se transmiten continuamente, de forma similar a la grabación a tiempo completo. Sin embargo, el servidor de grabación enmascara los flujos grabados hasta que el sistema detecta eventos de Integración de telefonía informática (CTI). Por lo tanto, solo se graba una parte de la sesión de comunicación cuando el servidor de grabación corta el flujo de medios después de recibir eventos de CTI.

Con la grabación selectiva, se conservan el ancho de banda y los ciclos de procesamiento porque los flujos de medios no fluyen a través de la red cuando no se requiere grabación.

Grabación continua

A partir de la versión 7.1, Avaya SBCE admite la grabación continua si el servidor de grabación en espera tiene información sobre el estado actual del servidor de grabación activo. Si el servidor de grabación activo falla, el servidor de grabación en espera continúa grabando la sesión de comunicación. El servidor de grabación solicita a Avaya SBCE que transmita los medios y los metadatos de esa sesión de comunicación al servidor de grabación activo.

Indicación segura de extremo a extremo

Los terminales de Avaya pueden mostrar un indicador seguro de extremo a extremo para las llamadas que usan protocolos seguros para ambas mitades de la llamada. Desde la versión 7.0 en adelante, Avaya SBCE proporciona una **Asegurable**en la página Configuración del servidor para indicar si el servidor es protegible. Avaya SBCE utiliza el **Asegurable**para determinar si la troncal y el servidor de llamadas pueden usar protocolos seguros y establece los valores apropiados para el encabezado Av-Secure-Indication.

El encabezado Av-Secure-Indicator en el mensaje INVITE saliente se establece en seguro cuando se cumplen las siguientes condiciones:

- El servidor troncal y el servidor de llamadas son asegurables.
- Los enlaces entrantes y salientes usan TLS y tienen un perfil audiovisual seguro (SAVP) o mensajes de parte de aplicación de capacidades de transacción (tcap) con un perfil SAVP.
- System Manager envía el encabezado Av-Secure-Indication como protegido.

Avaya SBCE establece el encabezado Av-Secure-Indication en no seguro cuando:

- No se cumple ninguna de las condiciones requeridas para configurar el encabezado Av-Secure-Indication como seguro.
- El mensaje de Respuesta tiene un perfil AVP.

Los mensajes posteriores, como Actualización sin SDP, PRACK sin SDP y ACK, deben mantener el valor de indicación segura de la respuesta de la solicitud anterior.

Para que el servidor troncal no sea seguro, el enlace troncal correspondiente con Session Manager también debe estar no seguro.

Nota:

Avaya SBCE depende de Avaya Aura®7.0 para admitir la función de indicación segura de extremo a extremo. Aura de Avaya®7.0 pone esta función a disposición de los usuarios.

Cifrado de medios usando AES-256

El estándar de cifrado avanzado (AES) es una especificación ampliamente utilizada para el cifrado de datos. Desde la versión 7.0 en adelante, Avaya SBCE admite el cifrado de medios mediante AES-256.

Los estándares AES describen un algoritmo de clave simétrica. AES tiene un tamaño de bloque fijo de 128 bits y un tamaño de clave de 128, 192 o 256 bits. Aunque AES-128 es suficientemente seguro, los usuarios muy conscientes de la seguridad pueden adoptar AES-192 o AES-256. Para aprovisionar esta función, Avaya SBCE es compatible con las siguientes suites criptográficas:

- AES_256_CM_HMAC_SHA1_32
- AES_256_CM_HMAC_SHA1_80

Las siguientes opciones están disponibles en el**Formato preferido #1**,**Formato preferido #2**, y **Formato Preferido#3**campos en la página Regla de medios:

- SRTP_AES_CM_256_HMAC_SHA1_32
- SRTP_AES_CM_256_HMAC_SHA1_80

Transcodificación

A partir de la versión 7.1, Avaya SBCE admite la transcodificación. La transcodificación traduce un flujo de medios codificado con un códec en un códec de medios codificado con otro códec. Avaya SBCE realiza la transcodificación cuando las entidades entrantes y salientes tienen códecs incompatibles. La oferta del Protocolo de descripción de sesión (SDP) contiene información sobre los códecs que prefiere el dispositivo que envía el mensaje. El dispositivo que recibe el mensaje responde a la oferta SDP utilizando el conjunto de códecs que admite el dispositivo receptor.

Para habilitar la función de transcodificación, debe ir a**Configuración específica del dispositivo**>**Opciones avanzadas**, haga clic en el**Control de funciones**pestaña y seleccione la**Transcodificación**casilla de verificación

Al proporcionar transcodificación, Avaya SBCE:

- Optimiza la disponibilidad del ancho de banda imponiendo el uso de diferentes códecs de compresión.
- Normaliza el tráfico en la red a un solo códec.
- Reduce el uso de procesadores de funciones de recursos multimedia y puertas de enlace de medios para admitir una gran cantidad de códecs.

Avaya SBCE admite la transcodificación de audio y la transcodificación para implementaciones de troncales. Todas las llamadas transcodificadas están ancladas a Avaya SBCE. No se admite la transcodificación de fax. Si una llamada tiene líneas m de audio y video, Avaya SBCE solo transcodifica el audio. Las videollamadas que requieren transcodificación se convierten en llamadas de audio.

Capacidades de transcodificación admitidas

Nombre del servidor	Máximo de sesiones transcodificadas	Máximo no transcodificado sesiones
Dell R210-II XL	100	5000
HP DL360 G8	200	6000
dell r620	200	6000
dell r320	200	6000
dell r630	1000	10000
HP DL360 G9	1000	10000

Estas capacidades varían de un códec a otro porque, según el algoritmo del códec, los ciclos de CPU de procesamiento difieren para cada flujo de medios. Las capacidades estimadas son con los códecs G711 y G729 y se basan en el tiempo de espera/conversación de 180 segundos.

Códecs compatibles con la transcodificación

Los siguientes códecs son compatibles para la transcodificación:

- PCMU
- PCMA
- G722
- G729
- G729AB
- G726–32
- Banda estrecha restringida OPUS
- OPUS de banda estrecha
- Banda ancha OPUS

Soporte para direcciones IPv6

A partir de la versión 7.1, Avaya SBCE admite direcciones IPv6 para servidores troncales SIP. Para respaldar la transición a IPv6, Avaya SBCE utiliza nodos de doble pila que ejecutan tanto IPv4 como IPv6. Avaya SBCE admite implementaciones de troncales con IPv4 solo para la empresa, e IPv6, doble pila o IPv4 solo para la red troncal o pública.

Avaya SBCE admite los siguientes escenarios de implementación:

- Red pública (no confiable): solo IPv6, doble pila, modo mixto
- Red privada/empresarial (de confianza): solo IPv4

Avaya SBCE admite:

- Dirección de unidifusión local única de IPv6 y dirección de unidifusión global de IPv6.
- Comunicación IPv6 con entidades como servidores SIP, terminales SIP, servidores DNS, servidor NTP, servidor syslog y Avaya Aura®Servidor multimedia.

Página758 de 3226.

Nota:

Si la respuesta de DNS tiene direcciones IPv4 e IPv6, Avaya SBCE se basa en las políticas de configuración para determinar los tipos de direcciones que se probarán.

- Comunicación IPv6 con EMS.

Desde la versión 7.2, Avaya SBCE admite:

- Comunicación IPv6 con servidor de grabación SIP.
- IPv6 en implementaciones de trabajadores remotos.

Avaya SBCE admite las siguientes funciones a través de IPv6:

- Alta disponibilidad (HA)
- Acceso a la interfaz web de EMS
- Sincronización de tiempo con el servidor NTP configurado
- Enlace troncal SIP

Avaya SBCE admite la semántica de tipos de direcciones de red alternativas (ANAT) para SDP a fin de permitir direcciones de red alternativas para flujos de medios. La semántica ANAT es útil en entornos con hosts IPv4 e IPv6. Cuando Avaya SBCE recibe una oferta SDP con semántica ANAT, Avaya SBCE:

- Determina si la red empresarial usa solo IPv4.
- Elimina la agrupación de líneas de medios y envía solo la dirección IPv4 en la línea m si la red empresarial usa IPv4.
- Selecciona una línea m según la configuración de preferencias de ANAT y establece el puerto en 0 en otras líneas m.

Las entidades SIP que generan una oferta SDP con semántica ANAT colocan la etiqueta sdp-anat-option-tag en el **Requerir encabezado**campo. Avaya SBCE admite la etiqueta sdp-anat-option. Avaya SBCE es compatible con UDP/RTP, TCP/RTP, TLS/SRTP y otras combinaciones de transporte en redes solo IPv6, de doble pila y de modo mixto.

Si tiene un entorno con hosts IPv4 e IPv6, debe ir a**Políticas de dominio**> **Reglas de medios**y seleccione**ANAT habilitado**. Para más información, ver*Administración de Avaya Session Border Controller para empresas*.

Solución de servidor perimetral para conferencias convergentes

La solución de conferencia convergente utiliza las funciones de Avaya Scopia®V8.5 y Avaya Aura® Conferencias para proporcionar una conferencia convergente y una solución de colaboración web en una arquitectura unificada.

En la solución de conferencia convergente, Avaya SBCE:

- Actúa como Edge Server para el conjunto de clientes convergentes. El servidor perimetral permite a los clientes acceder a la infraestructura de video empresarial de forma remota a través de firewalls que bloquean los puertos de medios.

- Proporciona cruce de cortafuegos para dispositivos SIP, HTTP y WebRTC y tuneliza los medios donde el cortafuegos bloquea los puertos de medios. Avaya SBCE permite que las transmisiones entren a través de puertos conocidos para TLS/TCP.
- Hace posibles las videollamadas federadas entre empresas. Estas llamadas pueden realizarse a través de terminales de video entre dos empresas que están detrás de una puerta de enlace SIP o un SBC y conectadas por un enlace troncal SIP.
- Facilita a los usuarios invitados no registrados marcar una videoconferencia o llamar desde una videoconferencia.

La solución de conferencia convergente comprende lo siguiente:

- Servidor de aplicaciones convergentes: los componentes que se colocan en el mismo servidor o se distribuyen según la escala y la topología de implementación. Los componentes incluyen una aplicación de gestión, enfoque de conferencia, agente de usuario SIP back-to-back, Gatekeeper H.323 y un Portal de usuario unificado.
- Puerta de enlace de servicios web (WSGW): la puerta de enlace de HTTP a SIP para clientes WebRTC y HTTP.
- Servidor de colaboración web: Avaya Aura®Conferencias aprovechadas para la colaboración web en tiempo real.
- Servidor de medios convergentes: procesamiento de medios basado en software para la transcodificación y composición de video, audio a gran escala y compatibilidad con audio/video WebRTC. El servidor utiliza Avaya Scopia®Estructura de la unidad de control multipunto (MCU) Elite. También puede utilizar Elite MCU tradicional con aspas de acelerador de hardware como alternativa.
- Clientes convergentes: nuevo conjunto de clientes de audio/video, incluidos clientes Meet Me, clientes ligeros basados en WebRTC como Simple WebRTC Chat (SWC), Avaya Equinox®y la serie de clientes Scopia XT.
- Servidor perimetral: Avaya SBCE, buscador de rutas (H.323) y Avaya Scopia®Servidor de escritorio. Avaya SBCE proporciona la funcionalidad de Session Border Controller para llamadas SIP, BFCP/FECC para la serie XT, funcionalidad de proxy inverso para HTTP y TURN/STUN para WebRTC. Avaya Scopia®
  Se requiere un servidor de escritorio para manejar la señalización y los medios para Avaya Scopia heredado® teléfonos móviles de escritorio.
- Infraestructura de gestión común para todos los componentes y dispositivos.
- Grabación de conferencias y sistema de gestión de contenidos mediante WildCat.

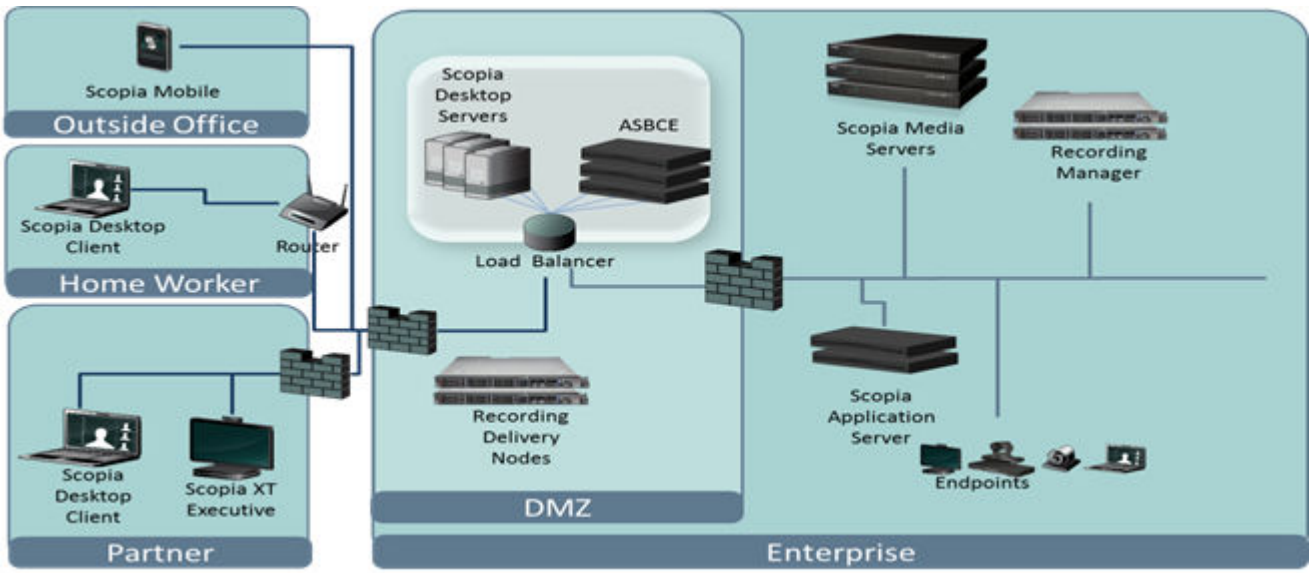


Figura 20: Componentes de la solución de conferencia convergente con Avaya SBCE como servidor perimetral

La solución es compatible con Avaya Aura®, IP Office e implementación en la nube, desde implementaciones distribuidas pequeñas a grandes, e implementaciones virtualizadas en entornos de nube.

Funciones de Avaya SBCE para la solución de conferencia convergente

Para la solución de conferencia convergente, Avaya SBCE 7.1 admite lo siguiente:

- Señalización de control TURN/STUN y relé de medios UDP para WebRTC con NATing simétrico.
- TURN/STUN sobre TCP para WebRTC.
- Multiplexado y demultiplexado RTP/RTCP o SRTP/SRTCP sobre TCP o TLS.
- Retransmisión de medios a través de la retransmisión TURN usando TCP de extremo a extremo sin convertir a UDP para la retransmisión TURN.
- Equilibrio de carga para TURN.
- Envío del estado de los dispositivos a Avaya Scopia®Balanceadores de carga y administración.
- Cálculo del ancho de banda para todas las sesiones de audio/video. Avaya SBCE proporciona esta entrada al equilibrador de carga iVIEW para un equilibrio de carga efectivo.
- Detección de DoS y límite de velocidad de la solicitud de señalización http o https desde conexiones remotas.
- Reescritura de URL basada en la redirección.
- Haga clic en conferencia para usuarios no registrados. Los terminales pueden llamar a través de Avaya SBCE a Avaya Scopia®MCU sin estar registrado en el dominio autorizado. Para las llamadas realizadas, el FQDN se resuelve y el transporte de prioridad de DNS se selecciona como TLS o TCP.

  Para que esta característica funcione, se requieren los siguientes cambios de configuración:

  - Crear un flujo de clic para llamar.

- Para escenarios marcados, configure un servidor o cliente DNS válido en Avaya SBCE. Asegúrese de que la interfaz de recepción del flujo de hacer clic para llamar coincida con la interfaz de señalización del flujo entrante seleccionado.

Soporte ENUM

A partir de la versión 7.1, Avaya SBCE es compatible con el protocolo de asignación de números E.164 (ENUM). Los números de teléfono en la PSTN se organizan utilizando el formato especificado en el estándar E.164. Por el contrario, Internet utiliza el Sistema de nombres de dominio (DNS) para vincular los nombres de dominio a las direcciones IP. ENUM define un método para convertir un número de teléfono a un formato que se puede usar con el DNS para buscar información de direccionamiento, como identificadores uniformes de recursos (URI). Los números que se ajustan al plan de numeración definido en E.164 son:

- Limitado a 15 dígitos.
- Precedido de un signo más (+) para indicar que el número incluye un código de llamada de país internacional.

ENUM traduce números E.164 a URI mediante el uso de registros de puntero de autoridad de nombres (NAPTR) almacenados en DNS. Con ENUM, las llamadas se pueden completar a través de Internet en lugar de transferir la llamada a PSTN. Por lo tanto, ENUM proporciona ahorros de costos para las empresas que se comunican con otras empresas mediante SIP. Si el número no está disponible en la base de datos ENUM, Avaya SBCE enruta la llamada al proveedor de servicios para enviar la llamada a la PSTN.

Proceso para convertir el número E.164

Cuando un usuario marca un número E.164, ENUM construye una cadena única de aplicación (AUS) a partir del número eliminando todos los caracteres que no son dígitos excepto el signo más (+). Por ejemplo, para el número marcado +44-207-946-0148, el AUS es +442079460148.

Luego, el AUS se convierte en una clave inicial, que es un nombre de dominio completo (FQDN), mediante los siguientes pasos:

1. Retire el signo más (+) inicial del AUS.
2. Invierta el orden de los dígitos e inserte puntos entre los dígitos. Por ejemplo, el número 442079460148 se cambia a 8.4.1.0.6.4.9.7.0.2.4.4.
3. Agregue la cadena .e164.arpa para cambiar el número a un nombre de dominio. Por ejemplo, 8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa.

Luego, el nombre de dominio se usa para solicitar registros NAPTR. Los registros NAPTR pueden contener el resultado final o los registros NAPTR pueden generar una nueva clave para solicitar más registros NAPTR del DNS. Al final de este proceso, se genera un SIP URI, que Avaya SBCE usa para actualizar el URI de la solicitud y continúa con el enrutamiento. Si una entrada de enrutamiento no está configurada en el perfil de enrutamiento correspondiente, Avaya SBCE usa este URI para determinar el destino.

Preservación de llamadas

Con la función de preservación de llamadas, el contexto de diálogo del agente de usuario SIP puede sobrevivir a una falla del Administrador de sesión incluso cuando se pierde el contexto del Administrador de sesión. El diálogo continúa con la señalización de extremo a extremo del agente de usuario intacto, a través de un administrador de sesión alternativo. La función de preservación de llamadas está disponible solo para flujos de elemento de enrutamiento SIP (SRE).

Para la conservación de llamadas, un grupo de conmutación por error de Session Manager que comprende un par de servidores de Session Manager se asocia con entidades pares. Las entidades pares, como Avaya SBCE, utilizan técnicas mejoradas de temporización y recuperación de SIP para brindar continuidad en la ruta de señalización durante la falla de Session Manager. Cuando Avaya SBCE detecta que no se puede acceder a un administrador de sesión, Avaya SBCE enruta el tráfico SIP a través del administrador de sesión alternativo mediante el uso del nombre de dominio del grupo de conmutación por error (FGDN) en los encabezados de ruta de registro y vía del administrador de sesión. El FGDN es un nombre de dominio completo (FQDN) que se resuelve en un conjunto ordenado de servidores de Session Manager dentro de un grupo de conmutación por error de Session Manager que proporciona un servicio SRE de alta disponibilidad. Cuando el Administrador de sesión preferido deja de responder,

La convención de nomenclatura para el grupo de conmutación por error es la siguiente:

- Nombre del grupo de conmutación por error:*SM primario-SM secundario*

  Por ejemplo, sm1–sm2.

- FGDN principal:*SM primario-SM secundario.sorbo de dominio*

  Por ejemplo, sm1–sm2.example.com.

- FGDN secundario:*SM primario-SM secundario-identificador.sorbo de dominio*

  Por ejemplo, sm1–sm2–2.example.com.

- Administrador de sesión FQDN:*SM.Dominio IP SM*

  Por ejemplo, sm1.ejemplo.com.

El grupo de conmutación por error de Session Manager puede contener dos o más instancias de miembros de Session Manager. El administrador de sesión principal transporta el tráfico para el grupo de conmutación por error en condiciones normales. Para obtener más información sobre la administración de la función de conservación de llamadas, consulte*Guía de administración y descripción de la función de conservación de llamadas*.

Para admitir la función de conservación de llamadas, Avaya SBCE:

- Mantiene una afinidad con el último administrador de sesión preferido en el grupo de conmutación por error para cada diálogo.
- Conserva el objetivo del grupo de conmutación por error establecido en el contexto del diálogo. Este almacenamiento en caché en el cuadro de diálogo evita consultas de DNS duplicadas innecesarias.
- Admite solicitudes con un FGDN en los encabezados Via, Next Hop Route o Record-Route.
- Restablece el socket TCP o TLS al administrador de sesión fallido si Avaya SBCE detecta que no se puede acceder al administrador de sesión preferido.

- Admite la conservación de llamadas solo en los tipos de transporte TCP y TLS.
- Cambia la afinidad del ámbito del diálogo al Administrador de sesión preferido solo cuando la instancia del Administrador de sesión preferido se vuelve inaccesible. Avaya SBCE vuelve a evaluar la afinidad seleccionando uno de los siguientes:
  - El Avaya SBCE alternativo con la prioridad más alta
  - El administrador de sesión alternativo con la prioridad más alta, excluyendo cualquier instancia alternativa de administrador de sesión en el FG que ya no esté disponible.
- Detecta que un Administrador de sesión está nuevamente en servicio y accesible dentro del intervalo configurado en el**Frecuencia**en la página Configuración del servidor en el**Latido del corazón**pestaña.

Importante:

La configuración de Heartbeat es obligatoria para la función de conservación de llamadas. El latido se utiliza para detectar el Administrador de sesión restaurado.

Admite confiabilidad de respuesta provisional con un mensaje de 100 rel y envía PRACK a todas las respuestas provisionales recibidas.

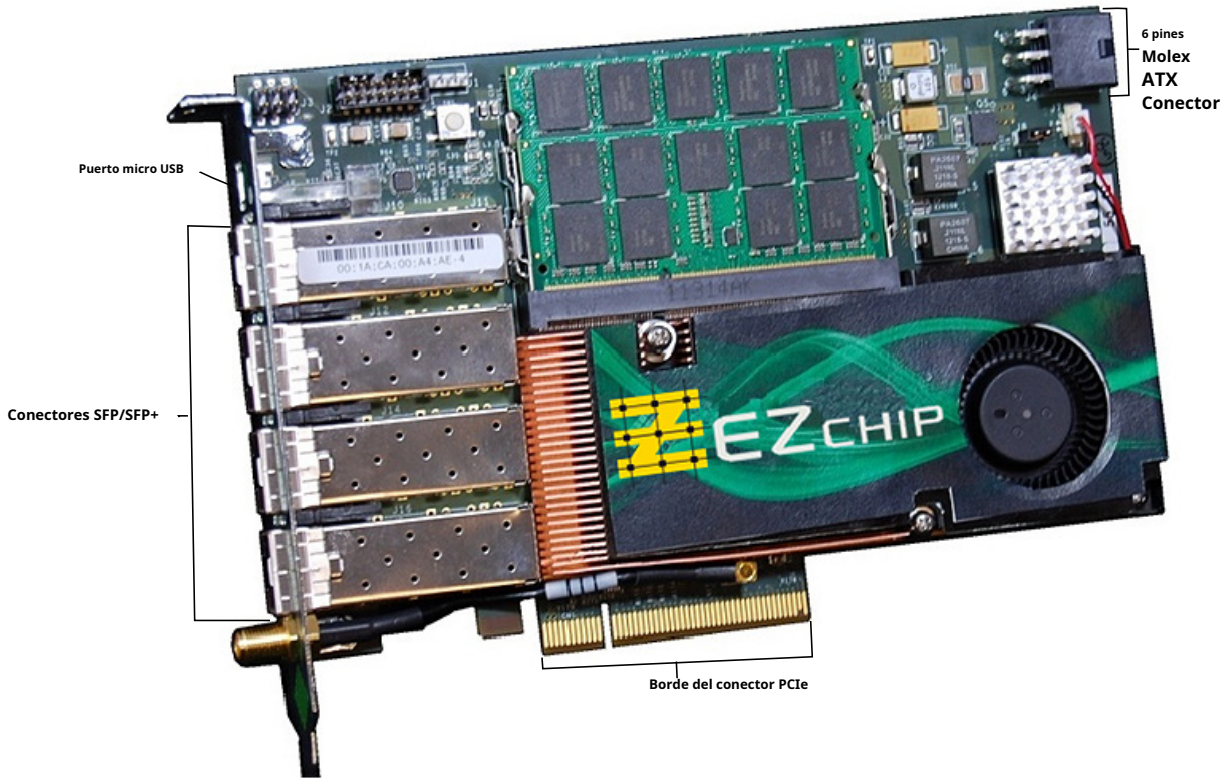
Compatibilidad con el adaptador de aplicaciones inteligente TILEncore-Gx36

Para cada sesión, Avaya SBCE admite paquetes de señalización y de medios. El número de paquetes de medios es significativamente mayor que los paquetes de señalización. Cuando aumenta la cantidad de sesiones en Avaya SBCE, la CPU disponible para procesar paquetes de medios puede dominar el servidor host, incluso antes de que se ocupe todo el ancho de banda de la red. Aumentar la cantidad de CPU disponible para el procesamiento de paquetes de medios o el procesamiento del plano de datos ayuda a que Avaya SBCE admita más sesiones simultáneas. El adaptador de aplicaciones inteligente TILEncore-Gx36 aumenta significativamente la cantidad de núcleos de plano de datos a costos más bajos sin requerir un servidor más grande. Por lo tanto, para brindar más capacidad, Avaya SBCE 7.1 es compatible con el adaptador de aplicación inteligente TILEncore-Gx36.

Descripción general del adaptador inteligente de aplicaciones TILEncore-Gx36

TILEncore-Gx36 es una tarjeta PCIe de una sola ranura de altura completa y media longitud que consta de un procesador TILEncore-Gx de 36 núcleos, memoria integrada y otros componentes para el procesamiento de paquetes. El adaptador requiere una única ranura PCIe en el host. El adaptador funciona como un coprocesador dentro de Avaya SBCE. El software del plano de datos de Avaya SBCE se ejecuta en el adaptador y el resto del software se ejecuta en el servidor host.

Este adaptador solo es compatible con HP DL360 G9 y Dell R630.



Características de TILEncore-Gx36

Rasgo	Descripción
AZULEJO-Gx8036 Procesador	Proporciona un procesador Gx8036 de 36 núcleos (mosaico), con cada mosaico funcionando a 1,2 GHz. Motor de equilibrio de carga y clasificación de paquetes a velocidad de cable que realiza la inspección, el análisis y la distribución iniciales de paquetes a mosaicos. Dos motores criptográficos separados con capacidad de hasta 40 Gbps de rendimiento.
La red Conectividad	Proporciona cuatro puertos físicos SFP/SFP+. Puede configurar cada puerto como Ethernet de 1 Gbps o 10 Gbps.
Adaptador/Anfitrión Interfaz	Opera bajo control de software basado en host. Funciona como un controlador de interfaz de red (NIC) estándar para paquetes como los paquetes de señalización SIP, que la tarjeta no procesa a bordo. Admite interrupciones señalizadas por mensajes (MSI y MSI-X), con las que se puede usar el escalado lateral de recepción (RSS) en el host.
Memoria	Proporciona memoria DDR3 (DDR3-1600) de 8 GB o 16 GB.
virtualización	Admite virtualización de E/S de raíz única (SR-IOV) con la que varios sistemas operativos invitados en un único servidor host pueden compartir el adaptador.

La tabla continúa...

Rasgo	Descripción
Poder y Térmico	Se puede alimentar a través del conector PCIe o del conector de alimentación ATX. Requiere 65 W de los dedos PCIe cuando se alimenta mediante PCIe. Los requisitos de flujo de aire varían entre 100 y 400 lfm, según la configuración interna del servidor.
Puertos	Proporciona cuatro puertos de red físicos, un puerto micro-USB y varios indicadores de estado en el panel posterior del adaptador Gx.
Consola conectividad	Proporciona UART integrado que se puede utilizar para una conexión en serie. La conexión micro-USB que admite la conectividad de la consola está disponible en el panel posterior de la placa. El bus PCIe se puede utilizar para conectarse al adaptador a través de un enlace Ethernet virtual.
Interruptores DIP	Proporciona interruptores DIP ubicados detrás de la tarjeta que se pueden usar para modificar: • Si la placa puede iniciarse a través de las interfaces UART y USB. • Operación de carril PCIe x4 o x8. • Modo operativo PCIe (complejo raíz, terminal o automático). • Uso de energía del conector perimetral. • Fuente de reloj de referencia PCIe para host o local.
Soportado Servidores	Se puede alojar en servidores HP DL360 G9 y Dell R630 en Avaya SBCE versión 7.1.
Aumento de capacidad	Proporciona ganancias de capacidad de hasta 20000 sesiones simultáneas para Avaya SBCE con adaptador TILEncore-Gx36.
Alta disponibilidad	Admite alta disponibilidad para pares de servidores homogéneos. En pares homogéneos de alta disponibilidad, los SBCE de Avaya son del mismo tipo, ambos HP DL360 G9 o ambos R630, y ambos habilitados para Gx o ambos solo para servidor.
IPv6	Admite direcciones IPv6 para Avaya SBCE con adaptador TILEncore-Gx36.
Transcodificación de medios	Admite la transcodificación de medios mediante el uso de Avaya Aura®Servidor multimedia para Avaya SBCE con adaptador TILEncore-Gx36.

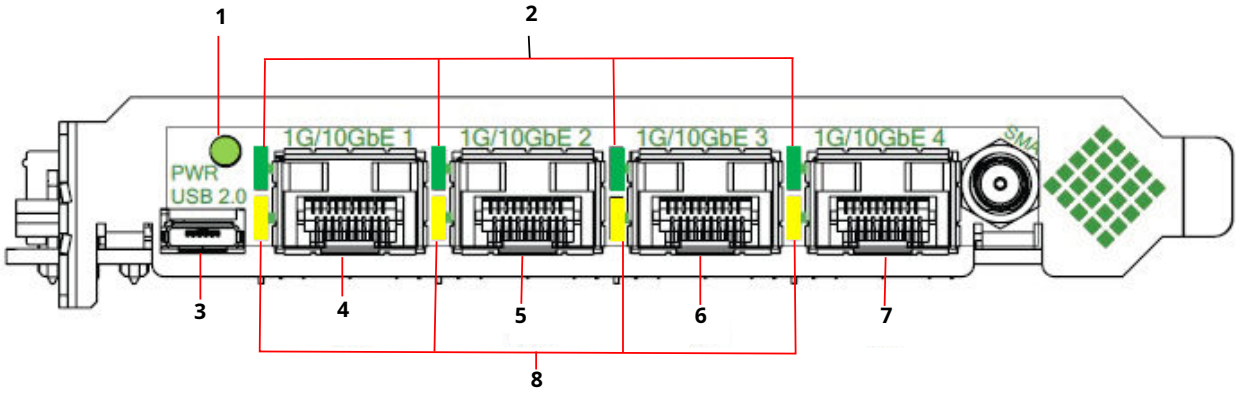
Configuración del adaptador TILEncore-Gx36 instalado en Avaya SBCE

- Cuatro transceptores SFP de 1 Gbps: en la versión 7.1, Avaya SBCE admite un ancho de banda combinado máximo de 4 Gbps.
- Arranca a través del bus PCIe: el software del adaptador se almacena en el disco del servidor host. Herramientas suministradas con Tilera Multicore. El entorno de desarrollo (MDE) se utiliza para arrancar el Gx y transferir una imagen de bootrom a la tarjeta.
- 8 GB de memoria
- Alimentación suministrada a través del conector de borde PCIe: no se requiere cableado adicional dentro del chasis del servidor host.
- Cable serie micro-USB: los SBCE de Avaya que utilizan el adaptador Gx se envían con un cable serie micro-USB que se puede utilizar para proporcionar conectividad de consola en el campo. El cable no viene instalado de fábrica.

- Interruptores DIP: posiciones predeterminadas de fábrica, que brindan la configuración necesaria que requiere Avaya SBCE. Para conocer las especificaciones de los interruptores DIP, consulte la Guía del usuario del Gx36.
- Cuatro interfaces de datos protegidas en Avaya SBCE: las interfaces se denominan A1, B1, A2 y B2. El adaptador está configurado para que estas interfaces estén dispuestas, comenzando desde la izquierda, como A1, A2, B1 y B2.

Para obtener información sobre cómo instalar el adaptador, consulte la documentación de Tilera.

Panel trasero del adaptador de aplicación inteligente TILEncore-Gx36



Nombre	Descripción
1	LED de alimentación El LED de encendido se enciende solo cuando todos los componentes principales de la placa están encendidos y en funcionamiento.
2	LED de enlace Los LED de enlace verdes se encienden cuando el enlace Ethernet funciona.
3	Puerto micro USB El puerto micro USB proporciona una conexión de consola a la tarjeta. Puede reiniciar el adaptador a través del puerto micro USB.
4	Interfaz de red A1 Cada puerto de red funciona a 1 Gbps o 10 Gbps cuando se usa un transceptor SFP.
5	Interfaz de red A2
6	Interfaz de red B1
7	Interfaz de red B2
8	LED de actividad Los LED de actividad amarillos se encienden cuando las interfaces de red de Avaya SBCE están habilitadas.

Capítulo 3: Interoperabilidad

Compatibilidad del producto

Para obtener la información de compatibilidad más reciente y precisa, vaya ahttps://support.avaya.com/CompatibilityMatrix/Index.aspx .

Servidores compatibles con Avaya SBCE

Servidor	Procesadores	Memoria del sistema	Almacenamiento a bordo
Dell R210 IIXL (centro)	Intel Xeon E3-1220 3,10 GHz de cuatro núcleos/4T	4GB (DDR3 1333 MHz)	500 GB (3,5 pulgadas SATA 3 Gb/s – 7,2 K)
Dell R210 II (núcleo)	Intel Xeon E3-1230 3,20 GHz de cuatro núcleos/4T	4GB (DDR3 1333 MHz)	500 GB (3,5 pulgadas SATA 3 Gb/s – 7,2 K)
Dell R210 IIXL (EMS)	Intel Pentium G850 2,90 GHz de doble núcleo/2T	2GB (DDR3 1333 MHz)	2 x 500 GB (3,5 pulgadas SATA 3 Gb/s – 7.2K)
dell r320	Intel®Xeon®E5-2430v2 2,5 GHz, 6 núcleos, 80 W	8GB (DDR4 1600 MT/s UDIMM)	2 x 300 GB 10K SAS
dell r330	Intel®Xeon®E3-1200v5 3,6 GHz, 4 núcleos: 80 W	16 GB (DDR4 2133 MT/s UDIMM)	Hasta cuatro unidades de disco duro intercambiables en caliente de 3,5 pulgadas o Hasta ocho unidades de disco duro intercambiables en caliente de 2,5 pulgadas
dell r620	Intel®Xeon®E5-2600, doble núcleo	32GB (DDR3 1333)	SATA de 2,5 pulgadas 3 Gb/s – 7,2 K
dell r630	2 x Intel®Xeon®E5-2640 2,6 GHz, 8 núcleos, 90 W	32 GB (DDR4 2133 MT/s RDIMM)	2 x 300 GB 10K SAS
HP DL360 G8	Intel®Xeon®E5-2400	hasta 384GB	(8) SFF SAS/SATA/SSD
HP DL360 G9	2 x Intel®Xeon®E5-2640 2,6 GHz, 8 núcleos, 90 W	32 GB (DDR4 2133 MT/s RDIMM)	2 x 300 GB 10K SAS
Portwell CAD-0208 (centro)	Intel®Átomo D510 1,66 GHz - Doble núcleo	2GB (SO-DIMM DDR2 667 MHz)	320 GB (2,5 pulgadas SATA 3 Gb/s – 7,2 K)
Portwell CAD-0230	Intel®Átomo C2000 1,7 GHz - Doble núcleo	2GB (SO-DIMM DDR3 1333 MHz)	Una unidad de disco duro de 2,5 pulgadas

La tabla continúa...

Servidor	Procesadores	Memoria del sistema	Almacenamiento a bordo
Avaya convergente Plataforma 100 servidor en serie con perfil 3	Intel Skylake S-4114, dos CPU por servidor, diez núcleos por CPU, veinte núcleos por servidor, frecuencia de núcleo de 2,2 Ghz	12 módulos RDIMM de 4 GB, 6 módulos RDIMM de 8 GB	Hasta cuatro HDD de 2,5 pulgadas 10K, SAS, HDD SAS de 600 GB
Avaya convergente Plataforma 100 servidor en serie con perfil 5	Intel Skylake G-6132, dos CPU por servidor, catorce núcleos por CPU, veintiocho núcleos por servidor, frecuencia de núcleo de 2,6 Ghz	12 módulos RDIMM de 16 GB	Hasta seis HDD SAS 10K de 2,5 pulgadas, HDD SAS de 600 GB

Nota:

Solo servidores Dell R210 II XL, Dell R620, Portwell CAD-0208, Portwell CAD-0230, Dell R320, Dell R330, Dell R630, HP DL 360 G8, HP DL 360 G9, Avaya Converged Platform 100 series con perfil 3 y Avaya El servidor de la serie Converged Platform 100 con perfil 5 admite nuevas instalaciones.

Productos Avaya

Para obtener la información de compatibilidad más reciente, vaya ahttps://support.avaya.com/CompatibilityMatrix/Index.aspx .

Requisitos de productos de terceros

Puerta de enlace SAL externa

Cuando se usa Secure Access Link (SAL) para el acceso remoto a Avaya SBCE para los servicios de Avaya, el cliente debe proporcionar un SAL Gateway. Los clientes pueden comprar SAL Gateway de Avaya. Los clientes también pueden proporcionar SAL Gateway si el servidor cumple con los requisitos de SAL especificados en el sitio web de soporte de Avaya enhttp://soporte.avaya.com . A veces, se puede usar un SAL Gateway integrado de System Platform en lugar de comprar otro servidor. Ver aviso de soporte de productoPSN003058u .

Compatibilidad del sistema operativo

Avaya SBCE y EMS utilizan RedHat Enterprise Linux 7.x en todas las plataformas.

Capítulo 4: Especificaciones de rendimiento

Capacidad admitida

Tipo de servidor	No-encriptado Sesiones con canalización	encriptado Remoto Trabajador Usuarios	cifrar d Sesiones con Presencia	SIPREC con SORBO canalización replicado Sesiones	Escopia Video sesión ns	transcodificado Sesiones	
	Estándar	Avanzado		Avanzado		Interno	Externo
Avaya Convergido Plataforma 100 servidor de serie con perfil 3 (Dell™ Borde energetico™ servidor R640)*	14,000	20,000	8,000	6,000	800	1,000	2,500
Avaya Convergido Plataforma 100 servidor de serie con perfil 5 (Dell™ Borde energetico™ servidor R640)*	30,000	20,000	10,000	10,000	800	1,000	5,000
Dell R630 con TILEncore Gx36 Inteligente Solicitud Adaptador	30,000	20,000	7,500	10,000	800	1000	5,000
HP DL360 G9 con TILEncore Gx36 Inteligente Solicitud Adaptador	30,000	20,000	7,500	10,000	800	1000	5,000

La tabla continúa...

dell r630 (Alto Capacidad)	14,000	20,000	7,500	6,000	800	1,000	2,500
HP DL360 G9 (Alto Capacidad)	14,000	20,000	7,500	6,000	800	1,000	2,500
Dell R330 (mediados Rango Capacidad)	6,000	5,000	2,000	3,000	200	300	1,250
HP DL360 G9 (rango medio Capacidad)	6,000	5,000	2,000	3,000	200	300	1,250
VMWare ESXi 6.x**	5,000	6,000	3,000	2,500	200	100	1,250
CAD de Portwell 0230	600	500	500	No Aplicable	No Aplicable	No Aplicable	No Aplicable
Nutanix***	5,000	6,000	3,000	2,500	200	100	1,250

Nota:

- Avaya SBCE es compatible con el servidor de la serie Avaya Converged Platform 100 con perfil 3 y perfil 5 (Dell™Borde energetico™R640 Server) de la versión 7.2.2.2 y posteriores.
- * * VMware ESXi 6.x es compatible con el tipo de implementación media de Avaya SBCE.
- * * * Avaya SBCE admite la implementación de KVM usando Nutanix desde la versión 7.2.1 y posteriores.

Nota:

Para los otros servidores admitidos que no se enumeran en la tabla anterior, se aplica la información de capacidad publicada en las versiones anteriores.

Redundancia y alta disponibilidad

Las funciones de redundancia y alta disponibilidad (HA) están disponibles en los servidores EMS y Avaya SBCE. El hardware que admite estas funciones son las plataformas Dell R210 II XL, Dell R320, Dell R620, Dell R630, Dell R330, HP DL360 G8 y HP DL360 G9. Estas funciones también están disponibles para servidores habilitados para TILEncore-Gx y Avaya SBCE implementados en un entorno virtualizado. Estas características admiten HA para pares de servidores homogéneos. En pares HA homogéneos, los dispositivos SBCE de Avaya son del mismo tipo.

La compatibilidad con HA para medios y señalización garantiza que la funcionalidad de seguridad de Avaya SBCE se brinde de manera continua, independientemente de las fallas de hardware o software. La alta disponibilidad requiere un mínimo de dos dispositivos SBCE de Avaya y un servidor EMS independiente.

Página771 de 3226.

Nota:

La alta disponibilidad requiere compatibilidad con el Protocolo de resolución de direcciones gratuitas (GARP) en los elementos de red conectados. Cuando el Avaya SBCE principal falla, el Avaya SBCE secundario transmite un mensaje GARP para anunciar que el Avaya SBCE secundario ahora está recibiendo solicitudes. El mensaje GARP anuncia que una nueva dirección MAC está asociada con la dirección IP de Avaya SBCE. Los dispositivos que no admiten GARP deben estar en una subred diferente con un enrutador compatible con GARP o un conmutador L3 para evitar la comunicación directa. Por ejemplo, para manejar GARP, los gateways de sucursal, Medpro, Crossfire y algunos PBX/IVR deben implementarse en una red diferente de Avaya SBCE, con un enrutador o conmutador L3. Si no coloca las interfaces SBCE de Avaya en una subred diferente, después de la conmutación por error, las llamadas activas tendrán audio unidireccional.

Todas las direcciones IP configuradas en la pantalla Configuración de red se comparten entre ambos dispositivos HA en el modo de implementación HA. Los dispositivos HA también están configurados con direcciones IP privadas y predeterminadas que se utilizan para replicar señales y datos de medios entre sí. Las interfaces configuradas no están operativas en el dispositivo de reserva o secundario hasta que el dispositivo se vuelve activo o principal. Cuando los dispositivos fallan, el dispositivo activo envía un mensaje GARP para actualizar las tablas ARP del dispositivo HA vecino para comenzar a recibir tráfico.

Avaya SBCE alta disponibilidad

El SBCE de Avaya se puede implementar como un par, ya sea en la DMZ de la empresa o en el núcleo, o dispersado geográficamente, donde cada SBCE de Avaya reside en una instalación física separada.

En cualquier configuración, los pares Avaya SBCE HA se pueden implementar en una empresa en una configuración de modo paralelo. En la configuración en paralelo, los paquetes de señalización se enrutan solo al Avaya SBCE principal o activo, que realiza todo el procesamiento de datos. Los puertos de interfaz en el Avaya SBCE en espera no procesan ningún tráfico. Las interfaces de administración en los dispositivos Avaya SBCE tienen diferentes direcciones IP, pero las interfaces de señalización o de medios tienen la misma dirección IP. En la conmutación por error, Avaya SBCE en espera anuncia la nueva MAC como la dirección L2 para la dirección IP común. Los dispositivos Avaya SBCE se sincronizan a través del latido en las interfaces dedicadas, y ambos dispositivos Avaya SBCE están en comunicación continua con Avaya EMS.

Cuando Avaya EMS detecta una falla en el Avaya SBCE activo, los puertos de interfaz de red del SBC activo se desactivan automáticamente. Los puertos del SBC en espera están habilitados. La detección de fallas y la transferencia operativa ocurren sin perder paquetes ni agregar una cantidad significativa de latencia en las rutas de datos. El EMS informa el cambio de estado al EMS para que el administrador del sistema tome medidas.

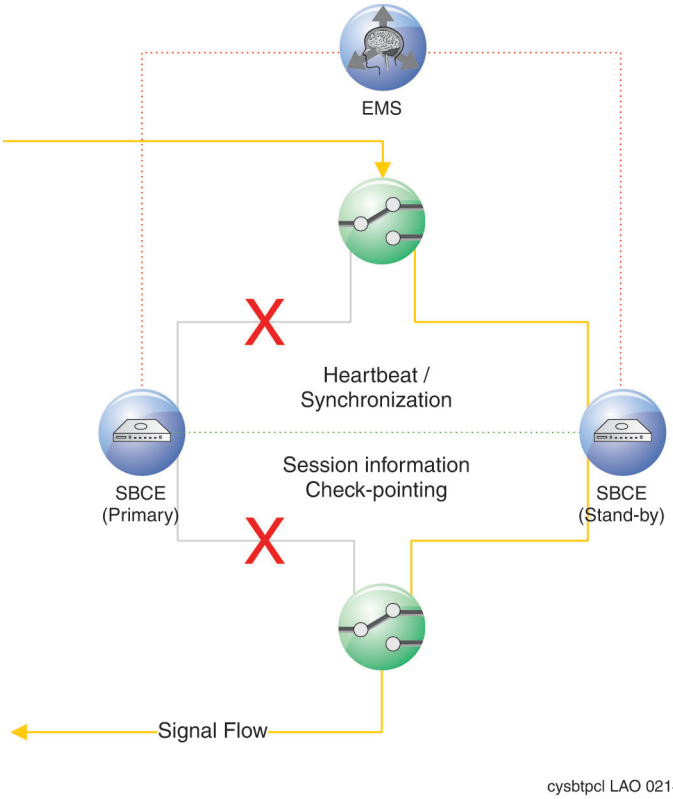


Figura 21: Topología típica de Avaya SBCE HA: modo paralelo (coubicado)

replicación ccsme

La replicación de EMS brinda a una empresa la opción de implementar dos servidores EMS de Avaya para garantizar un monitoreo y control de red ininterrumpidos. Los datos de EMS se replican entre los servidores de forma iterativa según lo determinen los campos definidos por el usuario en la interfaz GUI de EMS. Estos servidores pueden estar ubicados en la misma instalación o en diferentes ubicaciones geográficas.

Avaya SBCE 7.1 y versiones posteriores admiten la configuración activa/activa de EMS HA. Cuando un EMS falla, el otro EMS se puede utilizar sin intervención manual ni tiempo de inactividad.

Capítulo 5: Requisitos ambientales

Requisitos de altitud

Rangos de altitud Dell R210 II XL

Rango	Altitud de funcionamiento	Altitud no operativa
Limite bajo	- 50 pies (-15,2 m)	- 50 pies (-15,2 m)
Limite alto	10.000 pies (3048 m)	35.000 pies (10.668 m)

Dimensiones del hardware

Servidor	Altura	Ancho	Profundidad	Peso
Dell R210 IIXL (Centro)	1,7 pulg. (4,32 cm)	17,10 pulg. (43,45 cm)	15,50 pulg. (39,37 cm)	15.5 libras (7,03 kg)
Dell R210 II (núcleo)	1,7 pulg. (4,32 cm)	17,10 pulg. (43,45 cm)	15,50 pulg. (39,37 cm)	15.5 libras (7,03 kg)
Dell R210 IIXL (EMS)	1,7 pulg. (4,32 cm)	17,10 pulg. (43,45 cm)	15,50 pulg. (39,37 cm)	15.5 libras (7,03 kg)
Dell PowerEdge R320	1,7 pulg. (4,318 cm)	17,1 pulg. (43,434 cm)	24 pulgadas (60,69 cm)	25 libras (11,34 kg)
Dell PowerEdge R330	1,68 pulg. (4,28 cm)	17,09 pulg. (43,42 cm)	24 pulgadas (61,0 cm)	29,54 libras (13,4 kg)
Dell PowerEdge R620	1,7 pulg. (4,318 cm)	17,1 pulg. (43,434 cm)	26,9 pulg. (68,326 cm)	41,0 libras (19,1 kg)
Dell PowerEdge R630	1,7 pulg. (4,318 cm)	19 pulg. (48,26 cm)	27,6 pulgadas (70,104 cm)	43,0 libras (19,50 kg)
Portwell CAD-0208 (centro)	1,65 pulg. (4,20 cm)	7,10 pulg. (18,03 cm)	14,98 cm (5,90 pulg.)	15.5 libras (7,03 kg)
Portwell CAD-0230	1,65 pulg. (4,20 cm)	21,00 cm (8,27 pulg.)	21,00 cm (8,27 pulg.)	15.5 libras (7,03 kg)
HP Proliant DL360 G8	1,7 pulg. (4,318 cm)	17,1 pulg. (43,434 cm)	27,5 pulg. (69,85 cm)	42,3 libras (19,19 kg)
HP Proliant DL360 G9	1,7 pulg. (4,318 cm)	17,2 pulg. (43,68 cm)	27,5 pulgadas (69,85 cm)	44,0 libras (19,95 kg)

Requisitos de temperatura y humedad

Servidor	Temperatura de funcionamiento	Almacenamiento La temperatura	Humedad relativa
Dell R210 II XL (núcleo)	50 °F a 95 °F (10 °C a 35 °C)	- 40 °F a 149 °F (-40 °C a 65 °C)	20% a 90%, sin condensación
Dell R210 II (núcleo)	50 °F a 95 °F (10 °C a 35 °C)	- 40 °F a 149 °F (-40 °C a 65 °C)	20% a 90%, sin condensación
Dell R210 II XL (EMS)	50 °F a 95 °F (10 °C a 35 °C)	- 40 °F a 149 °F (-40 °C a 65 °C)	20% a 90%, sin condensación
dell r320	50 °F a 95 °F (10 °C a 35 °C)	- 40 °F a 149 °F (–40 °C a 65 °C)	20% a 80%, sin condensación
dell r330	41 °F a 104 °F (5 °C a 40 °C)	23 °F a 113 °F (–5 °C a 45 °C)	5% a 85%, sin condensación
dell r620	- 40 °F a 149 °F (–40 °C a 65 °C)	- 40 °F a 149 °F (–40 °C a 65 °C)	5% a 95%
dell r630	50 °F a 95 °F (10 °C a 35 °C)	50 °F a 95 °F (10 °C a 35 °C)	1% a 80%, sin condensación
Portwell CAD-0208 (centro)	41 °F a 95 °F (5 °C a 35 °C)	32 °F a 158 °F (0 °C a 70 °C)	20% a 90%, sin condensación
Portwell CAD-0230	32 °F a 104 °F (0 °C a 40 °C)	14 °F a 158 °F (–10 °C a 70 °C)	20% a 90%, sin condensación
HP DL 360 G8	50 °F a 95 °F (10 °C a 35 °C)	38,7 °C (101,7 °F)	5 a 95% no operativo 10 a 90% operativo
HP DL 360 G9	50 °F a 95 °F (10 °C a 35 °C)	- 22 °F a 140 °F (-30 °C a 60 °C)	8% a 80%, sin condensación

Nota:

Para altitudes superiores a 900 m o 2952 pies, consulte la documentación de Dell para conocer los rangos de temperatura de funcionamiento.

Requerimientos de energía

Servidor	Aporte	Nominal (110 V)	Potencia de CA máx.
Dell R210 IIXL (centro)	Interruptor automático de 110–240 VCA	2A	250W
Dell R210II (centro)	Interruptor automático de 110–240 VCA	2A	250W

La tabla continúa...

Servidor	Aporte	Nominal (110 V)	Potencia de CA máx.
Dell R210 IIXL (EMS)	Interruptor automático de 110–240 VCA	2A	250W
dell r320	110–240 VCA		300W
dell r330	110–240 VCA		350W
dell r620	110–240 VCA	2A	750W
dell r630	110–240 VCA		750W
Portwell CAD-0208 (centro)	Interruptor automático de 110–240 VCA	2A	Adaptador de corriente de 60 vatios
Portwell CAD-0230	12 V CC		40W
HP DL360p G8	100–240 VCA	15A	308,95W
HP DL 360 G9	110–240 VCA		800W

Requisitos de protección del sistema físico

El servidor está equipado con rejillas de ventilación a cada lado del chasis del equipo y rejillas de ventilación en la parte posterior. Asegúrese de seguir estas pautas:

- No bloquee estas salidas de aire.
- No coloque el servidor en un lugar donde la suciedad o el polvo puedan obstruir las rejillas de ventilación o entrar en el chasis y dañar los componentes internos.
- No instale el dispositivo en o cerca de una fuente de calor, incluidos los equipos cercanos que consumen mucha corriente o mucha energía, como bancos de interruptores. El calor excesivo puede hacer que el servidor se sobrecaliente y falle.

Nota:

El cliente debe asegurarse de que los peligros ambientales no interfieran con el funcionamiento del servidor SBCE de Avaya. Estos peligros pueden incluir calor excesivo, humedad excesiva, ventilación inadecuada o interferencia electromagnética de equipos cercanos.

Estándares regulatorios

Los servidores Avaya SBCE cumplen con los siguientes estándares.

Servidor	Certificaciones
Dell R210 II XL (núcleo)	CSA, FCC, UL, RoHS

La tabla continúa...

Servidor	Certificaciones
Dell R210 II (núcleo)	CSA, FCC, UL, RoHS
Dell R210 II XL (EMS)	CSA, FCC, UL, RoHS
dell r320	CSA, FCC, CE, UL, RoHS
dell r330	CSA, FCC, CE, UL, RoHS
dell r620	CSA, FCC, CE, UL, RoHS
dell r630	CSA, FCC, CE, UL, RoHS
HP DL360 G8	CSA, FCC, CE, UL, RoHS
HP DL360 G9	CSA, FCC, CE, UL, RoHS
Portwell CAD-0208 (núcleo)	CE, FCC, UL
Portwell CAD-0230	CE, FCC

Página777 de 3226.

Capítulo 6: Seguridad

Especificación de seguridad

Protección contra intrusiones de comunicaciones unificadas

Los sistemas de prevención de intrusiones (IPS) tradicionales monitorean el tráfico de la red para recopilar y analizar información de varias partes de la red para identificar posibles violaciones de seguridad. Esta información se utiliza para la prevención o mitigación posterior. A diferencia de los IPS tradicionales, los productos de seguridad SBCE de Avaya detectan cualquier evento anómalo, incluidos los ataques de día cero. Además, también evita prácticamente cualquier tipo de intrusión desde fuera de la empresa y uso indebido desde dentro de la empresa. Esta capacidad se debe a la flexibilidad sin igual y al ajuste detallado que se permite cuando los administradores de seguridad de la red establecen conjuntos de reglas de comunicaciones unificadas. La función de seguridad de Avaya SBCE IPS incluye:

- Protección contra inundaciones y fuzzing: protección contra ataques de denegación de servicio (DoS) basados en volumen y mensajes mal formados o fuzzing. Las reglas de depuración de protocolos personalizados detectan y eliminan los mensajes con formato incorrecto que pueden hacer que los servidores de llamadas u otros componentes críticos de la red dejen de responder. Los mensajes con formato incorrecto también pueden hacer que otras partes de la infraestructura de comunicaciones sean vulnerables debido al rendimiento degradado de los componentes críticos de los sistemas de comunicaciones unificadas, como servidores y terminales.
- Prevención de anomalías de medios: habilita selectivamente el tráfico de medios y hace cumplir las reglas sobre el tráfico transportado. El flujo de tráfico se basa en la señalización negociada y otras políticas configuradas, como evitar video o evitar módem/FAX.
- Prevención de suplantación de identidad: se aplican varias técnicas de validación para detectar y prevenir la suplantación de identidad, incluidas las huellas dactilares de punto final para diferentes campos de mensajes para activar otras validaciones y verificaciones.
- Prevención de ataques sigilosos: en función de los patrones de comportamiento de llamadas aprendidos de los extremos de los suscriptores, Avaya SBCE puede detectar llamadas molestas y molestas a un destino o usuario en particular. Estos productos pueden bloquear selectivamente a los abonados de los que proceden las llamadas.
- Prevención de reconocimiento: Avaya SBCE detecta y bloquea los informes de análisis de la capa de aplicación y bloquea a los atacantes que los originan.

Protección contra ataques

Los productos de seguridad SBCE de Avaya garantizan la integridad de todas las aplicaciones IP en tiempo real. Los productos de seguridad SBCE de Avaya mantienen el más alto nivel de seguridad, confiabilidad y disponibilidad de la red de comunicaciones al realizar estas tres funciones críticas: monitoreo, detección y protección.

Vigilancia

Cada SBCE de Avaya proporciona funciones completas de supervisión y gestión de la seguridad de la red. Estas capacidades abarcan cada aspecto de la red UC, incluidos todos los puntos finales, puertas de enlace de medios, servidores de llamadas, correo de voz (VM) y servidores de aplicaciones. Además, las capacidades de monitoreo y administración brindan un sistema de detección, mitigación y generación de informes en cascada y de múltiples capas que proporciona información en tiempo real basada en umbrales de eventos definibles por el usuario. Este sistema admite una interfaz gráfica de usuario (GUI) detallada denominada interfaz web de EMS. El EMS se puede instalar y ejecutar desde cualquier dispositivo de seguridad Avaya SBCE. El EMS también puede instalarse en una plataforma de servidor independiente y utilizarse como un sistema de gestión de elementos (EMS) independiente. Este EMS monitorea y coordina las actividades de seguridad de todos los dispositivos de seguridad Avaya SBCE instalados en una red.

Nota:

Tanto EMS como Avaya SBCE se pueden instalar en una caja. Sin embargo, a medida que crece su red y necesita más de un SBCE de Avaya, el EMS debe instalarse en una plataforma dedicada.

Detección

La capacidad de detección de la solución SBCE de Avaya utiliza numerosos algoritmos dinámicos y adaptables para detectar cualquier anomalía en el comportamiento aprendido de la persona que llama que se basa en criterios de Hora del día (ToD) y Día de la semana (DoW) definibles por el usuario. Estos algoritmos son lo suficientemente flexibles para adaptarse a circunstancias especiales, como fines de semana, días festivos y otros períodos de tiempo especificados por el usuario. La solución SBCE de Avaya también puede aprender y aplicar puntajes de confianza dinámicos, comenzando desde un puntaje desconocido y aumentando o disminuyendo a diferentes niveles según el patrón de comportamiento de la persona que llama, que puede ser Confiable, Conocido, Desconocido, Sospechoso o Spammer. La puntuación de confianza dinámica también depende de los comentarios de la parte llamada, incluida la Lista negra y la Lista blanca, lo que mejora aún más la capacidad crítica de tiempo para detectar comportamientos anómalos.

La capacidad de detección también puede recopilar y correlacionar múltiples eventos y actividades de diferentes nodos y puntos finales en la red para detectar ataques con precisión. De lo contrario, estos ataques podrían haber pasado desapercibidos si solo los informara un único punto de la red. La capacidad de detección puede inspeccionar la secuencia y el contenido de los mensajes para detectar anomalías de protocolo y cualquier instancia de escaneo de punto final. Finalmente, la capacidad de detección de la solución SBCE de Avaya puede validar el origen de una llamada o ataque malicioso sospechoso mediante la implementación de una técnica de detección única que se basa en las huellas dactilares aprendidas de la persona que llama.

Los productos de seguridad SBCE de Avaya pueden aprender continuamente patrones de llamadas y huellas dactilares de terminales. Estos productos también pueden analizar constantemente datos de eventos sin procesar basados en datos específicos definibles por el usuario.

criterios y tomar acción automática. Por lo tanto, los productos de seguridad SBCE de Avaya pueden evolucionar y adaptarse automáticamente para contrarrestar de manera efectiva cualquier amenaza nueva o existente.

Proteccion

El SBCE de Avaya proporciona una protección completa de la red al bloquear los ataques y, al mismo tiempo, pasar llamadas legítimas sin obstáculos. Este nivel excepcional de protección puede extenderse a un punto final, a un grupo específico de puntos finales oa todos los activos de la red. La extensión de esta protección se basa en conjuntos de reglas definidas por el usuario altamente flexibles llamadas Políticas de comunicaciones unificadas. Estas políticas se pueden implementar para discriminar con precisión o normalizar cualquier tráfico multimedia o de señalización entrante o saliente. Por lo tanto, todos los dispositivos de comunicación IP, como teléfonos físicos, teléfonos virtuales, teléfonos Wi-Fi y teléfonos inteligentes, están protegidos de manera efectiva. Los servidores de llamadas, los servidores de correo de voz, los servidores de medios, las puertas de enlace de medios y los servidores de aplicaciones también están protegidos, lo que asegura de manera efectiva toda la red contra todo tipo de ataques.

Fortalecimiento de Avaya SBCE

Las funciones de seguridad de nivel de sistema de capa 3/capa 4 incluyen reglas de firewall de IPTable para proporcionar restricciones en el tráfico entrante. Las restricciones son efectivas después del procesamiento de filtrado de contenido para el tráfico de datos para proteger Avaya SBCE de ataques de nivel IP/ICMP/TCP.

El tráfico saliente no está restringido.

Protección contra inundaciones de capa 3 y capa 4 y escaneos de puertos

Prevención de inundaciones ICMP

Cuando se detecta una inundación ICMP de un host, todas las demás solicitudes de ese host se bloquean durante un tiempo específico.

Bloqueo de exploración de puertos

Cuando se detecta un escaneo de puertos de un host, todas las demás solicitudes de ese host se bloquean durante un tiempo específico.

Restricciones de la interfaz de datos

- Se proporciona protección general en todas las interfaces de datos.
- Las reglas de control de desbordamiento del nivel de señalización de TCP se aplican dinámicamente en la IP de escucha y el puerto de escucha especificados por la aplicación.

Control de inundaciones de nivel de señalización TCP

Solo se permite un número específico de solicitudes en un período específico para los siguientes tipos de solicitudes:

- SINCRONIZACIÓN TCP

- ALETA
- PRIMERA

Configuración de seguridad de todo el sistema

La configuración de seguridad de todo el sistema es compatible con toda la línea de productos de

Avaya. Avaya SBCE tiene los siguientes tipos de protección:

- Protección General
- Restricciones de la interfaz de administración
- Restricciones de interfaz de datos

Para todos los productos, la interfaz de administración se detecta dinámicamente desde la configuración del sistema.

Para Avaya SBCE, no hay restricciones en la interfaz Ethernet interna, ethbint, y la interfaz Ethernet M1 externa, ethext, en la placa del coprocesador Com Express en la caja Avaya SBCE.

Para habilitar Avaya SBCE HA, los puertos TCP 1950 se permiten bidireccionalmente en la interfaz de datos.

Avaya SBCE HA no requiere reglas adicionales para habilitar el tráfico HA.

Seguridad de la instalación

Al instalar el paquete rpm de la aplicación, se agregan o actualizan reglas para esa versión. Después de reiniciar, ICU invoca el script de reglas adecuado para esa plataforma.

Funciones de seguridad DoS

Con la función de seguridad de denegación de servicio (DoS) del EMS, puede ver y editar los parámetros de control de respuesta a ataques de denegación de servicio distribuido (DDoS) y DoS. Estos parámetros se pueden aplicar a puntos finales SIP individuales o a su dominio principal. Además, Avaya SBCE admite informes de actividad DoS durante ciertos períodos de tiempo. La función DoS del servidor y las funciones DoS del dominio se clasifican además en función de los tipos de tráfico, como Trabajador remoto, Troncal y Trabajador remoto, y Troncal. Las siguientes reglas describen los métodos de entrada:

- Para Trabajador remoto, la entrada se toma de Número de trabajadores remotos y Máximo de sesiones simultáneas.
- Para Trunk, la entrada se toma de Max Concurrent Sessions.
- Para Trabajador remoto y Troncal, la entrada se toma de Número de trabajadores remotos y Máximo de sesiones simultáneas.

Reglas para establecer valores de umbral para diferentes tipos de tráfico:

- Server DoS es aplicable para umbrales iniciados. El umbral iniciado se aplica a cualquier solicitud SIP enrutada al servidor, independientemente de si se recibe alguna respuesta.
- En el cálculo de todos los valores de umbral, se considera el 10% del valor real.

- Server DoS también puede ser aplicable para el tráfico de trabajadores remotos en caso de un valor de umbral pendiente. El umbral pendiente significa una solicitud SIP para la cual no ha llegado una respuesta correspondiente del servidor.
- La función DoS del servidor también es aplicable en caso de que falle el valor del umbral. El umbral fallido implica que la solicitud de falla ha llegado para una solicitud SIP distinta de 401 y 407.

Lista de valores de umbral recomendados:

- El valor de umbral recomendado para la función DoS de origen único para la implementación de trabajadores remotos es de 300 mensajes.
- El valor de umbral recomendado para el enlace troncal es de 15 mensajes.
- El valor de umbral predeterminado para el trabajador remoto de Avaya en caso de DoS telefónico es de 200 mensajes.
- El valor de umbral recomendado para Call Walking en caso de implementación de trabajadores remotos: INVITACIÓN: 10 mensajes, Registro: 5 mensajes y Todos: 20 mensajes.

depurador de protocolo

La depuración de protocolos utiliza un mecanismo estadístico sofisticado para verificar exhaustivamente los mensajes de señalización SIP entrantes en busca de varios tipos de eventos y anomalías específicos del protocolo. El depurador de protocolo verifica ciertas características del mensaje, como el formato correcto del mensaje, la secuencia del mensaje, la longitud del campo y el contenido con las plantillas recibidas de Avaya. Los mensajes que violan las reglas de seguridad dictadas por las plantillas de depuración se eliminan mientras que los mensajes que violan las reglas de sintaxis se reparan. Los mensajes se reparan reescribiéndolos, truncándolos, rechazándolos o quitándolos, según las reglas de procesamiento impuestas por las plantillas. Avaya prepara plantillas de reglas de depuración de protocolos y el usuario puede editar las plantillas mínimamente.

La limpieza de protocolos para SIP le permite instalar un paquete de reglas de limpieza. También puede habilitar o deshabilitar las reglas de depuración contenidas en el paquete y eliminar el paquete del sistema. Además, puede ver una lista de todas las reglas de depuración instaladas.

Ocultación de topología

La ocultación de topología le permite cambiar los parámetros clave de los mensajes SIP para ocultar o enmascarar cómo aparece la red de su empresa ante un usuario malintencionado o no autorizado.

Reglas de cortafuegos

Las reglas de firewall protegen Avaya SBCE y las comunicaciones y señalización para Avaya SBCE. Las reglas del cortafuegos están codificadas y no se pueden configurar. Las reglas de firewall se pueden dividir en las siguientes categorías:

- Reglas comunes

- Normas de gestión
- Reglas de interfaz de datos

Reglas comunes

Se aplican reglas comunes a todas las interfaces. Las reglas comunes se dividen en las siguientes categorías:

- Restricciones ICMP
- Detección de escaneo de puertos
- Reglas de KILLSCAN

Restricciones ICMP

- Acepte siempre las respuestas de ping de ICMP.
- Cualquier dirección IP que envíe una solicitud de ping ICMP se agregará a la lista de pingflood.
- Cuando una IP en la lista de pingflood envía una solicitud de ping ICMP, descarte la solicitud si esa IP ha enviado cinco solicitudes de ping en un segundo.
- Aceptar todas las demás solicitudes de ping ICMP.
- Los datagramas de redirección ICMP para la red tienen una velocidad limitada a uno por segundo.
- Los datagramas de redirección de ICMP para el host tienen un límite de velocidad de uno por segundo.
- Los mensajes de destino inalcanzable de ICMP tienen un límite de velocidad de uno por segundo.
- Los mensajes ICMP de tiempo excedido tienen un límite de velocidad de uno por segundo.
- Los mensajes de encabezado de IP incorrectos de ICMP tienen un límite de velocidad de uno por segundo.
- Descartar todos los demás paquetes ICMP.

Detección de escaneo de puertos

Procedimiento

1. Siga las reglas de KILLSCAN.
2. Acepte todos los paquetes con estado NO VÁLIDO.

Reglas de KILLSCAN

1. Elimine la IP actual de la lista de exploración de puertos.
2. Cualquier dirección IP que envíe paquetes con indicadores FIN, PSH y URG configurados, pero sin indicadores SYN, RST o ACK, se agregará a la lista de exploración de puertos.
3. Cualquier dirección IP que envíe paquetes con indicadores SYN y RST establecidos se agregará a la lista de exploración de puertos.
4. Cualquier dirección IP que envíe paquetes con indicadores FIN y SYN configurados se agregará a la lista de exploración de puertos.
5. Cualquier dirección IP que envíe paquetes con indicadores FIN configurados, pero sin indicadores SYN, RST, PSH, ACK o URG se agregará a la lista de exploración de puertos.
6. Cualquier dirección IP que envíe paquetes con indicadores FIN, SYN, RST, PSH, ACK y URG establecidos se agregará a la lista de exploración de puertos.
7. Cualquier dirección IP que envíe paquetes sin ningún indicador FIN, SYN, RST, PSH, ACK o URG establecido se agrega a la lista de exploración de puertos.

8. Cualquier dirección IP que envíe paquetes con indicadores FIN, SYN, RST, PSH, ACK y URG establecidos se agregará a la lista de exploración de puertos.

9. Descarte todos los paquetes de cualquier IP en la lista de exploración de puertos.

Reglas de administración y MGMTPROTECT

Las reglas de administración se aplican solo a las interfaces de administración. El primer paso en las reglas de gestión es seguir las reglas de MGMTPROTECT, que se pueden dividir en las siguientes categorías:

- Restricciones de inundación de TCP
- Reglas SSH
- Reglas HTTPS
- Reglas de DNS
- Reglas de Syslog
- Reglas de OpenVPN

Reglas de gestión

- Siga las reglas de MGMTPROTECT.
- Aceptar todos los paquetes en estado RELACIONADO o ESTABLECIDO.
- Aceptar todos los paquetes en el puerto TCP 222.
- Aceptar todos los paquetes en el puerto TCP 443.
- Aceptar todos los paquetes en el puerto TCP 53.
- Aceptar todos los paquetes en el puerto UDP 53.
- Aceptar todos los paquetes en el puerto TCP 514.
- Aceptar todos los paquetes en el puerto UDP 514.
- Aceptar todos los paquetes en el puerto UDP 123.
- Descartar todos los demás paquetes.

Restricciones de inundación de TCP para todos los puertos

- Cualquier dirección IP que envíe paquetes con indicadores FIN configurados, pero sin indicadores SYN, RST, PSH, ACK o URG se agregará a la lista finrstlim.
- Cualquier dirección IP que envíe paquetes con indicadores RST configurados, pero sin indicadores FIN, SYN, PSH, ACK o URG se agregará a la lista finrstlim.
- Para cualquier dirección IP en la lista finrstlim que envíe diez paquetes en un segundo, descarte el paquete.

reglas SSH

- Cualquier dirección IP que envíe, en el puerto 222, paquetes con el indicador SYN, pero sin RST ni ACK, se agregará a la lista sshsyn.
- Para cualquier dirección IP en la lista sshsyn que envía, en el puerto 222:

  Quince paquetes con el indicador SYN, pero sin RST o ACK en 1 minuto durante el TTL del paquete anterior enviado, descartan el paquete.

Diez paquetes con la bandera SYN, pero sin RST o ACK en 30 segundos durante el TTL del paquete anterior enviado, rechazan el paquete. Se envía un mensaje de puerto ICMP inalcanzable para el paquete.

reglas HTTPS

- Cualquier dirección IP que envíe, en el puerto 443, paquetes con el indicador SYN, pero sin RST ni ACK, se agregará a la lista httpssyn.
- Para cualquier dirección IP en la lista httpssyn que envía, en el puerto 443:
  - Diez paquetes con la bandera SYN, pero sin RST o ACK en un segundo durante el TTL del paquete anterior enviado, descartan el paquete.
  - Cinco paquetes con la bandera SYN, pero sin RST o ACK en un segundo durante el TTL del paquete anterior enviado, rechazan el paquete. Envíe un mensaje de puerto ICMP inalcanzable.

reglas DNS

- Cualquier dirección IP que envíe, en el puerto TCP 53, paquetes con el indicador SYN, pero sin RST ni ACK, se agregará a la lista dnssyn.
- Para cualquier dirección IP en la lista dnssyn que envía, en el puerto TCP 53:
  - Diez paquetes con la bandera SYN, pero sin RST o ACK en un segundo durante el TTL del paquete anterior enviado, descartan el paquete.
  - Cinco paquetes con la bandera SYN, pero sin RST o ACK en un segundo durante el TTL del paquete anterior enviado, rechazan el paquete. Envíe un mensaje de puerto ICMP inalcanzable.

Reglas de interfaz de datos

Las reglas de interfaz de datos se aplican solo a las interfaces de datos. Todas las reglas DATAIFPROTECT predeterminadas están comentadas, aunque el comando protectsocket genera dinámicamente más reglas DATAIFPROTECT.

- Siga las reglas de DATAIFPROTECT.
- Aceptar todos los paquetes.

Comando de protección de socket

El comando protect-socket toma un tipo de hardware (1U), agregar o "eliminar", un esquema de protección (un número), una dirección IP para proteger y un puerto para proteger. A partir de estos, genera un conjunto de reglas de firewall para proteger esa IP y puerto, todo agregado a la lista de reglas DATAIFPROTECT.

- Cualquier dirección IP que envíe un paquete a la IP y puerto especificados con el indicador SYN pero no RST o ACK se agregará a la lista de aplicaciones.
- Para cualquier dirección IP en la lista de reglas que envía:
  - Diez paquetes con el indicador SYN, pero sin RST o ACK a la IP y puerto especificados en un segundo durante el TTL del paquete anterior enviado, descartan el paquete.
  - Cinco paquetes con la bandera SYN, pero sin RST o ACK a la IP y puerto especificados en un segundo durante el TTL del paquete anterior enviado, rechazan el paquete. Envíe un mensaje de puerto ICMP inalcanzable.

- Si el esquema de protección se da como 1, siga también estas reglas:
  - Para cualquier dirección IP que envíe veinte paquetes en estado ESTABLECIDO a la IP y el puerto especificados en un segundo, descarte el paquete.
  - Mantenga un registro de cualquier dirección IP que envíe un paquete en el estado ESTABLECIDO a la IP y el puerto especificados.
  - Para cualquier dirección IP que envíe tres paquetes en el estado NUEVO a la IP y el puerto especificados en un segundo, descarte el paquete.
  - Mantenga un registro de cualquier dirección IP que envíe un paquete en el estado NUEVO a la IP y el puerto especificados.
- Eliminar cualquier regla existente para aceptar paquetes.
- Aceptar todos los paquetes.

Especificación de utilización del puerto

Restricciones del puerto de la interfaz de administración

Solo los puertos seleccionados están permitidos en la interfaz de administración y el resto del tráfico TCP/UDP está bloqueado en la interfaz de administración.

Interno: entre uno o más SBCE de Avaya y el EMS

- SSH TCP-222.
- HTTPS TCP-443.
- OpenVPN UDP-1194.
- Registro del sistema TCP/UDP-514.
- NTP UDP-123.

Externo: entre el EMS y los SBCE de Avaya y un dispositivo externo

- SSH TCP-222.
- HTTPS TCP-443.
- Registro del sistema TCP/UDP-514.
- NTP UDP-123.
- DNS TCP/UDP-53 para DNS y los puertos de señalización y medios.
- SNMP versión 2 o 3 UDP-161 + 162. El agente SNMP recibe solicitudes en el puerto UDP 161 y el administrador SNMP recibe notificaciones de trampas e InformRequests en el puerto 162

paquetes TCP

Independientemente de los puertos TCP, solo se permite una cantidad específica de paquetes TCP desde un host dentro de un marco de tiempo específico.

puerto SSH

Las siguientes reglas se aplican al puerto SSH:

- Solo se permite un número específico de conexiones desde un host dentro de un marco de tiempo específico.
- Solo se responde a un número específico de solicitudes de conexión con ICMP inalcanzable.
- Las solicitudes de conexión adicionales se eliminan hasta que las solicitudes de conexión nuevas se detienen durante un período específico.

Asignaciones de puertos adicionales

servidor DNS

Si el servidor DNS no está en la DMZ, abra el puerto UDP 53 en Avaya SBCE a través de la GUI de EMS. Luego, Avaya SBCE puede acceder al servidor DNS.

SNMP

Si tiene su propio SNMP, abra los puertos SNMP UDP 161 y 162 en Avaya SBCE a través de la GUI de EMS. Luego, Avaya SBCE puede acceder al SNMP desde la DMZ.

registro del sistema

Si tiene su propio Syslog, abra el puerto 514 de Syslog UDP en Avaya SBCE a través de la GUI de EMS. Luego, Avaya SBCE puede acceder al Syslog desde la DMZ.

Puertos multimedia

El rango de puertos de medios predeterminado es de 35000 a 40000, pero se pueden configurar otros rangos de puertos de medios, si se requiere un rango de puertos de medios diferente.

Puertos de señalización SIP

Los siguientes puertos son puertos predeterminados. Se pueden configurar otros puertos.

- TCP/UDP 5060
- TLS5061

Puertos HTTP/HTTPS

Estos puertos se utilizan para las comunicaciones y los archivos de configuración y las descargas de firmware de Personal Profile Management (PPM). Configure estos puertos en Avaya SBCE a través de la GUI de EMS. Luego, los teléfonos pueden iniciar sesión y descargar archivos de configuración desde el servidor HTTP de Avaya o el servidor HTTPS.

- Puerto HTTP 8080 o puerto 80
- Puerto HTTPS 443

Puertos LDAP/LDAPS

- Puerto LDAP 389
- Puerto LDAPS 636

Aura de Avaya®Puerto de descarga del servidor multimedia

El puerto predeterminado es el puerto 7150.

Puerto de control compartido

En las implementaciones de trabajadores remotos donde los terminales están configurados en el modo de control compartido, habilite el puerto de control compartido en la interfaz interna de Avaya SBCE hacia Avaya Aura®la red. Este puerto podría ser cualquier puerto TLS no utilizado en la interfaz interna de Avaya SBCE, por ejemplo, el puerto 5063. Este puerto debe estar habilitado en el firewall interno entre Avaya SBCE y Avaya Aura®la red.

Para obtener más información sobre el uso del puerto, consulte*Matriz de puertos de Avaya: ASBCE*.

Capítulo 7: Requisitos de licencia

Avaya SBCE utiliza el Sistema de entrega y licencia de productos (PLDS) de Avaya para crear licencias de la versión 7.2 y descargar el software Avaya SBCE. El archivo de licencia generado por PLDS se descarga al EMS. PLDS no está integrado con WebLM. Utilice PLDS para realizar operaciones como activaciones de licencias, actualizaciones de licencias, movimientos de licencias y descargas de software.

Hay dos versiones con licencia de Avaya SBCE:

- Los servicios estándar ofrecen enlaces troncales SIP seguros.
- Los servicios avanzados agregan usuario de espacio de trabajo móvil, replicación de medios y otras funciones a la oferta de servicios estándar.

Aura de Avaya®Las licencias de Mobility Suite y Collaboration Suite incluyen Avaya SBCE.

Nota:

Se requieren licencias y un servidor WebLM para una actualización a la versión 7.2 o una nueva instalación de Avaya SBCE versión 7.2.

Características de la licencia SBCE de Avaya

Para utilizar una función, debe asegurarse de que el archivo de licencia que cargue en WebLM tenga las licencias adecuadas para la función. No puede configurar o usar una función si la licencia correcta para esa función no está presente en el archivo de licencia.

Función de licencia	Descripción
VALUE_SBCE_STD_SESSION_1	Especifica el número de licencias de sesión estándar.
VALUE_SBCE_STD_HA_SESSION_1	Especifica el número de licencias de sesión de HA de servicio estándar.
VALUE_SBCE_ADV_SESSION_1	Especifica la cantidad de licencias de sesión para trabajadores remotos, grabación de medios y cifrado. **Nota:** Debe comprar e implementar una licencia de sesión estándar con cada función de licencia avanzada.
VALUE_SBCE_ADV_HA_SESSION_1	Especifica el número de licencias de sesión de HA de servicio avanzado.

La tabla continúa...

Función de licencia	Descripción
VALUE_SBCE_VIDEO_CONF_SVC_SESSIO N_1	Especifica el número de Avaya Scopia®Licencias de sesión de videoconferencia.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Especifica el número de Avaya Scopia®licencias de sesión HA de videoconferencia.
VALUE_SBCE_CES_SVC_SESSION_1	Especifica el número de licencias de sesión de Client Enablement Services.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Especifica el número de licencias de sesión de alta disponibilidad de Client Enablement Services.
VALUE_SBCE_TRANS_SESSION_1	Especifica el número de licencias de sesión de transcodificación.
VALUE_SBCE_TRANS_HA_SESSION_1	Especifica el número de licencias de sesión de alta disponibilidad de transcodificación.
VALUE_SBCE_ELEMENTS_MANAGED_1	Especifica la cantidad máxima de elementos SBCE de Avaya administrados.
VALOR_SBCE_VIRTUALIZACIÓN_1	Especifica que se permite la descarga de archivos VMware OVA para Avaya SBCE.
VALUE_SBCE_ENCRYPTION_1	Especifica el cifrado Avaya SBCE y es necesario para las licencias avanzadas.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_ 1	Especifica la configuración de HA para la instalación.
FEAT_SBCE_DYNAMIC_LICENSING_1	Especifica que se permiten licencias dinámicas o agrupadas para Avaya SBCE.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Especifica el cifrado Avaya SBCE solo para señalización.

Detalles del servidor WebLM

Avaya SBCE usa WebLM para los requisitos de licencia.

El archivo de licencia contiene la siguiente información:

- Nombre del producto
- Versión de software compatible
- Fecha de caducidad
- Identificación del anfitrión

  El ID de host principal de WebLM se usa para crear el archivo de licencia.
- Funciones con licencia
- Capacidad con licencia

Puede instalar el archivo de licencia SBCE de Avaya en System Manager WebLM, WebLM local o servidor WebLM independiente.

Página790 de 3226.

No utilice IP OfficeWebLM para instalar el archivo de licencia de Avaya SBCE. Avaya SBCE no es compatible con IP OfficeWebLM.

Utilice los siguientes formatos de URL para instalar una licencia en el servidor WebLM de System Manager o en el servidor WebLM independiente:

- Servidor WebLM de System Manager: https://<SMGR_server_IP> :52233/WebLM/LicenseServer
- Servidor WebLM independiente: https://<WEBLM_server_IP> :52233/WebLM/LicenseServer

Para instalar una licencia a través de un servidor WebLM local en:

- Avaya SBCE en un entorno virtualizado: descargue el archivo OVA de WebLM desde PLDS e implemente el archivo OVA en la máquina virtual.
- Dispositivo de hardware Avaya SBCE: Seleccione el**Usar servidor WebLM local**casilla de verificación

Las opciones para configurar la dirección IP del servidor WebLM están disponibles en la página Administración del sistema de la interfaz web de EMS.

Advertencia:

El EMS virtual no puede ejecutar un WebLM local.

Capítulo 8: Recursos

Documentación

La siguiente tabla enumera los documentos relacionados con este producto. Descargue los documentos del sitio web de soporte de Avaya enhttp://soporte.avaya.com

Título	Descripción	Audiencia
Implementación		
Implementación de Avaya Session Border Controller para empresas	Instalación de hardware y procedimientos de configuración preliminar para instalar Avaya SBCE en una red VoIP empresarial SIP.	Implementación ingenieros
Implementación de Avaya Session Border Controller para empresas en un entorno virtualizado	Procedimientos de instalación virtual y configuración preliminar para instalar Avaya SBCE en una red VoIP empresarial SIP.	Implementación ingenieros
Actualización de Avaya Session Border Controller para empresas	Procedimientos para actualizar a Avaya SBCE 7.2.	Implementación ingenieros
Mantenimiento y solución de problemas		
Administración de Avaya Session Border Controller para empresas	Procedimientos de configuración y administración.	Implementación ingenieros, Administradores
Solución de problemas y mantenimiento de Avaya Session Border Controller for Enterprise	Procedimientos de solución de problemas y mantenimiento.	Implementación ingenieros, y ingenieros de ventas
Referencia		
Matriz de puertos de Avaya: ASBCE 7.2	Información del puerto.	Implementación ingenieros, Administradores, y ingenieros de ventas

Enlaces relacionados

Búsqueda de documentos en el sitio web de soporte de Avaya en la página 101

Página792 de 3226.

Búsqueda de documentos en el sitio web de soporte de Avaya

Procedimiento

1. Navegue hastahttp://soporte.avaya.com/ .
2. En la parte superior de la pantalla, escriba su nombre de usuario y contraseña y haga clic en**Acceso**.
3. Haga clic en**Soporte por producto**>**Documentos**.
4. en**Ingrese su producto aquí**, escriba el nombre del producto y luego seleccione el producto de la lista.
5. En**Elija Liberar**, seleccione un número de versión apropiado.
6. En el**Tipo de contenido**filtro, haga clic en un tipo de documento o haga clic en**Seleccionar todo**para ver una lista de todos los documentos disponibles.

   Por ejemplo, para guías de usuario, haga clic en**Guías de usuario**en el**Tipo de contenido**filtrar. La lista muestra los documentos solo de la categoría seleccionada.
7. Haga clic en**Ingresar**.

Enlaces relacionados

Documentación en la página 100

Capacitación

Los siguientes cursos están disponibles en el sitio web de Avaya Learning enwww.avaya-learning.com . Después de iniciar sesión en el sitio web, ingrese el código del curso o el título del curso en el**Búsqueda**campo y haga clic**Vamos** para buscar el curso.

Nota:

Los cursos de capacitación de Avaya o los cursos de aprendizaje de Avaya no brindan capacitación sobre ningún producto de terceros.

Código del curso	Título del curso
5U00090E	Acceso al conocimiento: controlador de borde de sesión de Avaya
5U00160E	Acceso a la colección de conocimiento: Soporte básico de Avaya Unified Communications

Visualización de videos de mentores de Avaya

Los videos de orientación de Avaya brindan contenido técnico sobre cómo instalar, configurar y solucionar problemas de los productos de Avaya.

Acerca de esta tarea

Los videos están disponibles en el sitio web de soporte de Avaya, enumerados bajo el tipo de documento de video y en el canal administrado por Avaya en YouTube.

Procedimiento

- Para encontrar videos en el sitio web de soporte de Avaya, vaya ahttp://soporte.avaya.com y realice una de las siguientes acciones:
  - En**Búsqueda**, escribeVídeos de orientación de Avayapara ver una lista de los videos disponibles.
  - En**Búsqueda**, escriba el nombre del producto. En la página Resultados de la búsqueda, seleccione**Video**en el **Tipo de contenido**columna de la izquierda.
- Para encontrar los videos de Avaya Mentor en YouTube, vaya awww.youtube.com/AvayaMentor y realice una de las siguientes acciones:
  - Ingrese una palabra clave o palabras clave en el**Canal de búsqueda**para buscar un producto o tema específico.
  - Desplácese hacia abajo en Listas de reproducción y haga clic en el nombre de un tema para ver la lista disponible de videos publicados en el sitio web.

Nota:

Los videos no están disponibles para todos los productos.

Apoyo

Vaya al sitio web de soporte de Avaya enhttp://soporte.avaya.com para obtener la documentación, los avisos de productos y los artículos de conocimiento más actualizados. También puede buscar notas de la versión, descargas y resoluciones de problemas. Utilice el sistema de solicitud de servicio en línea para crear una solicitud de servicio. Chatea con agentes en vivo para obtener respuestas a tus preguntas o solicita a un agente que te conecte con un equipo de soporte si un problema requiere experiencia adicional.

Glosario

ARP	protocolo de resolucion de DIRECCION
códec	Codificador/Decodificador
Ataque de día cero	Ver Ataque de día cero.
DDoS	Denegación de servicio distribuida
Zona desmilitarizada (DMZ)	Un término relacionado con la red informática que se refiere a la "zona neutral" entre la red privada de una empresa y la red pública externa. Por lo general, se inserta un host de computadora o una pequeña red en esta zona neutral para evitar que los usuarios externos obtengan acceso directo a la red interna.
Negación de servicio (DoS)	El objetivo o resultado final de ciertos tipos de ataques maliciosos u otras actividades contra una red, donde está prohibido el acceso a los servicios, recursos o puntos finales de la red.
Digerir Autenticación (DA)	Un esquema de autenticación del Protocolo de transporte de hipertexto (HTTP) mediante el cual las contraseñas de los usuarios se cifran antes de enviarse a través de Internet, lo que certifica la integridad de los datos del Localizador uniforme de recursos (URL). La desventaja de DA es que, aunque las contraseñas están encriptadas, los datos que se intercambian no lo están; se envía en claro.
Denegación distribuida de Servicio (DDoS)	Un tipo más sofisticado de ataque DoS en el que se explota una vulnerabilidad común para penetrar primero en sistemas muy dispersos o puntos finales individuales y luego usar esos sistemas para lanzar un ataque coordinado. Mucho más difícil de detectar que simples ataques DoS.
DMZ	Zona desmilitarizada
DoS	Negación de servicio
DoW	Día de la semana
ccsme	Sistema de gestión de elementos
FW	cortafuegos
GARP	Protocolo de resolución de direcciones gratuitas
interfaz gráfica de usuario	Interfaz gráfica del usuario

Página795 de 3226.

DECIR AH	Ataque de alta disponibilidad o cosecha
Alta disponibilidad	La función SBCE que permite implementar dos dispositivos de seguridad SBCE como un par integral, en el que uno de los dispositivos funciona como principal y el otro como alternativo o de reserva. Conectados por una señal de latido y una base de datos compartida, los dos dispositivos de seguridad SBCE brindan protección contra fallas en caso de que uno de los dispositivos no funcione correctamente.
HTTP	Protocolo de Transferencia de Hipertexto
ICMP	Protocolo de mensajes de control de Internet
ICMP	Protocolo de mensajes de control de Internet
SOY	Mensajería instantánea
Intrusión	Un usuario o proceso malintencionado que se hace pasar deliberadamente por un usuario o proceso legítimo.
IP	protocolo de Internet
IPS	Sistema de protección contra intrusos
ES P	Proveedor de servicios de telefonía por Internet
Latencia	La cantidad de tiempo que tarda un paquete en cruzar una conexión de red, desde el remitente hasta el receptor. Además, la cantidad de tiempo que un dispositivo de red (cortafuegos, enrutador, etc.) retiene un paquete antes de que se reenvíe a su siguiente destino.
MAC	Código de autenticación de mensajes
MCD	Detección de llamada de máquina
NAT	Traducción de Direcciones de Red
NTP	Protocolo de tiempo de red
RTP	Protocolo de transporte en tiempo real
SBC	Controlador de borde de sesión
SBCE	Controlador de borde de sesión para empresas
Enchufes seguros Capa (SSL)	SSL es un método comúnmente utilizado para administrar la seguridad de un mensaje transmitido a través de Internet y se incluye como parte de la mayoría de los navegadores y productos de servidor web. Originalmente desarrollado por Netscape, SSL obtuvo el apoyo de varios desarrolladores influyentes de clientes/servidores de Internet y se convirtió en el estándar de facto hasta que evolucionó a Transport Layer Security (TLS).

La parte de "sockets" del término se refiere al método de sockets de pasar datos de un lado a otro entre un cliente y un programa de servidor en una red o entre capas de programa en la misma computadora (donde un "socket" es un punto final en una conexión) . SSL utiliza el sistema de cifrado de clave pública y privada Rivest, Shamir y Adleman (RSA), que también incluye el uso de un certificado digital.

Si un sitio web está alojado en un servidor compatible con SSL, se puede habilitar SSL y se pueden identificar páginas web específicas que requieren acceso SSL.

TLS y SSL no son interoperables. Sin embargo, un mensaje enviado con TLS puede ser manejado por un cliente que maneja SSL pero no TLS.

SORBO	protocolo de Iniciacion de Sesion
SNMP	Protocolo Simple de Manejo de Red
CORREO NO DESEADO	Un término común utilizado para describir la inundación deliberada de direcciones de Internet o buzones de correo de voz con múltiples copias del mismo mensaje digital o de voz en un intento de forzarlo a los usuarios que de otro modo no elegirían recibirlo. El SPAM puede ser malicioso o simplemente molesto, pero en cualquier caso, el costo de enviar esos mensajes corre en su mayor parte a cargo del destinatario o de los transportistas y no del remitente (SPAMMER).
Parodia	Un método frecuente de engañar a los extremos de VoIP para obtener acceso y manipular sus recursos (por ejemplo, falsificar una dirección de Internet para que un usuario malintencionado parezca un usuario de Internet conocido o inofensivo y de confianza).
SRTP	Protocolo de transporte seguro en tiempo real
SSL	Capa de conexión segura
ATURDIR	Travesía simple de UDP a través de NAT
TCP	Protocolo de Control de Transmisión
TCP/IP	Protocolo de Control de Transmisión / Protocolo de Internet
TFTP	Protocolo trivial de transferencia de archivos
TLS	Transport Layer Security
ToD	Hora del día
Trombón	La situación en la que el tráfico de medios RTP se origina en un punto determinado dentro de una red y sigue una ruta fuera de esa red hacia otra red (la

	red de acceso, por ejemplo) y de regreso a un destino cercano a donde se originó. Ver Anti-trombón.
tunelización	Un método de seguridad utilizado para garantizar que los paquetes de datos que atraviesan una red pública no segura lo hagan de una manera segura que evite la interrupción o la manipulación.
GIRO	Transversal mediante NAT de retransmisión
UDP	Protocolo de datagramas de usuario
máquina virtual	Mensaje de voz
VoIP	Voz sobre Protocolo de Internet
vpn	Red privada virtual
Ataque de día cero	Un tipo particular de explotación que se aprovecha de una vulnerabilidad de seguridad en una red el mismo día en que la vulnerabilidad en sí misma se vuelve de conocimiento general. Por lo general, dado que la vulnerabilidad no se conoce de antemano, a menudo no hay forma de protegerse contra un exploit o ataque hasta que sucede.
Zombi	Un elemento de red IP que ha sido tomado subrepticiamente por un atacante, generalmente sin el conocimiento del usuario.

Índice

A

Serie ACP100 76
despliegue de seguridad de red adicional 19
oferta de servicios avanzados 11
Compatibilidad con AES-256
cifrado de medios ..... sesenta y cinco
requisitos de altitud 82
servidor AMAX ..... 83 , 84
ANA 66
Detección de anomalías ..... 11 , 12 , 87
Aura de Avaya®aplicaciones en Amazon Web Services
visión general 18
Avaya SBCE
descripción general de la arquitectura ..... dieciséis , 46
soporte para troncales IPO desde direcciones IP dinámicas 59
soporte para transcodificación ..... sesenta y cinco
Avaya SBCE conectado a múltiples subredes, usando una sola VLAN 52
Avaya SBCE conectado a varias subredes en dos interfaces. 51
Modelos de implementación de Avaya SBCE 14

B

BFCP
arquitectura 40
descripción 38
visión general 38
Arquitectura BFCP 40
control de acceso fronterizo 14
UC sin fronteras 10

C

manejo de llamadas
WebRTC 45
detección de patrón de llamada 87
certificaciones de servidor 84
CES
proxy seguro 60
validación de códec 13
dominio
proteger-zócalo 93
reglas comunes de cortafuegos 90
reglas comunes 91
matriz de compatibilidad 77
centro de control 87
conferencia convergente
servidor perimetral 67
Conferencia convergente
caracteristicas 69

D

reglas del cortafuegos de la interfaz de datos 90
Restricciones de la interfaz de datos 89
DebianLinux 77
instalación del paquete debian 89
Dell R210II ..... 76 , 83 , 84
Dell R320 76
Dell R620 76
Dell R630 76
negación de servicio 89
desplegar
múltiples SBCE en modo HA 45
múltiples SBCE en modo no HA 44
despliegue
Múltiples SBCE 44
detector
escaneo de puertos 91
detección 87
Reglas de DNS 93
Puerto del servidor DNS 95
cambios en el documento 8
Informes de actividad DoS 89
Ataques DoS 11
Puntuaciones dinámicas de confianza 87

mi

Correspondencia de números E.164 70
servidor perimetral
conferencia convergente 67
sistema de gestión de elementos 10
ccsme 10
Adquisición de EMS 81
huellas dactilares de punto final 87
indicación segura de extremo a extremo 64
ENUM 70
algoritmo 70
Procesando 70
requisitos ambientales para el servidor 83,84
Adaptador EZChip 72

F

conmutación por error 80
control de la cámara del otro extremo 37
reglas del cortafuegos
común 90
interfaz de datos 90
administración 90
reglas de firewall, generando 93
protección contra inundaciones 86
piso 38

Página799 de 3226.

silla de piso 38
control de piso 38
servidor de control de piso 38
participante de piso 38
Corrección de errores de reenvío
FEC 42
protección contra fuzzing 86

GRAMO

apoyo del GARP 79

H

plataformas de hardware 10
garantia de equipo 9
Manipulación de encabezados 23
alta disponibilidad 79
SBCE de Avaya 80
HP DL360 G8 76
HP DL360 G9 76
Puertos HTTP/HTTPS 95
reglas de https 93

yo

ICMP
restricciones 91
Inundación ICMP 88
Prevención de inundaciones ICMP 88
motor de identidad 44
iDRAC
plataformas de hardware 61
iLO 60
subsistema de gestión de la información 13
despliegue en línea 14
elemento de inteligencia ..... 12 ,13
IP Office SSL 23
Reglas de cortafuegos de IPTable 88
Direcciones IPv6 66

k

KILLSCAN
normas 91
Descripción general de KVM 19

L

Funciones de seguridad de capa 3 y 4 88
administración de licencias
Compatibilidad con WebLM 43
descarga de licencia 97
función de licencia
SBCE 97
Licencia
Licencia *(continuado)*
servicios avanzados 97
servicios estándar 97
sistema operativo linux 77
Inicio sesión 54

METRO

reglas de gestión y MGMTPROTECT 92
reglas de administración de firewall 90
Restricciones del puerto de la interfaz de administración 94
Restricciones de la interfaz de administración 89
depósito de almacenamiento maestro 13
MDA 29
medios de comunicación
desanclar 22
anclaje de los medios 22
Prevención de anomalías en los medios 86
elemento mediático 12,13
puertos de medios 95
Tarjeta Medpro TN2302 79
usuario del espacio de trabajo móvil 22
vigilancia 87
monitoreo, detección y protección 87
MontaVista Linux 77
varias puertas de enlace en la misma red 53
varias subredes 48
descripción general de varias subredes 48
escenario de múltiples subredes
Avaya SBCE conectado a varias subredes en dos interfaces 51
múltiples escenarios de subred
varias puertas de enlace en la misma red 53
múltiples subredes en una sola interfaz, usando una sola VLAN 52
interfaz de datos única 50
múltiples subredes en una sola interfaz 50
multi Alquiler 56

norte

NAT transversal 13
Seguridad de la red 19
nuevas características ..... 21 ,22

O

reglas de oferta e intercambio para BFCP 38
almacenamiento a bordo 76
despliegue de un solo cable 14
móvil one-x
proxy CES seguro 60

PAGS

configuración en modo paralelo 80

Página800 de 3226.

clave
politicas 20
PLD 97
asignaciones de puertos
DNS 95
HTTP/HTTPS 95
medios de comunicación 95
señalización SIP 95
SNMP 95
Registro del sistema 95
Restricciones portuarias 94
bloqueo de exploración de puertos 88
Portwell CAD-0208 ..... 76, 83, 84
requisitos de alimentación del servidor 83
prevención 88
procesadores 76
Compatibilidad del producto 76
protección contra inundaciones de capa 3 y capa 4 y escaneos de puertos 88

R

tiempo real
Estado del servidor SIP 43
prevención de reconocimiento 86
REFERIRSE 27
Usuarios Registrados
registros de usuarios 43
re invitar 30
documentación relacionada 100
usuario remoto 22
trabajador remoto 22
replicación
ccsme 81
restricciones
interfaz de datos 88
reutilización de la conexión de IP Office para la entrega de llamadas 59
proxy inverso 36
RTCP 30
generación de informes de seguimiento 35
Detección de anomalías RTP 13
normas
interfaz de datos 93
cortafuegos 93

S

requerimientos de seguridad 84
Pasarela SAL 77
SBCE
función de licencia 97
Endurecimiento SBC 88
escenarios 40
Interoperabilidad de Scopia y Avaya SBCE con SRTP 47
implementación de subred filtrada 14
paquete de reglas de depuración 90
plantillas de lavado 90
campo asegurable 64
ciclo de vida de la seguridad 11
configuraciones de seguridad 89
servidor
certificaciones 84
dimensiones 82
Requisitos medioambientales 83
requerimientos de humedad 83
requerimientos de energía 83
requisitos de temperatura 83
servidores 76
capacidad 78
Soporte del agente de capacidad de servicio 55
Error del administrador de sesión
preservación de la llamada 71
Módulo SigMa 10
descifrado de señales 12
elemento de señalización 12
manipulacion de la senalizacion 23
inicio de sesión único 44
Procesamiento de llamadas SIP 24
Descodificación SIP 12
SIPREC
grabación continua 64
caracteristicas 62
grabación selectiva 64
Soporte SIPREC
visión general 61
Puertos de señalización SIP 95
Enlace troncal SIP 24
Módulo de integración de troncales SIP 10
Validación SIP 12
requisitos del sitio
la seguridad 84
Puertos SNMP 95
garantia del software 9
suplantación de identidad 11, 12, 86
Consideraciones de SRTP 48
Cifrado SRTP de medios 14
Soporte SRTP 47
Reglas de puerto SSH 95
Reglas SSH 92
SSLVPN 23
servicios estándar
configuración 10
oferta 10
Prevención de ataques sigilosos 86
apoyo 102
remoto 23
soporte bajo garantía 9
Puerto Syslog 95
configuraciones del sistema 10
memoria del sistema 76
Requisitos del sistema
altitud 82
humedad 83
energía 83

Página801 de 3226.

Requisitos del sistema*(continuado)*
la temperatura 83

T

Restricciones de inundación de TCP 92
Restricciones de paquetes TCP 95
Nivel de señalización TCP
control de inundaciones 88
Reglas de control de desbordamiento del nivel de señalización TCP 88
requerimientos térmicos 84
TILEncore-Gx36 72
Adaptador TILEncore-Gx36
panel trasero 75
Adaptador Tilera 72
tarjeta TN2302 79
ocultación de topología 90
rastroSBC
archivos de registro 54
visión general 54
Ventajas de traceSBC 55
capacitación 101
despliegue de dos hilos 14

tu

UCI 25
Proxy de UC 10
políticas de comunicaciones unificadas 88
seguridad de las comunicaciones unificadas 11

V

vídeos 101
Cifrado TLS de red privada virtual 14
VLAN
usar 47

W

garantía 9
WebLM 97
detalles del servidor 98
WebRTC
manejo de llamadas 45

Características

intertel CODES

Powered by: intersel®

Introducción

Intertel Codes es una aplicación de escritorio que administra los permisos de los códigos y extensiones para realizar llamadas y posteriormente permite que dichas llamadas se realicen a través del conmutador solo si el código o si la extensión cuenta con los permisos necesarios. Para un desempeño óptimo de la aplicación, administra una base de datos interna permitiendo así la fácil identificación de números de marcación y su tipo de llamada según lo marca la IFT. No es invasiva con su configuración actual de conmutador por lo que su implementación y mantenimiento son sencillos y requieren de pocos esfuerzos.

Problemática

El Instituto Federal de Telecomunicaciones ha anunciado un nuevo plan de marcación para todas las llamadas locales, a celular local, celular nacional y llamadas de larga distancia nacional. Esta nueva marcación afectará a todos los usuarios de telefonía (teléfonos residenciales, teléfonos comerciales, móviles, etc). Todas las personas sin importar si están dentro de una empresa o en sus casas realizando llamadas deberán ahora realizar las llamadas de la siguiente manera:

	Actualmente		A partir del nuevo plan de marcación del IFT	
Tipo de llamada	Lo que anteriormente marcaban	Cantidad de dígitos marcados	Ahora deberán marcarlo de esta manera	Cantidad de dígitos marcados
Llamadas locales	Número telefónico 2106080	México, Guadalajara y Monterrey 8 dígitos. El resto del país son 7 dígitos.	Código de área + número 662 2106080	10
Llamadas a celular local	044 + Código de área + número 044 55 12345678	13 dígitos	Código de área + número 55 12345678	10
Llamadas a celular nacional	045 + Código de área + número 045 662 87654321	13 dígitos	Código de área + número 662 87654321	10
Llamadas de larga distancia nacional	01 + Código de área + número 01 55 32165498	12 dígitos	Código de área + número 55 32165498	10

Para el caso de las empresas, los conmutadores actualmente están diseñados para administrar los permisos de marcación en base a los prefijos de los números. Es decir, para identificar las llamadas a celular tienen configurado

que el 044 son las llamadas a celular local y 045 son para celulares nacionales. Lo mismo para para identificar si es una llamada de larga distancia nacional utilizando el prefijo 01, etc. Al momento de que el IFT elimine los prefijos en las marcaciones a los conmutadores y la marcación de estos tipos de llamadas se estandarice a 10 dígitos, no les será fácil identificar qué tipo de llamada están realizando los usuarios y por consecuencia, no se podrán mantenerla administración de permiso para que los usuarios realicen o no estos tipos de llamadas como actualmente lo hacen.

Si en su empresa desea continuar o mantener esta administración de permisos de marcación para los usuarios en base a códigos o extensiones, Intertel Codes es para usted.

Características del Intertel Codes

1. Soporta simultáneamente ambos tipos de marcaciones indicados por el Instituto Federal de Telecomunicaciones (IFT): la marcación tradicional utilizando los prefijos 01, 044 y 045, así como la marcación a 10 dígitos, la cual elimina los prefijos de la marcación tradicional.
2. Identificación de tipos de llamadas:
    - Local
    - Celular local
    - Larga distancia nacional
    - Celular nacional
    - Larga distancia Internacional
    - Internas
    - Red
    - Servicios
    - Números 800
    - Números 900
3. Permite configurar tipos de llamadas personalizadas.
4. Administración de permisos de marcación configurables por código de autorización, por extensión o ambos. Los permisos pueden ser para marcar:
    - A cualquiera de los tipos de llamadas
    - Para un solo tipo de llamada
    - Para combinaciones de tipos de llamadas (cualquiera que esta sea)

- Para todos los tipos de llamadas
- Para ninguno de los tipos de llamadas (Ej. Restricción para solo recibir llamadas en una extensión, pero no hacer)

Ejemplos de configuración de permisos para realizar llamadas:

- Permitir realizar solo llamadas locales
- Permitir realizar solo llamadas locales y celulares locales
- Permitir realizar solo llamadas a celulares locales y llamadas a celular nacional
- Permitir realizar solo Llamadas a celular nacional
- Permitir realizar todas las llamadas
- Permitir solo llamadas internas o de red
- No permitir llamadas, de ningún tipo, pero si recibir.
- Entre otras

El FAC no permitirá que se realicen llamadas con el código o con la extensión si estas no están configuradas para ser efectuadas.

5. Maneja tantas llamadas simultaneas como permita el conmutador y las líneas troncales contratadas por la empresa.
6. En ocasiones se requerirá de licenciamiento y/o hardware adicional.
7. Actualización periódica y automática de la base de datos del Instituto Federal de Telecomunicaciones.
8. Soporta diferentes tipos de marcación. Ejemplo: Prefijo + Número + Código y Prefijo + Código + Número (configurable desde el portal).
9. Creación de clases de servicios.
10. Configuración de perfiles de marcación de salida. Esto es útil para sacar los distintos tipos de llamada por diferentes troncales.
11. Estados de los servicios. Desde el portal puede monitorear el estado de los servicios de restricción y sincronización de Intertel Codes.
12. Importación masiva de clases de servicio, extensiones y códigos de autorización por medio de una plantilla.

Requerimientos:

a) Un código de autorización registrado directo en el conmutador para ser utilizado por el sistema ICodes.
b) Sistema ICodes instalado con su sentinel de hardware o sentinel de software.
c) Crear troncal SIP interna apuntada a la computadora donde se instalará Intertel Codes. Esto permitirá que las llamadas pasen por la aplicación y se validen los permisos configurados a las extensiones.
d) Acceso a Internet a nuestra página que actualizará de forma periódica la base de datos de los dígitos de marcación que permitirán la identificación de los tipos de llamadas

Compatibilidad con:

- Conmutador Cisco Call Manager versión 8 o superior
- Alcatel OXE 12 o superior
- Avaya IP Office 10 o superior
- Sistema Operativo Windows 10 Pro o superior (a reserva del driver a utilizar)
- Sistema Operativo Windows Server 2012,2019 (a reserva del driver a utilizar)
- Para virtualización comunicarse con el fabricante.
- Teléfonos digitales.

Traducido del inglés al español - www.onlinedoctranslator.com

Configuración de fecha y hora

Puede cambiar la configuración de fecha y hora utilizada por el servidor a través de las páginas de configuración web del servidor. los**Sistema** El menú muestra la fecha y hora actual del servidor.

Para cambiar la configuración de fecha y hora del servidor:

1. Acceso a los menús de configuración web del servidor.
2. Seleccione**Ajustes**.
3. Seleccione**Sistema**.
4. Seleccione el**Fecha y hora**sección.
   - **Fecha**
     Para un servidor que no usa NTP, este campo muestra la fecha actual del servidor y permite cambiarla. Si usa NTP, este campo está atenuado. Para servidores virtuales, este campo no se utiliza. Si no usa NTP, el servidor virtual toma su tiempo de la plataforma de host del servidor virtual.
   - **Tiempo**
     Para un servidor que no utiliza NTP, este campo muestra la hora UTC actual del servidor y permite cambiarla. Si usa NTP, este campo está atenuado. Para servidores virtuales, este campo no se utiliza. Si no usa NTP, el servidor virtual toma su tiempo de la plataforma de host del servidor virtual.
   - **Zona horaria**
     En algunos casos, la hora que muestra o utiliza una función debe ser la hora local en lugar de la hora UTC. los**Zona horaria**El campo determina el desplazamiento apropiado aplicado a la hora UTC anterior. Tenga en cuenta que cambiar la zona horaria puede causar una*"Sesión expirada"*que aparezca un mensaje en el navegador, en cuyo caso deberá volver a iniciar sesión.
   - **Habilitar protocolo de tiempo de red**
     Cuando se selecciona, el servidor obtiene la fecha y la hora actual de los servidores NTP enumerados en la**Servidores NTP** Listado abajo. A continuación, utiliza esa fecha y hora y realiza solicitudes regulares de NTP para actualizaciones.
     - **Servidores NTP**
       Con**Habilitar protocolo de tiempo de red**seleccionado, use este campo para ingresar la dirección IP de un servidor o servidores NTP a usar. Ingrese cada dirección como una línea separada. El administrador de red o ISP puede tener un servidor NTP para este propósito. Una lista de servidores NTP de acceso público está disponible en http://support.ntp.org/bin/view/Servers/WebHome . Sin embargo, es su responsabilidad cumplir con la política de uso del servidor elegido. Elija varios servidores NTP no relacionados en caso de que uno de los servidores se vuelva inalcanzable o su reloj no sea confiable. El servidor usa las respuestas que recibe de cada servidor NTP para determinar la confiabilidad.
       - El sistema IP Office también puede usar NTP para obtener la hora del sistema.
     - **Sincronice el reloj del sistema antes de iniciar el servicio**
       Utilice esta opción para sincronizar el reloj del sistema con un servidor horario NTP antes de iniciar otros servicios. No utilice esta opción si no se puede acceder de forma fiable al servidor horario. Esperar a que ocurra la sincronización puede bloquear el uso del sistema hasta que haya pasado un tiempo de espera.
     - **Usar fuente de hora local**
       Cuando no se selecciona, el NTP externo tiene prioridad sobre el reloj del sistema interno. Si se selecciona, el reloj del sistema local se utiliza como fuente de tiempo. Solo use esta opción si el reloj del sistema está sincronizado con otra fuente confiable, por ejemplo, un dispositivo de reloj controlado por radio.
5. Haga clic en**Ahorrar**.

Traducido del inglés al español - www.onlinedoctranslator.com

Engage The Power of We™

Controlador de borde de sesión de Avaya para empresas

Una solución de seguridad para redes basadas en SIP que implementan aplicaciones de comunicaciones unificadas

Para beneficiarse de las últimas soluciones de comunicación y colaboración, las empresas recurren cada vez más a las redes basadas en SIP.

Ya sea para reducir costos usando telefonía IP o para aprovechar las últimas aplicaciones de mensajería multimedia, conferencias y comunicaciones unificadas (UC), SIP está emergiendo como el estándar de la industria.

Ventajas de SIP

Debido a que están diseñados para voz de alta fidelidad, video de alta definición y otras aplicaciones de colaboración en tiempo real, los operadores ofrecen cada vez más troncales SIP (Protocolo de inicio de sesión). Los troncales SIP admiten de manera rentable más extensiones telefónicas y ayudan a reducir los costos de comunicaciones locales, gratuitas, nacionales e internacionales de larga distancia.

Con el apoyo de una red SIP, una empresa en crecimiento puede implementar de manera más fácil y rentable las últimas aplicaciones de UC para los empleados, independientemente de dónde trabajen: en la oficina, en casa o de viaje. La productividad que resulta de estas aplicaciones colaborativas en tiempo real puede ser un factor importante
ventaja competitiva.

Seguridad de troncales SIP

Sin embargo, los troncales SIP también presentan un desafío de seguridad: existe una vulnerabilidad en el punto donde el troncal SIP se conecta a la red pública, lo que puede dejar a una empresa expuesta a ataques de piratas informáticos, como suplantación de identidad, secuestro de llamadas,
escuchas ilegales y fraude telefónico. Además del daño potencial a los negocios
Los mandatos de operaciones, privacidad y seguridad, como los de la información crediticia y de salud (p. ej., PCI e HIPAA), requieren que se aborden estas vulnerabilidades, lo que impone importantes sanciones financieras y legales por incumplimiento.

Trabajador remoto sin VPN Seguridad

Los clientes comerciales ahora se enfrentan a un mundo en evolución donde los usuarios ya no están confinados dentro de las paredes de la empresa. Las tendencias hacia el acceso móvil a los recursos del sistema, el teletrabajo y BYOD están creando la necesidad de brindar servicios colaborativos y de UC basados en SIP a estos usuarios remotos de una manera flexible pero segura. Avaya Session Border Controller for Enterprise ofrece una nueva solución para esta necesidad teniendo en cuenta la seguridad.

"El servicio de atención al cliente está en el corazón de lo que hacemos, y como líder en contacto subcontratado servicios del centro, nuestro los clientes cuentan con nosotros para garantizar una calidad superior funciones y seguro Servicio. Avaya SBCE nos ayuda a lograrlo, y lo hace pensando en el ahorro de costos. Podemos reducir nuestro hardware gastos, simplificar implementaciones, y utilizar menos recursos, ahorrándonos tiempo y dinero. Avaya SBCE es fundamental para ayudar a proteger nuestra red, mientras entrega el beneficios de ahorro de costos de enlace troncal SIP".

–Richard Blake, Gerente, TI telecomunicaciones, teleactuación

Seguridad para SIP-redes basadas

- Una clara línea de defensa donde el troncal SIP se encuentra con el público la red
- Secundario comunicaciones aplicaciones que conducir competitivo ventaja
- Protección contra:
  - Ataques de denegación de servicio (DoS)
  - Suplantación de identidad
  - Secuestro de llamadas
  - Bloqueo de fraude de peaje
  - Escuchar a escondidas y robo de informacion
- Proveedor múltiple compatibilidad
  - Cisco 8.x y 9.x (CUCM)
  - Mitel
  - Shoretel
  - Microsoft Lync
- Política detallada aplicación

Seguridad multidominio

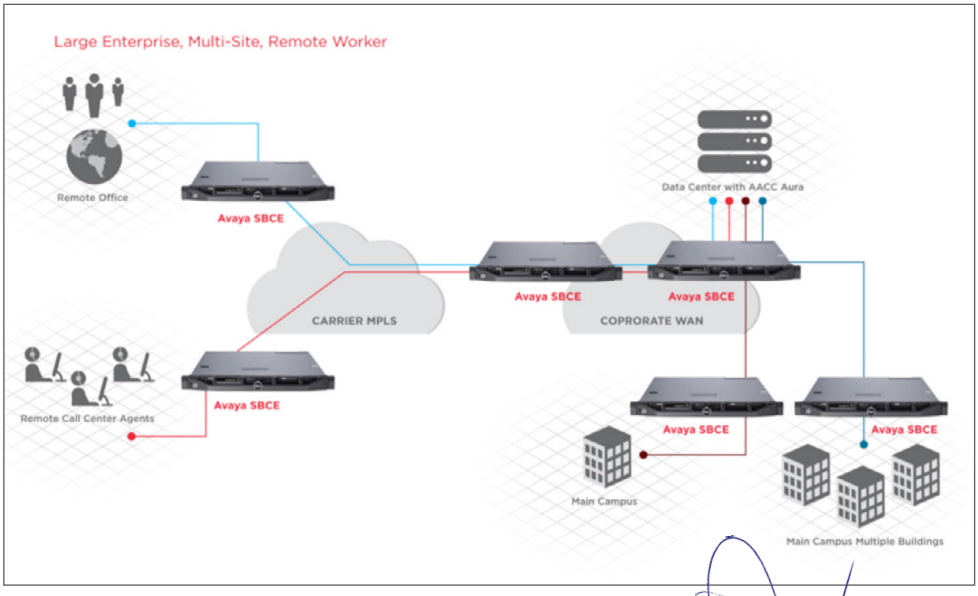
El soporte de red para múltiples usuarios que se conectan a través de redes de varios niveles, tanto en la nube pública como en la privada, es una necesidad. Esto es especialmente cierto para las grandes empresas multinacionales o las instalaciones de comunicación gubernamentales a gran escala. La criticidad de se entiende mantener un acceso seguro independientemente de la ubicación, pero la solución no siempre es tan obvia. Avaya Session Border Controller for Enterprise ayuda a proporcionar las funciones necesarias para la seguridad de red a red, así como la seguridad de red a usuario. Esto significa que para una gran

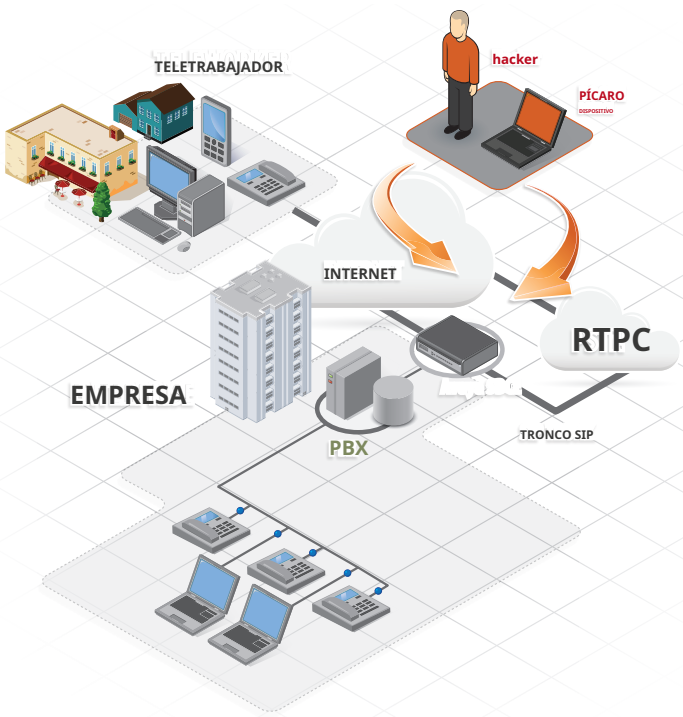
escala, red extendida geográficamente, todas las capas de acceso a la red pueden mantenerse seguras. Las capacidades consecutivas de Avaya Session Border Controller para Enterprise ayudará a garantizar el acceso seguro de los usuarios sin importar cuán extenso y diverso sea.

Nube

A medida que más empresas buscan alternativas alojadas para sus entornos de colaboración, se vuelve aún más crítico que las interfaces entre la empresa y el host sean seguras y manejables. Session Border Controller for Enterprise ofrece una interfaz que ayuda a respaldar la protección de la red y el control empresarial del tráfico de VOIP. Avaya ve un mayor interés en las configuraciones que son una arquitectura híbrida, aplicaciones alojadas y empresas en las instalaciones.

aplicaciones Session Border Controller for Enterprise es la protección necesaria para ayudar a abordar el soporte de protocolo adecuado y una infraestructura de red verdaderamente integrada y segura.





Una solución para empresas en crecimiento

El controlador de borde de sesión de Avaya para empresas (Avaya SBCE) ayuda a abordar las vulnerabilidades de seguridad en las redes SIP en una solución rentable, de caja única y fácil de implementar.

Operado fácilmente desde una interfaz gráfica de usuario (GUI) intuitiva, Avaya SBCE establece una demarcación precisa donde los troncales SIP se encuentran con la red empresarial, presentando una clara línea de defensa. Ayuda a brindar seguridad de clase empresarial que ayuda a mitigar los riesgos de denegación de servicio (DoS) y amenazas en la capa de aplicación, así como el fraude telefónico. La aplicación detallada de políticas ayuda a respaldar el cumplimiento continuo.

Con Avaya SBCE implementado, las empresas en crecimiento pueden adoptar las comunicaciones colaborativas y unificadas aplicaciones que impulsan la ventaja competitiva.

Solución de caja única para seguridad de red SIP

Avaya Session Border Controller for Enterprise proporciona una arquitectura de seguridad de nivel de aplicación avanzada en un solo dispositivo: SIP Firewall, Session Border Controller, Sistema de detección de intrusiones y Sistema de prevención de intrusiones (IDS/IPS), Controlador de acceso, Autenticación, Unificado

Proxy de comunicaciones y aplicación de políticas para todas las aplicaciones de comunicaciones unificadas en tiempo real.

Ayudar a proteger y brindar soporte para BYOD

Los dispositivos de consumo están llegando a la empresa. Las empresas pueden aprovechar BYOD (traiga su propio dispositivo) como una forma de reducir costos, aumentar productividad y mejorar la comunicación y la colaboración. El desafío es cómo decir sí a BYOD mientras se mantiene el control de la red.

Sesión Avaya controlador fronterizo para empresas con Oficina de PI

Avaya IP Office es la solución que muchos las empresas recurren para obtener información completa y fácil implementado unificado comunicaciones

Con más que 300.000 sistemas instalado en todo el mundo, IP Office es un abanderado de la industria, entregando el comunicaciones y herramientas de productividad empleados de hoy necesitan rendir al máximo.

Cuando se implementa Avaya IP Office en junto con SIP troncos, el Avaya Borde de sesión Controller for Enterprise trabaja de la mano para ayudar a proteger contra amenazas de seguridad.

A medida que más empresas están buscando alternativas hospedadas para sus colaboración ambientes, es se vuelve aún más crítico para el interfaces entre empresa y anfitrión ser seguro y manejable.

El borde de la sesión Controlador para La empresa es la protección necesaria para ayudar a apoyar adecuadamente soporte de protocolo y un verdaderamente integrado y red segura infraestructura.

Todas las empresas se ven afectadas y hablan de BYOD, pero lo que puede perderse en la conversación es el hecho de que BYOD es más que un dispositivo. administración. Avaya admite BYOD con una combinación de seguridad, autenticación, redes y políticas. La solución de Avaya incluye autenticación de dispositivos, control de acceso para dispositivos cableados e inalámbricos, acceso remoto seguro y soporte a través de una variedad de servicios.

Avaya Session Border Controller for Enterprise está diseñado para habilitar de forma segura muchas implementaciones, que incluyen:

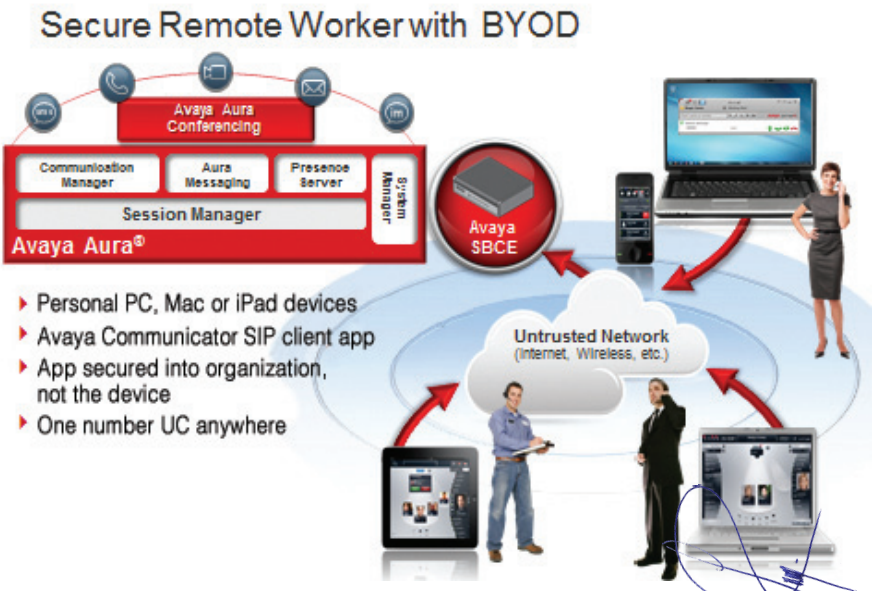
- Permitir que los trabajadores remotos se conecten sin VPN, ofreciendo soporte de Bring Your Own Device (BYOD) sin la sobrecarga administrativa de una solución de red privada virtual (VPN)
- Ayude a proteger las aplicaciones de UC que ingresan al núcleo de la empresa
- Ayude a asegurar el acceso fronterizo para el intercambio local competitivo y titular

Soporte para legado Comunicaciones

La seguridad para el acceso remoto no es solo un problema para los nuevos sistemas; incluso los sistemas de llamadas heredados ven requisitos para agregar una colaboración móvil segura. Avaya Session Border Controller for Enterprise ha sido ampliamente probado para compatibilidad con Avaya Aura®e instalaciones Avaya IP Office, así como para dar soporte a los sistemas heredados de nuestros clientes. El controlador de borde de sesión de Avaya para empresas admitirá:

- Plataforma Avaya Aura versión 6.1 y superior
- Avaya IP Office 9.0
- Avaya Communication Server 1000 versión 7.6

Mantener un acceso remoto seguro es nuestro objetivo para todas las soluciones de colaboración y los requisitos de movilidad empresarial.



Página813 de 3226.

virtualización

La necesidad de reducir CapEx y consolidar el entorno de red ha llevado a muchas empresas a utilizar una solución de aplicación virtual para la colaboración en tiempo real. Extender los beneficios de la infraestructura

La virtualización ofrece una implementación menos costosa. Además, el paso a la virtualización puede generar ahorros continuos en los gastos operativos de TI debido al soporte para una arquitectura de sistema común. Los requisitos de acceso seguro para sistemas basados en SIP

las comunicaciones también pueden reducir significativamente los requisitos de hardware para el diseño del sistema. El controlador de borde de sesión de Avaya para empresas ofrece una solución virtualizada para la gestión, así como el dispositivo principal. Esto respaldará el cambio general a una solución de colaboración virtualizada para todos los clientes a medida que cumplan con los

requisitos empresariales para el acceso SIP y la seguridad de los trabajadores remotos.

El software de aplicación central Avaya Session Border Controller for Enterprise y EMS están disponibles como archivos OVA para su instalación en VMware. Hay más detalles disponibles en la guía de implementación de Avaya Session Border Controller for Enterprise VMware disponible en el**Sitio web de soporte de Avaya**.

Avaya SBCE Recursos de VMware	**ccsme**	**SME y SBCE**
vCPU	3 vCPU	4
Procesador mínimo	2,4 GHz (Xeon x5670 o equivalente)	2,4 GHz
reserva de CPY	7200 MHz	9600 MHz
Memoria virtual	4G	8G
almacenamiento virtual	80G	80G
NIC compartidas	2@100Mbps o 1000Mbps	4@100Mbps o 1000Mbps

La sesión de Avaya controlador fronterizo para Enterprise ofrece una solución virtualizada para la gestión como así como el dispositivo central, apoyando el cambio general a un sistema virtualizado solución de colaboración para cualquier empresa.

Como parte de la Soporte de Avaya para un virtualizado solución de colaboración, Avaya Aura Virtualized El medio ambiente proporciona un conjunto completo de UC y colaboración aplicaciones todas compatible con VMware y listo para la instalación en un cliente proporcionado virtualizado infraestructura.

Especificación	SBCE de rango bajo Portwell (núcleo)	SBCE de gama media		SBCE de gama media (fuente de alimentación dual)	
		Dell (núcleo)	ccsme de Dell	Dell (núcleo/EMS)	HP (núcleo/EMS)
tipo de producto	Avaya SBCE	Avaya SBCE	Avaya ccsme	Avaya SBCE, EMS	Avaya SBCE, EMS
Sesiones de troncales SIP	250	6000	N / A	6000	N / A
Trabajador remoto Sesiones	250	1200	N / A	1200	N / A
Número de parte	271023	271021	271022	308596	308597
Tipo de plataforma	CAD-0208-3402-900	PE R210 II XL (OEM)	PE R210 II XL (OEM)	PE R620 (OEM CR2)	DL 360pG8 (CR2 OEM)
BIOS	08.00.15	1.1.1	1.1.1	2.2.2	P71 03/01/2013
Procesador principal	ÁTOMO D510 – 1,66 GHz	Xeon E3-1220-3,1 GHz (núcleo cuádruple - 80W)	Pentium G850 2,9 GHz (Doble núcleo)	Xeon E5-2630 2,3 GHz (núcleos hexagonales)	Xeon E5-2630 2,3 GHz (núcleos hexagonales)
Memoria	2GB DDR2 667MHz SODIMM	4GB (2X2GB) DDR3 1333 MHz, UDIMM	2GB (1 X 2GB) DDR3 1333 MHz, UDIMM	16 GB (4 de 4 GB) DDR3 1600 MHz, RDIMM	16 GB (4 de 4 GB) DDR3 1600 MHz, RDIMM
REDADA	No	No	RAID 1	RAID 1	RAID 1
Unidades de disco duro	320 GB (SATA)	250/500 GB (SATA)	2 x 500 GB (SATA)	2 de 300 GB (SAS)	2 de 300 GB (SAS)
Unidad óptica	No	No	No	DVD+/-RW	DVD+/-RW
Flash compacto	No	No	No	No	No
Tarjetas PCI	-	1 X puerto cuádruple NICP-CIe-4	1 X H200 (SAS/SATA) Controlador RAID	1 NIC de puerto dual de 1 GbE	1 NIC de puerto dual de 1 GbE
TPM	No	No	No	No	No
Pantalla LED	No	Sí	Sí	Sí	Sí
Interfaces (Puertos)					
Datos	4 de 1 GbE	6 de 1 GbE	2 de 1 GbE	6 de 1 GbE	6 de 1 GbE
USB	2	2	2	2	2
Consola	1 (RJ-45)	1 (DB 9 - Mujer)	1 (DB 9 - Mujer)	1 (DB 9 - Mujer)	1 (DB 9 - Mujer)
vga	Sí	Sí	Sí	Sí	Sí
Ventilador reemplazable	No	No	No	No	No
Duro reemplazable Conducir	No	No	No	Sí	Sí
fuente de alimentación redundante	No	No	No	Sí	Sí
Desvío de puerto	No	No	No	No	No
Factor de forma	1U (Escritorio o Rack Montar)	1U	1U	1U	1U
Bisel	-	Dell OEM-Avaya de marca	Dell OEM-Avaya de marca	Dell OEM-Avaya de marca	OEM de HP-Avaya de marca

Especificación	SBCE de rango bajo Portwell (núcleo)	SBCE de gama media		SBCE de gama media (fuente de alimentación dual)	
		Dell (núcleo)	ccsme de Dell	Dell (núcleo/EMS)	HP (núcleo/EMS)
Dimensiones					
Altura	1,7 pulgadas	1,7 pulgadas	1,7 pulgadas	1,7 pulgadas	1,7 pulgadas
Ancho	11,75 pulgadas	17,1 pulgadas	17,1 pulgadas	17,1 pulgadas	17,1 pulgadas
Profundidad	5,75 pulgadas	15,5 pulgadas	15,5 pulgadas	26,9 pulgadas	27.5
en caja					
Altura	7,5 pulgadas	10 en	10 en	11.5	8.8
Ancho	12 en	24 en	24 en	24.25	23.31
Profundidad	15 en	32 pulgadas	32 pulgadas	36.25	38.69
Peso					
Unidad	3 libras	15.5 libras	16,2 libras	41 libras	42,3 libras
en caja	6 libras	30 libras	31 libras	48 libras	49 libras
Aporte	Adaptador de CA de 100/240 V (12 V CC)	100/240 V CA	110/240 V CA	110/240 V CA	110/240 V CA
corriente nominal (110V)	0,2 A	1.1A	1.1A	1.5A	1.5A
Corriente máxima (110V)	0,5 A	2A	2A	4.5A	4.5A
Alimentación de CA (máx.)	40 vatios	250 vatios	250 vatios	500 vatios	500 vatios
Ambiental					
Funcionamiento nominal Temperatura	20oC	20oC	20oC	20oC	20oC
Temperatura de funcionamiento Rango	5oC ~ 35oC	10oC ~ 35oC	10oC ~ 35oC	10oC ~ 35oC	10oC ~ 35oC
Humedad relativa	20% ~ 90%	10% ~ 90%	10% ~ 90%	10% ~ 90%	10% ~ 90%
Temperatura de almacenamiento	0oC ~ 75oC	- 40oC ~ 65oC	- 40oC ~ 65oC	- 40oC ~ 65oC	- 30oC ~ 60oC
Certificaciones y Cumplimiento	FCC, CE, UL y RoHS	FCC, CE, CSA, UL y RoHS	FCC, CE, CSA, UL y RoHS	FCC, CE, CSA, UL y RoHS	FCC, CE, CSA, UL y RoHS
HTS	8517.62.0050				
ECCN	H/W = 5A002 (A.1), S/W = 5D002 (C.1)				
Licencia de exportación	Excepción: ENC - Restringido a usuarios finales "no gubernamentales". Ref: Sección 740.17(A), (B)(1) y (B)(2)				
CCATS	G072860				

Acerca de Avaya

Avaya es un proveedor global líder de cliente y equipo soluciones de compromiso y servicios disponibles en una variedad de soluciones locales y en la nube flexibles opciones de despliegue. Tela de Avaya-redes basadas soluciones ayudan a simplificar y acelerar la despliegue de negocios aplicaciones criticas y servicios. Para mayor información por favor visite **www.avaya.com**.

© 2015 Avaya Inc. Todos los derechos reservados.
Avaya y el logotipo de Avaya son marcas comerciales de Avaya Inc. y están registradas en los Estados Unidos y otros países. Todas las demás marcas comerciales identificadas con ®, TM o SM son marcas registradas, marcas comerciales y marcas de servicio, respectivamente, de Avaya Inc. 02/15 • UC4834-09

Provide FEEDBACK for this document

Portal de Reportes

Manual de Usuario

Interfases y Sistemas Electrónicos, S.A.P.I. de C.V. (Intersel), ha preparado este documento para uso del personal, licenciatarios y clientes de Intersel. La información aquí contenida es propiedad de Intersel y no deberá ser fotocopiada, traducida o convertida a ninguna forma legible por máquinas o equipo electrónico, ya sea en partes o completo, sin el permiso por escrito de Intersel.

Intersel se reserva el derecho, sin aviso previo, de modificar o revisar la totalidad o parte de este documento, o cambiar las características o especificaciones del producto, sin ningún tipo de responsabilidad por cualquier tipo de pérdidas, costos, o daños, incluyendo daños por consecuencias, causados por la utilización de estos materiales.

Este producto y su documentación están inscritos en el Registro Público del Derecho de Autor.

Todos los derechos reservados. © 2018 por Interfases y Sistemas Electrónicos, S.A.P.I. de C.V.
Microsoft, Windows, MS-DOS son marcas registradas de Microsoft Corp.

Todas las otras marcas y nombres de productos son marcas registradas de sus respectivos propietarios.

Fecha de revisión de este manual: septiembre, 2018.

Prefacio

Agradecemos su preferencia al haber adquirido nuestro producto. Esperamos que satisfaga plenamente sus necesidades y adicionalmente supere sus expectativas.

Es nuestra intención que este manual le permita operar su Portal de Reportes, sin embargo, en caso de que usted no encuentre respuesta a algún tema, no dude en llamar a su distribuidor autorizado con quien adquirió este paquete, o bien, directamente con su ejecutivo de cuenta de Intersel. Nos dará mucho gusto poder atenderle.

Agradeceremos nos haga saber sus comentarios, sugerencias o críticas acerca de nuestros productos, servicios, documentación, soporte técnico, servicio y atención de nuestros distribuidores, y en general cualquier aspecto relacionado.

Intersel
Interfases y Sistemas Electrónicos S.A.P.I. de C.V.
Oficina Corporativa
Plaza las Palmas
Blvd. Solidaridad No. 335
Edif. A Nivel 2
Col. Paseo del Sol, C.P. 83246.
Hermosillo, Sonora, México
Teléfono:
+52 (662) 210-60-80
Email: info@intersel.com.mx
Búsquenos en Internet:
http://intersel.com.mx/

Tabla de contenido

Prefacio 2

Capítulo 1. Conociendo el Portal de Reportes 6

Introducción 6
Interfaz gráfica del Portal de Reportes 6
Acceso al Portal de Reportes 6
Acceso al portal con autenticación anónima 7
Acceso al portal con autenticación básica 8
Elementos del Portal de Reportes 8
Panel de resultados 10
Menú de opciones 10
Logotipo 10
Idioma 10
Sitio activo 10
Gestión de reportes 10
Cuenta de usuario 11
Cuenta de usuario 11
Perfil 11
Información personal 11
Foto de perfil 12
Cambio de contraseña 12
Acciones 13
Manual de ayuda del Portal de Reportes 14
¡Qué hay de nuevo en la versión! 14
Salir del Portal 14
Personal a cargo 14
Directorio telefónico 16
Compartir archivos 17
Carga de archivos 17
Descarga de archivos 18

Capítulo 2. Dashboard 19

Tableros de mando (Dashboards) 19
¿Qué es un tablero de mando o dashboard? 19
Mis elementos 20
Dashboard 21
Desempeño 24
Mayores consumos 26
Totales 28
Plantillas (Layout) 31
Cambiar plantilla 31
Indicadores (widget) 31
¿Qué es un Indicador o widget? 31
Agregar un indicador 32
Quitar un indicador 32

Mover un indicador 32
Descripción del indicador 32
Imprimir un indicador 32
Aplicar configuración de indicadores (widgets) para todos los sitios 32
Restaurar configuración de indicadores (widgets) 33

Capítulo 3. Reportes 35

Conociendo los elementos que forman a la interfaz de Reportes 35
Búsqueda. 35
Favoritos. 35
Reportes. 35
Categorías 36
Propiedades de un reporte 37
Reportes “Favoritos” 37
Hacer un reporte como uno de mis favoritos 37
Quitar un reporte de mis favoritos 37
Vista previa de un reporte 38
Generación de reportes con un máximo de información de un año. 38
Generación de reportes con un máximo de 50,000 registros. 38
Histórico de reportes 39
Filtros 40
Título del reporte. 42
Descripción. 42
Elementos de un reporte ejecutado 42
Barra de herramientas 42
Título del reporte. 44
Filtros. 44
Gráfica. 44
Logotipo. 45
Nombre de la empresa. 45
Panel de información. 45
Página actual. 45
Periodo/Rango de fechas. 45
Sitio activo. 46
Ruta de navegación. 46
Usuario y fecha de generación. 46
Drill-down. 46
Ordenamiento. 46
Clasificación de reportes 47
Análisis de facturación 47
Análisis de llamadas 50
Análisis de productividad y tráfico 52
Consolidados 54
Declaración de llamadas 56
Especiales 57
Facturas Fijas 58
Hoteles y Hospitales 59
Mapas 61
Planes tarifarios 63

Sistema....63
Telefonía Fija....65
Telefonía Móvil....68
Tráfico Erlang....69
Envío automático de reportes....70
Envío de reporte por correo al momento....71
Programar periodicidad de envío....72
Frecuencia por día....74
Frecuencia por semana....75
Frecuencia por mes....75
Mis reportes programados....76
Editar mis reportes programados....77
Consultar mis reportes programados....77
Borrar mis reportes programados....77
Administrar reportes de otros usuarios....77
Búsqueda de Reportes....78
Capítulo 4. Declaración de llamadas....79
Capítulo 5. Gestión de Reportes....81
Reportes Especiales....81
Gestión de reportes....82
Capítulo 5. Sección Hotelera....84
Introducción....84
Interfaz gráfica de Sección Hotelera....84
Panel de habitaciones:....85
Menú de opciones....85
Impresión....85
Búsquedas por huésped o habitación....85
Check in / Check out....85
Barra de navegación....86
Registro de entrada y salida de un huésped....86
Registro de entrada (Check In)....86
Registro de salida (Check out) / Consulta e Impresión de llamadas....86
¡Necesitamos su opinión!....88

Capítulo 1. Conociendo el Portal de Reportes

Introducción

El Portal de Reportes es una herramienta de trabajo poderosa, diseñada para personas que requieren explotar la información generada en la operación del mismo. Por medio de los reportes de este portal, podrá estar enterado del consumo telefónico de su empresa, de sus empleados, y de las líneas telefónicas fijas y móviles que tiene contratadas.

Pensando en que la operación de este portal sea lo más sencilla posible, se han clasificado los reportes en categorías y cada reporte ha sido identificado con un nombre específico, para que, de manera sencilla y rápida, pueda tener conocimiento sobre los resultados de salida que serán producidos.

La salida de un reporte puede ser generada en varios formatos y está preparada para su impresión en hojas tamaño carta. Los formatos disponibles son: PDF, documento de Word, documento de Excel, entre otros.

Para empezar y simplificar el aprendizaje de operación de esta aplicación, nos familiarizaremos con los elementos que conforman al Portal de Reportes, los cuales se describen en los capítulos siguientes.

Interfaz gráfica del Portal de Reportes

Acceso al Portal de Reportes

Solamente necesita conectarse a Internet o a la Intranet de su empresa y visitar la página del Portal de Reportes. Asegúrese de tener a su alcance el nombre o clave de usuario y la contraseña, ya que serán necesarios para para acceder a la aplicación web.

Para ingresar al Portal de Reportes, abra un *navegador web y escriba el nombre del dominio o dirección IP donde fue instalada la aplicación. Generalmente la ruta para ingresar será parecida a la siguiente: http://nombredeldominio/Int15/ipr. Esta información puede ser proporcionada por el administrador del sistema Intertel®, así como el usuario y contraseña para ingresar.

(*) Recomendamos usar el navegador Internet Explorer versión 11 o superior para tener acceso a todas las funcionalidades que se incluyen en la barra de herramientas, que aparece al momento de ejecutar algún reporte.

Dependiendo del tipo de autenticación (autenticación anónima o autenticación básica) que se haya configurado para los portales, dependerá el tipo de pantalla que se muestre para solicitar las credenciales de acceso. El tipo de autenticación configurada, es el tipo de seguridad que estará utilizando el portal para validar el acceso. Esto es un proceso interno y para usted como usuario solo cambia el diseño de la pantalla que le solicita las credenciales.

La autenticación anónima utiliza la seguridad propia del sistema Intertel®. La autenticación básica utiliza la seguridad de la red que puede ser la de Windows o de Active Directory, dependiendo de cómo se encuentre configurada la red de su empresa.

Para conocer más sobre el tipo de autenticación, consulte la Guía de instalación y configuración del sistema Intertel en la sección de "**Configurar tipo de autenticación a portales**" o el Manual de usuario del sistema Intertel, en la sección de "**Usuarios**".

Acceso al portal con autenticación anónima

Una vez que en su navegador ha proporcionado la ruta para el portal de reportes en la barra de direcciones y presionado Enter, el sistema le mostrará la pantalla de acceso del sistema Intertel® solicitándole las credenciales. Esta pantalla cuenta con los logos y diseño del sistema Intertel® tal como se muestra en la siguiente figura.

Proporcione el usuario (clave de usuario en Intertel®) y contraseña. Previamente este usuario y contraseña debieron haber sido creados y configurados con los permisos necesarios en Intertel® por el Administrador del sistema Intertel®.

Figura 1.1. Pantalla para acceder al Portal de Reportes cuando se tiene configurada autenticación anónima.

Por último, de clic en el botón de "Acceder", para que sea autenticado en el sistema y le muestre la pantalla principal del Portal de Reportes.

Acceso al portal con autenticación básica

Una vez que ha ingresado desde su navegador a la dirección del portal de reportes, se abrirá una ventana de Windows solicitándole las credenciales de acceso, tal como se muestra en la siguiente figura.

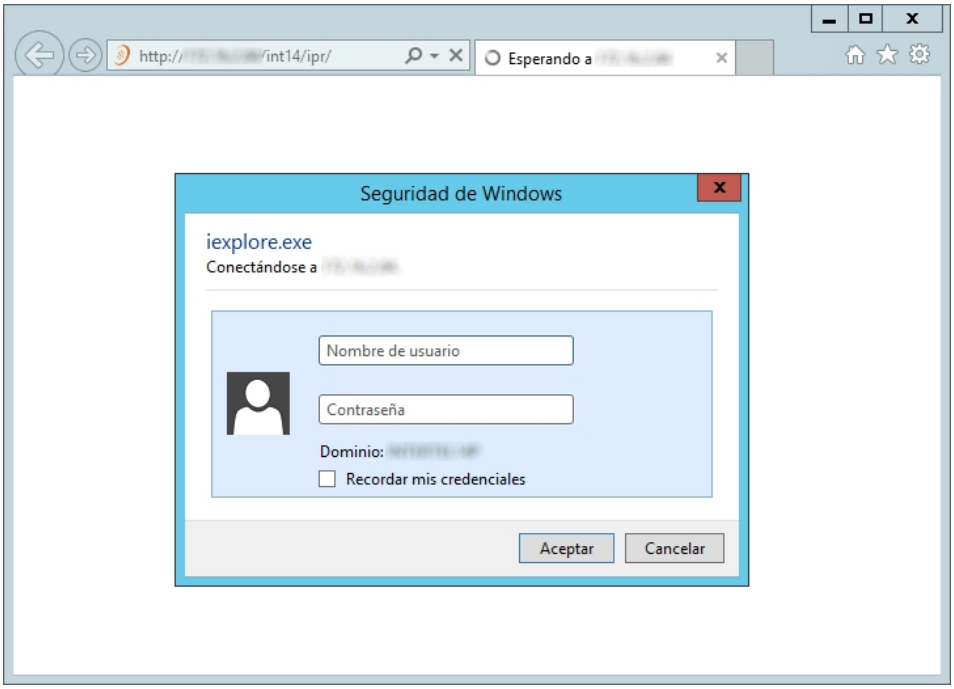


Figura 1.2. Pantalla para acceder al Portal de Reportes cuando se tiene configurada autenticación básica

Proporcione el usuario (usuario de Windows) y contraseña para que el sistema le muestre la pantalla principal del Portal de Reportes. Previamente el usuario debió haber sido configurado en el sistema Intertel® por el Administrador del sistema Intertel® para asignarle los permisos necesarios de acceso.

Elementos del Portal de Reportes

Una vez que el usuario es autenticado en el Portal de Reportes, se le mostrará la pantalla de inicio de la aplicación; la cual está formada de varias secciones. A través de estas secciones tendrá acceso a cada una de las funcionalidades que brinda este portal.

En la figura siguiente identificamos las secciones y opciones a las que tendrá acceso una vez autenticado.

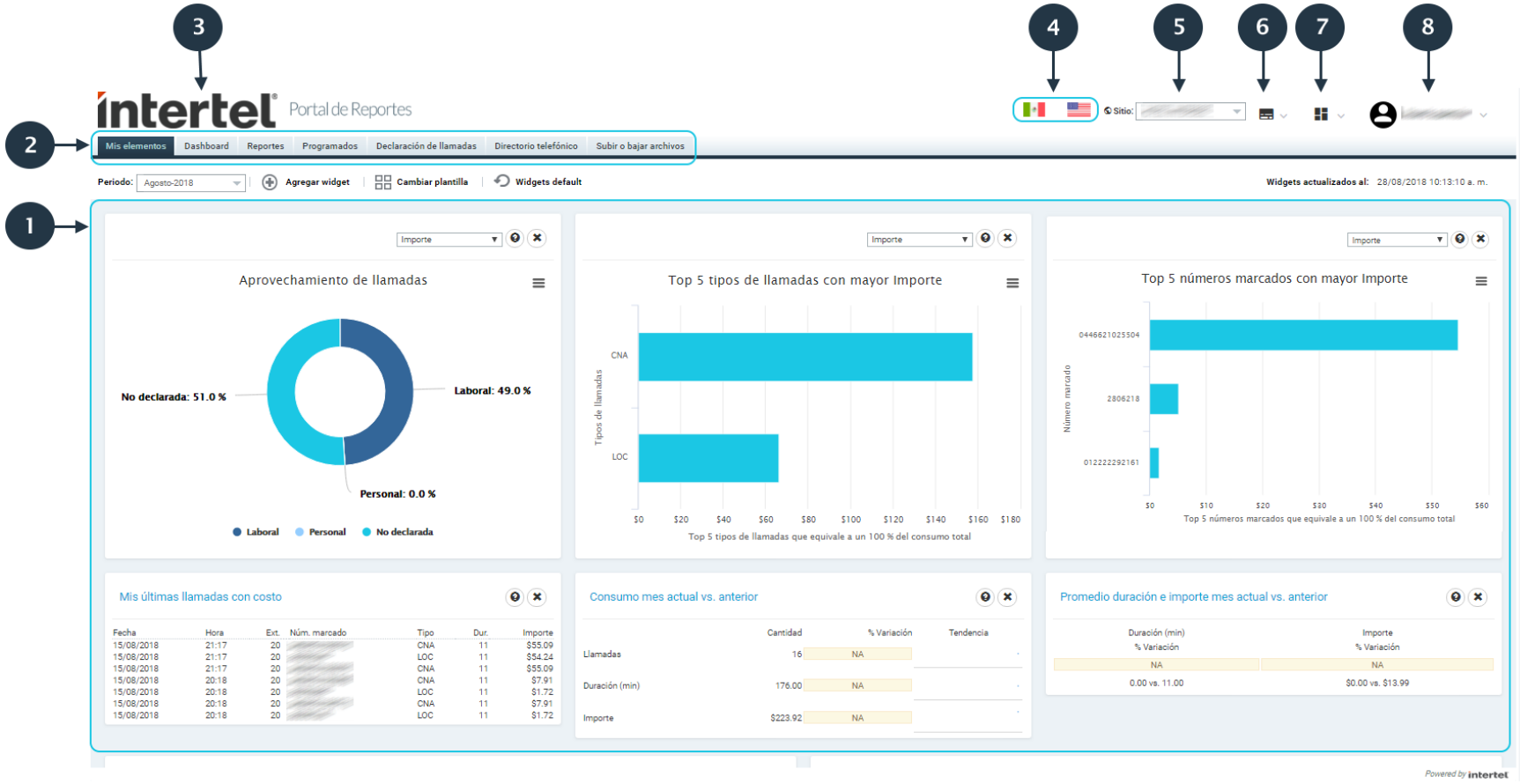


Figura 1.3. Pantalla de inicio del Portal de Reportes

1. Panel de resultados.
2. Menú de opciones.
3. Logotipo.
4. Idioma.
5. Sitio activo.
6. Gestión de reportes.
7. Indicadores dinámicos
8. Cuenta de usuario.

Panel de resultados

Este panel concentra los resultados de las diferentes opciones que pueden ser consultadas del menú principal. La información que se muestra en este panel es diferente, desde indicadores con consumos de telefonía fija, filtros para generar reportes, números marcados para ser declarados como laborales o personales, etcétera, dependiendo de la opción seleccionada.

Menú de opciones

En este menú se encuentran las opciones principales del Portal de Reportes. Desde aquí tendrá la facilidad de consultar su consumo telefónico por hacer llamadas con su código de autorización y/o extensión, por medio de indicadores o dashboards. También podrá ejecutar reportes y administrar aquellos que programó para que fueran enviados de manera periódica por correo electrónico. Además, podrá declarar el motivo de sus llamadas como laborales o personales. Y en caso de tener a su cargo a personal, podrá consultar el consumo de telefonía fija de cada uno de sus colaboradores, o si cuenta con los permisos necesarios, consultar los indicadores de consumo telefónico de telefonía fija de su empresa.

Logotipo

En este apartado usted puede visualizar el logotipo institucional de su empresa. En caso de que no se tenga configurado el logotipo de su empresa, por default se mostrará el logotipo del Sistema Intertel®.

Idioma

El Portal de Reportes está preparado para ser operado en idioma español (México) o inglés (Estados Unidos), simplemente debe dar clic en el icono de la bandera deseada para que el sistema muestre el idioma de su preferencia. Una vez que el usuario salga del Portal de Reportes y decida nuevamente ingresar, no tendrá que preocuparse por volver a especificar el idioma, siempre y cuando ingrese desde el mismo navegador web en el que realizó la configuración. En caso de que llegara a ingresar desde otro navegador web, entonces el Portal de Reportes tomará como idioma principal, el idioma español.

Sitio activo

Indica el nombre del sitio que en ese momento se encuentra seleccionado y sobre el cual se consulta la información que se muestra en el panel de resultados. Este nombre se actualiza una vez que selecciona de la lista desplegable, el nombre de otro sitio.

Gestión de reportes

Esta opción solo está disponible para usuarios del sistema Intertel® con permisos de administrador de sitio o administrador global. Desde aquí el administrador decide cuáles reportes deberán aparecer en cada sitio; o hacer que aparezcan en el portal aquellos reportes que el propio cliente ha creado.
También desde esta opción es posible consultar cuales son los reportes que ha generado o tratado de generar cierto usuario. Para obtener mayor información sobre cada una de las funcionalidades a las cuales puede tener acceso desde esta opción, consulte el capítulo 5 “Gestión de reportes” de este manual.

Cuenta de usuario

Indica el nombre del usuario que en ese momento se encuentra autenticado en el Portal de Reportes. Desde aquí también el usuario puede cambiar su información personal, así como su foto de perfil, o renovar su código de autorización, inclusive modificar su contraseña para ingresar al portal. Así mismo tendrá la facilidad de consultar el listado de los reportes que últimamente ha generado.

Cuenta de usuario

Desde este apartado el usuario que se encuentra en sesión puede consultar el grupo de características laborales que lo definen o lo identifican como colaborador de la empresa. Por ejemplo, información personal, así como información de los elementos que le fueron asignados, como son extensiones, códigos de autorización y/o dispositivos móviles, como es el celular. También tiene la facilidad de cambiar su contraseña con la que ingresa a los Portales Web de Intertel® a los que tenga acceso, inclusive podrá renovar su código de autorización. En las secciones siguientes explicaremos detalladamente las características a las cuales tendrá acceso desde este apartado.

Perfil

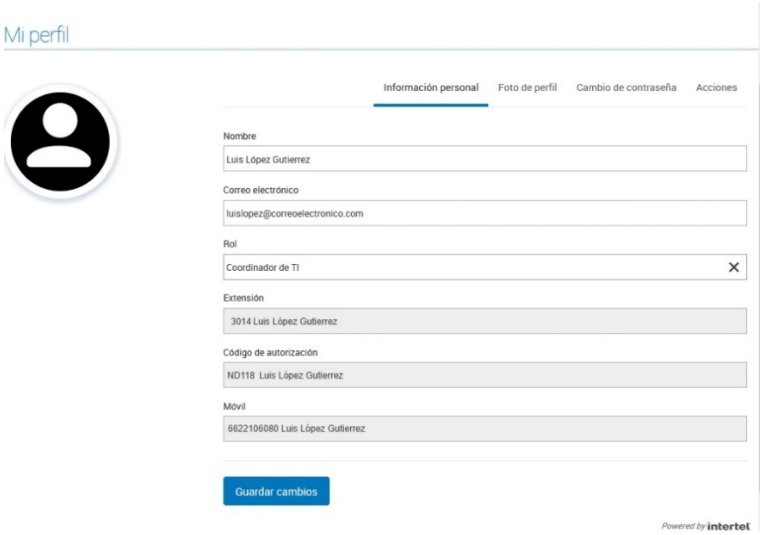


Figura1.4. Mi perfil – información personal

Información personal

Los datos que se muestran en esta sección son con los que el administrador del sistema Intertel® identificó al usuario que usted utiliza para ingresar a los Portales Web, en este caso al Portal de Reportes. Los datos son los siguientes:

- **Nombre:** Muestra el nombre con el cual fue identificado a su usuario en el sistema Intertel®. Generalmente este dato hace referencia a su nombre personal. Este dato puede ser cambiado por usted mismo y los cambios se verán reflejados en el sistema, sin tener necesidad de que sean validados por el administrador del sistema Intertel®.

- **Correo electrónico:** Muestra el correo electrónico que le fue configurado a su usuario en el sistema Intertel®. Este dato puede ser actualizado por usted mismo y los cambios se verán reflejados en el sistema, sin tener necesidad de que sean validados por el administrador del sistema Intertel®.
  Si desea especificar más de un correo electrónico, simplemente separe cada cuenta de correo usando el símbolo de punto y coma (;).
- **Rol:** Escriba el nombre del puesto que desempeña este usuario en su empresa.
- **Extensión:** Este dato es informativo y sirve para que usted pueda consultar las extensiones que le han sido asignadas. Por cada extensión se muestra el número de extensión y la descripción con la cual fue identificada en el sistema Intertel®.
- **Código de autorización:** Este dato es informativo y sirve para que usted pueda consultar los códigos de autorización que le han sido asignados. Por cada código se mostrará la clave de referencia y la descripción con el que fue identificado dicho código en el sistema Intertel®.
- **Móvil:** Este dato es informativo y sirve para que usted pueda consultar los dispositivos móviles o celulares que le han sido asignados. Por cada dispositivo móvil se muestra el número del celular y la descripción con el que fue identificado dicho dispositivo móvil en el sistema Intertel®.

Foto de perfil

Con el objetivo de personalizar su cuenta de usuario, podrá subir alguna foto de su preferencia para que esta sea mostrada en el Portal de Reportes. Simplemente seleccione la foto y guarde los cambios.

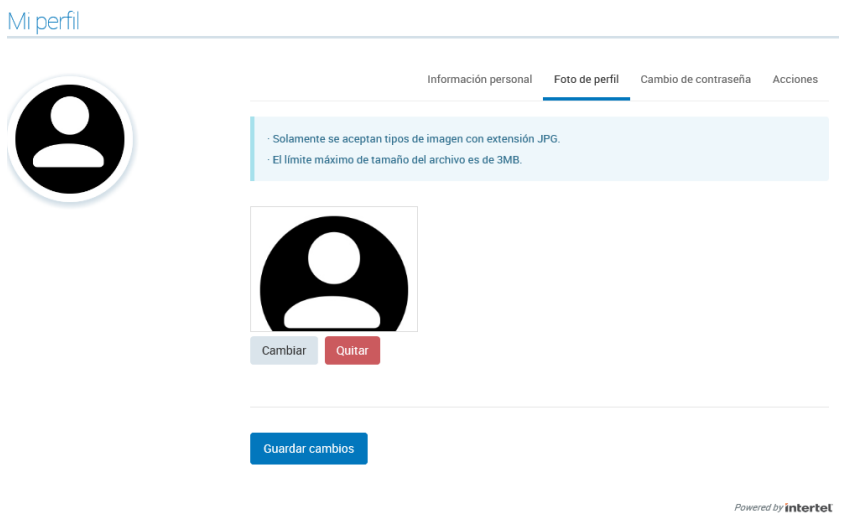


Figura 1.5. Mi perfil – cambiar foto

Cambio de contraseña.

En esta opción usted podrá cambiar la contraseña con la cual ingresa a sus Portales Web, en este caso el Portal de Reportes. Primero deberá escribir la contraseña actual y enseguida escribir la nueva contraseña. Esta contraseña deberá tener una longitud máxima de 20 caracteres y estar formada por dígitos y/o caracteres.

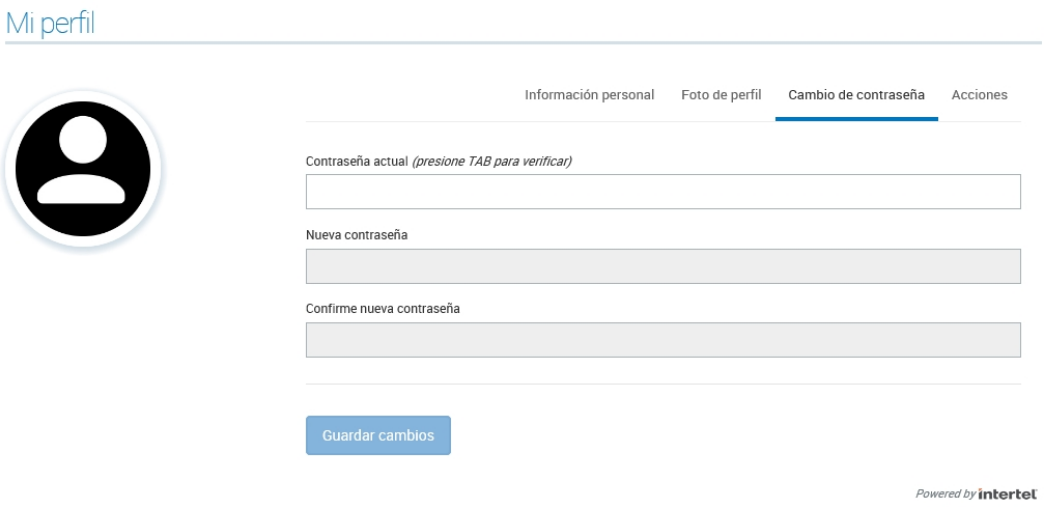


Figura 1.6. Mi perfil – cambio de contraseña

Acciones

Desde esta opción usted puede renovar hasta 2 veces al día todos los códigos de autorización que le hayan sido asignados. Simplemente debe dar clic en el botón de "Renovar" para realizar esta acción. Una vez hecho lo anterior el sistema Intertel® se encarga de enviar una notificación a su correo electrónico, así como al correo electrónico del supervisor del nivel jerárquico al que pertenece el código que se va a renovar, indicándoles el código renovado, así como el nuevo código asignado; pero para que pueda recibir este correo en su bandeja de entrada, será necesario que el administrador del sistema Intertel® realice las configuraciones necesarias. Por lo tanto, en caso de no recibir esta notificación comuníquese con el administrador del sistema Intertel® para que realice estas configuraciones.

Usted podrá hacer uso de este servicio dos veces al día, una vez que exceda la cantidad de intentos permitidos, la aplicación le notificará que será imposible renovar nuevamente su código de autorización, por lo cual deberá esperar hasta el día siguiente para intentarlo nuevamente.

Figura 1.7 Renovación de código de autorización.

IMPORTANTE: Para que esta opción le sea mostrada, su licencia del sistema Intertel® debe contar con el módulo de Smart manager activado, y que el administrador del sistema Intertel® haya habilitado la opción de "renovación de códigos" en la opción de "Opciones de operación" del sistema Intertel®. Si alguna de las dos condiciones anteriores no se cumple, entonces esta opción no aparecerá en la lista de servicios a consultar.

Manual de ayuda del Portal de Reportes

Al desplegar las opciones que se encuentran en la cuenta de usuario, usted podrá encontrar la guía de ayuda para aprender a usar el Portal de Reportes. Al presionar la opción Ayuda, en una ventana emergente, se mostrará el manual de usuario de la aplicación en formato PDF; por ese motivo será necesario que tenga instalado Adobe Reader para su consulta.

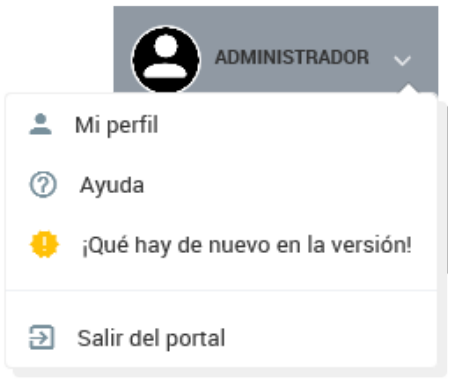


Figura 1.8. Cuenta de usuario

¡Qué hay de nuevo en la versión!

Si desea conocer que es lo nuevo que incluye el Portal de Reportes en la versión que acaba de adquirir, puede consultar la opción: "¿Qué hay de nuevo en la versión?" que se encuentra en el menú de "cuenta de usuario". Al dar clic sobre la opción anterior, se abrirá un listado donde podrá consultar las nuevas funcionalidades incluidas en el Portal de Reportes.

Salir del Portal

Esta opción se encuentra localizada dentro de la Cuenta de usuario. Al presionarla, da por terminada la sesión, permitiendo cerrar todas las conexiones al sistema de forma segura y adecuada.

Personal a cargo

Dentro de esta opción se muestra el total generado en importe por todas las llamadas realizadas por usuarios asignados al nivel jerárquico del cuál, él es responsable.

En caso de que alguno de los usuarios haya excedido el límite de consumo, de alguno de sus elementos, entonces, el importe total del nivel jerárquico se sombrará de color rojo indicando que se sobre pasó este límite.

Debajo del total global, se listan los usuarios asignados al elemento jerárquico del cual el usuario supervisor está a cargo.

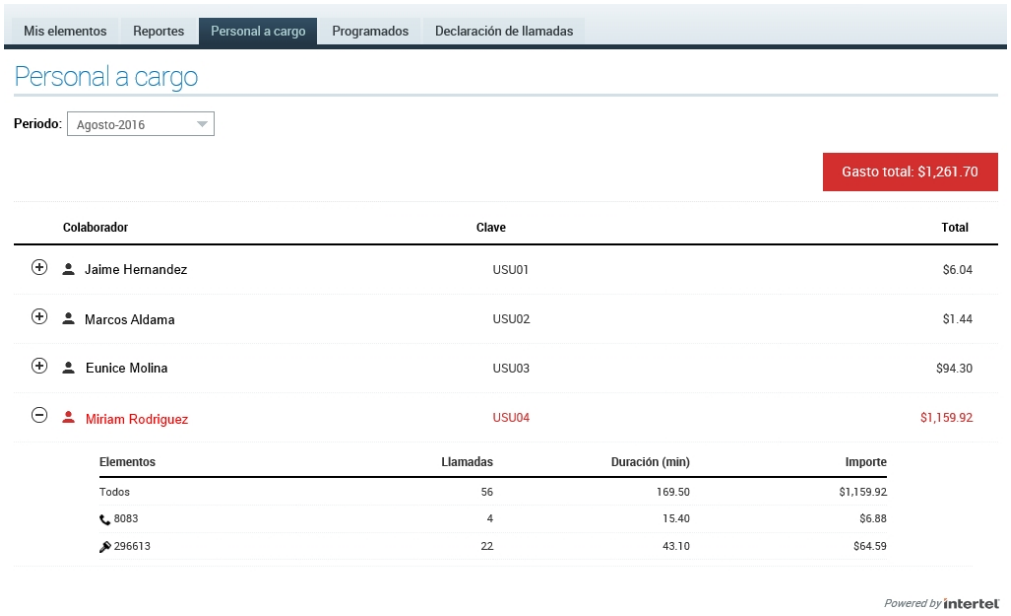


Figura 1.9 Tablero de indicadores de telefonía fija – Mis elementos

En este listado, el usuario supervisor puede visualizar a cuánto asciende el importe de llamadas, que ha realizado cada uno de los usuarios a su cargo, en el periodo seleccionado.

Al igual que con el total global, en caso de que algún usuario haya excedido el límite de consumo asignado para al menos uno de sus elementos, el registro se mostrará en color rojo.

El usuario supervisor también cuenta con la opción de ver el resumen de lo consumido por cada código o extensión que tenga asignada el usuario al presionar el icono con el símbolo de "más", que se encuentra localizado a la izquierda de cada colaborador de la lista.
En dicho resumen se muestra la clave el número de extensión o bien la clave de referencia del código de autorización, se muestra también, el total de llamadas realizadas en el periodo, el total de minutos consumidos entre todas las llamadas realizadas a través de ese elemento y, por último, el importe total generado.
Para quitar de la pantalla el resumen de cada elemento del usuario, solo bastará con presionar de nueva cuenta el ícono que ahora tiene el signo de menos.

IMPORTANTE: La pestaña de Personal a cargo se activa al momento de que un usuario es asignado como supervisor de un elemento jerárquico ya sea desde el catálogo de jerarquías del sistema Intertel o desde el catálogo de jerarquías de la administración. Adicionalmente, deben cumplirse los siguientes puntos:

- Dentro del elemento jerárquico deben existir usuarios con elementos asignados a su cargo como una extensión o un código de autorización.
- Deben existir llamadas realizadas por el usuario.
- Debe haberse activado y ejecutado la opción de "Comportamiento de consumo" del menú Configuración/Operación/Opciones de Operación/Portales web, del sistema Intertel.

También es importante tomar en cuenta que la información del personal a cargo es actualizada cada cierto tiempo, según la configuración que se tenga en la opción de "Comportamiento de consumo".

Directorio telefónico

Desde el Portal de Reportes usted tendrá acceso al listado telefónico de su empresa, siempre y cuando el administrador del sistema Intertel®, haya realizado la configuración necesaria para que esté disponible para todos los usuarios. Usted contará con la facilidad de imprimir todo el directorio, o bien exportarlo a PDF o CSV para mayor comodidad.

Para consultar alguna extensión o algún número celular, simplemente debe dar clic a la pestaña "Directorio Telefónico", para que se muestre un listado con todas las extensiones y/o móviles dados de alta en el sitio que se encuentra activo en ese momento en el Portal de Reportes.

En caso de no saber el número de extensión o móvil de alguna persona, o bien, si conoce el nombre de la persona con la que desea hablar, contará con la facilidad de realizar búsquedas específicas, ya sea por el número de la extensión, del móvil, o bien por el nombre o descripción con el que hayan sido identificados estos dispositivos. Simplemente escriba en el cuadro de búsqueda algunos dígitos para realizar búsquedas por extensión o móvil; o escriba algunas letras con las que considera haya sido identificada la extensión o el móvil, para que se muestre el listado de coincidencias.

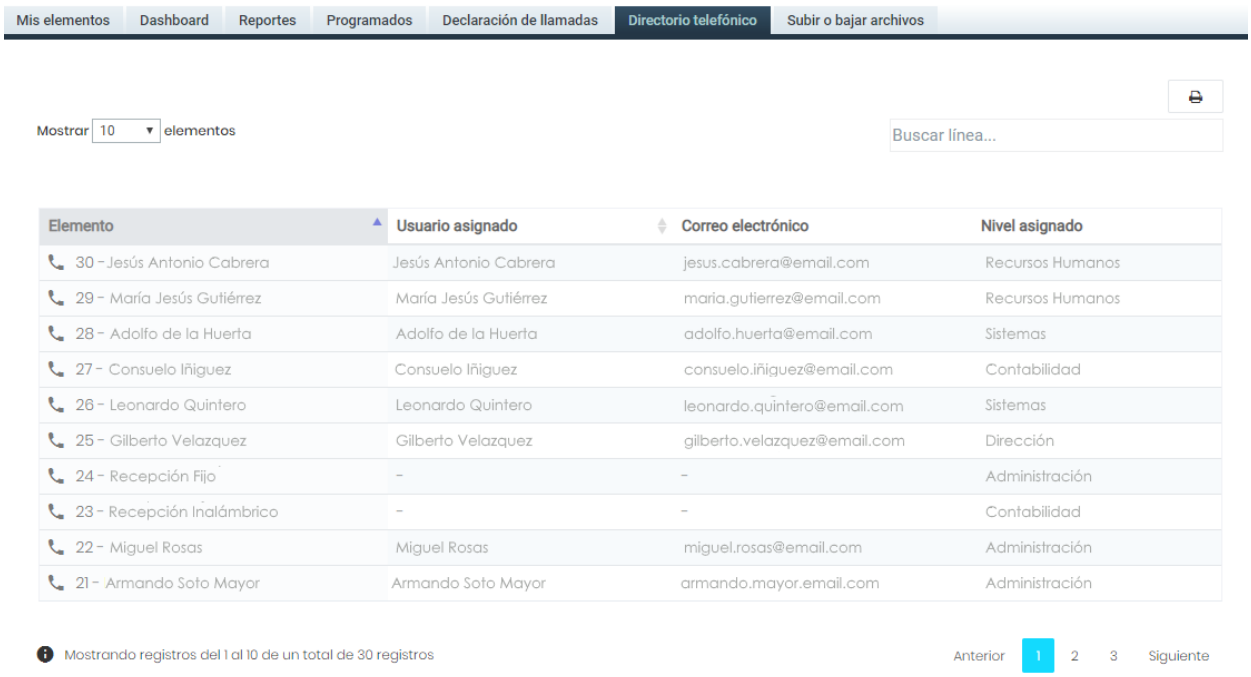


Figura 1.10 Directorio telefónico de la empresa

Compartir archivos

El Portal de Reportes te brinda la facilidad de compartir archivos usando las opciones de carga y descarga que vienen en la pestaña de "Compartir archivos". Si tu usuario dado de alta en el sistema Intertel tiene privilegios de consulta de tipo administrador de sitio o administrador global, entonces podrás contar con la facilidad de usar esta característica.

Podrás acceder a los archivos independientemente del sitio en el que te encuentres activo, es decir, este repositorio es común para todos los sitios mostrados en el Portal de Reportes. Enseguida conocerás la manera en la que podrás compartir archivos:

Carga de archivos

Podrás compartir archivos con una capacidad máxima de hasta 100 Mega bytes, simplemente selecciona la carpeta a donde el archivo deba pertenecer, y después arrastre y suelte el archivo en el recuadro sombreado con líneas grises. Por último, de clic en el botón de "Cargar" para que inicie el proceso de almacenamiento.

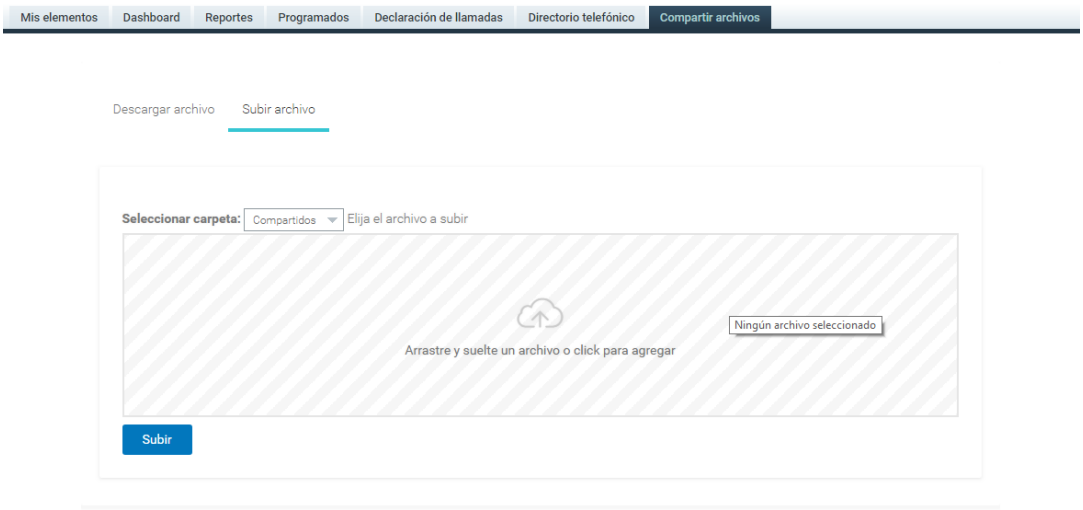


Figura 1.11 Opción para subir archivos.

Descarga de archivos

Al seleccionar esta opción aparecerán dos listados, el primer listado corresponde a las carpetas donde fueron almacenados los archivos por compartir, y de lado derecho el listado de los archivos disponibles a descargar.

Para iniciar una descarga seleccione primero la carpeta donde se encuentra el archivo; enseguida de lado derecho aparecerá el conjunto de archivos disponibles, por último, de clic sobre el archivo para que de manera automática inicie la descarga desde su navegador. Recuerde ir a la carpeta de "Descargas" de su equipo, ya que ahí será guardado este archivo.

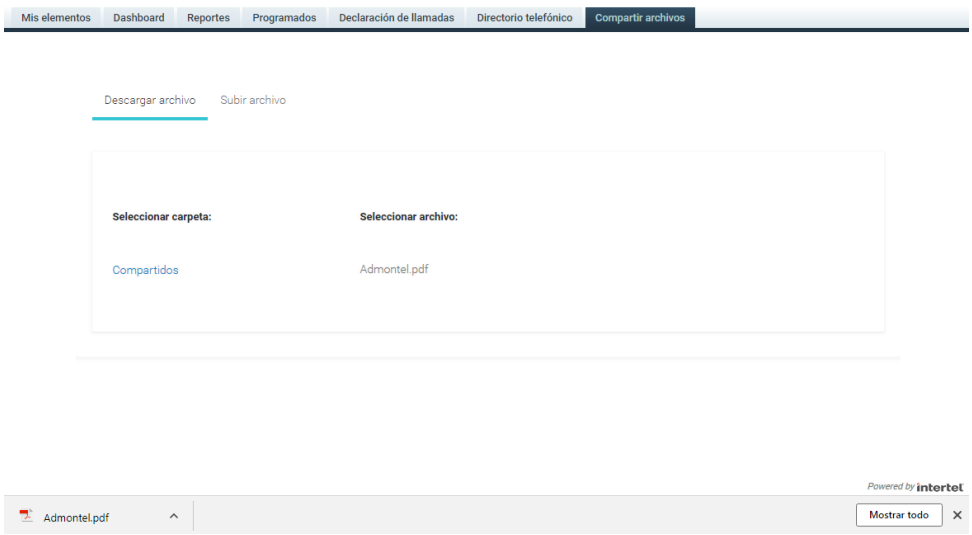


Figura 1.12 Opción para descargar archivos.

Capítulo 2. Dashboard

En la actualidad existen una extensa variedad de herramientas tecnológicas que proveen el acceso a grandes volúmenes de información. Gracias a estas herramientas tenemos a nuestro alcance grandes cúmulos de información, que creemos será sencillo analizarla para obtener resultados que sean útiles y en base a estos, tomar decisiones para gestionar nuestros negocios.

El problema con el que podemos llegar a encontrarnos, es que esta información es tan extensa que terminamos invirtiendo la mayor parte de nuestro tiempo en su análisis, lo cual ocasiona que dejemos de realizar el resto de nuestras actividades diarias, y cuando llegamos a obtener los resultados esperados, nos damos cuenta de que las acciones preventivas que deberíamos haber aplicado fueron detectadas muy tarde, de tal manera que la información que obtuvimos deja de sernos útil.

Una solución al problema anterior son los famosos tableros de mando, o comúnmente conocidos con el nombre de dashboards. Se han hecho populares por ser herramientas eficaces para lograr comunicar una gran cantidad de información, en pequeños espacios del monitor de su computadora o dispositivos móviles. Esta información es precisa y expresa lo que necesitamos conocer en el tiempo indicado, y va acompañado de un diseño visual enriquecido, el cual ofrece a los usuarios, procesar grandes trozos de información, con rapidez por medio de la percepción visual.

Tableros de mando (Dashboards)

¿Qué es un tablero de mando o dashboard?

Un dashboard o tablero de mando muestra un conjunto de indicadores, que en algunas ocasiones dependiendo de la naturaleza de la información contenida en el tablero, permite al usuario su personalización, seleccionando aquellos indicadores que considera valiosos para satisfacer algunas de sus necesidades específicas.

Estos indicadores proveen información relacionada con el consumo telefónico que proviene del conmutador (PBX) de su empresa, y pueden ser consultados por usuarios finales, así como por aquellos usuarios que tienen privilegios de consulta de tipo “Administrador de sitio” o “Administrador global en el sistema Intertel®.

El Portal de Reportes ofrece 5 tableros de mando: “Mis elementos”, “Dashboard”, “Desempeño”, “Mayores consumos” y “Totales”. En los primeros dos tableros, es posible que el usuario personalice el diseño visual a partir de un conjunto de plantillas (layouts) e indicadores (widgets) que están disponibles en la aplicación.

IMPORTANTE: Si desea personalizar el diseño de su tablero podrá hacerlo cambiando el tipo de plantilla o añadiendo o quitando los indicadores que no sean importantes para usted, para hacerlo consulte los temas de “Indicadores (widget)” y “Plantillas (Layout)” de esta sección.

La información que se muestra en cada indicador de los tableros: “Mis elementos” y “Dashboard” se actualiza mediante un proceso que es ejecutado a media noche, de tal forma, que los datos que son mostrados a través de estos indicadores hacen referencia a información del día anterior, aunque , el administrador del sistema tiene la posibilidad de configurar las horas del día, en las que se tenga que estar actualizando dicha información. Los datos a los cuales tiene acceso el usuario desde estos indicadores dependen de los privilegios de consulta que le hayan sido otorgados desde el sistema Intertel®.

A diferencia de los tableros anteriores, los tableros de: “Desempeño”, “Mayores consumos”, y “Totales” muestran un conjunto de indicadores que se encuentran fijos, y no son personalizables por el usuario, es decir, que no pueden ser ocultados y no pueden moverse de lugar a otro dentro del tablero. Sin embargo, algunos indicadores de estos tres tableros cuentan con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas, simplemente debe dar clic sobre el indicador que tenga un efecto de agrandamiento.

Los datos contenidos en cada uno de los tableros de “Desempeño”, “Mayores consumos”, y “Totales”, son actualizados con información: diaria, semanal o mensual, y el periodo de actualización es de 5 minutos o hasta de 60 minutos, los cuales pueden ser configurables por el administrador del sistema Intertel.

Mis elementos

En el tablero “Mis elementos” cualquier usuario que tenga acceso al Portal de Reportes podrá consultar información correspondiente a los elementos que le fueron asignados, como pueden ser extensiones y/o códigos de autorización. Los indicadores disponibles en esta sección se listan en la siguiente tabla:

Indicador (widget)	Descripción
Aprovechamiento de llamadas	Muestra el porcentaje de llamadas que han sido declaradas como personales o laborales durante un periodo de tiempo, incluso aquellas llamadas que aún se encuentran pendientes por declarar.
Consumo mes actual vs. anterior	Presenta un resumen con la cantidad total, total de duración y total de importe de las llamadas que realizó el usuario, en el mes o periodo seleccionado. Así mismo, indica el porcentaje de variación que hay entre, el mes seleccionado y el mes anterior. Además, contiene una pequeña gráfica para interpretar la tendencia.
Mis últimas llamadas	Muestra, como máximo, las últimas siete llamadas realizadas por el usuario en sesión en lo que va del mes actual o en el mes seleccionado y que hayan generado un costo mayor a cero. Estas llamadas son las que realizó con alguno de los elementos de tipo código de autorización o de tipo extensión libre (extensión que no requiere código para marcar), que están o estuvieron asignados a él, al momento de realizar la llamada.
Promedio importe y duración mes actual vs. Anterior	Muestra un resumen con el promedio y porcentaje de variación de importe y de duración, generados por las llamadas que realizó el usuario en el mes seleccionado, presentado contra el promedio y porcentaje de variación, de las llamadas generadas por el mismo usuario en el mes anterior al seleccionado.
Promedio por llamada	Indica el promedio en duración y el promedio en importe, generados por las llamadas que ha realizado el usuario en el mes en curso o en el mes seleccionado.

Resumen de telecomunicaciones	Muestra el listado y el acumulado en importe, duración y cantidad de llamadas, de cada uno de los elementos de telefonía fija (códigos de autorización y/o extensiones) asignados al usuario en sesión.
Top 5 tipos de llamadas con mayor importe	Presenta una gráfica con los 5 tipos de llamadas que más importe ha acumulado el usuario en sesión, en el mes actual o el mes seleccionado.
Top 5 números marcados con mayor importe	Presenta una gráfica con los 5 números marcados por el usuario en sesión, que hayan acumulado mayor importe para este usuario, en lo que va del mes en curso o en el mes que se haya seleccionado.
Top 5 lugares con mayor importe	Muestra una gráfica con las 5 localidades o lugares marcados por el usuario, que hayan acumulado mayor importe en lo que va del mes o en el mes seleccionado.

La siguiente figura, muestra un ejemplo de los indicadores localizados en el Tabí de **"Mis elementos"**.

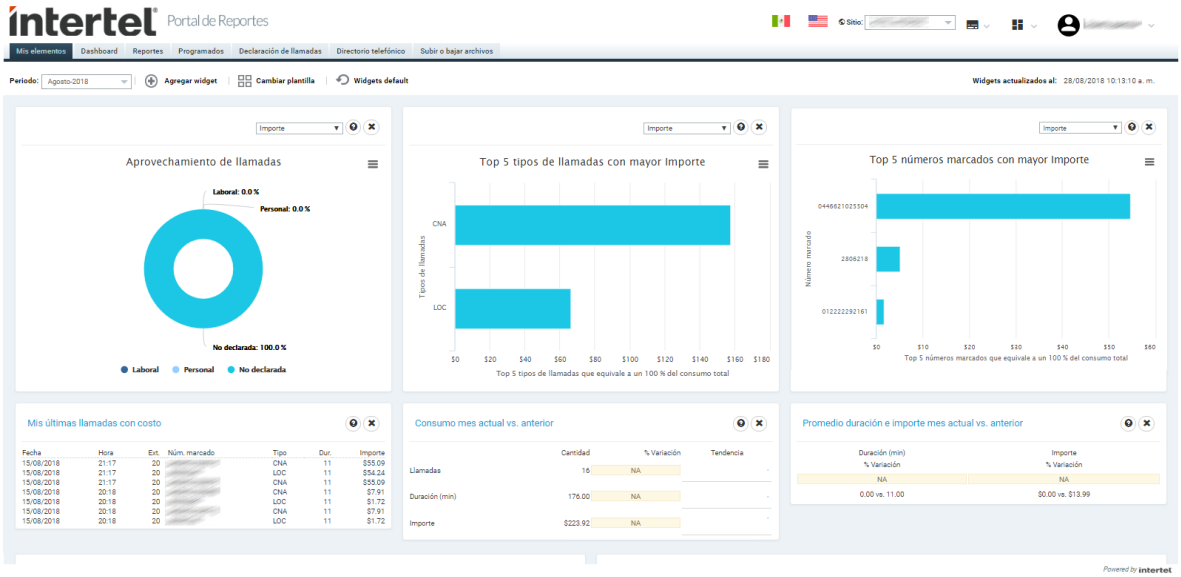


Figura 2.1. Tablero de indicadores de telefonía fija – Mis elementos

IMPORTANTE: Consulte al administrador del sistema Intertel en caso de que el selector de periodo muestre un mes y/o año diferente al actual. Es común que el selector pueda mostrar un mes y/o año diferente al actual, ya que este dato se obtiene del último mes que fue procesado por el "proceso de llamadas del sistema Intertel".

Dashboard

Este tablero solo está disponible para usuarios con permisos de tipo administrador de sitio o administrador global del sistema, y por medio de los indicadores que se encuentran en esta sección el usuario podrá consultar información perteneciente a toda la empresa. Los indicadores disponibles en esta sección se listan en la siguiente tabla:

Indicador (widget)	Descripción
Aprovechamiento de llamadas por cantidad de	Muestra el porcentaje de llamadas que han sido declaradas en su empresa como personales o laborales durante un periodo de tiempo, incluso aquellas llamadas que

llamadas, duración o importe.	aún se encuentran pendientes por declarar.
Consumo acumulado	Provee el consumo telefónico de un periodo o mes específico, que es obtenido por todos los códigos de autorización y extensiones dados de alta en el sistema Intertel®. Los rubros que se pueden consultar son el total de llamadas realizadas, la duración total de estas llamadas, así como su importe.
Comparativo top 5 tipos de llamadas con mayor importe	Presenta un comparativo de los 5 tipos de llamadas que han generado mayor importe en el sistema en lo que va del mes actual. Así mismo presenta el importe actual generado, la variación contra el mes anterior y el porcentaje que representa cada uno de esos 5 tipos de llamadas con respecto al importe total generado por todas las llamadas.
Consumo mes actual vs. Anterior	Provee la variación porcentual entre la cantidad de llamadas, duración e importe de las llamadas realizadas, entre el mes seleccionado contra las cantidades de estos mismos rubros del mes anterior. Así mismo ofrece un histórico con las tendencias consumidas en un periodo de 13 meses, partiendo del mes seleccionado.
Consumo "No Asignado"	Provee el consumo telefónico de un periodo o mes específico, que es obtenido por los códigos de autorización y extensiones que no están asociados a un nivel jerárquico. Los rubros que se pueden consultar son el total de llamadas realizadas, la duración total de estas llamadas, así como su importe.
"no asignado" mes actual vs. anterior	Provee la variación porcentual entre la cantidad de llamadas, duración e importe de las llamadas realizadas, entre el mes seleccionado contra las cantidades de estos mismos rubros del mes anterior. Así mismo ofrece un histórico con las tendencias consumidas en un periodo de 13 meses, partiendo del mes seleccionado. La información proporcionada en este indicador corresponde a los códigos de autorización y extensiones que no pertenecen a un nivel jerárquico del sistema Intertel®.
Promedio importe y duración mes anterior vs. mes actual	Provee un comparativo entre la duración promedio e importe promedio del mes anterior, contra la duración promedio e importe promedio del mes seleccionado, y sus equivalencias de porcentaje de variación.
Promedio por llamada	Muestra el número de llamadas promedio que se han realizado en el periodo o mes específico y su equivalente en duración.
Top 5 áreas con mayor importe, duración o cantidad de llamadas	Muestra los 5 niveles jerárquicos 3 ('Áreas) que obtuvieron mayor consumo telefónico (importe), en el periodo o mes seleccionado.
Top 5 centros de costo con mayor importe, duración o cantidad de llamadas	Muestra los 5 niveles jerárquicos 4 (Centros de costo) que obtuvieron mayor consumo telefónico (importe), en el periodo o mes seleccionado.
Top 5 compañías con mayor importe, duración o cantidad de llamadas.	Muestra los 5 niveles jerárquicos 1 (Compañías9 que obtuvieron mayor consumo telefónico (importe), en el periodo o mes seleccionado.
Top 5 departamentos con mayor importe, duración o cantidad de llamadas.	Muestra los 5 niveles jerárquicos 5 (Departamentos) que obtuvieron mayor consumo telefónico (importe), en el periodo o mes seleccionado.
Top 5 divisiones con mayor importe, duración o cantidad de llamadas	Muestra los 5 niveles jerárquicos 2 (Divisiones) que obtuvieron mayor consumo telefónico (importe) en el periodo o mes seleccionado.
Top 5 códigos con mayor	Muestra los 5 códigos de autorización, que obtuvieron mayor consumo durante el

importe, duración o cantidad de llamadas.	periodo o mes seleccionado.
Top 5 lugares con mayor importe, duración o cantidad de llamadas.	Muestra los 5 lugares que obtuvieron mayor consumo telefónico, durante el periodo o mes seleccionado.
Top 5 números marcados con mayor importe, duración o cantidad de llamadas.	Muestra los 5 números que fueron marcados y que obtuvieron mayor importe, durante el periodo o mes seleccionado.
Top 5 tipos de llamada con mayor importe	Muestra los 5 tipos de llamadas que obtuvieron mayor consumo durante el mes seleccionado, y su porcentaje de variación contra el periodo anterior. Así como el porcentaje equivalente del consumo total.
Top 5 usuarios con mayor importe, duración o cantidad de llamadas.	Muestra los 5 usuarios que obtuvieron mayor consumo telefónico en el mes seleccionado.
Últimas llamadas	Muestra las últimas 5 llamadas procesadas por el sistema Intertel®.

Algunas de las propiedades que tienen los indicadores que se encuentran en los tableros "Mis elementos" y "Dashboard", es que pueden ser ocultados, agregados o ser reubicados dentro de una plantilla, para que aparezcan en el orden que usted considere más importante. O también pueden ser impresos o exportados en formato PDF, JPEG, PNG, SVG. Enseguida se explica cómo podrá realizarlo.

- Para ocultar un indicador en el tablero, de clic en el icono .
- Para agregar un indicador en el tablero, de clic en el icono **Agregar widget**
- Para imprimir o exportar el indicador que se encuentra en el tablero, a formato PDF, JPEG,PNG,SVG, de clic en el icono

La siguiente figura, muestra un ejemplo de los indicadores localizados en el Tab de "Dashboard".

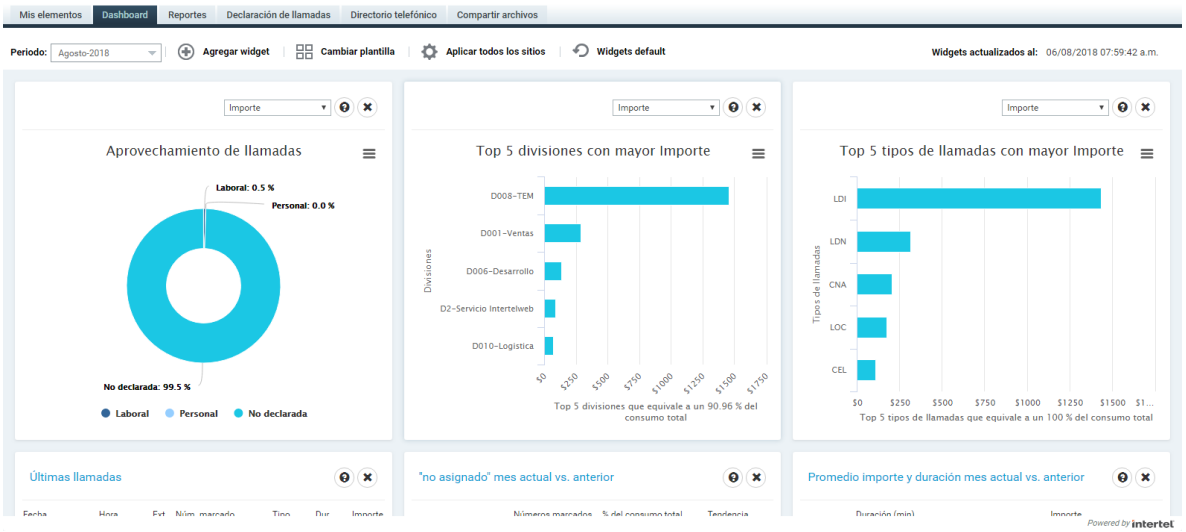


Figura 2.2. Tablero de indicadores de telefonía fija – Dashboard

IMPORTANTE: Consulte al administrador del sistema Intertel en caso de que el periodo muestre un mes y/o año diferente al actual. Es común que el selector pueda mostrar un mes y/o año diferente al actual, ya que este dato se obtiene del último mes que fue procesado por el "proceso de llamadas del sistema Intertel".

Desempeño

Este tablero está disponible para usuarios del sistema Intertel con permisos de consulta de tipo administrador de sitio o administrador global. Por medio de los indicadores que se encuentran en esta sección, el usuario podrá consultar información proporcionada por el conmutador, perteneciente a un sitio en particular de la empresa. Los datos registrados en este tablero son actualizados cada determinado minuto, los cuales son configurables por el administrador desde el sistema Intertel; de esta forma usted tiene conocimiento que la información mostrada a través de estos tableros, muestra las últimas actualizaciones que han sido registradas por el tarificador. Los indicadores disponibles en esta sección se listan en la siguiente tabla:

Indicador (widget)	Descripción
Total entrantes contestadas	La cantidad representada en este indicador se encuentra formada por el conjunto de llamadas entrantes que fueron contestadas por usuarios de su empresa. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Total salientes contestadas y perdidas	La cantidad representada en este indicador se encuentra formada, por el conjunto de llamadas realizadas (salientes) por usuarios de su empresa; estas llamadas pudieron o no haber sido contestadas. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Total perdidas entrantes y salientes	La cantidad representada en este indicador se encuentra formada por el conjunto de llamadas realizadas (salientes) o recibidas (entrantes) que no fueron atendidas por los usuarios. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Mayor duración entrante	Se trata de aquella llamada entrante que fue contestada por un usuario, y que obtuvo a diferencia del resto, el mayor tiempo de duración. Así mismo da a conocer el número de extensión donde fue atendida la llamada. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador
Mayor duración saliente	Se trata de aquella llamada realizada(saliente) por un usuario, y que obtuvo a diferencia del resto, el mayor tiempo de duración. Así mismo da a conocer el número de extensión por donde fue realizada la llamada. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador.
Llamada con mayor importe saliente	Se trata de aquella llamada realizada (saliente) por un usuario, y que obtuvo a diferencia del resto fue la más costosa. Así mismo da a conocer el número de extensión por donde fue realizada la llamada.
Tabla de posición	Muestra las 50 posiciones de aquellos lugares, tipos de llamada, códigos de

	autorización, extensiones o usuarios, que obtuvieron mayor cantidad de llamadas; con opción a consultar de este total de llamadas obtenidas, la duración total, así como la duración promedio. Los datos que se muestran en esta tabla son mostrados cada 15 segundos, de tal forma que usted puede consultar los 50 diferentes elementos (extensiones, códigos de autorización, lugares, tipos de llamada o usuarios) que aparecen en el listado. Las llamadas que son contabilizadas varían de acuerdo con el selector del elemento seleccionado, por ejemplo: 1. Para extensiones: Se contabilizan aquellas llamadas que fueron recibidas (entrantes) en la extensión, o aquellas que fueron realizadas (salientes) desde una extensión libre, es decir, que no pide código de autorización para hacer la llamada. 2. Para códigos de autorización: Se contabilizan aquellas llamadas realizadas (salientes) con el código de autorización. 3. Para lugares o tipos de llamadas: Se contabilizan de manera independiente, las llamadas entrantes de las salientes hacia un mismo lugar, de tal forma que pueden existir dos registros en el listado, con el mismo nombre del lugar, solo que un registro hará referencia a las llamadas entrantes y el segundo a las llamadas salientes. Las llamadas contabilizadas provienen de llamadas que hayan sido recibidas o realizadas, usando códigos de autorización y/o extensiones libres, es decir, aquellas extensiones que no ocupan de un código de autorización para poder realizar la llamada. 4. Para usuarios: Se contabilizan tanto las llamadas recibidas (entrantes) y realizadas (salientes) por el usuario, usando su código de autorización y/o extensión.

La siguiente figura, muestra un ejemplo de los indicadores localizados en el tablero de “Desempeño”.

Figura 2.3 Indicadores de desempeño

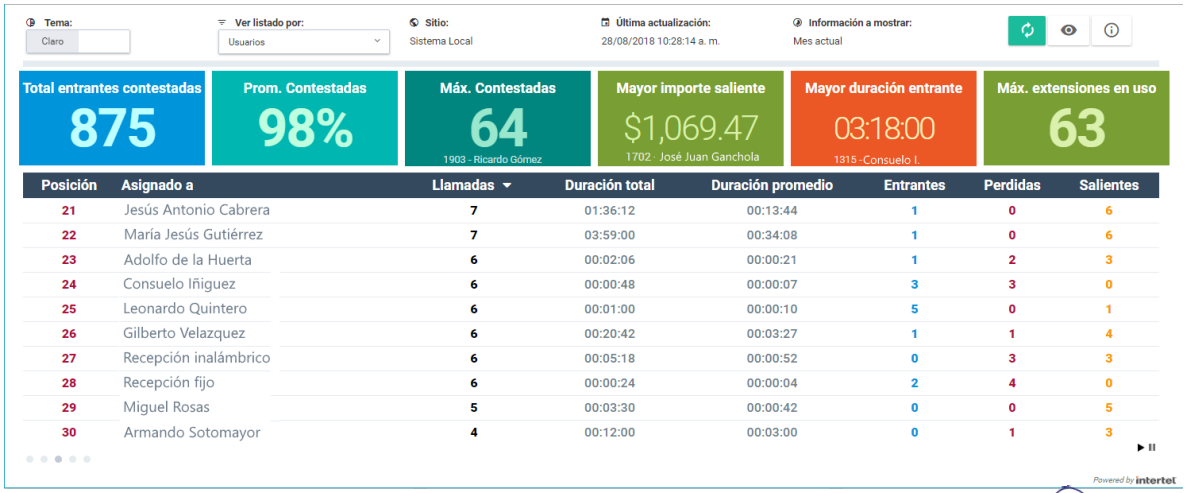
Mayores consumos

Este tablero está disponible para usuarios del sistema Intertel con permisos de consulta de tipo administrador de sitio o administrador global. Por medio de los indicadores que se encuentran en esta sección, el usuario podrá consultar información perteneciente a un sitio en particular de la empresa. Los datos registrados en este tablero son actualizados cada determinado minuto, los cuales son configurables por el administrador del sistema Intertel; de esta forma usted tiene conocimiento que la información mostrada a través de estos tableros, muestra las últimas actualizaciones que han sido registradas por el tarificador. Los indicadores disponibles en esta sección se listan en la siguiente tabla:

Indicador (widget)	Descripción
Total entrantes contestadas	La cantidad representada en este indicador se encuentra formada por el conjunto de llamadas entrantes que fueron contestadas por usuarios de su empresa. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Promedio contestadas	Representa el porcentaje de llamadas que fueron contestadas y recibidas (entrantes) por los usuarios. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador.
Max contestadas	Representa la cantidad máxima de llamadas que ha contestado una extensión en particular de su empresa. Así mismo da a conocer el número el número de la extensión. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Llamada con mayor importe saliente	Se trata de aquella llamada realizada (saliente) por un usuario, y que obtuvo a diferencia del resto fue la más costosa. Así mismo da a conocer el número de extensión por donde fue realizada la llamada.
Mayor duración entrante	Se trata de aquella llamada entrante que fue contestada por un usuario, y que obtuvo a diferencia del resto, el mayor tiempo de duración. Así mismo da a conocer el número de extensión donde fue atendida la llamada. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador.
Max extensiones en uso.	Da a conocer el número de extensiones que han registrado llamadas, estas llamadas pueden ser entrantes o salientes. Las llamadas contabilizadas en este indicador pudieron o no haber sido contestadas. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Tabla de posición	Muestra las 50 posiciones de aquellos lugares, tipos de llamadas, códigos de autorización, extensiones o usuarios, que obtuvieron mayor cantidad de llamadas; con opción a consultar de este total de llamadas obtenidas, la duración total, duración promedio, así como la cantidad de llamadas

	entrantes, salientes o perdidas. Los datos que se muestran en esta tabla son actualizados automáticamente cada 15 segundos, de tal forma que usted puede consultar los 50 diferentes elementos (extensiones, códigos de autorización, lugares o usuarios) que aparecen en el listado. Las llamadas que son contabilizadas varían de acuerdo con el selector del elemento seleccionado, por ejemplo: 1. Para extensiones: Se contabilizan aquellas llamadas que fueron recibidas (entrantes) en la extensión, o aquellas que fueron realizadas (salientes) desde una extensión libre, es decir, que no pide código de autorización para hacer la llamada. 2. Para códigos de autorización: Se contabilizan aquellas llamadas realizadas (salientes) con el código de autorización. 3. Para lugares o tipos de llamadas: Se contabilizan de manera independiente, las llamadas entrantes de las salientes hacia un mismo lugar, de tal forma que pueden existir dos registros en el listado, con el mismo nombre del lugar, solo que un registro hará referencia a las llamadas entrantes y el segundo a las llamadas salientes. Las llamadas contabilizadas provienen de llamadas que hayan sido recibidas o realizadas, usando códigos de autorización y/o extensiones libres, es decir, aquellas extensiones que no ocupan de un código de autorización para poder realizar la llamada. 4. Para usuarios: Se contabilizan tanto las llamadas recibidas (entrantes) y realizadas (salientes) por el usuario, usando su código de autorización y/o extensión.

La siguiente figura, muestra un ejemplo de los indicadores localizados en el tablero de "Mayores consumos:



Posición	Asignado a	Llamadas	Duración total	Duración promedio	Entrantes	Perdidas	Salientes
21	Jesús Antonio Cabrera	7	01:36:12	00:13:44	1	0	6
22	María Jesús Gutiérrez	7	03:59:00	00:34:08	1	0	6
23	Adolfo de la Huerta	6	00:02:06	00:00:21	1	2	3
24	Consuelo Iñiguez	6	00:00:48	00:00:07	3	3	0
25	Leonardo Quintero	6	00:01:00	00:00:10	5	0	1
26	Gilberto Velazquez	6	00:20:42	00:03:27	1	1	4
27	Recepción inalámbrico	6	00:05:18	00:00:52	0	3	3
28	Recepción fijo	6	00:00:24	00:00:04	2	4	0
29	Miguel Rosas	5	00:03:30	00:00:42	0	0	5
30	Armando Sotomayor	4	00:12:00	00:03:00	0	1	3

Figura 2.4 Indicadores de mayores consumos.

Totales

Este tablero está disponible para usuarios del sistema Intertel con permisos de consulta de tipo administrador de sitio o administrador global. Por medio de los indicadores que se encuentran en esta sección, el usuario podrá consultar información perteneciente a un sitio en particular de la empresa. Los datos registrados en este tablero son actualizados cada determinado minuto, los cuales son configurables por el administrador del sistema Intertel; de esta forma usted tiene conocimiento que la información mostrada a través de estos tableros, muestra las últimas actualizaciones que han sido registradas por el tarificador. Los indicadores disponibles en esta sección se listan en la siguiente tabla:

Indicador (widget)	Descripción
Entrantes perdidas.	Representada por el conjunto de llamadas recibidas (entrantes) que no fueron atendidas por los usuarios. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Salientes perdidas	Representada por el conjunto de llamadas realizadas (salientes) que no fueron atendidas por los usuarios. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Entrantes contestadas	Representa el total de llamadas recibidas (entrantes), que fueron contestadas por usuarios de su empresa. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Salientes contestadas	Representa el total de llamadas realizadas (salientes), que fueron contestadas por el destinatario. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Total salientes	La cantidad representada en este indicador se encuentra formada, por el conjunto de llamadas realizadas (salientes) por usuarios de su empresa; estas llamadas pudieron o no haber sido contestadas. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Duración promedio	Muestra la duración promedio del conjunto de llamadas realizadas (salientes) y recibidas (entrantes) que fueron atendidas por los usuarios de su empresa. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador.
Total entrantes	La cantidad representada en este indicador se encuentra formada por el conjunto de llamadas entrantes que fueron contestadas por usuarios de su empresa. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador.
Max extensiones en uso.	Da a conocer el número de extensiones que han registrado llamadas, estas llamadas pueden ser entrantes o salientes. Las llamadas contabilizadas en este indicador pudieron o no haber sido contestadas. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador. Este indicador cuenta con la característica de mostrar a manera de detalle las llamadas que están siendo contabilizadas dando clic sobre él.
Tiempo promedio de	Representa el tiempo promedio en segundos que han tardado en ser

respuesta	atendidas aquellas llamadas que han sido recibidas (entrantes), por los usuarios de su empresa. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador.
Llamada con mayor duración.	Se trata de aquella llamada realizada (saliente) o recibida (entrante) que fue atendida por el usuario y obtuvo a diferencia del resto, el mayor tiempo de duración. Las llamadas hechas entre las diferentes extensiones de su empresa no son contabilizadas en este indicador.
Tabla de información	Muestra los 50 lugares, Tipos de llamada, extensiones, códigos de autorización o usuarios, que obtuvieron mayor cantidad de llamadas; con opción a consultar de este total de llamadas obtenidas, la cantidad de llamadas contestadas, perdidas y salientes, así como la duración promedio de las llamadas que han sido contestadas, y duración promedio de las llamadas realizadas o salientes. Los datos que se muestran en esta tabla son actualizados automáticamente cada 15 segundos, de tal forma que usted puede consultar los 50 diferentes elementos (extensiones, códigos de autorización, lugares o usuarios) que aparecen en el listado. Las llamadas que son contabilizadas varían de acuerdo con el selector del elemento seleccionado, por ejemplo: 1. Para extensiones: Se contabilizan aquellas llamadas que fueron recibidas (entrantes) en la extensión, o aquellas que fueron realizadas (salientes) desde una extensión libre, es decir, que no pide código de autorización para hacer la llamada. 2. Para códigos de autorización: Se contabilizan aquellas llamadas realizadas (salientes) con el código de autorización. 3. Para lugares o tipos de llamada: Se contabilizan de manera independiente, las llamadas entrantes de las salientes hacia un mismo lugar, de tal forma que pueden existir dos registros en el listado, con el mismo nombre del lugar, solo que un registro hará referencia a las llamadas entrantes y el segundo a las llamadas salientes. Las llamadas contabilizadas provienen de llamadas que hayan sido recibidas o realizadas, usando códigos de autorización y/o extensiones libres, es decir, aquellas extensiones que no ocupan de un código de autorización para poder realizar la llamada. 4. Para usuarios: Se contabilizan tanto las llamadas recibidas (entrantes) y realizadas (salientes) por el usuario, usando su código de autorización y/o extensión.

La siguiente figura, muestra un ejemplo de los indicadores localizados en el tablero de “Totales”.

Figura 2.5 Indicadores de Totales.

Plantillas (Layout)

Cambiar plantilla

Existe un set de plantillas que puede usar para cambiar el aspecto visual en el que se muestran los indicadores del Portal de Reportes. Si desea seleccionar una plantilla diferente, deberá acceder a la opción de **"Cambiar plantilla"** que se encuentra enseguida de la opción **"Agregar indicador"**. Al hacer lo anterior se desplegará un listado con las plantillas existentes en la aplicación.

Basta con dar un clic sobre la plantilla deseada y posteriormente cerrar el listado para que los cambios sean aplicados. Generalmente las plantillas están formadas de uno o varios contenedores; estos pueden ser identificados por el número de cuadros que aparecen en la imagen. Un contenedor es una pequeña área en pantalla donde se aloja un indicador.

Cada vez que realiza un cambio de plantilla, los indicadores que tenía seleccionados previamente son reubicados en cada uno de los contenedores que se encuentran localizados al lado izquierdo de la plantilla seleccionada. Por ello será necesario que coloque cada indicador en el orden que usted considere conveniente. Para hacerlo consulte el tema de **"Mover un indicador** ", del siguiente tema.

Indicadores (widget)

¿Qué es un Indicador o widget?

Un indicador es la parte esencial de un tablero de mando, ya que en él se muestra información relevante, precisa, necesaria y disponible para ser usada de manera oportuna. Los indicadores del Portal de Reportes cuentan con la característica de poder ocultarlos, agregarlos, y en algunos de ellos exportarlos en formato imagen o PDF, incluso el poder imprimirlos.

Los indicadores o widgets contienen información solamente del sitio seleccionado, es decir, que los indicadores que aparezcan en el Tab de "Mis elementos", solo contendrán información generada de los elementos que tengan asignados en el sitio donde se encuentra el usuario en sesión y los indicadores para Administradores, contendrán información relacionada con el sitio que tengan seleccionado únicamente.

Agregar un indicador

Para agregar un indicador a un tablero de mando, es necesario dar clic en la opción **"Agregar widget"** que se encuentra enseguida del selector de **"Periodo"**; al hacer lo anterior aparecerá en una ventana modal con un listado de los indicadores que aún no han sido incluidos en el tablero.

Basta con agregar uno o más indicadores a la vez para que estos desaparezcan del listado.

Quitar un indicador

Desde la vista del tablero de mando (pestaña de Dashboard), cada indicador tiene una opción para ser cerrado, es decir, dejar de mostrarlo en el tablero; simplemente de clic en la marca con forma de flecha hacia abajo, ubicada en la parte superior izquierda de cada indicador y seleccione la opción "Eliminar". Cabe mencionar que, si usted cierra o elimina un indicador del tablero, podrá volverlo a agregar en el momento que desee dando clic en "Agregar widget".

Una vez que el indicador es cerrado, el resto de los indicadores son reubicados de manera automática en la plantilla, y el indicador que recién acaba de cerrar, vuelve a aparecer en el listado de indicadores disponibles.

Mover un indicador

Siempre que realice un cambio de plantilla o cuando se quita un indicador, la aplicación reubica de manera automática todos los indicadores que se encuentran en el tablero de mando. Lo anterior es un comportamiento natural. En el caso de que la reubicación no sea la esperada, usted podrá mover los indicadores en el orden que considere conveniente, para hacerlo posicione el puntero del ratón encima del indicador, de clic en él y sin soltar el botón del ratón deslice el indicador a su nueva ubicación (haga un drag and drop); por último, suelte el botón del ratón en el nuevo contenedor donde desea ubicar al indicador.

Descripción del indicador

Cada indicador al momento de ser agregado en el tablero, presentará un icono en forma de signo de interrogación que, al posicionarse sobre él, desplegará la descripción del dashboard. La descripción le permitirá al usuario conocer lo que incluye del indicador y con ello determinar cuál de ellos se adecua a sus necesidades.

Imprimir un indicador

Los widgets que incluyen gráficas, contarán con una opción para ser impresos en caso de que el usuario lo desee. La opción de impresión se localiza en la esquina superior derecha del widget. Una vez presionado este ícono, aparecerá la pantalla para configurar la impresión.

Aplicar configuración de indicadores (widgets) para todos los sitios

Una vez que ha seleccionado las plantillas y los indicadores que desea ver, así como el orden para mostrarlos en la pantalla, usted puede aplicar este diseño o configuración para todos los sitios que tenga a su cargo presionando la opción **"Aplicar todos los sitios"** que se localiza en la parte superior derecha de la

pantalla de Dashboard. De esta manera, usted no tendrá que configurar uno por uno los mismos indicadores en cada sitio.

Figura 2.6. Tablero de indicadores de telefonía fija

La configuración que aplica a todos los sitios, la puede realizar desde cualquier sitio que se encuentre seleccionado (combo localizado en la parte superior del Portal de Reportes.

Figura 2.7. Tablero de indicadores de telefonía fija

En caso de que haya aplicado la configuración para todos los sitios y desee que un solo sitio en particular tenga un indicador diferente, puede hacer el cambio ingresando directamente en el sitio. El sistema respetará la configuración que hizo para todos los demás sitios y para el que quedó diferente.

Restaurar configuración de indicadores (widgets)

Al presionar clic sobre la opción **"Widgets default"**, el sistema regresará la configuración original o default que tenían los indicadores. Esto es que, si el usuario en sesión seleccionó una plantilla, quitó y agregó widgets, los reorganizó, pero después requiere disponer de los widgets y configuración de plantilla que originalmente el sistema le había propuesto, con esta opción lo podrá realizar.

La restauración de los widgets y plantilla originales solo aplica para el sitio que está activo o seleccionado en ese momento. En caso de que requerir aplicarlo para todos los sitios, puede realizarlo con la opción: **"Aplicar todos los sitios"**.

La restauración a la configuración original se debe realizar de manera independiente para la sección (tab) de **"Mis elementos"** y para la sección (tab) de **"Dashboard"**; cada sección cuenta con su propia opción de **"Widgets default"**.

Figura 2.8. Tablero de indicadores de telefonía fija

Capítulo 3. Reportes

Conociendo los elementos que forman a la interfaz de Reportes

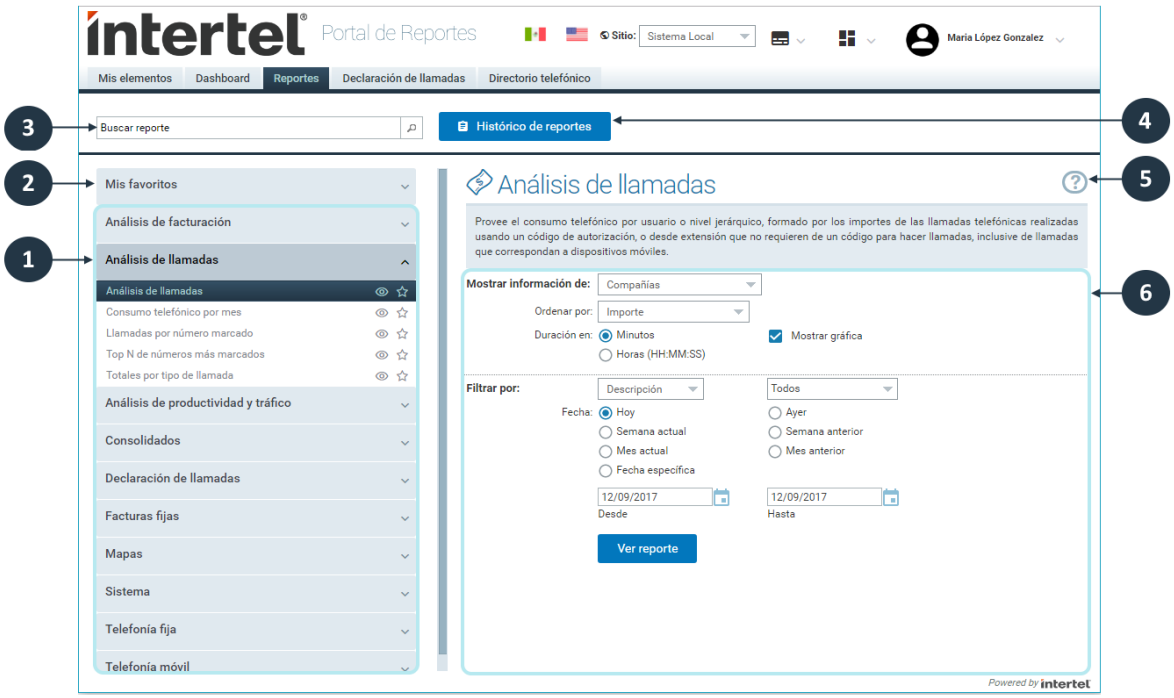


Figura 3.1. Interfaz de reportes

1. Menú de categorías y reportes.
2. Mis reportes favoritos.
3. Búsqueda de reportes.
4. Histórico de reportes.
5. Descripción del reporte.
6. Filtros.

Búsqueda.

Brinda la facilidad de buscar algún reporte. Simplemente escriba una frase que recuerde, o alguna palabra relacionada con el reporte, y la aplicación le mostrará un listado con los reportes que coincidan con la frase escrita. Recuerde utilizar signos de puntuación como es el acento, ya que algunos reportes lo usan, y en caso de no escribirlos correctamente, la búsqueda no le dará los resultados esperados.

Favoritos.

Aparecerá un listado de aquellos reportes que son considerados importantes para usted, y a los cuales puede acceder de manera rápida. Usted es quien decide que reportes aparecerán en esta sección. Para mayor información consulte el tema **"Mis favoritos"** de este manual.

Reportes.

En esta sección encontrarás el set básico de reportes disponibles del producto Portal de Reportes, cada reporte cuenta con un par de propiedades, como son el de ver como luce a través de una vista previa o

bien hacerlo como un reporte favorito. Cada reporte se encuentra clasificado en una categoría de acuerdo al tipo de información que contiene. A continuación, explicaremos a mayor detalle las categorías disponibles en el producto, así como las propiedades que forman a cada reporte.

Categorías

Cada reporte ha sido clasificado en alguna de las siguientes categorías: **Análisis de facturación, Análisis de llamadas, Consolidados, Declaración de llamadas, Especiales, Facturas fijas, Hoteles y Hospitales, Mapas, Planes tarifarios, Sistema, Telefonía fija, Telefonía móvil, y Tráfico Erlang,**

Si usted desea consultar datos que provienen de un conmutador (PBX), es conveniente que seleccione algún reporte de la categoría de Telefonía fija; o bien, si desea consultar información de la factura de sus dispositivos móviles, seleccione la categoría de Telefonía móvil. Ahora bien, si desea obtener datos donde vengan juntos los conceptos del conmutador y de la facturación de telefonía móvil, podrá hacerlo desde la categoría de Análisis de llamadas.

En caso de necesitar consultar cargos de servicios y de llamadas contenidos en la facturación de telefonía fija, deberá hacerlo desde algún reporte de la categoría de Facturación fija; o bien si desea conocer el aprovechamiento de uso telefónico de sus empleados dirigirse a la sección de Declaración de llamadas

Las clasificaciones anteriores estarán disponibles siempre y cuando su cuenta de usuario tenga los permisos de consulta necesarios. Estos permisos de consulta pueden variar entre cada sitio al cual usted tiene acceso.

Por ejemplo: si su cuenta de usuario tiene permisos para consultar información del dispositivo móvil que le dio la empresa en el sitio “Guadalajara”, entonces podrá consultar los reportes de las categorías de Telefonía móvil y de Análisis de llamadas. Si su usuario tiene permisos para consultar información relacionada con su extensión y/o código de autorización en el sitio de “México”, entonces tendrá acceso a los reportes que se encuentren en las clasificaciones de Telefonía fija y de Análisis de llamadas. Ahora bien, si su usuario tiene permisos para consultar información a partir de un nivel jerárquico en el sitio “Monterrey”, entonces usted tendrá acceso a los reportes de la categoría de Telefonía fija, Telefonía móvil y Análisis de llamadas.

La categoría de Facturación fija y Sistema, únicamente estarán disponibles para usuarios que tengan permisos del tipo “Administrador Global”. La categoría de Consolidados, estará disponible para Administradores; mientras que la categoría de Declaración de llamadas estará disponible siempre y cuando desde el sistema Intertel® tenga habilitada la opción para Declarar llamadas. En el caso de la categoría de “Planes tarifarios” le aparecerá solo si tiene configurado y activada la opción para el manejo de planes tarifarios.

Propiedades de un reporte

Reportes "Favoritos"

El Portal de Reportes tiene una sección donde aparece un listado de los reportes que son considerados importantes para usted, tal vez porque son reportes que usa frecuentemente o simplemente porque le proporcionan información relevante y de apoyo para la toma de decisiones.

Usted es quien decide cuales son los reportes que irán en esta sección. Cada usuario tiene sus propios reportes favoritos. Para incluir algún reporte como favorito, siga las instrucciones que se mencionan a continuación:

Hacer un reporte como uno de mis favoritos

- Busque el reporte que desea hacerlo uno de sus favoritos.
- Al lado derecho del nombre del reporte aparece una estrella. Posicione el ratón en ella para que cambie de color.
- Presione clic sobre la estrella para que tome un color sólido. Al hacer lo anterior se agregará el reporte a la sección de "Mis favoritos", creando un acceso directo.

Cada vez que un reporte es agregado a "Mis favoritos", la aplicación abrirá dicha sección y seleccionará el reporte que fue agregado.

Si usted desea remover o quitar algún reporte de esta sección, siga las instrucciones que se describen a continuación:

Quitar un reporte de mis favoritos

Existen dos formas en las que usted puede remover un reporte; puede hacerse directamente desde la sección de "Mis favoritos" o desde la clasificación original a donde pertenece el reporte.

A continuación, se explican los pasos que tendrá que seguir para remover un reporte marcado como favorito:

Desde la sección "Mis favoritos":

- Busque el reporte que desea remover.
- Al lado derecho del nombre del reporte aparece una bandeja de reciclaje. Posicione el ratón en ella para que cambie de color.
- Presione clic sobre la bandeja de reciclaje para que el reporte sea removido de la sección.

Desde la clasificación a donde pertenece el reporte:

- Busque el reporte que desea remover en alguna de las clasificaciones siguientes: Telefonía fija, Telefonía móvil, Telefonía fija y móvil, o Facturación fija (esta última categoría solo puede ser vista por usuarios que tienen permisos de administradores globales). Puede identificar de manera rápida los reportes marcados como favoritos, ya que la estrella que se encuentra a lado derecho del reporte, aparecerá iluminada de color amarillo sólido.

- Posicione el ratón en la estrella amarilla y de clic en ella para remover dicho reporte de la sección de favoritos. Al hacer lo anterior la estrella nuevamente cambiará de color, volviendo a su color original.

Vista previa de un reporte

Si necesita saber cómo lucirá el reporte que se encuentra por generar, de clic en el icono en forma de ojo ( ) que aparece al final del nombre de cada reporte. Al hacer lo anterior, aparecerá una pequeña imagen por medio de la cual podrá consultar como es que luce el reporte. Esta propiedad es útil para que tenga conocimiento de la información que podrá consultar a través de cada reporte, sin tener necesidad de generarlo.

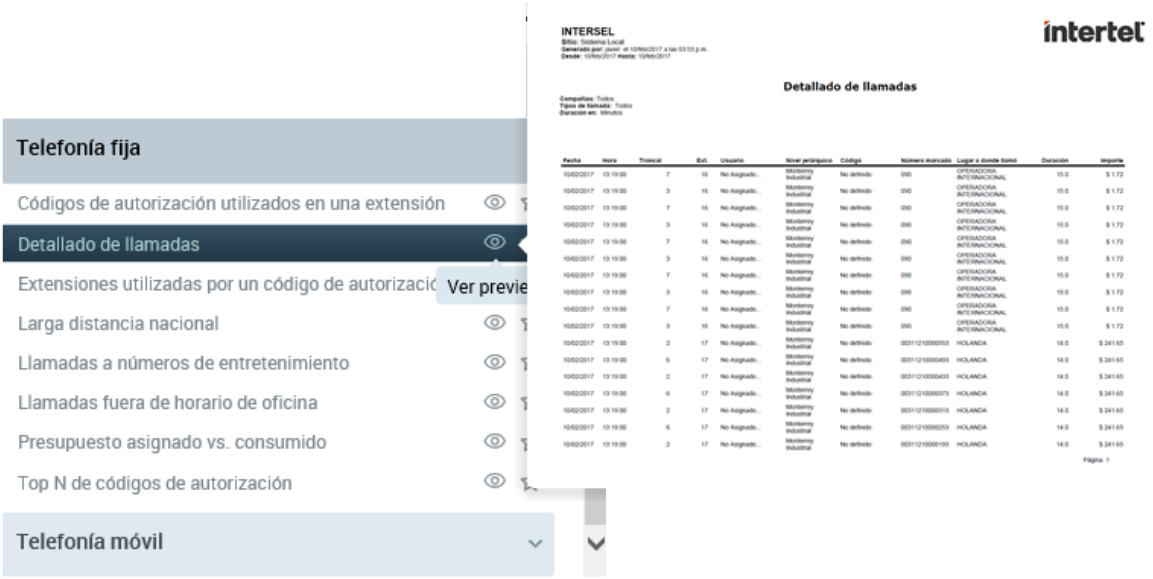


Figura 3.2 Vista previa de un reporte

Generación de reportes con un máximo de información de un año.

Los reportes del portal que cuentan con filtros por rangos de fechas (fecha inicial y fecha final), permiten mostrar información de máximo un año. Es decir, suponiendo que la fecha actual sea el 20 de agosto, del 2015, usted puede generar el reporte con un rango del 20 de agosto del 2014 al 20 de agosto del 2015 o bien, puede generar el reporte con un rango del 15 de septiembre del 2010 al 15 de septiembre del 2011. El rango que usted seleccione, siempre y cuando el rango no exceda de un año.

Generación de reportes con un máximo de 50,000 registros.

Por cuestiones de rendimiento, los reportes generados por el portal de Reportes han sido limitados para presentar hasta 50,000 registros, tanto para mostrarse en pantalla a través del paginado, como al momento de exportarse a cualquiera de los formatos. En caso de que la información que deba presentar el reporte exceda este número de registros, aparecerá una leyenda indicando al usuario este suceso. Para estos casos le sugerimos realizar búsquedas más precisas y/o generar los reportes con rangos de fechas más cortos.

Histórico de reportes

Todo usuario con acceso al Portal de Reportes tiene disponible esta opción, por medio de la cual, puede consultar el conjunto de reportes que ha ido generando cada vez que ha usado el portal. El primer reporte a mostrar, será el último que el usuario haya generado.

Para el caso de usuarios con privilegios de consulta de tipo administrador, además de ver sus reportes generados, también tendrá la facilidad de consultar, los reportes que fueron generado por un usuario en particular. Simplemente deberá seleccionar el nombre del usuario y dar clic en el botón de filtrar para que muestre el listado de reportes generado por el usuario

Por cada reporte se podrá consultar la siguiente información:

- Nombre del reporte: Mostrará el nombre del reporte que el usuario decidió consultar.
- Usuario: Nombre del usuario que generó el reporte.
- Última corrida: Hora en la que se generó el reporte.
- Status: Presentando el estatus "ejecutado" cuando el reporte haya sido generado de manera satisfactoria, y "abortado" cuando el reporte sufrió alguna dificultad al momento de mostrar información.

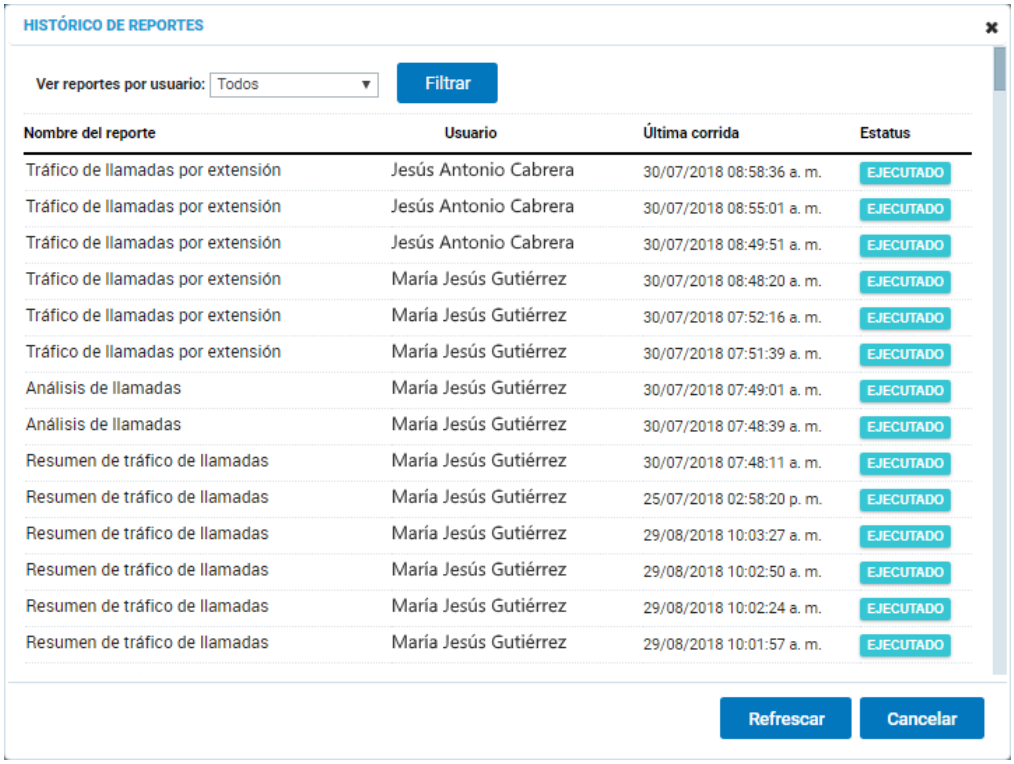


Figura 3.3 Listado de reportes generados por usuario

Filtros.

En esta sección se encuentran los filtros que necesitan ser especificados para que el reporte muestre la información esperada. Existen filtros que son comunes entre reportes, y otros que son específicos, esto debido al tipo de información que despliega cada reporte.

Enseguida se describen brevemente los filtros que son comunes entre los reportes, y cuál será el resultado que obtendremos al haberlos seleccionado.

- **Mostrar información de:**

A través de este filtro el Portal de Reportes interpreta que la primera información que se mostrará en el reporte, corresponderá a niveles jerárquicos (compañías, divisiones, áreas, centros de costo, departamentos, niveles 6-10), a usuarios, extensiones, códigos de autorización, dispositivos móviles, o incluso cuentas.
Los elementos descritos anteriormente se encontrarán disponibles dependiendo del tipo de reporte que se desea obtener, o de los privilegios que tenga asignados el usuario que se encuentra en sesión para consultar información.

Este filtro va acompañado de una opción de búsqueda: **"Filtrar por:"**. Con este filtro usted podrá:

- **Realizar búsquedas específicas:** Útil si la información que desea mostrar en el reporte, se trata de un elemento en particular, ya sea un nivel jerárquico, un usuario, un código de autorización, una extensión o un dispositivo móvil. Las búsquedas específicas pueden hacerse ya sea por la clave o descripción del elemento que desea buscar.

  Si la cantidad de coincidencias es mayor a la que se pueda mostrar en el selector, este buscador le brinda controles de navegación y un registro con el total de coincidencias, para su mayor comodidad.
- **Mostrar todos los elementos:** Se desplegará en el reporte ejecutado, todos los elementos de un mismo tipo, este tipo es definido por el filtro de **"Mostrar información de:"**, es decir pueden ser todas las compañías, las divisiones, las áreas, etc., o todos los usuarios, extensiones, códigos de autorización o todos los dispositivos móviles.

La información que se despliega en los filtros anteriores **"Mostrar información de:"** y de **"Filtrar por:"**, será a la que tenga permiso de consultar el usuario que se encuentre activo en el Portal de Reportes. Si desea tener acceso a toda la información de su empresa, es decir a todos los usuarios, extensiones, códigos, y dispositivos móviles deberá tener permisos de Administrador global o Administrador de sitio.

- **Información ordenada por:**
  Los datos que se muestran en los reportes pueden ser ordenados de mayor a menor por alguno de los siguientes rubros: por importe, por cantidad de llamadas, por duración o por fecha. Estas opciones deben seleccionarse antes de ejecutar un reporte.

- **Fechas:**
  Útil para consultar información de un día en específico, de un rango de fechas, o de un periodo de tiempo en particular. Existen diversas opciones de fechas, las cuales cambian de un reporte a otro, debido a la naturaleza de cada reporte.
  Enseguida se explican todas las opciones de fechas que brinda el Portal de Reportes; algunas de estas pueden usarse al momento de programar reportes, para que sean enviados de manera automática por correo electrónico.

  Las opciones compatibles con el envío automático de reportes por correo electrónico se muestran a continuación:

  - **Hoy:** Muestra información del día actual.
  - **Ayer:** Muestra información del día anterior a hoy.
  - **Semana actual:** Muestra información de la semana actual, iniciando con el día domingo y terminando en el día sábado.
  - **Semana anterior:** Muestra información de la semana anterior a la actual.
  - **Mes actual:** Muestra información del mes actual, iniciando con el primer día del mes y terminando con el día de hoy.
  - **Mes anterior:** Muestra información del mes anterior al actual.
  - **Último periodo de facturación:** Muestra información de la última factura cargada.

Existen dos opciones más de fechas, pero estas no son compatibles con el envío automático de reportes por correo electrónico. Estas opciones son:

- **Fecha específica:** Muestra información correspondiente a un rango de fechas, del tipo "Desde"-"Hasta". Los valores permitidos que podrá especificar en este filtro deberán estar comprendidos por los últimos 365 días, contando el día actual.

- **Periodo de facturación:** Muestra información correspondiente a un periodo de facturación en específico. Al seleccionar esta opción podrá seleccionar uno de los 12 últimos periodos de facturación que hayan sido cargados en el sistema Intertel®.

Las opciones de fecha que se explicaron anteriormente toman como base la fecha y hora del servidor en donde está instalado el Portal de Reportes. Por ese motivo es muy importante que, al momento de desplegar la información en el reporte, verifique que la fecha seleccionada corresponda con la fecha del día en el que realmente se encuentra, de no ser así, comuníquese con el encargado de administrar el sistema Intertel® para que tome las medidas correspondientes.

Botón Ver Reporte:

Al presionar este botón, se ejecuta el reporte y se muestra en una nueva ventana del navegador web.

Título del reporte.

Indica el nombre del reporte que se ha seleccionado del menú lateral.

Descripción.

Ofrece una explicación breve sobre el funcionamiento del reporte.

Elementos de un reporte ejecutado

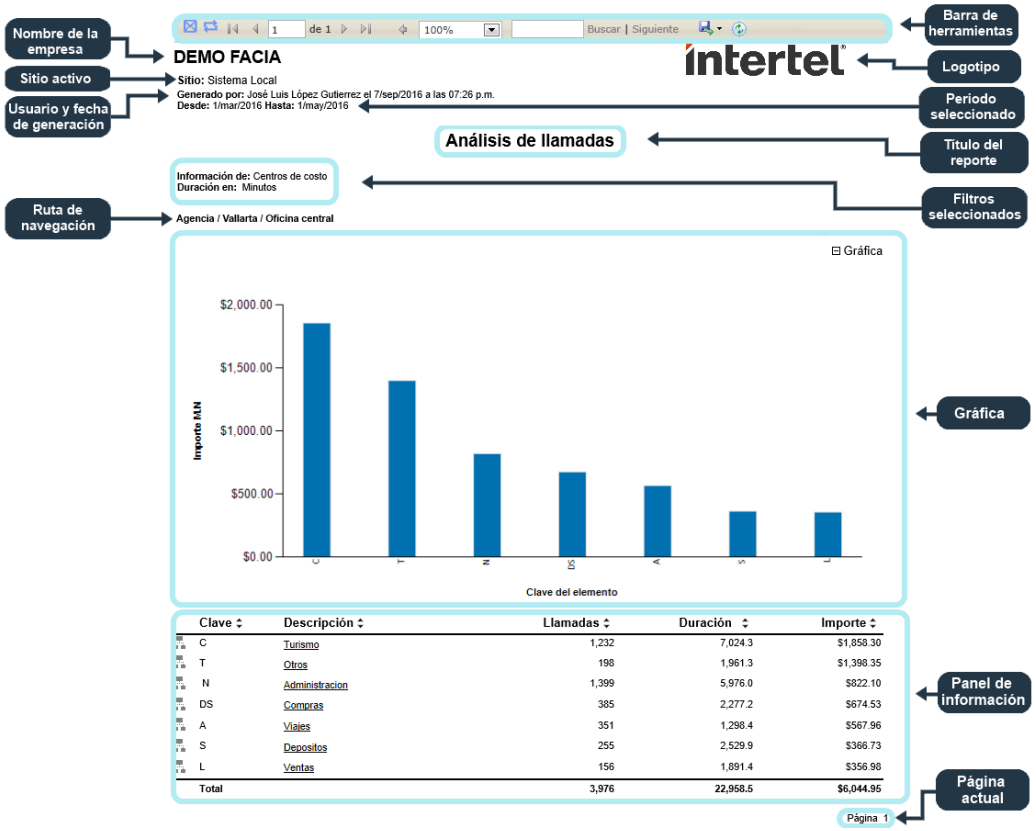


Figura 3.4. Elementos de un reporte ejecutado.

Barra de herramientas.

Localizada en la parte superior del reporte una vez que este es ejecutado. Contiene las opciones necesarias para navegar entre las páginas del reporte, o para buscar algún dato en su contenido, así como de otras facilidades, como pueden ser: su impresión, o exportación a diferentes recursos, como son documentos de Excel, Word, PDF, MHTML, XML y TIFF, o para programarlo y enviarlo automáticamente por correo electrónico.

En la figura siguiente se muestran las funcionalidades a las que tendrá acceso desde esta barra de herramientas:

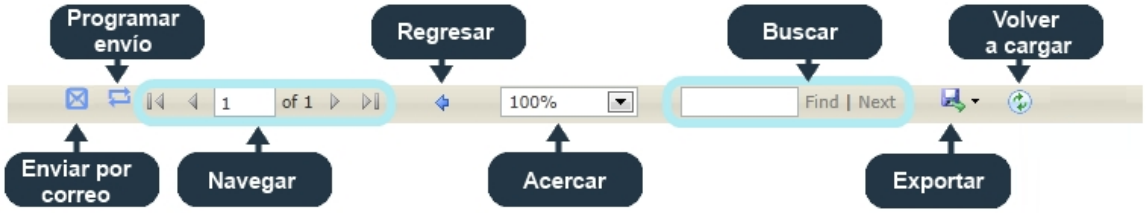


Figura 3.5. Funciones incluidas en la barra de herramientas de un reporte

- **Acercar.**

Útil para cuando la información contenida en el reporte aparece con letra pequeña.

La característica de **"Acercar"** solo puede ser accedida si está utilizando Internet Explorer 9 o superior; si usted está usando otro navegador web, mantenga presionadas al mismo tiempo, las teclas **CTRL** y la tecla del símbolo **+**, para obtener el mismo resultado. Por último, para volver la pantalla a su estado original, presione al mismo tiempo las teclas **CTRL** y la tecla **0**.

- **Buscar.**

Escriba aquí la palabra, número o serie de letras que necesite identificar de manera rápida en la información contenida en el cuerpo del reporte. Posteriormente presione Enter o de clic en la opción de "Find/Buscar", para que se muestren en el detalle del reporte, las coincidencias en otro color. En caso de que existan más de una coincidencia de clic en la opción de "Next/Siguiente" que se encuentran en la misma barra de herramientas.

- **Exportar.**

Al seleccionar esta opción, toda la información que haya sido desplegada en el reporte, es decir el detalle de las llamadas y la gráfica, será exportada a Word, PDF, Excel, archivo XML, formato MHTML y TIFF. Seleccione la opción que se adecue a sus necesidades.

Para la exportación a Excel, considere que solo se incluirán el número de registros que acepte Excel, aun cuando el reporte en pantalla haya presentado mayor número de registros.

Si desea imprimir el reporte deberá exportar el reporte a Word, Excel o PDF, y después realizar la impresión, o bien imprimirlo desde la opción de impresión que viene en el navegador.

- **Navegar.**

Útil para navegar o cambiarse entre las páginas del reporte en caso de que los resultados del reporte sobrepasen el límite de registros mostrados en una página.

- **Programar envío.**

Brinda al usuario la programación de reportes para que sean enviados de manera automática y periódica (diaria, semanal, mensual) a un grupo de personas, usando sus correos electrónicos. Consulte el tema de **"Envío automático de reportes"** de este manual para obtener mayor información.

- **Enviar por correo**

Permite enviar en ese momento el reporte que se está mostrando en pantalla a una cuenta de correo electrónico. Podrá seleccionar el formato del reporte (PDF, Excel, Word) con el cual desea que se envíe.

> Las características de "Programar periodicidad" y de "Enviar por correo al momento", están disponible si usted cuenta con una instalación de SQL Server 2016 Estándar o superior, SQL Server 2014 estándar o superior, SQL Server 2012 estándar o superior o bien, SQL Server 2008 R2 estándar o superior.

- **Volver a cargar.**

Refresca o actualiza la información contenida en la página.

- **Regresar.**

Le brinda la facilidad de regresar a la página anterior del reporte, una vez que utiliza la funcionalidad de drill-down.

Título del reporte.

Indica el nombre del reporte generado.

Filtros.

Sección donde se muestran los filtros que fueron especificados previamente por el usuario antes de ejecutar el reporte.

Gráfica.

En este panel se despliegan diferentes tipos de gráficas: de barras, de líneas o de pastel, dependiendo del tipo de reporte que haya seleccionado.

Comúnmente la gráfica de barras es utilizada para mostrar información relacionada con las Llamadas telefónicas de su empresa; esta información puede ser el importe, duración o las veces en que habló a un

número telefónico. La gráfica de pastel, es utilizada para mostrar el porcentaje de llamadas identificadas como personales, laborales o incluso aquellas que aún se encuentran sin declarar; el porcentaje de cada tipo de llamada, se hace en base a 3 rubros, estos son: por importe, por duración o por cantidad de llamadas. La gráfica de líneas es usada para representar las estadísticas de consumo telefónico anual de su empresa.

La gráfica puede ocultarse, dando clic en el símbolo de menos (-) que aparece a lado izquierdo de la palabra **"Gráfica"** en la esquina superior derecha de la gráfica; al hacer lo anterior este símbolo cambiará por el de más (+). El símbolo de menos (-) nos indica que la gráfica está lista para ser ocultada, y, en caso de quererla mostrar nuevamente, será necesario dar clic en el símbolo de más (+).

Logotipo.

Sección donde se muestra el logo de su empresa.

Nombre de la empresa.

Indica el nombre con la que fue programada la llave de activación del sistema Intertel®. Generalmente este nombre, es el de su empresa.

Panel de información.

En esta sección se despliegan los resultados del reporte ejecutado. Los datos mostrados en este panel, varían de acuerdo al tipo de reporte y a los parámetros que seleccionó desde la sección de filtros.

El contenido de los reportes generalmente inicia con el identificador o clave del elemento que seleccionó en el filtro de **"Mostrar información de:"**, es decir, por niveles jerárquicos (compañías, divisiones, áreas, centros de costo, departamentos, niveles 6-10), por usuarios, por códigos de autorización, por extensiones o por dispositivos móviles; enseguida aparecerá la descripción del dicho elemento.

Posteriormente se presenta información relacionada con el detalle de las llamadas, por ejemplo: el número de veces que llamó a un mismo número telefónico, la duración que corresponde al total de llamadas realizadas, así como, su importe total. El contenido de cada reporte varía dependiendo del tipo de reporte a ejecutar; consulte el tema de **"Clasificación de reportes"** para conocer las diferencias.

Página actual.

Indica el número de página mostrada en pantalla, útil especialmente cuando el reporte generado contiene muchos registros.

Periodo/Rango de fechas.

Al tratarse de datos que provienen del conmutador, indica el rango de fechas "Desde - Hasta" que corresponde con la información mostrada en el Reporte. O bien si se trata de reportes donde se muestra información de telefonía móvil, o datos de facturación de telefonía fija, indica periodos de facturación.

Sitio activo.

Sitio en el que se encuentra consultando información.

Ruta de navegación.

Indica la trayectoria de los niveles jerárquicos que han sido consultados al momento de dar drill-down.

Usuario y fecha de generación.

Indica el nombre de la persona que generó el reporte, así como la fecha y hora en el que fue ejecutado.

Ahora que conocemos los elementos y funcionalidades que brinda el portal, exploraremos la variedad de reportes a los que tendremos acceso desde esta herramienta de trabajo.

Drill-down.

Algunos reportes cuentan con la opción de "Desglose" o "Drill-down", la cual está activa cuando en el detalle o cuerpo del reporte, los elementos del sistema Intertel® como son los niveles jerárquicos, usuarios, extensiones, códigos de autorización o dispositivos móviles aparecen subrayados o con un hipervínculo. Al dar un clic sobre la descripción del elemento o sobre una de las barras contenidas en la gráfica, se despliega información relacionada con dicho elemento, partiendo de lo general a lo particular.

Por ejemplo, si genera un reporte donde la información que desea consultar es por una división en especial, al dar drill-down, se presentará el reporte de las áreas incluidas en dicha división, y al dar clic sobre alguna área, se presentarán los centros de costo incluidos en dicha área. Recuerde que la información desplegada al momento de dar drill-down depende de los permisos de seguridad que le hayan sido configurados a su usuario, dentro del sistema Intertel®.

Ordenamiento.

Para facilitar el análisis de la información que le presentan los reportes del módulo IPR, se cuenta con opciones de ordenamiento dentro de cada reporte. Es decir, una vez que se ha generado el reporte, usted puede ordenarlo por el dato de su interés, ya sea de forma ascendente o descendente.

Para activar esta funcionalidad, solo presione clic sobre icono que se encuentra al lado del título de la columna que desea ordenar. Al realizar esta acción todos los registros que le muestra el reporte se ordenarán por la columna seleccionada de manera ascendente. De tratarse de un dato numérico, el orden quedaría del 1 al 10 por ejemplo. En caso de ser un dato de tipo texto, se ordenarán de la A la Z. Presione clic de nuevo sobre la columna y los registros se ordenarán de forma descendente, es decir, del 10 al 1 por ejemplo, o de la Z a la A, según sea el caso.

Recuerde que por cuestiones de rendimiento los reportes están limitados a solo mostrar 50,000 registros, por lo que el ordenamiento solo se aplica a los primeros 50,000 registros que se encuentren en la base de datos.

Solo es posible activar el ordenamiento por una columna a la vez y solo aplicará para aquellas columnas que cuenten con el icono "Flecha arriba/Flecha abajo".

Al momento de exportar el reporte a cualquiera de los formatos disponibles en el módulo, éste conservará el ordenamiento que se haya seleccionado. Lo mismo aplicará al momento de la impresión.
Dependiendo de la cantidad de información, es posible que, al activar el ordenamiento de cualquiera de las columnas, el reporte tome unos momentos en mostrarse en pantalla, ya que, para el sistema, el ordenamiento representa el volver a generarlo.

Una vez explicados los elementos de la interfaz gráfica del Portal de Reportes y las características disponibles para cada reporte, describiremos en el siguiente tema, la información que obtendrá por cada reporte en sus resultados de salida.

Clasificación de reportes

Para que la operación del Portal de Reportes fuera lo más sencilla posible, los reportes han sido clasificados por categorías. Esta clasificación se hace en base al tipo de información que muestra cada reporte al ser generado.
Además de estas clasificaciones, cada reporte ha sido identificado con un nombre lo más descriptivo posible, para que usted interprete de manera sencilla, el tipo de datos que podrá consultar a través del mismo.

Las clasificaciones de reportes son las siguientes: **Análisis de facturación, Análisis de llamadas, Consolidados**, **Declaración de llamadas**, **Especiales**, **Facturas fijas**, **Hoteles y Hospitales**, **Mapas**, **Planes tarifarios**, **Sistema**, **Telefonía fija**, **Telefonía fija**, **Telefonía móvil** y **Tráfico Erlang,**
A continuación, se listan los reportes de cada una de las clasificaciones y se describe el tipo de información que muestra cada clasificación y cada reporte.

Análisis de facturación

En esta clasificación se podrán consultar los resultados de la conciliación de las llamadas que reportan las facturas de los proveedores de telefonía fija contra las llamadas que reporta el conmutador. Esta categoría solo estará disponible para los usuarios de tipo Administrador global, es decir, para los usuarios con permiso para administrar todos los sitios de Intertel®.
Los reportes que se presentan en esta categoría se describen a continuación, solo recuerde que para que pueda ver información en ellos, es necesario que la factura del proveedor de telefonía fija sea cargada al sistema Intertel® y adicionalmente se haya ejecutado el proceso de Análisis de cuenta maestra. Para mayor información sobre cómo hacer este proceso, consulte el manual de usuario de Intertel® en el capítulo de “Análisis de facturación”.

Reporte	Descripción
Análisis del resultado por tipo de llamada	Muestra un resumen a nivel comparativo de los totales de importe, duración y cantidad de llamadas por cada tipo de llamada que se encontraron en el recibo contra los que se registraron en el sistema. Este reporte permitirá al Administrador del sistema analizar y detectar los posibles ajustes de configuración de tarifas a realizar en el sistema, así como posibles ajustes en la detección de los tipos de llamadas.

	prefijos de marcación, entre otros. El reporte solo estará disponible para usuarios de tipo Administrador global.
Detallado de resultados del análisis de facturación	El reporte presenta el resultado del proceso de comparación de las llamadas provenientes del conmutador y procesadas por Intertel® contra las llamadas que se listan en la factura del proveedor de telefonía fija, en el periodo de facturación seleccionado. Entre los datos de los resultados se muestran las llamadas que se registraron en Intertel® y no se encontraron en la factura, las llamadas que se encuentran en la factura, pero no en Intertel®, las llamadas que coinciden en ambas partes y las llamadas que coinciden en ambas partes pero que tienen diferencias en el rango de duración o importe.
Gráfico del resumen de análisis de facturación	Presenta un comparativo de las llamadas provenientes del conmutador y procesadas por el sistema Intertel®, contra las llamadas detectadas en la facturación del periodo y carrier seleccionado. Además, indica las diferencias en totales y en porcentaje entre lo reportado por el conmutador y lo reportado por el proveedor de telefonía fija. Este comparativo es el resultado del "Análisis de facturación" que realizó Intertel®.
Llamadas del recibo no encontradas en el sistema	Muestra el listado de llamadas que se encuentran en la factura, pero no se encontraron procesadas en el sistema Intertel®, aun utilizando los rangos de (+/-) configurados para aceptar las diferencias de duración y de importe.
Llamadas del sistema no encontradas en el recibo	Muestra el listado de llamadas que se encuentran en el sistema, pero no se encontraron en la factura de telefonía fija, aun utilizando los rangos de (+/-) configurados para aceptar las diferencias de duración y de importe.
Porcentajes de precisión por tipo de llamadas	Presenta los porcentajes de precisión o de acercamiento en importe, duración y cantidad de los principales tipos de llamada contenidos en el recibo telefónico, contra los tipos de llamadas registrados en el sistema. Con esta información, el Administrador del sistema podrá identificar en donde se encuentran las diferencias, para así determinar si requerirá realizar algún otro ajuste en las configuraciones de Intertel® (tarifas, prefijos de marcación, porcentajes de precisión en el análisis de facturación, clasificación de tipos de llamadas, entre otros). El reporte solo está disponible para usuarios de tipo Administrador global.
Resumen de resultados del análisis de facturación	Muestra el resumen de las llamadas y del servicio medido incluyendo las diferencias entre lo que el sistema procesó y lo que la factura reportó.

A continuación, se presenta una imagen de uno de los reportes de la categoría “Análisis de facturación”:

DEMO FACIA

Sitio: Sistema Local
Generado por: Administrador el 15/sep/2016 a las 07:23 p.m.
Periodo: Mayo-2016

Gráfico del resumen de análisis de facturación

TELMEX

Llamadas procesadas

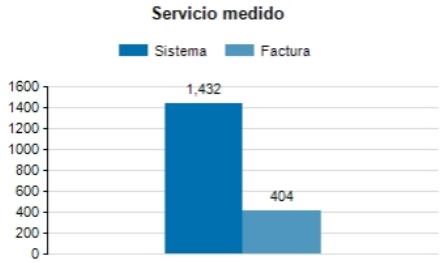
	Cantidad	%
Facturadas	244	30.96%
Sin facturar	544	69.04%
Total	**788**	**100.00 %**

Llamadas facturadas

	Cantidad	%
Procesadas	244	60.40 %
Sin procesar	160	39.60 %
Total	**404**	**100.00 %**

Servicio medido

	Sistema	Factura
Totales	1,432	404



Página: 1

Figura 3.6. Análisis de Facturación – Reporte Grafico del resumen del análisis de facturación

Análisis de llamadas

Los reportes que se encuentran bajo esta clasificación consideran como importe total, la suma de los montos que provienen de llamadas hechas desde una extensión y/o código de autorización, y de los importes obtenidos por algún dispositivo móvil.

En la mayoría de ellos, permite drilldown, comenzando desde el resumen, hasta llegar al detallado de llamadas.

A continuación, se describe brevemente cada uno de los reportes que se encuentran disponibles en esta sección.

Reporte	Descripción
Análisis de llamadas	Provee el consumo total telefónico por usuario o nivel jerárquico, formado por los importes obtenidos de llamadas telefónicas hechas desde una extensión abierta (extensiones que no piden un código de autorización para hacer una llamada) y/o código de autorización; así como de llamadas hechas desde un dispositivo móvil.
Consumo telefónico por mes	Muestra las tendencias de consumo telefónico durante un año, con opción a consultar un rango de meses, iniciando con el mes de enero, hasta llegar al mes seleccionado. Los consumos que se muestran corresponden a los diferentes tipos de llamadas de telefonía fija y móvil, que se hayan realizado desde una extensión y/o código de autorización, y a las *llamadas contenidas en el detallado de llamadas de las facturas de telefonía móvil que fueron importadas en el sistema Intertel®.
Llamadas por número marcado	Útil para consultar la cantidad de llamadas, duración e importe que tiene un número que fue marcado, así como el lugar a donde llamó y el detallado de llamadas que corresponden a ese número.
Top N de números más marcados.	Contiene un listado de los números telefónicos fijos y/o móviles que fueron más marcados.
Totales por tipo de llamada	Presenta los totales de llamadas registrados en el sistema, agrupados por tipos de llamadas y mostrando los totales por importe, por duración o por cantidad. Así mismo, indica los totales por la hora en la que se realizaron las llamadas, por el día de la semana o por la fecha. Con este reporte el usuario podrá identificar por ejemplo las horas o los días pico, es decir, podrá identificar los momentos en donde hay más tráfico de llamadas.

A continuación, se presenta una imagen de uno de los reportes de la categoría de Análisis de llamadas. Este reporte lleva el mismo nombre que su categoría:

DEMO FACIA

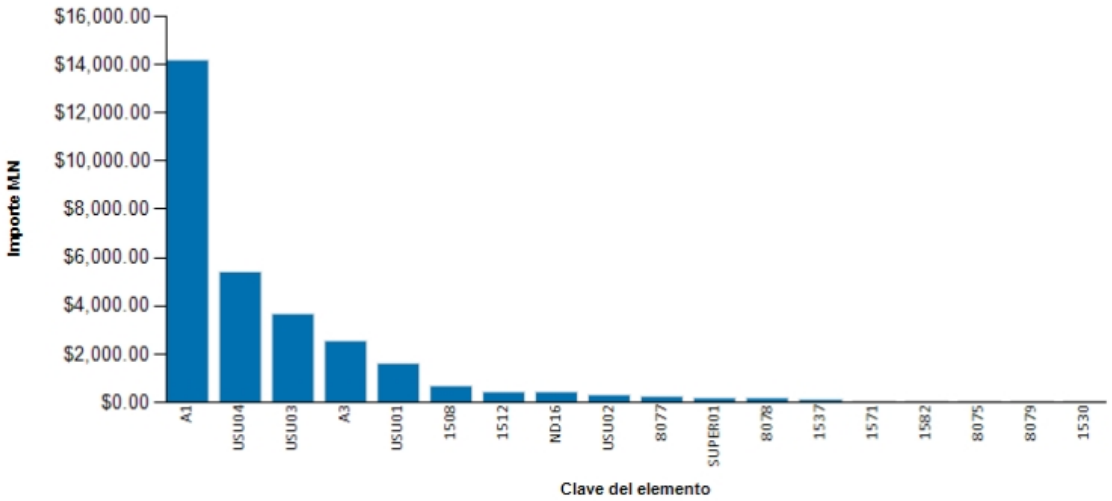
Sitio: Sistema Local
Generado por: Administrador el 19/sep/2016 a las 12:11 p.m.
Desde: 1/abr/2016 **Hasta:** 30/abr/2016

Análisis de llamadas

Información de: Compañías
Duración en: Minutos

COMPANIA UNO / DIVISION UNO

⊟ Gráfica



Clave	Descripción	Llamadas	Duración	Importe
A1	[illegible]	3,193	10,050.4	$14,184.11
USU04	[illegible]	256	953.4	$5,442.06
USU03	[illegible]	480	1,234.0	$3,660.68
A3	[illegible]	793	1,686.3	$2,531.03
USU01	[illegible]	70	423.2	$1,619.73
1508	[illegible]	51	453.6	$704.85
1512	[illegible]	49	223.3	$417.46
ND16	[illegible]	256	450.6	$405.92
USU02	[illegible]	38	58.8	$317.74
8077	[illegible]	157	430.9	$231.40
SUPER01	[illegible]	116	345.4	$194.92
8078	[illegible]	76	391.4	$176.06
1537	[illegible]	61	310.7	$104.92
1571	[illegible]	32	132.9	$53.32
1582	[illegible]	37	175.8	$49.88
8075	[illegible]	28	49.1	$44.72
8079	[illegible]	20	58.2	$17.20
1530	[illegible]	5	8.5	$6.88
Total		**5,718**	**17,436.5**	**$30,162.88**

Página 1

Figura 3.7. Análisis de llamadas

Análisis de productividad y tráfico

Los reportes que se encuentran bajo esta clasificación consideran todas las llamadas que fueron registradas por el conmutador, las cuales han sido clasificadas bajo tres tipos:

- **Entrantes:** Aquellas llamadas que provienen desde la red telefónica pública.
- **Salientes:** Aquellas llamadas que se hacen desde la empresa hacia un número telefónico que hace uso de la red telefónica pública.
- **Interextensión:** Aquellas llamadas que son realizadas entre las diferentes extensiones de la empresa.

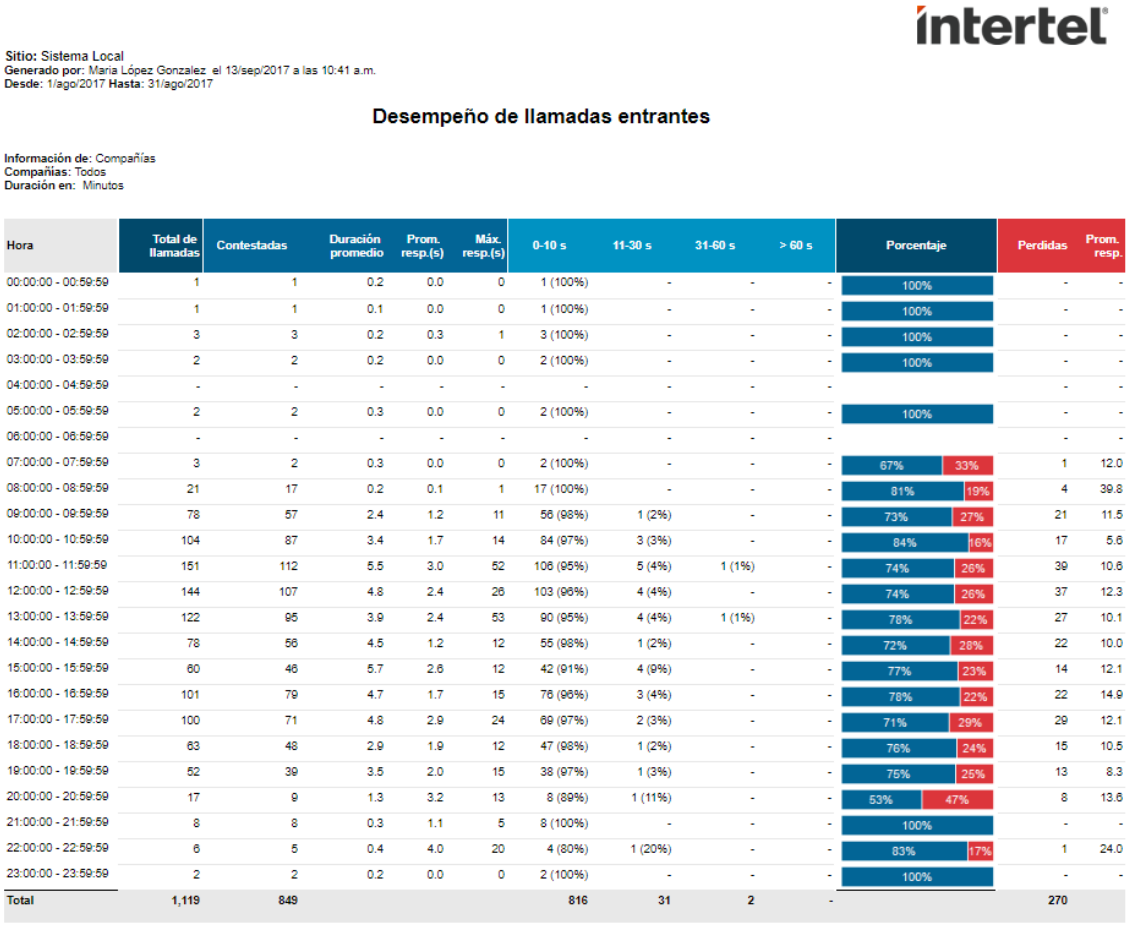
El set de reportes contenido en esta clasificación permite navegar entre los diferentes elementos (drilldown), como son: niveles jerárquicos, usuarios, extensiones y/o códigos de autorización, hasta consultar el detalle de llamadas.

A continuación, se describe brevemente cada uno de los reportes que se encuentran disponibles en esta sección.

Reporte	Descripción
Análisis de llamadas entrantes no directas	Los datos contenidos en este reporte provienen de aquellas llamadas que participaron en diferentes eventos: ya sea de tipo transferencias, conferencias, desvíos, o aquellas que fueron atendidas por algún buzón de voz. Las llamadas se identifican en base a dos clasificaciones principales: llamadas atendidas (contestadas) y llamadas no atendidas (perdidas); y por cada tipo de evento es posible consultar la cantidad total de llamadas, el porcentaje equivalente en base al total de llamadas, así como su importe y duración.
Análisis de llamadas entrantes y salientes	Brinda la facilidad de consultar la cantidad total de llamadas que fueron recibidas (entrantes) así como la cantidad total de llamadas que realizaron (salientes) los usuarios de su empresa, y del total de llamadas de ambos tipos (entrantes y salientes), identificar cuantas llamadas fueron contestadas y cuantas fueron perdidas.
Análisis de llamadas entrantes y salientes por hora	Por medio de este este reporte puede consultar por cada hora del día, el total de llamadas que han sido atendidas, así como las que no lo fueron. Estas llamadas son agrupadas de acuerdo si el tipo de llamada fue entrante o saliente. Adicional a la información anterior, es posible consultar el tiempo máximo que tardó en atenderse una llamada, así como su tiempo de espera promedio.
Análisis de llamadas entrantes y salientes por horarios	A través de este reporte tendrá conocimiento de la cantidad de llamadas que se hacen (salientes) o se reciben (entrantes) en su empresa durante cada hora del día (24 hrs.). Las llamadas son clasificadas de acuerdo a uno de los siguientes tipos: interextensión, entrantes y salientes. Así mismo tendrá conocimiento del total de llamadas que no han sido contestadas (perdidas). El valor contabilizado como llamada perdida, comprende las llamadas entrantes, salientes e interextensiones que no fueron atendidas.
Desempeño de llamadas entrantes	Útil para monitorear por cada hora del día, el tiempo promedio de espera, en la que los usuarios de su empresa tardan en contestar llamadas. Del total de llamadas contestadas se crean subconjuntos de llamadas, las cuales son agrupadas dependiendo del tiempo que esperaron en ser atendidas. Los rangos son: 0-10 seg. ,11-30 seg., 31-60 seg., o mayores a 60 seg. Así mismo provee un comparativo a manera de porcentaje, del total de llamadas entrantes, cuantas fueron contestadas, contra el porcentaje de llamadas perdidas.
Horas Pico	Utilice este reporte para identificar el día y hora en que su empresa obtuvo mayor

	tráfico de llamadas; con opción a consultar a mayor detalle, los tipos de llamadas que se realizaron en ese día y a esa hora, así como la cantidad de llamadas que provienen de la red pública telefónica (PSTN), o de aquellas llamadas que se hicieron a través de la misma infraestructura de su empresa (llamadas en RED).
Llamadas entrantes directas y no directas	Provee el total de llamadas hechas hacia los DID's (llamadas directas) contratados en su empresa, así como el total de llamadas que fueron redireccionadas por algún evento de tipo transferencia, desvío, etc. (llamadas no directas). Por ambas clasificaciones de llamadas tendrá también conocimiento de consultar la cantidad total de llamadas, porcentaje de llamadas respecto al total, importe promedio y tiempo promedio de espera, de aquellas llamadas que fueron contestadas (atendidas) o perdidas (no atendidas).
Llamadas entrantes perdidas	Por medio de este reporte se puede tener conocimiento del total de llamadas que fueron recibidas (entrantes) en su empresa, pero, que por algún motivo estas se perdieron. Mientras se va navegando entre los niveles jerárquicos o usuarios hasta llegar a una extensión, es posible consultar el registro de cada llamada que iba dirigida a dicha extensión y cuál fue la causa por la cual la llamada se perdió. El conjunto de llamadas perdidas que se contabilizan en este reporte son categorizadas de acuerdo a uno de los siguientes motivos: • **Abandonada:** Conjunto de llamadas que fueron redireccionadas o atendidas por un sistema de menús configurables o IVR, las cuales no fueron contestadas. • **Bloqueada:** Conjunto de llamadas hechas por el emisor las cuales no fueron contestadas por que en la extensión participante se activó el bloqueo de llamadas entrantes, lo cual ocasiona que el emisor escuche tono de ocupado. • **Buzón:** Cuando el receptor por alguna razón no puede contestar la llamada y el buzón de voz atiende la llamada del emisor. • **Error:** Conjunto de llamadas hechas por el emisor, que por diversos motivos no pudieron ser atendidas por el receptor. • **No contestada:** El emisor hace una llamada y expira el tiempo en el que el receptor atienda a la llamada. El emisor hace una llamada y cuelga antes de que el receptor pueda contestarla. • **Ocupado:** Cuando el receptor se encuentra en llamada y no atiende a la llamada. • **Rechazada:** Conjunto de llamadas hechas por el emisor las cuales no fueron contestadas, porque la extensión participante, activó la opción de rechazar una llamada entrante.
Llamadas finalizadas por origen o destino	Provee el total de llamadas que fueron terminadas por la fuente que origino la llamada (emisor), o bien por la fuente que recibió la llamada (destinatario). Las llamadas anteriores son clasificadas en tres categorías: llamadas entrantes, salientes o internas.
Resumen de tráfico de llamadas	Por medio de este reporte es posible tener conocimiento de la cantidad de llamadas entrantes o salientes, que fueron contestadas y perdidas. Así mismo provee por ambos tipos (entrantes y salientes), el tiempo promedio de respuesta en la que el usuario tarda en atender una llamada, así como el tiempo promedio de respuesta en la que el receptor tarda en contestarla, así como la duración promedio de las llamadas que fueron atendidas.
Tracking de llamadas redireccionadas por extensión	Provee el registro de llamadas de tipo transferencias y conferencias que fueron procesadas por el sistema Intertel, con opción a consultar las extensiones participantes, así como la serie de eventos que fueron registrados por el conmutador.
Tráfico por extensión con estatus	Provee el registro de todas las llamadas que ha sido recibidas o realizadas desde una extensión. Las llamadas registradas pueden haber sido realizadas usando códigos de autorización. El detalle que provee este reporte arroja si el tipo de llamada fue saliente, entrante, si fue o no contestada, así como el tiempo de espera transcurrido, una vez que la llamada fue o no atendida.

A continuación, se presenta una imagen de uno de los reportes de la categoría de Análisis de llamadas. Este reporte lleva el mismo nombre que su categoría:



intertel

Sitio: Sistema Local
Generado por: Maria López Gonzalez el 13/sep/2017 a las 10:41 a.m.
Desde: 1/ago/2017 **Hasta:** 31/ago/2017

Desempeño de llamadas entrantes

Información de: Compañías
Compañías: Todos
Duración en: Minutos

Hora	Total de llamadas	Contestadas	Duración promedio	Prom. resp.(s)	Máx. resp.(s)	0-10 s	11-30 s	31-60 s	> 60 s	Porcentaje	Perdidas	Prom. resp.
00:00:00 - 00:59:59	1	1	0.2	0.0	0	1 (100%)	-	-	-	100%	-	-
01:00:00 - 01:59:59	1	1	0.1	0.0	0	1 (100%)	-	-	-	100%	-	-
02:00:00 - 02:59:59	3	3	0.2	0.3	1	3 (100%)	-	-	-	100%	-	-
03:00:00 - 03:59:59	2	2	0.2	0.0	0	2 (100%)	-	-	-	100%	-	-
04:00:00 - 04:59:59	-	-	-	-	-	-	-	-	-		-	-
05:00:00 - 05:59:59	2	2	0.3	0.0	0	2 (100%)	-	-	-	100%	-	-
06:00:00 - 06:59:59	-	-	-	-	-	-	-	-	-		-	-
07:00:00 - 07:59:59	3	2	0.3	0.0	0	2 (100%)	-	-	-	67% 33%	1	12.0
08:00:00 - 08:59:59	21	17	0.2	0.1	1	17 (100%)	-	-	-	81% 19%	4	39.8
09:00:00 - 09:59:59	78	57	2.4	1.2	11	56 (98%)	1 (2%)	-	-	73% 27%	21	11.5
10:00:00 - 10:59:59	104	87	3.4	1.7	14	84 (97%)	3 (3%)	-	-	84% 16%	17	5.6
11:00:00 - 11:59:59	151	112	5.5	3.0	52	106 (95%)	5 (4%)	1 (1%)	-	74% 26%	39	10.6
12:00:00 - 12:59:59	144	107	4.8	2.4	26	103 (96%)	4 (4%)	-	-	74% 26%	37	12.3
13:00:00 - 13:59:59	122	95	3.9	2.4	53	90 (95%)	4 (4%)	1 (1%)	-	78% 22%	27	10.1
14:00:00 - 14:59:59	78	56	4.5	1.2	12	55 (98%)	1 (2%)	-	-	72% 28%	22	10.0
15:00:00 - 15:59:59	60	46	5.7	2.6	12	42 (91%)	4 (9%)	-	-	77% 23%	14	12.1
16:00:00 - 16:59:59	101	79	4.7	1.7	15	76 (96%)	3 (4%)	-	-	78% 22%	22	14.9
17:00:00 - 17:59:59	100	71	4.8	2.9	24	69 (97%)	2 (3%)	-	-	71% 29%	29	12.1
18:00:00 - 18:59:59	63	48	2.9	1.9	12	47 (98%)	1 (2%)	-	-	76% 24%	15	10.5
19:00:00 - 19:59:59	52	39	3.5	2.0	15	38 (97%)	1 (3%)	-	-	75% 25%	13	8.3
20:00:00 - 20:59:59	17	9	1.3	3.2	13	8 (89%)	1 (11%)	-	-	53% 47%	8	13.6
21:00:00 - 21:59:59	8	8	0.3	1.1	5	8 (100%)	-	-	-	100%	-	-
22:00:00 - 22:59:59	6	5	0.4	4.0	20	4 (80%)	1 (20%)	-	-	83% 17%	1	24.0
23:00:00 - 23:59:59	2	2	0.2	0.0	0	2 (100%)	-	-	-	100%	-	-
Total	**1,119**	**849**				**816**	**31**	**2**	**-**		**270**	

Figura 3.8. Análisis de productividad y tráfico

Consolidados

Esta categoría presenta los reportes que concentran información de todos los sitios configurados en el sistema Intertel®, es decir, los reportes de esta categoría muestran información consolidada de todo el sistema con la opción de seleccionar uno, varios o todos los sitios, así como la opción de seleccionar las columnas que se desea ver en el reporte. Por ejemplo, en esta categoría se podrán obtener resúmenes de llamadas de todo el sistema sin importar su ubicación o sitio en el que fueron registradas.

La categoría de consolidados solo estará disponible para usuarios de tipo administrador global (administrador de todos los sitios).

Reporte	Descripción
Consolidado por carriers	Muestra el consumo mensual consolidado de todos los sitios, de su proveedor de servicios telefónicos, así como el tráfico de llamadas entrantes y salientes, por los rubros de cantidad, duración e importe; con la facilidad de consultarlos por cada tipo de llamada, y por cada sitio.
Consolidado por códigos	El reporte lista los códigos de autorización registrados en todo el sistema, incluyendo

de autorización	los totales de llamadas generados por cada uno de ellos (importe, duración y cantidad de llamadas). Cuenta con la opción para seleccionar uno, varios o todos los sitios del sistema.
Consolidado por extensión	El reporte, lista todas de las extensiones registradas en el sistema, sin importar el conmutador en el que están asociadas. El reporte incluye los totales de llamadas generados por cada extensión (importe, duración y cantidad de llamadas). Cuenta con la opción para listar las extensiones de uno, varios o todos los sitios del sistema.
Consolidados por nivel	Presenta los totales de llamadas (importe, cantidad y duración) realizadas por cada nivel jerárquico (niveles y subniveles) registrados en el sistema y los agrupa por sitio. El reporte también agrupa los totales por tipo de llamadas e indica la ruta o ubicación completa de cada uno de los niveles jerárquicos.
Consolidado por sitio	Genera un listado de los sitios registrados en el sistema, indicando los totales de importe, duración y cantidad de llamadas, clasificados por tipo de llamada.
Consolidado por tipo de llamadas	Brinda una visión general del consumo telefónico de su empresa durante un periodo de 13 meses consecutivos. También tendrá conocimiento del consumo obtenido por cada tipo de llamada realizada en su empresa. Así mismo puede consultar el tráfico de las llamadas entrantes, salientes e internas de un periodo determinado.
Consolidado por usuarios	Muestra el listado de usuarios de todo el sistema, es decir, de cualquier sitio al que pertenezcan. Incluye los totales por cada tipo de llamada que realizó cada usuario (importe, duración y cantidad de llamadas), así como la ubicación jerárquica a la que está asignado el usuario.
Días sin llamadas procesadas	Indica la fecha y día de la semana en los que no se procesaron llamadas en el sistema, es decir, que no se tarificaron por cualquier razón. Con esta información el Administrador del sistema podrá vigilar que el sistema cuente con llamadas del día y en caso de que no, podrá tomar acciones como indagar si hubo algún fallo en el Proceso de llamadas, en la recepción o buscar alguna otra causa del porque no se tienen llamadas para mostrar en los reportes de las fechas que indique el reporte de días sin procesar. Caso contrario también se podrá identificar si hubo llamadas en días que no deberían hacerse.

A continuación, se presenta una imagen de uno de los reportes de la categoría de Consolidados:

DEMO FACIA

Generado por: Administrador el 19/sep/2016 a las 12:26 p.m.
Desde: 1/abr/2016 **Hasta:** 30/abr/2016

Consolidado por usuarios

Duración en: Minutos

			Larga distancia						TOTALES		
			Llamadas nacionales			Llamadas internacionales					
Sitio	Clave usuario	Descripción usuario	Cantidad	Duración	Importe	Cantidad	Duración	Importe	Cantidad	Duración	Importe
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	2	9.8	$73.32	2	9.8	$73.32
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	1	5.3	$65.98	1	5.3	$65.98
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	19	182.4	$1,554.21	19	182.4	$1,554.21
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	12	25.8	$294.14	12	25.8	$294.14
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	26	300.4	$2,988.86	26	300.4	$2,988.86
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	100	480.7	$5,100.64	100	480.7	$5,100.64
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sistema Local	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sub total			**0**	**0.0**	**$0.00**	**160**	**1,004.4**	**$10,077.15**	**160**	**1,004.4**	**$10,077.15**
Sitio DOS	[illegible]	[illegible]	98	295.8	$168.56	0	0.0	$0.00	98	295.8	$168.56
Sitio DOS	[illegible]	[illegible]	3	14.6	$5.16	0	0.0	$0.00	3	14.6	$5.16
Sitio DOS	[illegible]	[illegible]	5	59.5	$8.60	0	0.0	$0.00	5	59.5	$8.60
Sitio DOS	[illegible]	[illegible]	2	119.6	$3.44	0	0.0	$0.00	2	119.6	$3.44
Sitio DOS	[illegible]	[illegible]	12	285.0	$20.64	0	0.0	$0.00	12	285.0	$20.64
Sitio DOS	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sitio DOS	[illegible]	[illegible]	42	87.0	$72.24	0	0.0	$0.00	42	87.0	$72.24
Sitio DOS	[illegible]	[illegible]	6	51.6	$10.32	0	0.0	$0.00	6	51.6	$10.32
Sitio DOS	[illegible]	[illegible]	6	32.5	$10.32	0	0.0	$0.00	6	32.5	$10.32
Sitio DOS	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sitio DOS	[illegible]	[illegible]	2	23.8	$3.44	0	0.0	$0.00	2	23.8	$3.44
Sitio DOS	[illegible]	[illegible]	8	133.7	$15.03	0	0.0	$0.00	8	133.7	$15.03
Sitio DOS	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sitio DOS	[illegible]	[illegible]	36	324.6	$61.92	0	0.0	$0.00	36	324.6	$61.92
Sitio DOS	[illegible]	[illegible]	26	203.0	$44.72	0	0.0	$0.00	26	203.0	$44.72
Sitio DOS	[illegible]	[illegible]	6	19.9	$10.32	0	0.0	$0.00	6	19.9	$10.32
Sitio DOS	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sitio DOS	[illegible]	[illegible]	5	49.3	$8.60	0	0.0	$0.00	5	49.3	$8.60
Sitio DOS	[illegible]	[illegible]	4	37.3	$6.88	0	0.0	$0.00	4	37.3	$6.88
Sitio DOS	[illegible]	[illegible]	63	375.5	$108.36	0	0.0	$0.00	63	375.5	$108.36
Sitio DOS	[illegible]	[illegible]	6	123.9	$10.32	0	0.0	$0.00	6	123.9	$10.32
Sitio DOS	[illegible]	[illegible]	0	0.0	$0.00	0	0.0	$0.00	0	0.0	$0.00
Sitio DOS	[illegible]	[illegible]	2	1.3	$3.44	0	0.0	$0.00	2	1.3	$3.44
Sub total			**332**	**2,237.9**	**$572.31**	**0**	**0.0**	**$0.00**	**332**	**2,237.9**	**$572.31**
Total			**332**	**2,237.9**	**$572.31**	**160**	**1,004.4**	**$10,077.15**	**492**	**3,242.3**	**$10,649.46**

Figura 3.9. Consolidados – Reporte de Consolidado por usuarios

Declaración de llamadas

Los reportes que se encuentran bajo esta clasificación, estarán disponibles siempre y cuando desde el sistema Intertel® haya sido habilitada la opción para tener acceso al módulo de Declaración de llamadas. Por medio de estos reportes tendrá conocimiento sobre el aprovechamiento de uso telefónico que están haciendo cada uno de sus empleados, ya que podrá consultar por cada llamada realizada, si estas fueron de carácter personal o laboral.

A continuación, se describe brevemente cada uno de los reportes que se encuentran disponibles en esta sección.

Reporte	Descripción
Aprovechamiento de Llamadas	Provee un indicador de medición para analizar la productividad de sus empleados, debido a que puede comparar la cantidad de llamadas, la duración o el importe de cada llamada que ha sido declarada como personal y laboral; así como de aquellas que aún se encuentran pendientes por declarar.
Inventario de cuentas	Provee un listado con la dirección, ubicación y números telefónicos que están asociados a las cuentas que han sido dadas de alta en el sistema Intertel®. Este reporte está disponible solo para Administradores de Sitio o Administradores

	globales del sistema Intertel®.
Llamadas declaradas [Telefonía fija]	Muestra un listado (máximo 50,000 registros) de llamadas declaradas entre laborales, personales o no declaradas, y que fueron realizadas desde extensiones abiertas (extensiones que no piden un código de autorización para hacer una llamada), o llamadas realizadas usando un código de autorización. **En caso de querer mostrar una cantidad mayor de registros en este reporte, consulte el apéndice D de la guía de instalación y configuración de nuestros productos.**
Llamadas declaradas [Telefonía móvil]	Muestra un listado de máximo 50,000 llamadas declaradas, ya sean llamadas laborales, personales o no declaradas, que fueron realizadas desde un dispositivo móvil. **En caso de querer mostrar una cantidad mayor de registros en este reporte, consulte el apéndice D de la guía de instalación y configuración de nuestros productos.**
Usuarios sin declarar llamadas	Muestra el listado de usuarios que tienen activado la declaración de llamadas y que no han realizado dicha declaración, o bien, que aún tienen números telefónicos pendientes por declarar en el periodo de fechas seleccionado al momento de generar el reporte. El reporte muestra la siguiente información: Clave de usuario, descripción del usuario (nombre), jerarquía a la que pertenece y cantidad de números telefónicos marcados por el usuario que se encuentran sin declarar. El reporte solo está disponible para usuarios de tipo administrador de sitio o administradores globales.

A continuación, se presenta una imagen de uno de los reportes de la categoría de Declaración de llamadas:

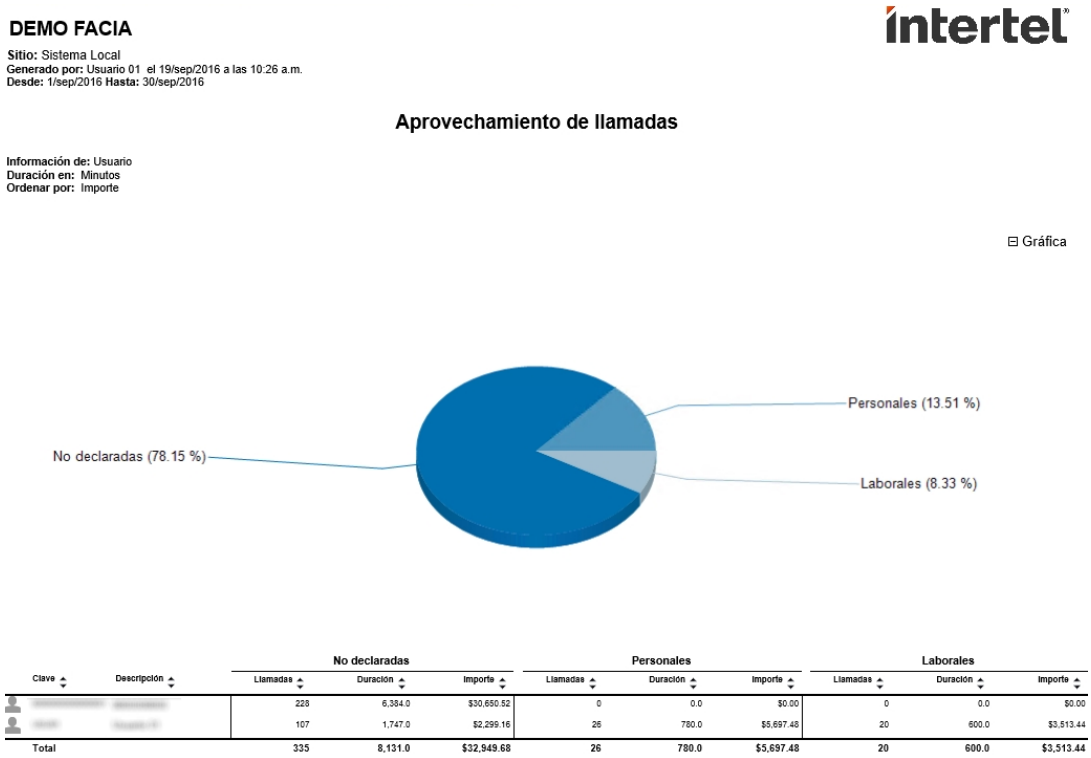


Figura 3.10. Declaración de llamadas – Reporte de Aprovechamiento de llamadas

Especiales

Esta categoría aparecerá siempre y cuando existan reportes hechos a la medida de sus necesidades, y hayan sido agregados en el Portal de Reportes. El listado de reportes que se encuentra en esta clasificación está ordenado alfabéticamente, lo anterior para facilitar su localización. Al igual que el resto

de los reportes del Portal de Reportes, podrán ser programados de manera automática para enviarlos por correo electrónico, o bien colocarlos en la sección de reportes favoritos, activándolos a través del icono de favoritos (), siempre y cuando su servidor de SQL cuente con esta facilidad.

La información que pueda consultar en estos reportes dependerá de los privilegios de consulta que le hayan sido asignados a su usuario. Estos privilegios son configurados por el administrador del sistema Intertel®. Si por alguna razón no puede consultar información una vez ejecutado el reporte, esto quiere decir que usted no cuenta con los privilegios correspondientes.

Facturas Fijas

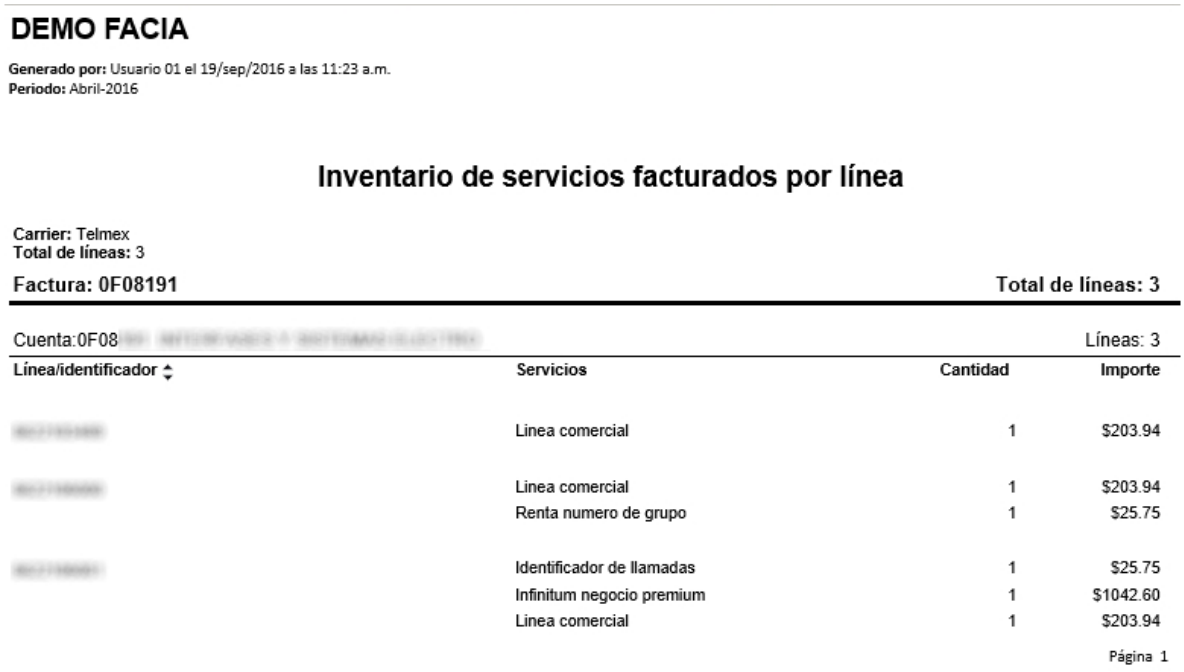
A través de los reportes que se encuentran en esta clasificación se obtienen datos que provienen de la factura que le proporciona su proveedor de servicios de telefonía fija, y que previamente fueron cargados al sistema Intertel®.

Los reportes que se incluyen en esta sección solo son visibles para un usuario que tenga permisos de administrador global, del sistema Intertel®. Adicionalmente, la información que presentan los reportes son a nivel global, es decir no importa cual sitio se encuentre seleccionado, los reportes siempre mostrarán información de toda la empresa.

La información que explotará con estos reportes toma como base, los cargos por servicio que son cobrados en la factura. A continuación, se describen brevemente cada uno de uno de los reportes que se encuentran disponibles en esta sección:

Reporte	Descripción
Gasto histórico mensual por línea	Provee el gasto que ha tenido cada línea durante 12 periodos consecutivos de facturación. El gasto facturado comprende los importes que la línea obtuvo por los conceptos de servicio medido, rentas, largas distancias nacionales e internacionales, llamadas a celulares locales y nacionales, así como descuentos.
Gasto histórico mensual por servicio	Provee el gasto de cada servicio que ha sido facturado, durante los últimos 12 periodos consecutivos de facturación.
Inventario de servicios facturados por línea	Provee un listado de las líneas que aparecen como activas en la última factura que fue cargada en el sistema y los servicios asociados a estas líneas. Los servicios incluidos en este reporte son aquellos que generan un costo constante, entre cada periodo de facturación. Por ejemplo: servicios de tipo renta, enlaces etc. excluyendo los servicios de consumo de llamadas, como son las largas distancias o el servicio medido.
Llamadas entrantes “800” nacionales	Provee un listado del tráfico de llamadas entrantes de tipo 800 nacional por línea telefónica, y su equivalente en duración e importe.
Tendencias de gasto por carrier	Provee un histórico con el gasto facturado por cada proveedor de servicio telefónico, de los últimos 12 periodos consecutivos de facturación, con opción a consular el desglose del gasto por los conceptos de servicio medido, rentas, larga distancia nacional e internacional, así como de llamadas a celulares locales y nacionales.
Top N de líneas con mayor gasto	Contiene un listado de las “N” líneas telefónicas, troncales y/o enlaces que obtuvieron mayor gasto, en un periodo de facturación.
Variación de servicios vs. periodo anterior	Muestra las variaciones por cantidad de servicios y su equivalencia en importe, como resultado de la comparación entre los servicios que generan un costo constante, de los últimos dos periodos consecutivos de facturación. Los servicios comparados son de tipo rentas, enlaces, etc. excluyendo los servicios de consumo de llamadas, como

	son las largas distancias o el servicio medido.



DEMO FACIA

Generado por: Usuario 01 el 19/sep/2016 a las 11:23 a.m.
Periodo: Abril-2016

Inventario de servicios facturados por línea

Carrier: Telmex
Total de líneas: 3

Factura: 0F08191 **Total de líneas: 3**

Cuenta:0F08[illegible] Líneas: 3

Línea/identificador	Servicios	Cantidad	Importe
[illegible]	Linea comercial	1	$203.94
[illegible]	Linea comercial	1	$203.94
	Renta numero de grupo	1	$25.75
[illegible]	Identificador de llamadas	1	$25.75
	Infinitum negocio premium	1	$1042.60
	Linea comercial	1	$203.94

Página 1

Figura 3.11. Facturación fija – Reporte de Inventario de servicios facturados por línea

Hoteles y Hospitales

En esta clasificación se encuentra disponible solo cuando en el sistema Intertel® se tiene activado el módulo de Interfaz para Hoteles y Hospitales. Para mayor información sobre cómo activar dicho módulo consulte el manual de usuario o la guía de instalación y configuración del sistema Intertel®.

A través de estos reportes se podrá tener mayor visibilidad sobre las llamadas que se envían al PMS para su cobro, además de obtener el detalle de las llamadas de los huéspedes con sus respectivas duraciones e importes, así como reportes de apoyo para los cortes del día o del turno.

Los reportes disponibles en esta clasificación se listan a continuación:

Reporte	Descripción
Detallado check in - check out	Este reporte proporciona el listado de llamadas efectuadas durante la estancia del huésped en el hotel u hospital. Con dicha información el huésped podrá cotejar el cargo por servicio telefónico que se le está haciendo a su habitación por medio del sistema hotelero u hospitalario. Solo se deberá indicar la extensión de la habitación y el horario en el que el huésped estuvo registrado. Los campos a desplegar en el reporte son: Folio, Fecha, Hora, Número marcado, Lugar a donde llamó, Duración de la llamada, Importe, Impuesto y Total.
Detallado de llamadas por cobrar	Muestra el listado de llamadas realizadas al servicio de operadora: Operadora Nacional, Operadora Internacional, Otras Operadoras. Una vez generado el reporte mostrará la siguiente información: Fecha de la llamada, Hora de la llamada, Número de Extensión, Descripción de la extensión, Número marcado (operadora a la que le marcaron), Lugar a donde llamó (descripción de la operadora: Información, La hora, Operadora Nacional, etc.), Duración de la llamada e Importe (costo de la llamada).

Detallado de llamadas por huésped	Lista las llamadas realizadas por los huéspedes en los diferentes turnos que se tienen registrados en el hospital u hotel. El operador del sistema podrá generar el reporte con el detallado de llamadas que se realizaron en un turno en específico o en todos los turnos, hechas por un huésped en particular o por todos. El reporte muestra los siguientes campos: Folio de la llamada, Fecha, Hora, Turno, Número marcado, Lugar a donde marcó, Duración, Importe, Impuesto y Total.
Detallado de llamadas salientes sin costo	Muestra el detallado de llamadas realizadas por los huéspedes y/o colaboradores de la empresa, que no generaron costo en el sistema ya sea porque aún no tienen una tarifa asignada o porque en realidad en el plan configurado ese tipo de llamada no genera un costo. El operador puede seleccionar si desea generar el reporte por un turno en particular o por todos. También puede seleccionar si desea ver la información de una sola extensión o de todas, y además puede filtrarlo por tipo de servicio, en especial el tipo de servicio que se haya asignado a los huéspedes. Una vez generado el reporte, se muestra un detallado agrupado por extensión, con los siguientes datos: Fecha de la llamada, Hora de la llamada, Turno en el cual se realizó la llamada, Número marcado, Lugar a donde llamó, Tipo de la llamada, Duración e Importe de la llamada.
Detallado por status de cargo PMS	Muestra las llamadas que el tarificador envió al sistema hotelero o sistema hospitalario indicando el *status de recepción en dicho sistema, además de confirmar si la habitación estaba ocupada en el momento que se efectuó la llamada. Los datos desplegados en el reporte son: Fecha de la llamada, hora, extensión, descripción de la extensión, número marcado, lugar a donde llamó, status del Cargo, Status de la Extensión, Folio de recibo, duración e importe.
Detallado por tipo de servicio y turno	Muestra el detallado de llamadas agrupado por tipo de servicio y por turno, el cual le ayudará a identificar las llamadas que realizaron los huéspedes en los diferentes turnos operativos y cuánto está generando de ingreso económico por cada una de las llamadas. Los datos que muestra el reporte son: Fecha de la llamada, hora, extensión, número marcado, lugar a donde llamó, duración, costo de la llamada, costo del servicio (ingreso económico generado), impuesto, importe total (incluyendo el costo de la llamada más el costo del servicio).
Ingresos por tipo de servicio	Indica el importe generado por tipo de servicio (equivalente al ingreso o utilidad) por turno, horario del día, día de la semana, fecha específica y/o tipo de llamada. Los datos que se incluyen en el reporte son: tipo de llamada, día de la semana (o día del mes), hora del día y utilidad.
Resumen de auditoría por turno	Muestra por cada turno operativo, un resumen de las llamadas realizadas de cada extensión indicando: la extensión, la descripción de la extensión, la cantidad de llamadas realizadas de dicha extensión, la duración total, el costo total de las llamadas, el cargo total del servicio, el impuesto total y el importe total.

*El status de recepción de la llamada que envió el sistema Intertel al sistema hotelero u hospitalario (PMS), así como el status de ocupación de la habitación, dependerá de que el PMS cuente con la capacidad de notificar a Intertel dicho status.

A continuación, se muestra una imagen de uno de los reportes de la categoría de Hoteles y Hospitales:

DEMO FACIA

Sitio: Sistema Local
Generado por: Usuario 01 el 19/sep/2016 a las 11:03 a.m.
Desde: 1/sep/2016 **Hasta:** 30/sep/2016

Detallado de llamadas por cobrar

Tipo de Servicio: Todos
Tipo de operadora: Todos
Duración en: Minutos

Fecha	Hora	Ext	Descripción	Número	Lugar	Duración	Importe
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	28.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	27.0	$ 0.00
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	26.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	26.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	26.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	26.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	26.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	26.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	26.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	26.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	25.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	25.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	25.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	25.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	25.0	$ 1.72
14/09/2016	09:59:00	[illegible]	[illegible]	[illegible]	[illegible]	25.0	$ 1.72

Figura 3.12. Hoteles y Hospitales – Reporte de Detallado de llamadas por cobrar

Mapas

Los reportes contenidos en esta categoría desplegarán los mapas geográficos del país o zona que se indique en el nombre del reporte. Al generar el reporte se indicará por cada zona, país, estado o ciudad según corresponda los totales de llamadas que se realizaron hacia ese lugar en el periodo de fechas seleccionado. Con dichos reportes el usuario podrá identificar los destinos a los que más se realizan llamadas o que tuvieron mayor duración y/o importe.

Reporte	Descripción
Estados Unidos de América	Presenta el mapa de Estados Unidos de América divido en estados, y mostrando el importe, la duración o la cantidad de llamadas realizadas hacia cada estado. Los estados se sombrearán con 5 diferentes colores aproximadamente según los rangos de importe, duración o cantidad de llamadas (unidad de medida que se haya seleccionado en el filtro). Por ejemplo: En color rojo se mostrarán los estados con mayor importe, en color naranja los que le siguen con importe, luego amarillo, luego

	verde y luego verde fuerte para los que tienen el menor importe. Lo mismo pasará si en el filtro se seleccionó cantidad de llamadas o duración.
México	Presenta el mapa de México divido en estados, y mostrando el importe, la duración o la cantidad de llamadas realizadas hacia cada estado. Los estados se sombrearán con 5 diferentes colores aproximadamente según los rangos de importe, duración o cantidad de llamadas (unidad de medida que se haya seleccionado en el filtro). Por ejemplo: En color rojo se mostrarán los estados con mayor importe, en color naranja los que le siguen con importe, luego amarillo, luego verde y luego verde fuerte para los que tienen el menor importe. Lo mismo pasará si en el filtro se seleccionó cantidad de llamadas o duración
Mundial	Muestra el mapa con todos los continentes e indicando los países de cada uno de ellos. Cada país es sombreado con un color para indicar que hubo llamadas realizadas hacia ese país. Los países con colores más fuertes son los que más importe, duración o cantidad de llamadas tuvieron según la selección en el filtro del reporte. El color va cambiando según van disminuyendo las llamadas hacia los demás países. Son aproximadamente 5 colores diferentes para indicar los rangos de importe, duración o cantidad de llamadas.

En seguida se muestra una imagen de uno de los reportes de la categoría de Mapas:

62

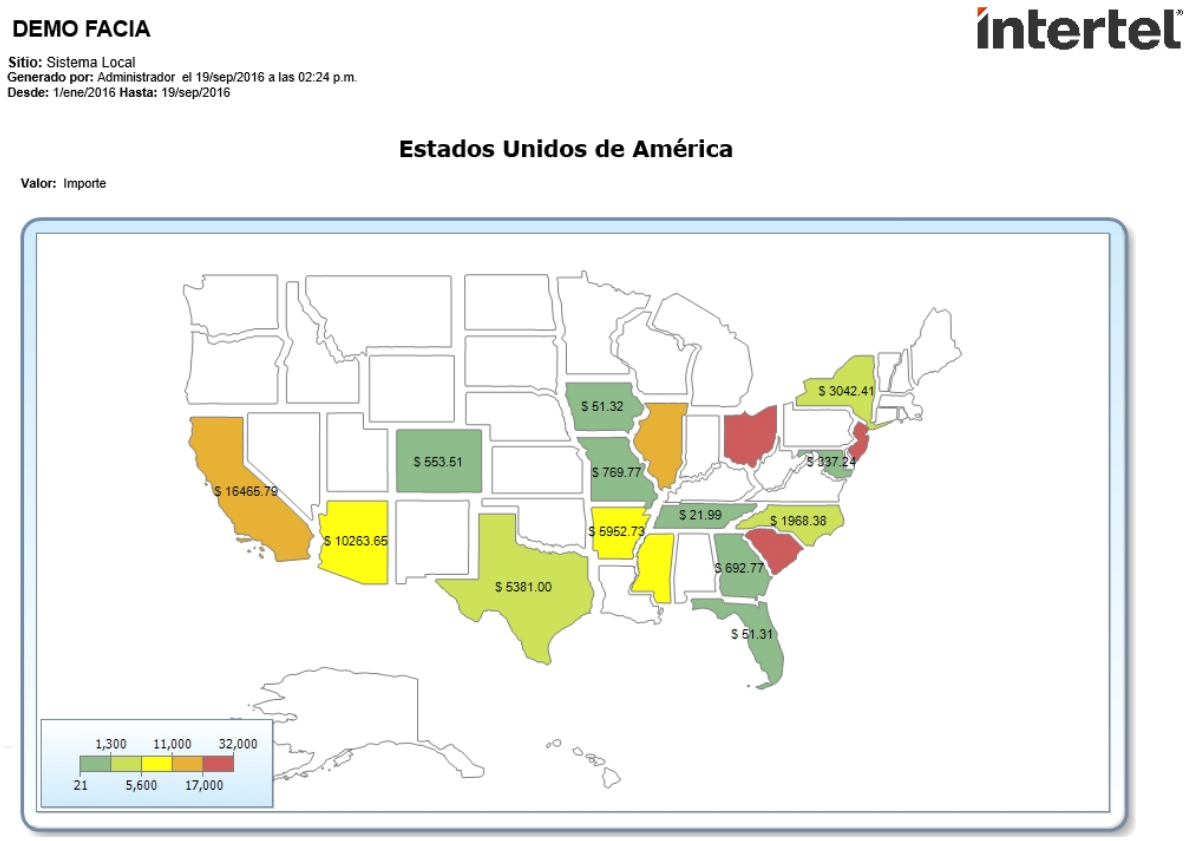
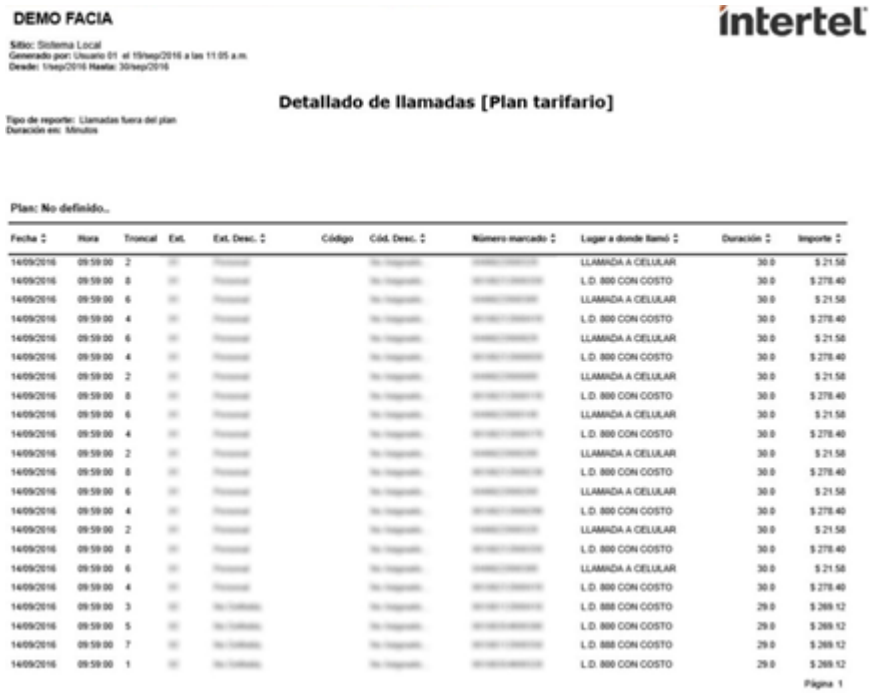


Figura 3.13. Mapas – Mapa de Estados Unidos de América

Planes tarifarios

Esta clasificación estará disponible siempre y cuando se haya activado el uso de planes tarifarios desde el menú principal de Configuración / Opciones de operación / Proceso de llamadas del sistema Intertel®, y que el usuario tenga privilegios de consulta del tipo "Administrador de sitio" y/o "Administrador global".
Los reportes incluidos en esta categoría muestran las llamadas que fueron procesadas bajo estos planes, así como el inventario de planes tarifarios y sus características. A continuación, se describe brevemente cada uno de los reportes que se encuentran disponible en esta sección.

Reporte	Descripción
Detallado de llamadas [Plan tarifario]	Brinda la facilidad de obtener el detalle de las llamadas que fueron cubiertas por un plan tarifario en particular, o bien aquellas llamadas que quedaron fuera del plan. La consulta de estas llamadas se puede obtener por un plan tarifario en específico o agrupadas por cada uno de los planes existentes en el sistema.
Planes tarifarios	Muestra un listado a manera de inventario, de los planes o paquetes tarifarios existentes en el sistema. Por cada plan a manera de detalle, se puede consultar, si se trata de un paquete de minutos o de cantidad de llamadas; así mismo se tiene conocimiento sobre el costo del paquete y el costo de la llamada.


DEMO FACIA

intertel

Detallado de llamadas [Plan tarifario]

Plan: No definido..

Fecha	Hora	Troncal	Ext.	Ext. Desc.	Código	Cód. Desc.	Número marcado	Lugar a donde llamó	Duración	Importe
14/09/2016	09:59:00	2						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	8						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	6						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	4						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	6						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	4						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	2						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	8						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	6						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	4						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	2						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	8						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	6						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	4						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	2						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	8						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	6						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	4						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	2						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	8						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	6						LLAMADA A CELULAR	30.0	$ 21.58
14/09/2016	09:59:00	4						L.D. 800 CON COSTO	30.0	$ 278.40
14/09/2016	09:59:00	3						L.D. 800 CON COSTO	29.0	$ 269.12
14/09/2016	09:59:00	5						L.D. 800 CON COSTO	29.0	$ 269.12
14/09/2016	09:59:00	7						L.D. 800 CON COSTO	29.0	$ 269.12
14/09/2016	09:59:00	1						L.D. 800 CON COSTO	29.0	$ 269.12

Página 1

Figura 3.14. Planes Tarifarios - Detallado de llamadas

Sistema

Intertel® cuenta con algunos reportes que muestran información referente al sistema y que son de gran utilidad para el usuario que lo administra. Estos reportes se encuentran en la categoría de Sistema y solo son visibles para usuarios de tipo Administrador Global, es decir, con permisos de "Administrador de todos los sitios".
Los reportes incluidos en esta clasificación se describen brevemente en la siguiente tabla:

Reporte	Descripción
Alarmas	Este reporte lista todas las alarmas generadas por el sistema Intertel® de uno, varios

	o todos los sitios. Estas alarmas son las configuradas en el sistema Intertel® de escritorio en el menú "Configuración/Alarmas del sistema". Las alarmas configuradas y listadas en este reporte pueden ser: de proceso nulo (sin llamadas procesadas), sin recepción de detallado de llamadas, poco espacio en disco duro, poco espacio en respaldo de histórico de llamadas o bien, otras alarmas que el usuario Administrador del sistema haya configurado tales como: llamadas con duraciones excesivas, a cierto número marcado, etc.
Bitácora de acceso a portales	Muestra un listado de los usuarios que han ingresado a cada uno de los módulos de Portal de Reportes, Portal Personal y Administración Web. El reporte muestra el nombre del módulo al que accedió, la clave del usuario, el nombre del usuario, así como la fecha y la hora en la que ingresó. El reporte podrá ser generado por rango de fecha y por módulo (uno en particular o por los tres antes mencionados).
Elementos asignados a niveles jerárquicos	El reporte de elementos mostrará la lista de usuarios, la lista de códigos de autorización o la lista de extensiones registradas en el sitio e incluirá la ubicación jerárquica a donde se encuentren asignados cada uno de estos elementos. El usuario que genere el reporte podrá indicar si desea visualizar toda la ruta de ubicación de los elementos o solo los últimos niveles jerárquicos. Por ejemplo: podrá ver que el usuario Juan Perez se encuentra ubicado en el área "Monterrey", en el Centro de costo "Ventas", en el departamento "Ventas Directas".
Histórico de renovación de códigos de autorización	Este reporte muestra el historial de códigos que se le han renovado al usuario por medio del sistema, incluyendo: la clave de referencia del código, el código real anterior, el código real nuevo, la fecha y hora de renovación y el status del código (activo o inactivo). También indica el supervisor del usuario y el correo electrónico al que se envió la notificación de la renovación.

DEMO FACIA

intertel®

Sitio: Sistema Local
Generado por: Administrador el 19/sep/2016 a las 02:32 p.m.
Desde: 1/jun/2016 **Hasta:** 19/sep/2016

Bitácora de acceso a portales

Log de portal: Todos

Portal	Clave usuario	Descripción	Fecha acceso	Hora acceso
IIW	⊞ MARVIZU	Total accesos:3		
IPR	⊞ TTORRES	Total accesos:4		
	⊟ CGONZALEZ	Total accesos:6		
		José Carlos Gonzalez	15/09/2016	13:41:43
		José Carlos Gonzalez	15/09/2016	16:40:47
		José Carlos Gonzalez	15/09/2016	16:56:20
		José Carlos Gonzalez	15/09/2016	17:44:49
		José Carlos Gonzalez	15/09/2016	17:47:25
		José Carlos Gonzalez	15/09/2016	18:25:49
	⊞ JMARTINEZ	Total accesos:32		
	⊞ DVALLES	Total accesos:1		
	⊞ APEREZ	Total accesos:2		
Total de accesos		**48**		

Página 1

Figura 3.15. Sistema – Reporte de Bitácora de acceso a portales

Telefonía Fija

Los reportes que se encuentran bajo esta clasificación muestran datos que provienen del conmutador o PBX de su empresa. A continuación, se describe brevemente cada uno de los reportes que se encuentran disponibles en esta sección.

Reporte	Descripción
Códigos de autorización utilizados en una extensión	El reporte permite conocer cuáles son los códigos de autorización que se han utilizado para realizar llamadas desde una extensión en particular.
Detallado de llamadas	Provee un listado con máximo 50,000 llamadas que fueron realizadas ya sea desde extensiones abiertas (extensiones que no piden un código de autorización para hacer una llamada), o llamadas realizadas usando un código de autorización. Cada llamada o registro es ordenado por fecha, importe o cantidad de llamadas. Entre los datos de las llamadas que se muestran se encuentran los siguientes dependiendo de los privilegios de consulta asignados: fecha y hora de llamada, número marcado, lugar a donde marcó, extensión, código de autorización, usuario, elemento jerárquico, troncal, duración, importe. **En caso de querer mostrar una cantidad mayor de registros en este reporte, consulte el apéndice D de la guía de instalación y configuración de nuestros productos.**
Extensiones utilizadas por un código de autorización	Presenta la lista de extensiones en donde se ha utilizado un código de autorización en particular para realizar las llamadas. Ejemplo: El código de autorización "123" ha realizado llamadas desde las extensiones 1304, 1305, 1306 y 1602.
Larga distancia nacional	Muestra un listado del tráfico de llamadas por estado y ciudad de la república mexicana; así como su duración e importe. Estas llamadas son realizadas usando códigos de autorización, o desde extensiones que no necesitan de un código para hacer llamadas.
Llamadas a números de entretenimiento	Provee un listado de las llamadas que fueron identificadas en el sistema Intertel®, como llamadas de entretenimiento. Generalmente estas llamadas inician con 01 900, aunque es posible identificar alguna otra desde el sistema Intertel®, de acuerdo a su prefijo de marcación.
Llamadas fuera del horario de oficina	Presenta el detallado de las llamadas que fueron realizadas o contestadas en horas no hábiles, de acuerdo al horario laboral configurado en el sistema Intertel®. El reporte puede ser generado por un elemento o nivel jerárquico en particular y filtrarse por los tipos de llamadas de interés.
Presupuesto asignado vs. consumido	Este reporte presenta un comparativo por mes, entre el consumo telefónico obtenido por las extensiones y los códigos dados de alta en el sistema, contra el presupuesto que les fue asignado. Este presupuesto es aplicable por los rubros de cantidad de llamadas, duración e importe. De esta forma es posible supervisar la buena utilización de sus recursos telefónicos.
Resumen ejecutivo de consumos	Útil para que personal encargado de un departamento o área laboral se mantenga informado con las tendencias mensuales de consumo telefónico de su departamento o

<table>
<tr><td></td><td>área laboral. Incluye varios subreportes de tipo TOP 10, con las extensiones, códigos o colaboradores que generan mayor consumo en su departamento, con opción a consultar a mayor detalle esta información, a través de un subreporte de tráfico de llamadas agrupado por tipo de llamada. Así mismo incluye un apartado de tráfico, con los diferentes tipos de llamadas que comúnmente se realizan en el departamento.</td></tr>
<tr><td>Top N de códigos de autorización</td><td>Contiene un listado de los “N” códigos de autorización con mayor consumo, duración o tráfico de llamadas.</td></tr>
<tr><td>Top N de extensiones</td><td>Contiene un listado de las “N” extensiones con mayor consumo, duración o tráfico de llamadas.</td></tr>
<tr><td>Top N de llamadas a celular</td><td>Contiene un listado con las “N” llamadas a números celulares locales y/o nacionales que fueron más marcados, que obtuvieron mayor duración, o aquellos que tuvieron mayor importe.</td></tr>
<tr><td>Top N de troncales</td><td>Contiene un listado con las “N” troncales que obtuvieron mayor consumo, duración o tráfico de llamadas.</td></tr>
<tr><td>Tráfico agrupado por tipo de llamada</td><td>Útil si desea consultar cuanto ha sido el consumo, el tráfico de llamadas, o el tiempo que han invertido sus empleados realizando diferentes tipos de llamadas durante un periodo de tiempo. Estas llamadas se encuentran clasificadas en alguno de los siguientes grupos:

<table>
<tr><th>Grupo de llamadas</th><th>Detalles de la llamada</th></tr>
<tr><td>ENT</td><td>Entrantes.</td></tr>
<tr><td>LOC</td><td>Locales.</td></tr>
<tr><td>LDN</td><td>Larga Distancia Nacional.</td></tr>
<tr><td>LDI</td><td>Larga distancia internacional.</td></tr>
<tr><td>OLD</td><td>Otras Largas Distancias. Dentro de este grupo encontramos a las siguientes llamadas:
✲ L8I – Larga Distancia 800 Internacional.
✲ L8N – Larga Distancia 800 Nacional.
✲ 900 – Entretenimiento
✲ 880 – Lada 880 con costo.
✲ 801 – Entretenimiento.</td></tr>
<tr><td>CEL</td><td>Celular local 044.</td></tr>
<tr><td>CNA</td><td>Celular nacional 045.</td></tr>
<tr><td>OOP</td><td>Otras Operadoras. Dentro de este grupo encontramos a las siguientes llamadas:
✲ OPI – Operadora Internacional.
✲ OPN – Operadora Nacional.</td></tr>
<tr><td>* INT</td><td>Internas. Dentro de este grupo encontramos a las siguientes llamadas:
✲ RED – Red.
✲ INT – Internas.
✲ IE – Inter extensión.</td></tr>
<tr><td>* OTRAS</td><td>Dentro de este grupo encontramos a las siguientes llamadas:
✲ NOI – No identificada.
✲ TRC – Troncal especial.
✲ TRI – Troncal especial internacional.
✲ TRN – Troncal especial nacional.
✲ Cualquier otro tipo de llamada que el Administrador del sistema haya configurado.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Tráfico por extensión</td><td>Provee el detallado de todas las llamadas que ha salido por una extensión, a la cual tiene permisos de consultar.</td></tr>
<tr><td>Tráfico por troncal</td><td>Provee un detallado del tráfico de llamadas que ha salido por cada una de las troncales de su empresa, clasificadas por tipo de llamada Estas llamadas se encuentran clasificadas en alguno de los siguientes grupos:

<table>
<tr><th>Grupo de llamadas</th><th>Detalles de la llamada</th></tr>
<tr><td>ENT</td><td>Entrantes.</td></tr>
<tr><td>LOC</td><td>Locales.</td></tr>
<tr><td>LDN</td><td>Larga distancia nacional.</td></tr>
<tr><td>LDI</td><td>Larga distancia internacional.</td></tr>
<tr><td>OLD</td><td>Otras largas distancias. Dentro de este grupo encontramos a las siguientes llamadas:
✲ L8I – Larga Distancia 800 Internacional.
✲ L8N – Larga Distancia 800 Nacional.
✲ 900 – Entretenimiento
✲ 880 – Lada 880 con costo.
✲ 801 – Entretenimiento.</td></tr>
<tr><td>CEL</td><td>Celular local 044.</td></tr>
<tr><td>CNA</td><td>Celular nacional 045.</td></tr>
<tr><td>OOP</td><td>Otras Operadoras. Dentro de este grupo encontramos a las siguientes llamadas:
✲ OPI – Operadora Internacional.
✲ OPN – Operadora Nacional.</td></tr>
<tr><td>* INT</td><td>Internas. Dentro de este grupo encontramos a las siguientes llamadas:
✲ RED – Red.
✲ INT – Internas.
✲ IE – Inter extensión.</td></tr>
<tr><td>* OTRAS</td><td>Dentro de este grupo encontramos a las siguientes llamadas:
✲ NOI – No identificada.
✲ TRC – Troncal especial.
✲ TRI – Troncal especial internacional.
✲ TRN – Troncal especial nacional.
✲ Cualquier otro tipo de llamada que el Administrador del sistema haya configurado.</td></tr>
</table>
</td></tr>
<tr><td>Uso de códigos de autorización</td><td>Muestra el listado de códigos de autorización que no han sido utilizados para generar llamadas en el periodo de tiempo seleccionado.
Este reporte le permitirá conocer cuáles son los códigos que ya no están en uso para que el Administrador del sistema pueda determinar si será necesario depurarlos o si aún desea conservar su histórico. El reporte muestra la clave de referencia del código, la descripción del código, el usuario al que está asignado y el elemento jerárquico al que pertenece.
El reporte solo está disponible para usuarios de tipo Administrador.</td></tr>
<tr><td>Uso de extensiones</td><td>Muestra las extensiones que no han sido utilizadas para realizar o recibir llamadas en el periodo de tiempo seleccionado. El reporte muestra el número de extensión, la descripción de la extensión, el usuario al que está asignada dicha extensión y el elemento jerárquico al que</td></tr>
</table>

	pertenece. El reporte solo está disponible para usuarios de tipo Administrador.

(*) Algunos tipos de llamadas no vienen configurados por omisión en el sistema Intertel® y /o es necesario que el Administrador los asocie a los prefijos de marcación correspondientes para que puedan ser desplegados en los grupos que se despliegan en los reportes de tráfico.

A continuación, se presenta una imagen de uno de los reportes que conforman la categoría de Telefonía fija:

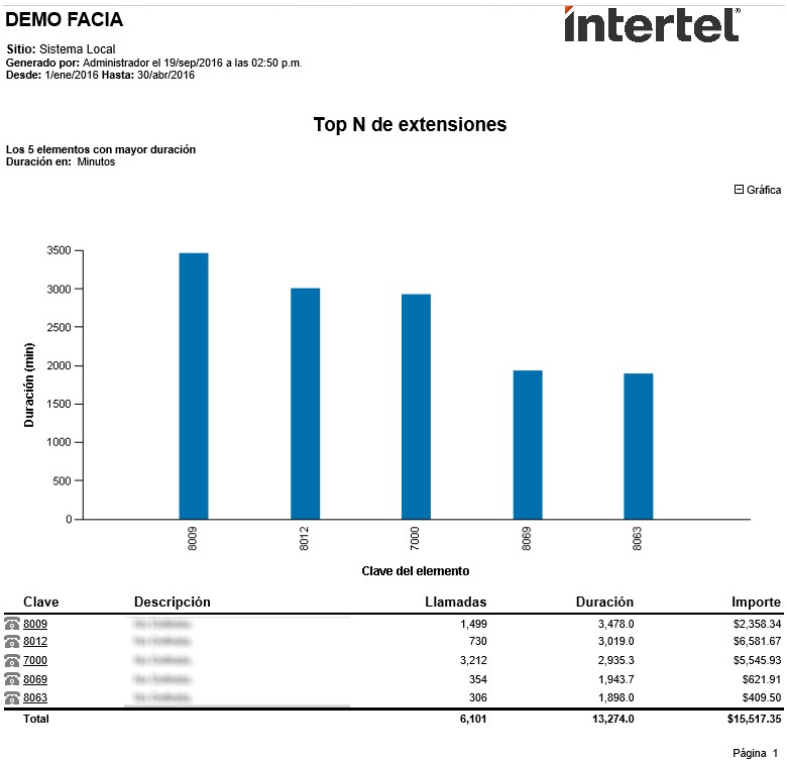


Figura 3.16. Telefonía fija – Reporte de Top N de extensiones

Telefonía Móvil

Los reportes que se encuentran bajo esta clasificación, muestran datos que provienen de la factura que le proporciona su proveedor de servicios de telefonía móvil, y que previamente fueron importados al sistema Intertel®.

A continuación, se describe brevemente cada uno de los reportes que se encuentran disponibles en esta sección.

Reporte	Descripción
Cargos por servicio de	Provee, por periodo de facturación, el cargo obtenido por cada dispositivo móvil y/

Nextel	un desglose de dichos cargos por tipo de servicio.
Cargos por servicio de Telcel	Provee, por periodo de facturación, el cargo obtenido por cada dispositivo móvil y un desglose de dichos cargos por tipo de servicio.
Detallado de llamadas	Provee un registro y costo de las 50,000 llamadas que fueron realizadas desde un dispositivo móvil. Cada llamada o registro es ordenado por la fecha, importe o cantidad de llamadas. Las llamadas de los dispositivos móviles se muestran por carrier. **En caso de querer mostrar una cantidad mayor de registros en este reporte, consulte el apéndice D de la guía de instalación y configuración de nuestros productos.**
Top N de dispositivos móviles	Contiene un listado de los "N" dispositivos móviles con mayor consumo, duración o tráfico de llamadas.

A continuación, se presenta un ejemplo de uno de los reportes de la categoría de Telefonía móvil:

DEMO FACIA

Sitio: Sistema Local
Generado por: Usuario 01 el 19/sep/2016 a las 12:28 p.m.
Periodo: Abril-2016

Detallado de llamadas

Usuario: Todos
Carrier: Telcel
Tipos de llamada: Telcel Entrante, Telcel Saliente
Duración en: Minutos

Fecha	Hora	Móvil	Usuario	Nivel jerárquico	Número marcado	Lugar a donde llamó	Tipo llamada	Duración	Importe
24/03/2016	00:11:43					CONEXIONGPRS	Saliente	0.0	$0.00
25/03/2016	00:10:43					CONEXIONGPRS	Saliente	0.0	$0.00
25/03/2016	23:10:43					CONEXIONGPRS	Saliente	0.0	$0.00
26/03/2016	09:09:49					FRONTERA	Entrante	0.0	$2.59
26/03/2016	09:10:38					FRONTERA	Entrante	0.0	$2.59
26/03/2016	10:13:43					CONEXIONGPRS	Saliente	0.0	$0.00
26/03/2016	10:13:43					CONEXIONGPRS	Saliente	0.0	$0.00
26/03/2016	10:20:18					FRONTERA	Entrante	0.0	$0.00
26/03/2016	10:32:57					TELCEL HERMO	Saliente	0.0	$0.00
26/03/2016	11:12:43					CONEXIONGPRS	Saliente	0.0	$0.00
26/03/2016	11:20:48					TELCEL CULIA	Saliente	0.0	$0.00
26/03/2016	11:27:53					TELCEL HERMO	Saliente	0.0	$0.00
27/03/2016	15:12:43					CONEXIONGPRS	Saliente	0.0	$0.00
27/03/2016	15:57:46					AZ TUCSON	Entrante	0.0	$0.00
27/03/2016	15:57:48					AZ TUCSON	Entrante	0.0	$0.00
27/03/2016	15:58:29					AZ TUCSON	Entrante	0.0	$0.00
27/03/2016	17:13:43					CONEXIONGPRS	Saliente	0.0	$0.00
28/03/2016	00:33:27					HERMOSILLO	Saliente	0.0	$0.00
28/03/2016	00:34:20					HERMOSILLO	Saliente	0.0	$0.00
28/03/2016	00:35:18					HERMOSILLO	Saliente	0.0	$0.00
28/03/2016	00:36:08					HERMOSILLO	Saliente	0.0	$0.00

Figura 3.17. Telefonía móvil – Detallado de llamadas de Telefonía móvil

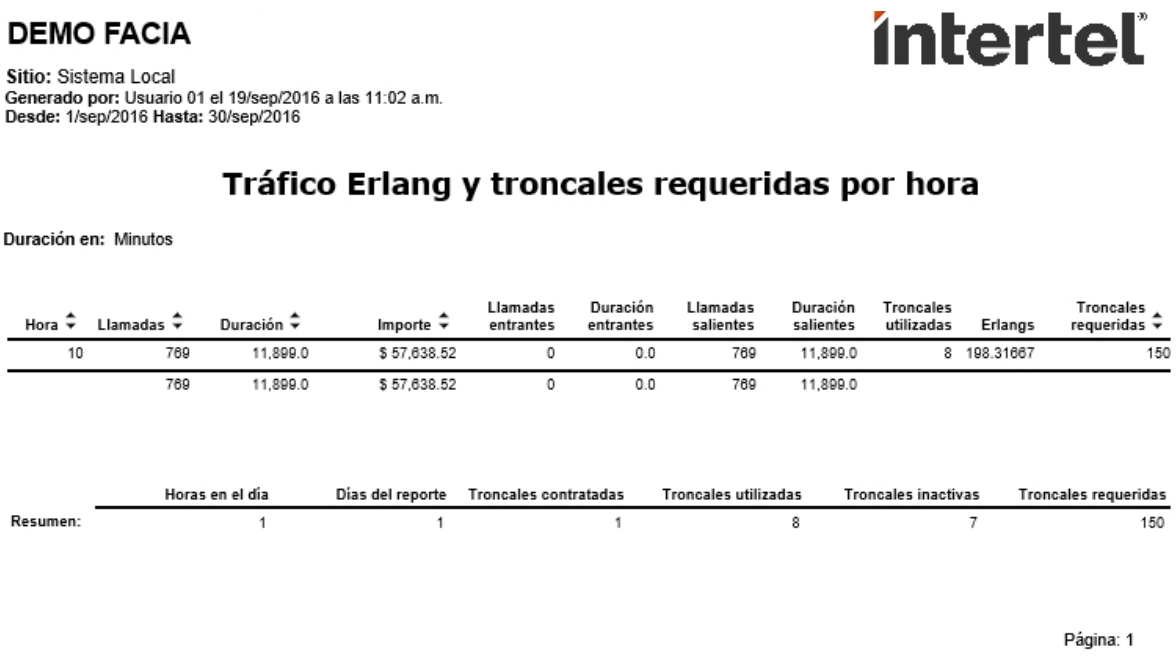
Tráfico Erlang

Los reportes que se presentan en esta categoría son para apoyo al administrador del sistema Intertel®, para determinar cuántas troncales están usando y cuántas troncales en realidad son necesarias, según el tráfico de llamadas que se maneja en el sitio seleccionado. Con estos reportes, el administrador podrá darse una idea del uso (ocupación) de las líneas troncales que le servirán para la toma de decisiones. La categoría Tráfico Erlang solo está disponible para usuarios con permisos para administrar todos los sitios de Intertel®.

A continuación, se listan los reportes incluidos en la sección Erlang:

Reporte	Descripción
Tráfico Erlang y troncales requeridas	Muestra el total de llamadas, de duración y de importe de las llamadas entrantes y de las llamadas salientes por cada hora, indicando el número de troncales utilizadas y haciendo el cálculo de las troncales requeridas para ese tráfico en ese horario. Así mismo muestra el cálculo para el valor Erlang.

A continuación, se muestra un ejemplo del Reporte de Táfico Earlang:



DEMO FACIA

Sitio: Sistema Local
Generado por: Usuario 01 el 19/sep/2016 a las 11:02 a.m.
Desde: 1/sep/2016 **Hasta:** 30/sep/2016

Tráfico Erlang y troncales requeridas por hora

Duración en: Minutos

Hora	Llamadas	Duración	Importe	Llamadas entrantes	Duración entrantes	Llamadas salientes	Duración salientes	Troncales utilizadas	Erlangs	Troncales requeridas
10	769	11,899.0	$ 57,638.52	0	0.0	769	11,899.0	8	198.31667	150
	769	11,899.0	$ 57,638.52	0	0.0	769	11,899.0			

	Horas en el día	Días del reporte	Troncales contratadas	Troncales utilizadas	Troncales inactivas	Troncales requeridas
Resumen:	1	1	1	8	7	150

Página: 1

Figura 3.18. Táfico Earlang

Para el correcto cálculo de este reporte, es necesario que el conmutador envíe en el detallado de llamadas al sistema Intertel, el dato de la troncal por la cual salen o entran las llamadas. Adicionalmente, en el sistema Intertel debe estar configurado el horario de oficina.

Por otro lado, para que esta categoría se muestre en el portal de reportes, es necesario que se active la sección "Erlang" del menú Opciones de operación del sistema Intertel, así como el realizar la configuración correspondiente en el menú Opciones de operación/configuración Erlang. Consulte el manual de usuario del sistema Intertel para mayor detalle.

Envío automático de reportes

La mayoría de las veces las actividades de nuestro trabajo requieren que estemos redactando informes, o elaborando reportes que deben ser enviados periódicamente a nuestros jefes inmediatos.

El Portal de Reportes cuenta con la funcionalidad de enviar de manera automática y periódica un reporte a un grupo de personas, por medio de sus correos electrónicos. Las frecuencias de envío pueden variar, ya sea que se envíen a diario, por semana o por mes.

Cada una de estas opciones puede ser configurada para enviarse cada cierto número de días, ciertos días de la semana, ciertos días del mes, etc. En el tema siguiente explicaremos las opciones de frecuencia disponibles y los pasos que tendrá que realizar para aprender a programar el envío de reportes.
Hay ocasiones en las que usted necesita solo enviar el reporte por correo en un evento único, sin necesidad de programar un envío o una periodicidad de envíos. Al generar el reporte usted cuenta con la opción para enviarlo en ese momento.

La funcionalidad de envío de reportes por correo, está disponible si usted cuenta con una instalación de SQL Server 2008 R2, SQL Server 2012 standard o superior o SQL Server 2014 estándar o superior.

Envío de reporte por correo al momento

Una vez que usted ha generado el reporte, en la barra de herramientas del reporte, usted contará con la opción para enviarlo por correo en ese momento. Solo deberá presionar el icono de ”Envío por correo”. Posteriormente se abrirá una ventana adicional solicitándole los siguientes datos, los cuales deberá llenar en su totalidad. La información solicitada para el envío se describe a continuación:

Datos del destinatario

- **E-mail:** Escriba el correo electrónico de la persona que recibirá el reporte (solo una cuenta de correo).
- **Asunto:** Escriba una breve descripción del reporte que se encuentra enviando por correo.
- **Descripción:** Si requiere informar más detalles del reporte que se encuentra por enviar, o explicar el contenido del mismo, podrá hacerlo usando esta sección.
- **Adjuntar como:** Aquí deberá seleccionar el formato en que el reporte será enviado por correo. Los formatos disponibles son: Word, Excel y PDF.

Por último, presione el botón Aceptar para que el correo sea enviado.

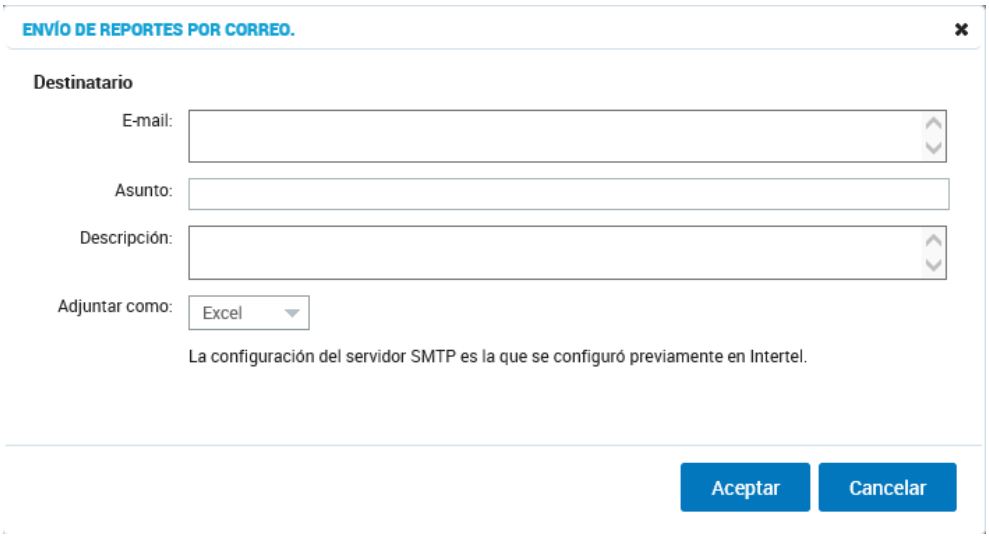


Figura 3.19. Pantalla para enviar un reporte por correo en el momento.

Programar periodicidad de envío

A través de esta funcionalidad los reportes pueden ser enviados de manera periódica y automática a una o varias direcciones de correo electrónico.

Cualquier usuario que cuente con permisos para ingresar al Portal de Reportes puede programar un reporte. Esta programación será válida únicamente para el sitio en el que el usuario se encuentre en sesión, y cuando se cuente con la versión de SQL Server indicada para esta funcionalidad.

La programación de envíos de reportes es independiente entre los usuarios, es decir, que cada usuario puede programar los reportes que requiera sin necesidad de que sean los mismos o con las mismas frecuencias que las programaciones de los demás usuarios. Sin embargo, el reporte que se envíe será generado solo con la información que tenga derecho a ver el usuario que programó la frecuencia de envío del reporte.

Para hacer las programaciones es necesario configurar la frecuencia de envío o la periodicidad con la que el reporte será generado y enviado, así como la lista de personas que recibirán el reporte, entre otros datos.

Para que usted pueda programar un reporte, previamente deberá realizar los siguientes pasos:

1. Haber seleccionado el reporte que desea enviar por correo electrónico.
2. Haber especificado los filtros necesarios y haber ejecutado el reporte, tal como desee que se genere para este y los próximos envíos.
3. Haber presionado el botón de "Programar periodicidad" localizado en la barra de herramientas que aparece una vez que ejecutas el reporte.

Si no le es posible ver la opción de "Programar periodicidad", se debe a que la versión de SQL que maneja en su empresa no es compatible con esta funcionalidad, por lo cual no podrá realizar la programación.
Seguidos los pasos anteriores aparecerá la ventana de "Programación de envío automático de reportes".
Desde esta ventana deberá especificar las propiedades de destinatario y opciones de frecuencia necesarias, para que el reporte quede programado. Enseguida se describen los campos contenidos en esta ventana, y las opciones de frecuencia correspondientes.

A continuación, se presenta una imagen de la ventana de programación de envío automático con periodicidad:

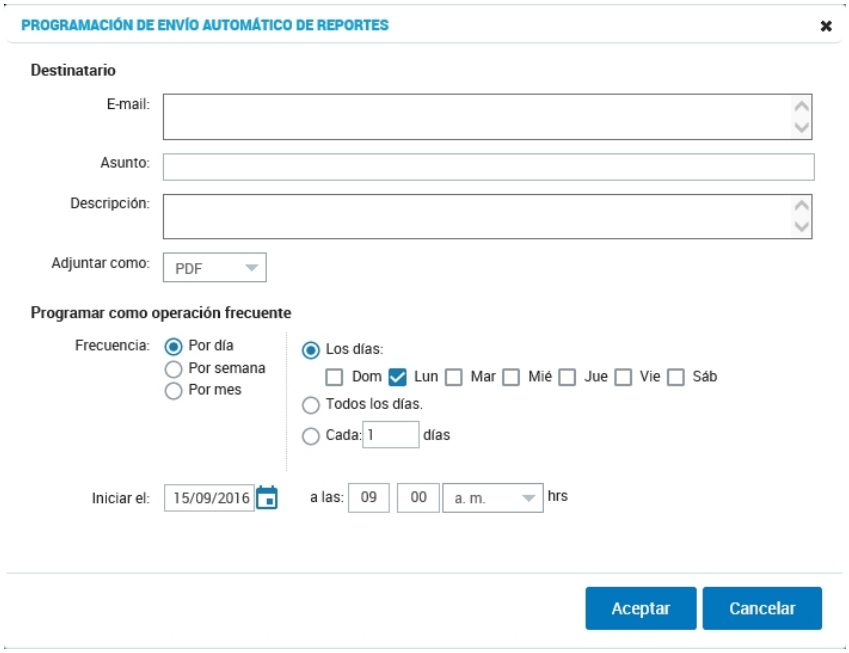


Figura 3.20. Pantalla para programar un reporte de manera automática y periódica.

En seguida se describe cada uno de los campos requeridos para la programación de envío del reporte:

Datos del destinatario

- **E-mail:** Escriba los correos electrónicos de las personas que recibirán el reporte; puede escribir más de un correo electrónico siempre y cuando sean separados por el signo de punto y coma (;).
- **Asunto:** Escriba una breve descripción del reporte que se encuentra enviando por correo.
- **Descripción:** Si requiere informar más detalles del reporte que se encuentra por enviar, o explicar el contenido del mismo, podrá hacerlo usando esta sección.

- **Adjuntar como:** Aquí deberá seleccionar el formato en que el reporte será enviado por correo. Los formatos disponibles son: Word, Excel y PDF.

Una vez proporcionados los datos del destinatario, es necesario que seleccione la frecuencia o periodicidad con las que se realizará el envío del reporte, para ello deberá seleccionar el tipo de frecuencia. Las frecuencias disponibles son tres: diaria, semanal y mensual, cada una de ellas tienen a su disposición varias

> Es muy importante que verifique la fecha y hora en la que iniciará el envío, ya que, a partir de estos datos, inicia el conteo de días, semanas o meses, en el que se llevará acabo el envío del reporte de manera automática.

opciones de configuración que se ven directamente relacionadas con dos campos, esto son la fecha y la hora en que iniciará el envío.

A continuación, se detallan las opciones de frecuencia y sus diferentes combinaciones de envío, para que seleccione la que satisfaga sus necesidades:

Frecuencia por día

Al seleccionar la frecuencia por día, en el lado izquierdo de la pantalla le serán habilitadas las opciones de Los días, Todos los días y Cada N días.

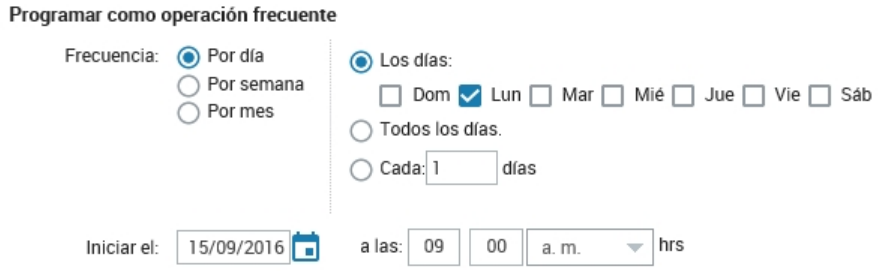


Figura 3.21. Opciones de frecuencia por día.

- **Los días:** Seleccione el o los días de la semana en que el reporte será enviado. Podrá seleccionar todos los días de la semana o alguno en especial; simplemente de clic en el día o en los días que requiera.
- **Todos los días:** Al seleccionar esta opción, el reporte será enviado todos los días de la semana, es decir de domingo a sábado, los 365 días del año.
- **Cada N días:** Seleccione esta opción si necesita enviar un reporte cada "N" cantidad de días. Supongamos que nos encontramos en el día primero de junio del 2013 y son las 4:00 p.m., si hacemos uso de estos valores y decidimos enviar un reporte cada 10 días, entonces el reporte sería enviado a los destinatarios en las siguientes fechas: 10/junio/2013, 20/junio/2013, 30/junio/2013, etc. a las 4:00 p.m.

Frecuencia por semana

Al seleccionar la frecuencia por semana, del lado izquierdo le serán mostradas las opciones Repetir cada y Cada N semanas.

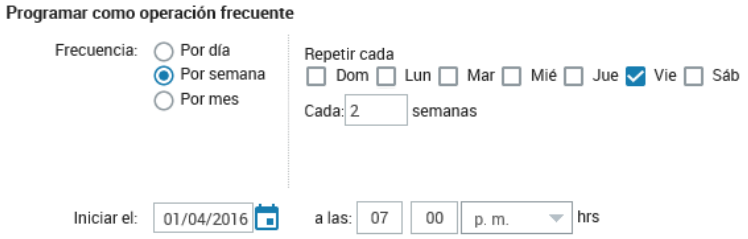


Figura 3.22. Opciones de frecuencia por semana.

- **Repetir cada:** Seleccione el(los) día(s) de la semana en el cual desea que se envíe el reporte. Después de haber seleccionado el día, indique el número de semanas que deberán pasar para que el reporte sea enviado. Por ejemplo, si nos encontramos en el día primero de junio del 2013, y son las 4:00 p.m., y necesitamos que los días lunes de cada segunda semana se envíe el reporte, deberá seleccionar el día lunes y en el campo de Cada "N" semanas, escribir el número 2. Al hacer lo anterior el sistema enviará el reporte el día Lunes 10/jun/2013, Lunes 24/jun/2013, etc. Siempre y cuando sean las 4 p.m.

Frecuencia por mes

Al seleccionar la frecuencia por mes, del lado derecho de la pantalla se habilitarán los filtros Enviar cada y Día del mes.

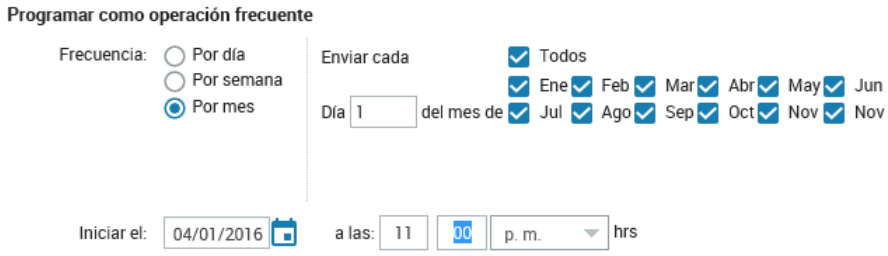


Figura 3.23. Opciones de frecuencia por mes.

- **Enviar cada:** Indique el día y el mes, o meses en los que se enviará el reporte. Por ejemplo: si nos encontramos en el día primero de junio del 2013 y son las 4:00 p.m., y necesitamos que trimestralmente se envíe el reporte cada día primero de mes, entonces deberá captura en el campo de día el número 1, y seleccionar los meses de marzo, junio, septiembre y diciembre. Al hacer lo anterior los destinatarios recibirán cada día primero, de cada 3 meses a las 4:00 p.m., el reporte en su bandeja de entrada.

Por último, presione el botón "Aceptar" para que el sistema registre la programación que acaba de realizar. Con esto el reporte queda programado y preparado para ser enviado a la frecuencia de tiempo que configuró y a las cuentas de correo electrónico especificadas.

El reporte que recibirán los destinatarios, será el primero que se muestra al momento en que este es ejecutado. Es decir, se recibirá el reporte principal y no aquellos que se despliegan al momento ir dando drill-down. Si desea verificar que sus reportes fueron programados exitosamente, diríjase a la pestaña de "Programados" del menú del Portal de Reportes, ahí aparecerá el reporte que anteriormente programó. En caso de que no aparezca, tendrá que realizar la programación nuevamente.
Para tener mayor conocimiento sobre la administración que podrá realizar en sus reportes programados, consulte el tema de **"Mis reportes programados"** y "**Administrar reportes programados de otros usuarios**" de este manual.

Mis reportes programados

Desde esta sección se realiza la administración de los reportes que decidió programar de manera automática y periódica para que fueran enviados a un grupo de personas a sus correos electrónicos. Recuerde que el listado de reportes corresponde al sitio que se encuentra activo en ese momento.
La administración consiste en poder consultar y editar las opciones con las que fue configurado el reporte, es decir, los destinatarios, el formato del reporte, y las opciones de frecuencia de envío. Así como de depurar o eliminar aquellos reportes que ya no considera necesarios que se envíen.
Al seleccionar la pestaña de "Programados", se le presentará la siguiente pantalla:

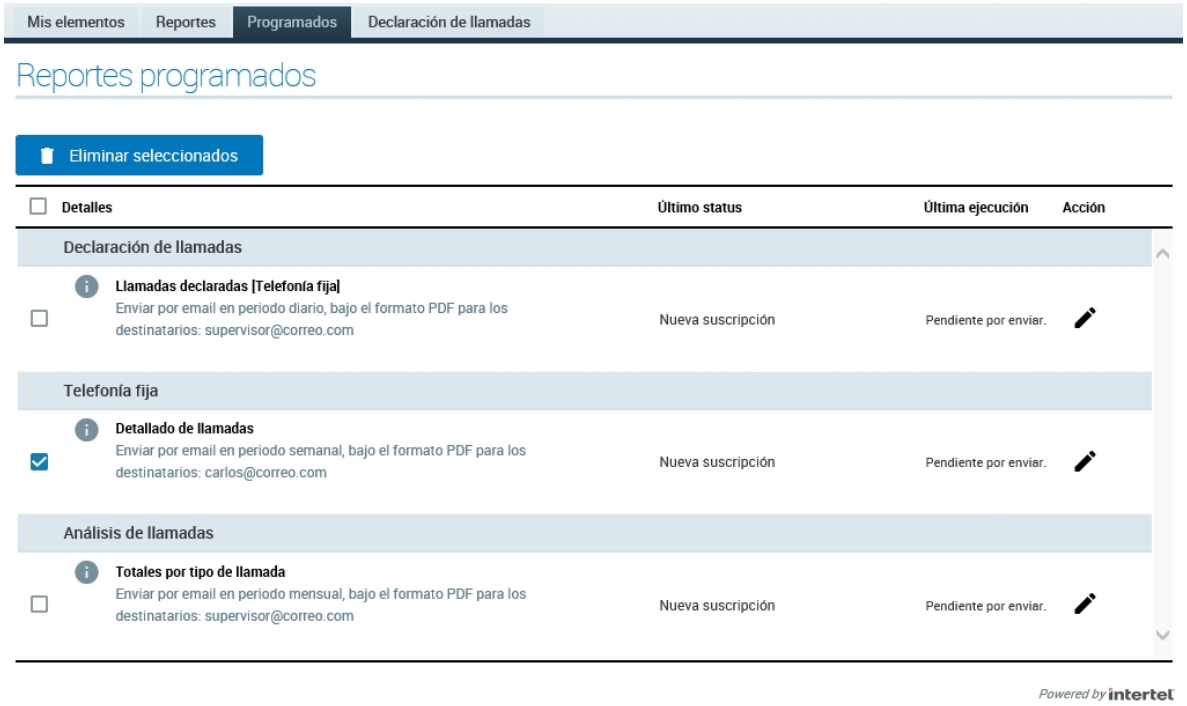


Figura 3.24. Pantalla de reportes programados.

Enseguida describiremos cada una de las opciones a las que tendremos acceso desde esta pestaña de Programación del menú del Portal de Reportes:

Editar mis reportes programados

En caso de ser necesario, usted podrá editar los parámetros del destinatario, el tipo de formato con que se envía el reporte o de frecuencia, con los que programó algún reporte. Para hacerlo deberá dar clic en el icono con imagen de un lápiz que aparece a lado derecho del nombre de cada reporte.
Al hacer lo anterior se le mostrará la pantalla de programación de envío automático de reportes, con los valores que había configurado anteriormente, de tal manera que todos los campos estarán disponibles para su edición. Modifique el o los campos que necesite y presione el botón Aceptar para grabar el cambio.

Consultar mis reportes programados

Como se mencionó anteriormente, los reportes que usted programó, le serán listados dentro de la pestaña "Programados". En caso de no haber programado reportes para envío, aparecerá en esta sección, una leyenda indicándole que no existen reportes programados.
Cada reporte programado aparecerá clasificado de acuerdo a la categoría a la que pertenece en la sección de Reportes. Y podrán ser identificados por su nombre, y por los parámetros con los que fueron configurados.
Por cada reporte usted podrá consultar los correos electrónicos de las personas a las que les será enviado; el formato en que decidió adjuntar el reporte y la frecuencia de envío (diaria, semanal o mensual).

Para consultar un reporte programado, solo posicione el mouse sobre el icono informativo que aparece a lado izquierdo del nombre del reporte (no es necesario hacer clic). La información le será desplegada en un recuadro.

Borrar mis reportes programados

Si existen reportes que no deban seguirse enviando de manera automática, entonces será necesario que estos sean borrados de la lista de sus reportes programados. Usted tiene la opción de borrar un reporte, un conjunto, o todos a la vez.

Para borrar un reporte o un conjunto de reportes, deberá dar clic en el cuadro (checklist) que aparece a lado izquierdo de cada reporte para que quede marcado y posteriormente de clic en el botón de "Eliminar seleccionados" que se encuentra localizado en la parte superior derecha del listado de reportes programados. En caso de querer borrar todos los reportes, presione clic sobre el cuadro (checkbox) principal que aparece a un costado de la columna de Detalles. Al hacer lo anterior se iluminará cada checkbox que le corresponde a cada reporte. Por último, deberá dar clic en el botón de "Eliminar seleccionados".

Administrar reportes de otros usuarios

Cómo usuario Administrador del sistema, además de tener acceso a las programaciones de reportes que realizó él mismo (opción de "Mis suscripciones"), puede tener acceso a la administración de las programaciones de reportes que hicieron los demás usuarios. Esto facilita el mantenimiento ya que por ejemplo si un usuario realizó la programación de un reporte a un grupo de personas para envío mensual para cada 1ro. del mes y aparte realizó un envío programado de un reporte personal. Suponiendo que el usuario ya no labore más en la empresa y requieren que el reporte se envíe los días 15 en lugar del 1ro. El administrador podrá ingresar a esta sección y editarlo. Además, podrá eliminar la programación del

reporte personal de ese usuario para que no se sature el servidor con envíos o peticiones que ya no son requeridas.

Por omisión, al momento de que el administrador ingresa a la opción de "Programados" se despliega el listado de todas las programaciones de todos los usuarios. Para que el administrador pueda diferenciar entre las programaciones de envío de reportes que él realizó de los demás, solo debe seleccionar la opción "Mis suscripciones" del combo "Ver suscripciones por usuario", localizada en la parte superior izquierda. Después presione el botón "Filtrar".

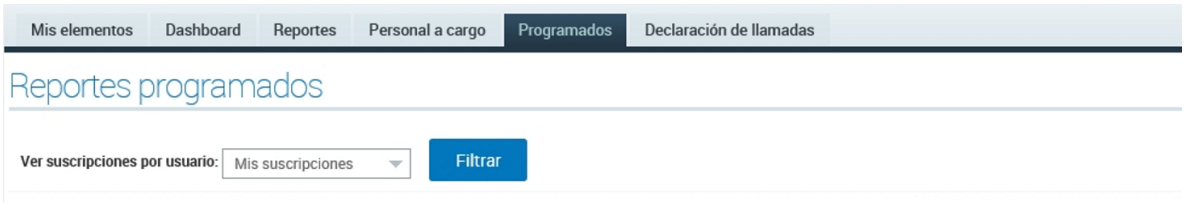


Figura 3.25. Mis reportes programados

En caso de requerir revisar los reportes programados por un usuario en particular, solo seleccione del combo antes mencionado, la clave del usuario y presione el botón "Filtrar".

Los reportes programados que se listen en este apartado, podrán ser consultados en cuanto a los parámetros configurados para su envío, así como también podrán ser editados o eliminados si así se desea, tal como se describe en la sección "Mis reportes programados" del presente manual de usuario.

Búsqueda de Reportes

El Portal de Reportes cuenta con la facilidad de buscar reportes de una manera eficiente y sencilla, simplemente será necesario escribir una frase que recuerde del reporte, y el sistema le mostrará las coincidencias en una lista desplegable tal y como se muestra en la imagen siguiente:

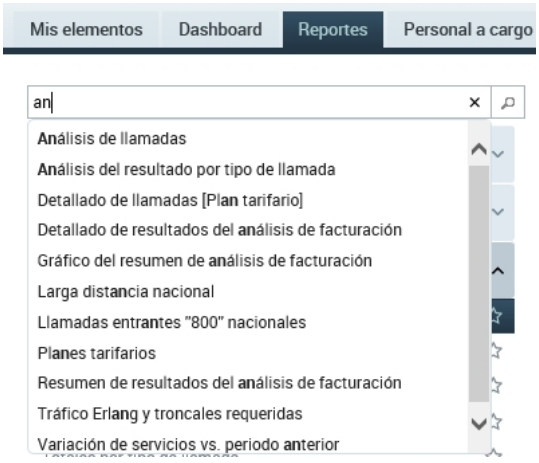


Figura 3.26. Búsqueda de reportes.

Al momento de seleccionar el reporte de la lista, la aplicación se dirigirá a dicho reporte, y le mostrará la sección de filtros, para que seleccione los valores necesarios y después proceda a su ejecución.

Capítulo 4. Declaración de llamadas

La Declaración de llamadas es una herramienta que le brinda a la empresa mantener el control de las llamadas, siempre y cuando esté asociada a una política bien estructurada. A través de esta funcionalidad, su empresa puede tener un indicador del porcentaje de llamadas que sus colaboradores han realizado con motivos personales o laborales.

La declaración se efectúa por número marcado, es decir, si un colaborador de su empresa marcó 10 veces al número telefónico 156-89-22, solo deberá declarar una sola vez el motivo de la llamada. Esta declaración es individual, es decir, si el colaborador declaró el número telefónico 156-89-22 como laboral, puede haber otros usuarios que declaren ese mismo número, pero, como tipo personal.

Para comenzar con el proceso de declaración debe seleccionar la pestaña de "Declaración de llamadas" contenida en el menú del Portal de Reportes. Al realizar esto, el sistema le mostrará un listado con los números que usted marcó en el mes actual y que aún no ha declarado.

Si el sistema detecta que existe una gran cantidad de llamadas pendientes por declarar, entonces le muestra las primeras 100 llamadas, y una vez que estas hayan sido declaradas, le mostrará otras 100 llamadas más. En caso de querer consultar o declarar llamadas de otros periodos, podrá hacerlo usando los selectores de fechas desde-hasta que se encuentran en la parte superior del listado.

Si no recuerda el número telefónico al que habló, podrá consultar el detalle de cada llamada que realizó a ese número; es posible que al identificar la hora y fecha pueda recordar si el número telefónico al que habló fue por motivos laborales o personales. Para hacerlo de clic en el signo de (+) que aparece al lado izquierdo del número marcado.

Así mismo, si en su empresa manejan cuentas, es decir una descripción con la cual se identifica a un grupo de números telefónicos, podrá especificarla asociándola al número que marcó, al momento en que realice su declaración

Para declarar algún número de los que marcó con el motivo de alguna cuenta, deberá seleccionar el grupo de cuentas que se despliega en la columna de "Motivo"; hecho lo anterior aparecerá un cuadro de texto en la columna de "Cuenta" y desde aquí podrá realizar alguna de las siguientes acciones:

1. **Buscar una cuenta:** Si conoce la cuenta puede escribir parte de la palabra o un grupo de letras para que el sistema le muestre un listado de coincidencias; o en caso de no conocerla presione la flecha hacia debajo de su teclado para que aparezca el listado con todas las cuentas disponibles.

2. **Crear una nueva cuenta:** En caso de no encontrar la cuenta a la que desea asociar el número que marcó, también tiene la posibilidad de crearla. Simplemente escriba el nombre de la nueva cuenta en el cuadro de texto y presione la tecla "Enter".

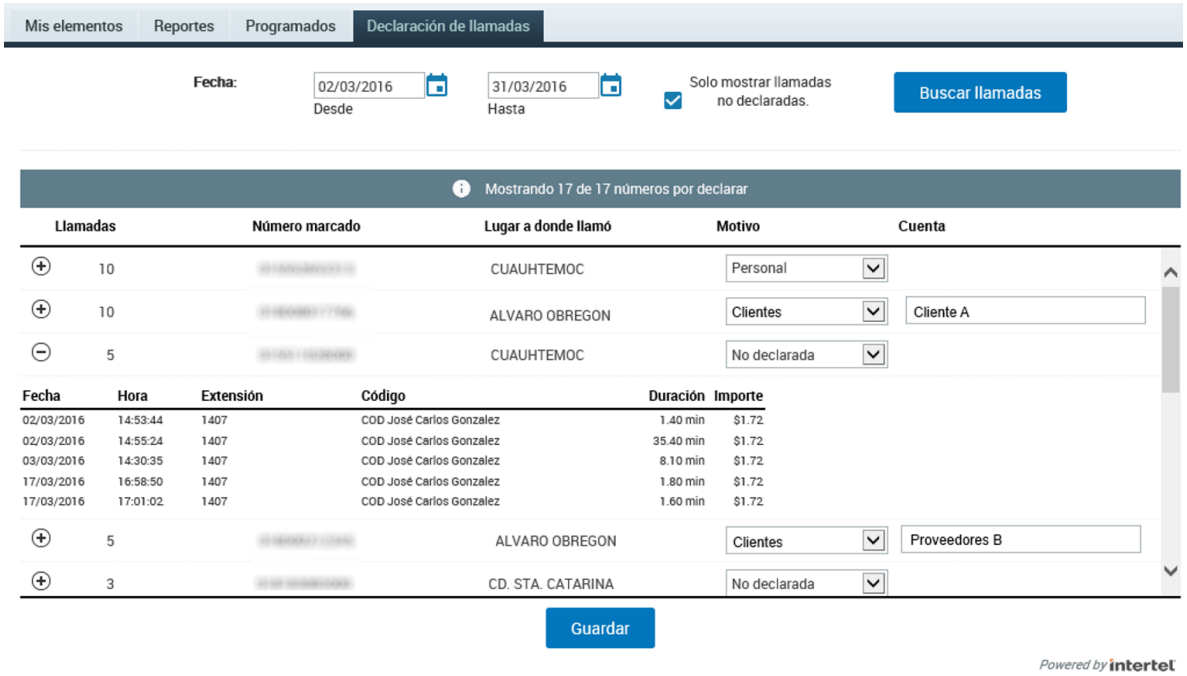


Figura 4.1. Declaración de Llamadas con motivos Laborales o Personales.

Recomendamos que su declaración la realice diariamente para que le sea más fácil recordar el lugar a donde llamó.

Capítulo 5. Gestión de Reportes

Esta sección contiene opciones para administrar los reportes que se muestran en el Portal, es decir para que el usuario Administrador pueda configurar cuales reportes del portal deberán mostrarse o cuales reportes deberán ocultarse. También, en caso de requerirse, se podrán agregar nuevos reportes con opciones de este menú.

La sección de "**Gestión de reportes**" en el Portal de Reportes, solo estará disponible para usuarios Administradores de todos los sitios, es decir, para usuarios de tipo Administrador Global.

La opción se encuentra localizada en la parte superior del Portal de Reportes, entre el combo de selección del sitio y el nombre del usuario en sesión, tal como se muestra en la siguiente figura:

Figura 5.1. Gestión de reportes.

Al presionar clic sobre esta opción, se abrirá un menú con dos opciones: **"Reportes especiales"** y **"Gestión de reportes"**.

En los puntos siguientes, se describirá lo que incluye cada una de estas opciones.

Reportes Especiales

En este menú, el usuario con permisos de administrador global, podrá agregar nuevos reportes (personalizados) o bien, eliminar los reportes personalizados que él mismo haya publicado en el Portal.

Cabe mencionar que esta sección es solo para administrar reportes personalizados e incluidos por el Administrador global del sistema. Los reportes por default que provee el portal de Reportes de Intertel®, no podrán ser afectados.

Para explicar con mayor detalle la administración de los **reportes especiales**, hemos creado un manual de usuario enfocado en tema. Por favor, **diríjase al manual "Especiales.pdf"** disponible en el disco de instalación del sistema Intertel®, para conocer los pasos de cómo agregar o eliminar reportes especiales. Para acceder a él solo coloque el disco de instalación en su unidad de disco y deje que en automático ingrese. Posteriormente presione clic en la opción "Manuales" y después, presione la opción "Ver manuales Reportes especiales". También puede acceder al manual de Especiales.pdf, dando clic derecho en la unidad correspondiente al disco desde el explorador de Windows y dando doble clic sobre el archivo "Especiales.pdf" localizado en la raíz del disco.

Para visualizar el manual de Reportes especiales, deberá contar con el software Acrobat Reader instalado.

Gestión de reportes

Dentro de esta sección el Administrador podrá indicar cuales reportes del IPR se deberán mostrar a todos los usuarios o solo a usuarios de tipo Administrador, cuales reportes se desplegarán en algún sitio en particular o en todos y/o cuales reportes no se mostrarán en el menú para ningún usuario.
Para ingresar a esta sección solo presione clic en el icono "Gestión de reportes" localizada en la parte superior del IPR y posteriormente, presione clic en la opción "Reportes especiales", tal como se muestra en la siguiente figura.

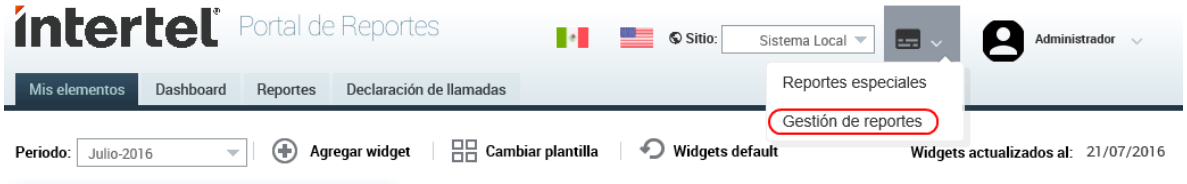


Figura 5.2. Gestión de reportes.

Una vez en esta sección, el sistema le desplegará la lista de reportes disponibles en el módulo agrupados por las categorías de reportes que se muestran en el IPR. Además, cada reporte contará con su título y una descripción breve de su propósito.

Figura 5.3. Gestión de reportes.

Detalles

En esta columna se incluye el nombre y una descripción breve del propósito del reporte.

Sitio

En la columna sitio, se indica para cual sitio de Intertel® se encuentra disponible el reporte.

Acción / Configurar visibilidad del reporte

Al presionar clic en el icono de editar localizado en la columna de Acción para cada reporte, el administrador podrá configurar la disponibilidad del reporte seleccionado en el menú.

La siguiente figura, muestra la pantalla donde se edita un reporte para que sea mostrado a todos los usuarios o de forma privada, así como la edición de la configuración del o de los sitios donde se mostrará dicho reporte.

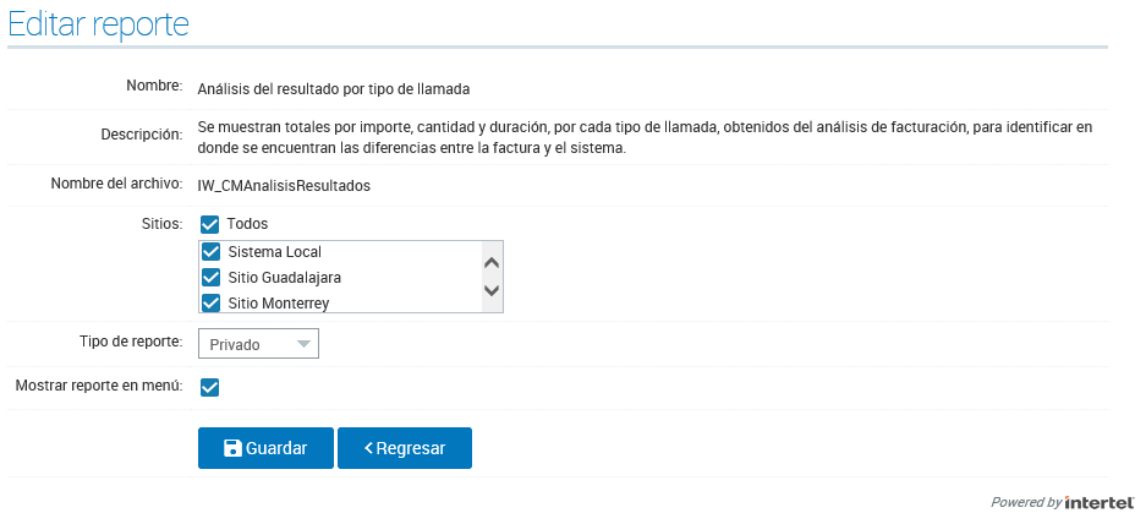


Figura 5.4. Gestión de reportes.

Active la casilla del sitio en la cual desea que el reporte se muestre. Active la casilla ”Todos”, en caso de que el reporte se deba estar disponible para todos los sitios del sistema.
Posteriormente, seleccione en el combo “Tipo de reporte” para el tipo de usuario que deberá desplegarse el reporte: “Privado” para cuando el reporte solo deberá mostrarse para usuarios de tipo Administrador. “Público” para cuando el reporte deba mostrarse a todos los usuarios.
Adicionalmente puede deshabilitar la casilla “Mostrar reporte en menú” para el caso en el que desee que el reporte no esté disponible en el portal para ningún usuario. Por default estará habilitada, lo cual indica que el reporte se encontrará visible en el menú.
Por último, presione clic en el botón “Guardar” para que el sistema registre la configuración. En caso de que no desee guardar la configuración, solo presione el botón “Regresar” para que el sistema ignore los movimientos que acaba de realizar y regrese a la lista de reportes a administrar.

Realice este procedimiento de edición para cada uno de los reportes que considere.
Por omisión, todos los reportes se despliegan en todos los sitios, pero depende del propósito del reporte el que se muestren a todos los usuarios o solo a usuarios administradores. Esto último lo podrá validar en la sección de “Clasificación de reportes” del presente manual, por cada reporte.

Capítulo 5. Sección Hotelera

Introducción

La Sección Hotelera del Portal de Reportes es una solución ideal para aquellos hoteles que no cuentan con un sistema de gestión hotelera o PMS. Su función principal es dar visibilidad al registro de llegada y salida de una persona (Check in – Check out), así como de mostrar el seguimiento y costos de llamadas telefónicas que fueron realizadas por el huésped, durante su estancia en una habitación.

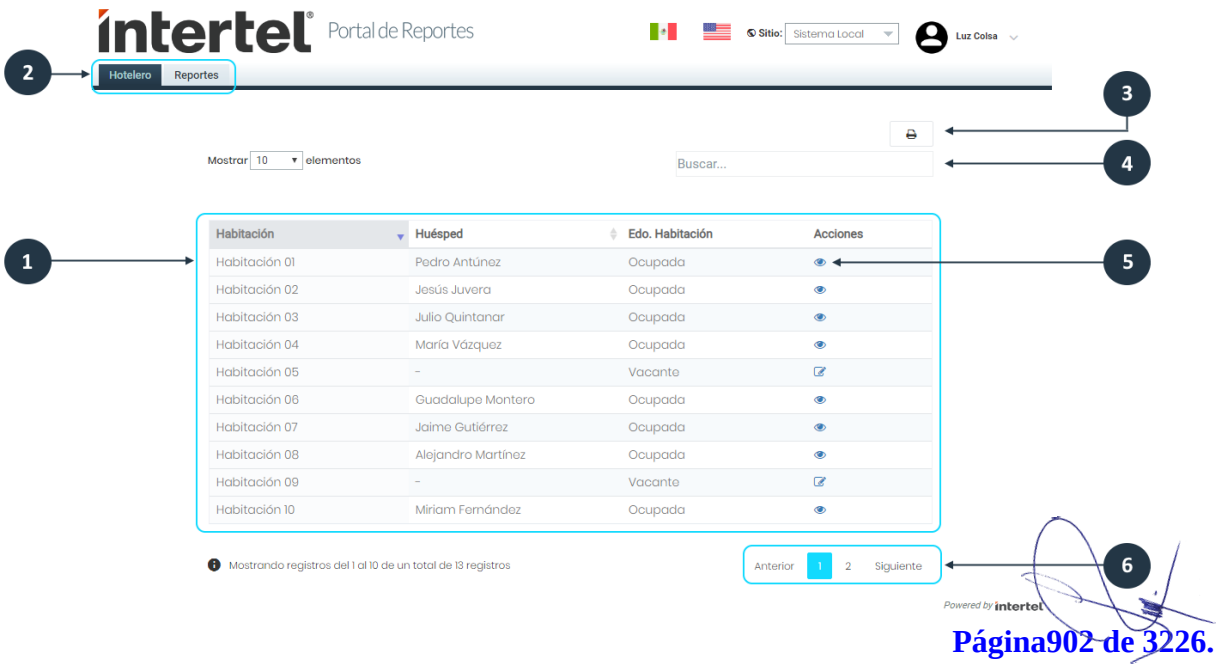
Combinada con las funcionalidades de Smart Manager, contamos con una herramienta más completa, a través de la cual podemos llegar a restringir llamadas, o indicar el o los tipos de llamadas que se podrán hacer desde cada habitación. Para lograr lo anterior, será necesario que la licencia que haya adquirido del sistema Intertel tenga habilitado el módulo de Smart Manager.

Desde esta sección usted cuenta con las siguientes facilidades:

- Registrar la llegada de un huésped a una habitación (Check in).
- Registrar la salida de un huésped de una habitación (Check out)
- Consulta e impresión de registro de llamadas realizadas por el huésped durante su estancia.
- Generación de set de reportes Hoteleros.
- Configurar los tipos de llamadas que podrá hacerse desde cada habitación /Restricciones de llamadas, combinándolo con el módulo de Smart Manager.

Interfaz gráfica de Sección Hotelera

La interfaz de la sección Hotelera ha sido diseñada para que de manera sencilla realice el Check in y Check out de una habitación; las opciones necesarias para hacerlo se muestran en la imagen siguiente:



1. Panel de habitaciones.
2. Menú de opciones.
3. Impresión.
4. Búsqueda por huésped o habitación.
5. Check in / Check out.
6. Barra de navegación.

Panel de habitaciones:

En esta sección aparecerá el registro de todas las habitaciones de su hotel, y el estado en que se encuentra cada una de estas habitaciones, es decir podrá consultar si están vacantes u ocupadas. En caso de que la habitación esté ocupada, aparecerá el nombre de la persona que hizo la reservación, y por medio de diferentes acciones, tendrá la facilidad de consultar el registro de llamadas realizado por el huésped durante su estancia antes de hacer el check out.

Menú de opciones

En este menú se encuentran las opciones principales de la Sección Hotelera. Desde aquí tendrá la facilidad de consultar el listado de habitaciones vacantes u ocupadas, registrar la hora de entrada y salida del huésped, así como a generación de reportes con información de sus habitaciones. Para tener mayor conocimiento sobre el listado de reportes disponibles en esta sección, vaya al capítulo 3: Reportes, y consulte la sección de Hoteles y Hospitales de este manual.

Impresión

Al dar clic sobre el botón de impresión usted podrá imprimir el listado de habitaciones, o el listado de llamadas realizadas por el huésped, que estén visibles en pantalla. Por lo cual si desea una impresión de todas las habitaciones o todas las llamadas realizadas por el huésped, recuerde seleccionar del filtro "mostrar elementos", la opción de "todos".

Búsquedas por huésped o habitación

Contará con la facilidad de realizar búsquedas ya sea por el nombre del huésped o número de habitación (clave de la extensión del sistema Intertel). Simplemente teclee algunos dígitos de la extensión o habitación, o bien el nombre del huésped, para que le sean mostradas las coincidencias en pantalla. No es necesario que escriba en su totalidad el número dehabitación o el nombre del huésped para que obtenga resultados, con solo teclear las primeras letras del nombre o bien algunos dígitos de la habitación.

TIP: Sugerimos que la extensión que vaya a ser creada en el sistema Intertel sea identificada con el número de la habitación, debido a que las consultas que se hagan desde la sección Hotelera serán a través de la clave de la extensión.

Check in / Check out

Desde estas opciones registrará la hora de llegada y salida del huésped, así como la consulta de las llamadas que realizó el huésped durante su estancia.

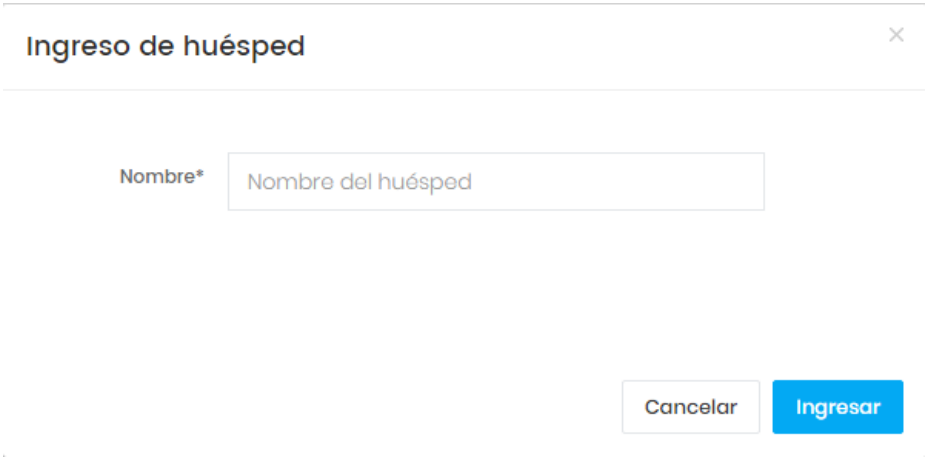
Barra de navegación

A través de ella puede navegar o cambiar de página cuando la cantidad de habitaciones a mostrar, supera la cantidad de elementos que se listan en el panel. Esta opción trabaja en conjunto con el selector de elementos a mostrar; usted decide si se muestran hasta 20 habitaciones por página, o bien, el total de habitaciones existentes en su sistema.

Registro de entrada y salida de un huésped

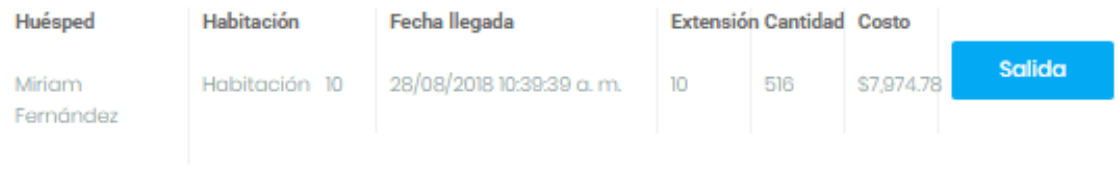
Registro de entrada (Check In)

Para registrar la llegada de un huésped deberá verificar que el estado de la habitación se encuentre como "Vacante". Para hacerlo, de clic sobre la columna de "Huésped" para que de manera ordenada, muestre en primera instancia todas las habitaciones que están disponibles; hecho lo anterior de clic en el icono de un Lápiz sobre una nota , para ingresar el nombre del huésped; una vez realizado el registro, cambiará el estado de la habitación a "Ocupado" y aparecerá en la columna de "Huésped" el nombre con el que haya registrado a la persona en el sistema.

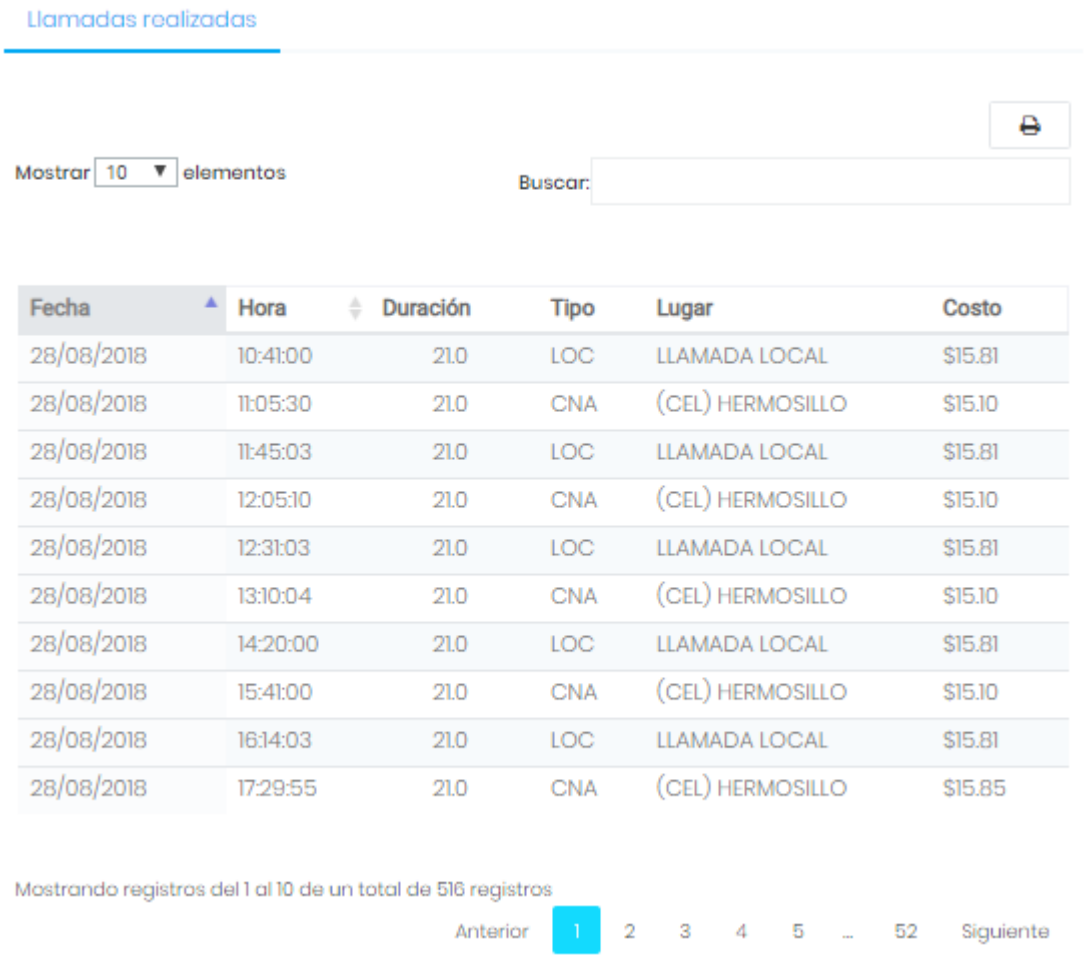


Registro de salida (Check out) / Consulta e Impresión de llamadas

Cuando el huésped decida abandonar la habitación, simplemente de clic en el icono en forma de ojo para tener acceso a la opción de salir de la habitación, es decir hacer el Check out. Al dar clic sobre el botón "Salida" le indicaremos al sistema que la habitación quedará en estado "Vacante".



Desde este apartado también tendrá acceso a consultar las llamadas que realizó el huésped durante su estancia, así como el costo generado por cada una de estas. Y en caso de ser necesario tendrá la facilidad de imprimir el detalle de estas llamadas, haciendo uso de la opción de impresión dando clic en el botón de impresora .



¡Necesitamos su opinión!

Tenemos como objetivo el seguir brindándole el producto de mayor calidad e innovación en el mercado. Estamos seguros de que usted es el que puede ofrecer las mejores ideas y sugerencias. Si usted piensa que hay alguna manera de mejorar, ¡estaremos en la mejor disposición para recibir su opinión!

¡Muchas gracias por su preferencia!

Intersel
Interfases y Sistemas Electrónicos S.A.P.I. de C.V.
Oficina Corporativa
Plaza las Palmas
Blvd. Solidaridad No. 335
Edif. A Nivel 2
Col. Paseo del Sol, C.P. 83246.
Hermosillo, Sonora, México
Teléfono: +52 (662) 210-60-80
Email: info@intersel.com.mx

Búsquenos en Internet:
http://intersel.com.mx/

IP Office™ Plataforma 11.0

Administración de Avaya one-X Portal para IP Office

Contenido

1. Administración de one-X Portal para IP Office

1.1 Lo nuevo de 11.0 ... 7
1.2 Iniciar sesión ... 8
1.3 Cerrar sesión ... 8

2. Menús de administración

2.1 Estado ... 12
2.1.1 Tablero ... 12
2.1.2 Estado de los componentes ... 13
2.1.3 Estado del servidor de MI/presencia ... 13
2.1.4 Resiliencia ... 14
2.1.5 Eventos clave recientes ... 15
2.1.6 Sesiones activas ... 16
2.1.7 Entorno ... 16
2.2 Configuración ... 17
2.2.1 Proveedores ... 17
2.2.2 Usuarios ... 22
2.2.3 CSV ... 23
2.2.4 Marca ... 23
2.2.5 MI/Presencia ... 24
2.2.6 Servicio Exchange ... 25
2.2.7 Configuración SMTP ... 26
2.2.8 Acceso telefónico a conferencias ... 27
2.2.9 Resistencia ... 28
2.2.10 Nombre de dominio de host ... 30
2.2.11 Syslog ... 30
2.2.12 Limpieza de conferencia ... 31
2.2.13 Enlace de CTI central ... 32
2.2.14 Bloquear versiones del cliente ... 33
2.3 Seguridad ... 33
2.3.1 Protocolo HTTP/HTTPS ... 33
2.3.2 Configuración TLS ... 34
2.3.3 Autenticación ESNA ... 34
2.3.4 Certificado ... 34
2.4 Diagnóstico ... 35
2.4.1 Configuración de registros ... 35
2.4.2 Visor de registros ... 37
2.4.3 Rutas de red ... 37
2.4.4 Conexiones de IP Office ... 38
2.4.5 Integridad de base de datos ... 38
2.4.6 Validación de datos de usuario ... 39
2.4.7 Programación de llamadas/conferencias ... 40
2.4.8 Visualización de conferencias ... 41
2.4.9 Volcar memoria ... 42
2.4.10 Volcar subprocesos ... 42
2.5 Integración de directorios ... 42
2.5.1 Sincronización de directorios ... 42
2.5.2 Búsqueda de directorios de LDAP ... 42
2.5.3 Directorio del sistema ... 44
2.6 Configuración de gadget ... 45
2.6.1 Lista de gadgets externos ... 45
2.6.2 Importación de gadgets ... 45
2.6.3 Exportación de gadgets ... 46
2.7 Archivo MI ... 47
2.7.1 Buscar archivo ... 47
2.8 Conferencias web ... 48
2.8.1 Control de conferencias ... 48
2.9 Ayuda y asistencia técnica ... 49

3. Tareas de mantenimiento

3.1 Reiniciar el servicio ... 52
3.2 Configuración del registro de llamadas ... 53
3.3 Conmutador de IP Office ... 54
3.3.1 Incorporación de una unidad adicional de IP Office ... 54
3.3.2 Modificación de la información de IP Office ... 56
3.3.3 Resistencia ... 57
3.4 Gadgets ... 60
3.4.1 Búsqueda de URL del gadget ... 60
3.4.2 Importación de gadgets ... 61
3.4.3 Exportación de gadgets ... 63
3.4.4 Agregar un gadget externo ... 64
3.4.5 Editar un gadget externo ... 64
3.4.6 Habilitar un gadget externo ... 65
3.4.7 Desactivar un gadget externo ... 65
3.4.8 Eliminar un gadget externo ... 65
3.5 Usuarios ... 66
3.5.1 Incorporación o eliminación de usuarios ... 66
3.5.2 Edición de la configuración de usuarios ... 66
3.6 Directorios ... 68
3.6.1 Incorporación de una fuente de directorios externos de LDAP ... 68
3.6.2 Verificación del directorio externo de LDAP ... 70
3.6.3 Verificación y actualización del directorio del sistema ... 71
3.7 Actualización/regreso a versión anterior ... 72
3.7.1 Actualización de one-X Portal para IP Office ... 72
3.7.2 Regreso a la versión anterior de one-X Portal para IP Office ... 73
3.7.3 Eliminación de one-X Portal para IP Office ... 74
3.8 Mensajería instantánea/Presencia ... 76
3.8.1 Configuración del servidor de MI ... 77
3.8.2 Configuración de MI del usuario ... 79
3.8.3 Inicio del servidor de MI ... 79
3.8.4 Búsqueda en el archivo de MI ... 80
3.8.5 Integración de calendario de Exchange ... 81
3.8.6 Activación de la consola de administrador de XMPP ... 82
3.8.7 Activación del archivado de MI ... 82
3.8.8 Desactivación de archivo de MI ... 83
3.8.9 Desactivación de la consola de administrador de XMPP ... 83
3.9 Conferencias ... 84
3.9.1 Visualización de conferencias ... 84
3.9.2 Visualización de conferencias programadas ... 85
3.9.3 Eliminación de una conferencia programada ... 86
3.9.4 Mensaje de notificación de conferencia ... 86
3.9.5 Mensajes de correos electrónico de conferencia ... 87
3.9.6 Establecer la URL de colaboración web ... 88
3.10 Registro remoto ... 89
3.11 Solución de problemas ... 93
3.12 Incorporación de administradores adicionales ... 94

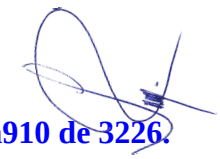
4. Menús AFA

Página908 de 3226.

4.1 Iniciar sesión 96
4.2 Estado del sistema 97
4.3 Configuración 97
4.4 Operaciones de base de datos 98
4.4.1 Respaldar 98
4.4.2 Restaurar 99

5. Historial de documentos

Índice 106



Capítulo 1.

Administración de one-X Portal para IP Office

1. Administración de one-X Portal para IP Office

Además de la operación habitual que realiza el usuario final, la interfaz web de one-X Portal para IP Office también sirve para una serie de funciones de administración y mantenimiento. La presente documentación incluye el uso de esos menús de administración.

1.1 Lo nuevo de 11.0

El siguiente es un resumen de las nuevas funciones de administrador de la versión 11.0 de IP Office de one-X Portal para IP Office, versión FP4:

- **Cantidad de usuarios y clientes conectados**
  El tablero 12 ahora muestra la cantidad de usuarios conectados.
- **Detalles del usuario que inicia sesión**
  El menú Sesiones activas 16 ahora muestra una lista con detalles de los clientes usuarios conectados, la versión del cliente, etc.
- **Botón Borrar sesiones**
  El menú Usuarios 22 ahora incluye un botón Borrar sesiones que puede utilizarse para desconectar a los clientes actualmente conectados del usuario.
- **Inicios de sesión fallidos**
  El menú Eventos clave recientes 15 ahora incluye inicios de sesión de usuario fallidos. Esto ocurre cuando un usuario realiza más de 5 intentos de conexión fallidos en un período de 10 minutos.
- **Controles de bloqueo de cliente**
  El servidor puede configurarse para bloquear la conexión de versiones específicas de clientes. Esto se realiza a través del nuevo menú Bloquear versiones del cliente 33.

1.2 Iniciar sesión

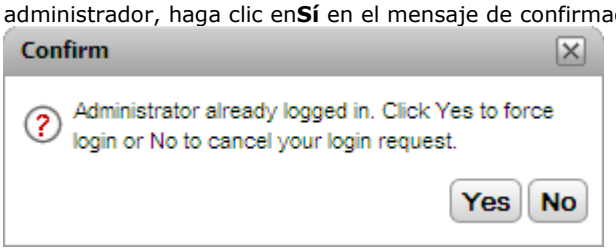
El acceso a los menús de administración para one-X Portal para IP Office se realiza a través del explorador Web al igual que el acceso de usuarios, pero con la incorporación de ***?admin=true*** a la URL. Solo un usuario a la vez puede iniciar sesión como administrador.

De manera predetermina, los servidores de one-X Portal para IP Office basados en Linux usan la **Autenticación referida**. Esto significa que los derechos de la administración del portal se asignan a los usuarios de seguridad establecidos en la configuración de seguridad del servicio IP Office que se ejecuta en el mismo servidor. De manera predetermina es el usuario **Administrador**; sin embargo, otros usuarios de servicio también pueden configurarse para el acceso de administrador del portal. Si se desactiva la opción de autenticación referida, el portal usa su propia cuenta de administrador local para un servidor basado en Windows, como a continuación.

Los servidores basados en Windows usan una cuenta de **Administrador** local almacenada en la propia configuración del portal (o **Superusuario** para los menús de AFA). El instalador cambia la contraseña predeterminada como parte del proceso de instalación.

Para iniciar sesión:

1. En el explorador Web, ingrese la URL con el formato ***https://<nombre del servidor>:<puerto de servidor>/onexportal-admin.html***, donde:
   - ***<nombre del servidor>*** es el nombre o la dirección IP del servidor de one-X Portal para IP Office.
   - ***<puerto del servidor>*** es el número de puerto que usa one-X Portal para IP Office. Será 9443 o 8443 para el acceso HTTPS.
   - Puede utilizar ***http://*** en lugar de ***https://*** y ***8080*** como puerto, si se configuró acceso no seguro. Consulte Protocolo 33.
   - O bien, puede seleccionar **Inicio de sesión del administrador** en el menú de inicio de sesión de usuario común.
2. Ingrese el nombre y la contraseña de administrador de one-X Portal para IP Office como se configuraron durante la instalación.
   - Si existe ya una sesión conectada como administrador, aparece la siguiente casilla de mensaje de confirmación. Para finalizar la sesión del administrador iniciada e iniciar sesión con sus credenciales de administrador, haga clic en**Sí** en el mensaje de confirmación.

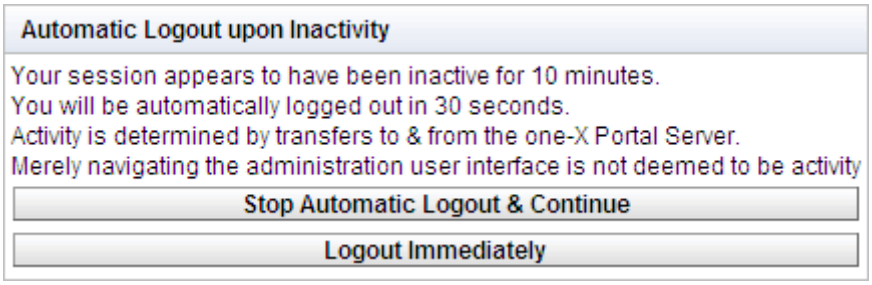


3. Haga clic en **Iniciar sesión**.

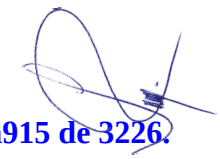
1.3 Cerrar sesión

La opción **Cerrar sesión** ubicada en la parte superior derecha de los menús de administración de one-X Portal para IP Office puede utilizarse para cerrar sesión.

Además del cierre de sesión manual, después de 10 minutos el sistema también le preguntará si desea permanecer conectado. Si no responde, la sesión se cerrará automáticamente.



Capítulo 2.
Menús de administración



2. Menús de administración

El menú de administración de one-X Portal para IP Office ofrece una variedad de opciones para controlar y configurar la aplicación one-X Portal para IP Office.

Menú	Submenú	Descripción
Estado	Tablero 12	Muestra un resumen del estado del servidor.
	Estado de los componentes 13	Indicar el último cambio de estado de los componentes del servidor.
	Estado del servidor de MI/presencia 13	Muestra el estado actual del componente del servidor de mensajería instantánea.
	Resiliencia 14	Mostrar el estado de los servidores en una configuración de resistencia. *(solamente IP Office Server Edition)*
	Eventos clave recientes 15	Ver los últimos 20 eventos en el servidor.
	Sesiones activas 16	Mostrar la cantidad de sesiones que one-X Portal para IP Office ha almacenado en la memoria caché.
	Entorno 16	Mostrar un resumen de la computadora del servidor one-X Portal para IP Office.
Configuración	Proveedores 17	Ver y editar los proveedores.
	Usuarios 22	Ver y editar la configuración de los usuarios de one-X Portal para IP Office.
	CSV 23	Exportar el directorio del usuario y el del sistema.
	Marca 23	Especifique el texto que se muestra en las páginas de one-X Portal para IP Office después de que el usuario ha iniciado sesión.
	MI/Presencia 24	Controle el estado de servidor de MI/presencia como Administrador.
	Servicio Exchange 25	Configure el servidor Exchange para validar la información de minería de calendario y de presencia de los usuarios.
	Configuración SMTP 26	Establezca los detalles de correo electrónico para enviar notificaciones de conferencias.
	Acceso telefónico a conferencias 27	Determine el texto fijo que se incluirá en las notificaciones de conferencias programadas.
	Resistencia 28	Utilizado en IP Office Application Server para configurar si el portal admite resistencia. *(solamente IP Office Server Edition)*
	Nombre de dominio de host 30	Establece la URL que se usa para las conferencias de colaboración web en las invitaciones de conferencias.
	Syslog 30	En los servidores basados en Windows, active los informes Syslog a una dirección remota.
	Limpieza de conferencia 31	Configure el tiempo durante el cual se conservarán los detalles de conferencia.
	Enlace de CTI central 32	Configure si el servidor obtiene información automáticamente sobre otros sistemas de IP Office de una red y si los admite.
	Bloquear versiones del cliente 33	Configure versiones y compilaciones específicas de clientes que no serán compatibles con el servidor.
Seguridad	Protocolo HTTP/HTTPS 33	Establezca si el servidor utilizará HTTPS o HTTPS y HTTP.
	Configuración TLS 34	Configurar las opciones de compatibilidad TLS.
	Autenticación ESNA 34	Configura la dirección del servidor ESNA para utilizar en la autenticación de inicio de sesión de usuarios en una cuenta ESNA.
	Certificado 34	En los servidores basados en Windows, importe el certificado de seguridad que se utilizará para el acceso encriptado.
Diagnóstico	Configuración de registros 35	Configurar el nivel y el método de registro admitido.
	Visor de registros 37	Instalar e iniciar Chainsaw para ver registros.
	Rutas de red 37	Comprobar la ruta de la conexión IP a una dirección IP.
	Conexiones de IP Office 38	Comprobar la ruta de la conexión IP a una unidad de IP Office.
	Integridad de base de datos 38	Comprobar la estructura de la base de datos.

Menú	Submenú	Descripción
	Validación de datos de usuario 39	Identifique la causa posible del error en el inicio de sesión del usuario o la corrupción de datos del usuario y restablezca los datos corruptos.
	Programación de llamadas/conferencias 40	Elimine una conferencia programada.
	Visualización de conferencias 41	Muestra los detalles de las conferencias históricas y las programadas para el futuro de todos los usuarios. Permite la eliminación y modificación de esas conferencias.
	Volcar memoria 42	Crea un registro de diagnóstico del uso actual de memoria del servidor.
	Volcar subprocesos 42	Crea un registro de diagnóstico de los subprocesos en curso del procesador.
Integración de directorios	Sincronización de directorios 42	Forzar una actualización del directorio del sistema por parte del servidor.
	Directorio del sistema 44	Ver el directorio del sistema one-X Portal para IP Office.
	Búsqueda de directorios de LDAP 42	Ver el directorio externo para el que se ha configurado el servidor one-X Portal para IP Office.
Configuración de gadgets	Lista de gadgets externos 45	Se incluyen los gadgets externos que están en el sistema.
	Importar gadgets externos 61	Importe gadgets externos.
	Exportar gadgets externos 46	Exporte gadgets externos.
Conferencias web	Control de conferencias 48	Vea los detalles de cualquier conferencia web que actualmente se esté ejecutando en el servidor.
Archivo MI	Buscar archivo 47	Busque las conversaciones de MI entre los contactos del sistema.
Ayuda y asistencia técnica	Ayuda 49	Acceder a la ayuda de one-X Portal para IP Office instalada en el servidor.
	Asistencia técnica de Avaya 49	Acceder al sitio Web de asistencia técnica de Avaya para las aplicaciones de Avaya.
	Acerca de 49	Ver información sobre la versión de one-X Portal para IP Office.

Es importante comprender que los menús de administrador de one-X Portal para IP Office funcionan como un editor fuera de línea. En un menú en particular, los datos se obtienen de la base de datos (por medio del comando **OBTENER**), se editan y luego vuelven a enviarse a la base de datos (por medio del comando **INGRESAR**).

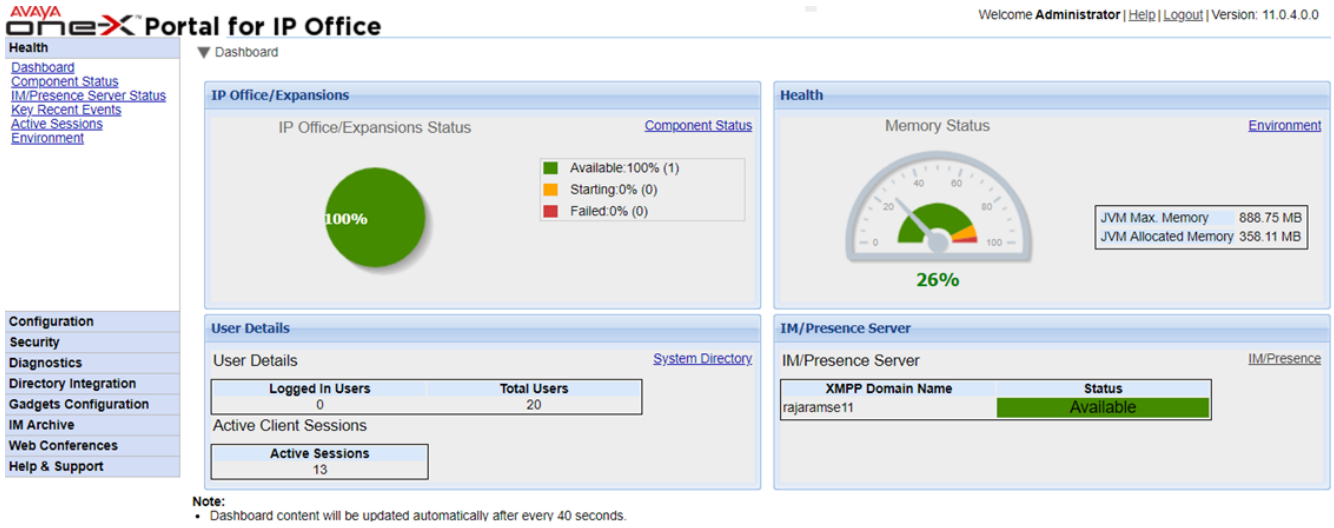
En cada menú, es posible hacer clic en los iconos ▶ ▼ que sirven para mostrar u ocultar una breve descripción de la función y el contenido de los menús.

2.1 Estado

Esta sección le permite ver el estado de los distintos componentes del servidor.

2.1.1 Tablero

En el menú Tablero, se proporciona un resumen del estado del servidor.

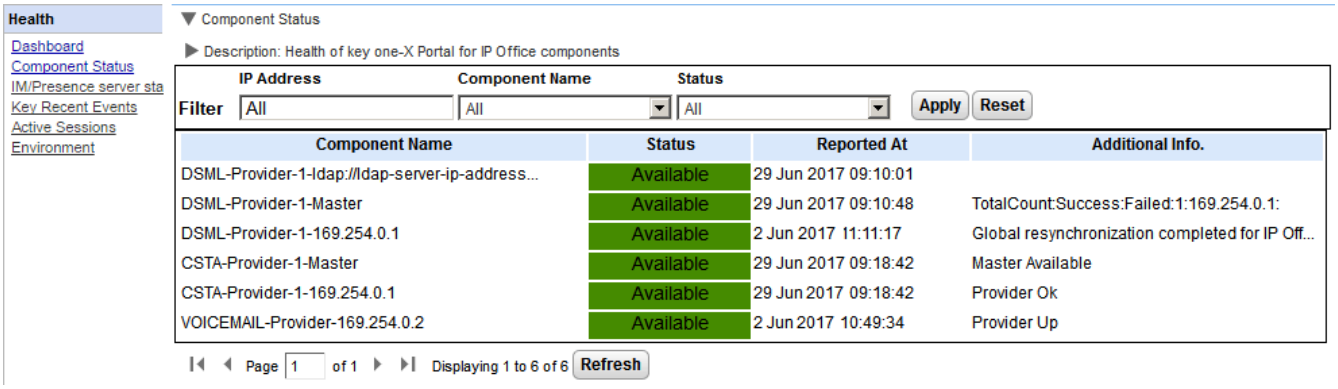


- **IP Office/Estado de expansión**
  En esta sección, se resume el estado de las conexiones desde el servidor del portal hasta los sistemas de IP Office que está admitiendo.
- **Estado**
  En esta sección, se resume el uso de la memoria de los servidores.
- **Detalles del usuario**
  En esta sección, se resume el número de usuarios configurados y conectados. También muestra la cantidad de sesiones activas, lo que incluye usuarios de Avaya Communicator for Web, el complemento de Outlook, one-X Portal para IP Office.
- **Servidor de presencia/MI**
  En esta sección, se resume el estado del componente XMPP del servidor.

2.1.2 Estado de los componentes

El menú **Estado de los componentes** muestra los últimos cambios de estado registrados de cada uno de los principales componentes de la aplicación one-X Portal para IP Office.

- Para los servidores de UCM Windows, deben haber un proveedor maestro de CSTA más 1 proveedor de CSTA para cada sistema IP Office que se admita. Esto también rige para los sistemas Linux que admitan una red de IP Office Server Edition pero no usen el modo enlace de CTI centralizado 32.
- Para un servicio en una red de IP Office Server Edition y que use el modo de enlace de CTI centralizado, debe haber solo un proveedor de DMSL para el sistema IP Office primario. También debe haber un proveedor de CSTA para el sistema IP Office primario, a menos que se use la resiliencia del portal, en cuyo caso también debe haber un proveedor de CSTA para el sistema IP Office secundario.
- Debe haber un proveedor de LDAP DSML si se usa LDAP.

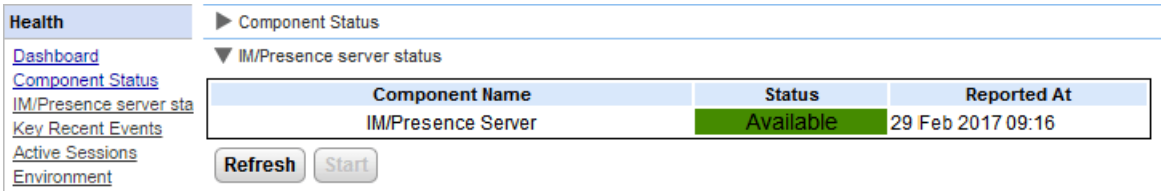


Para ver el estado del componente:

1. Seleccione **Estado** y, a continuación, **Estado de los componentes**.
2. Haga clic en **Obtener todo** para recuperar los registros de estado de la base de datos de one-X Portal para IP Office.
3. Utilice los controles de página para navegar por los registros.
4. La opción **Eliminar** elimina el registro de estado, pero no afecta el componente. Las casillas de verificación y la opción **Eliminar selección** pueden utilizarse para eliminar varios registros.

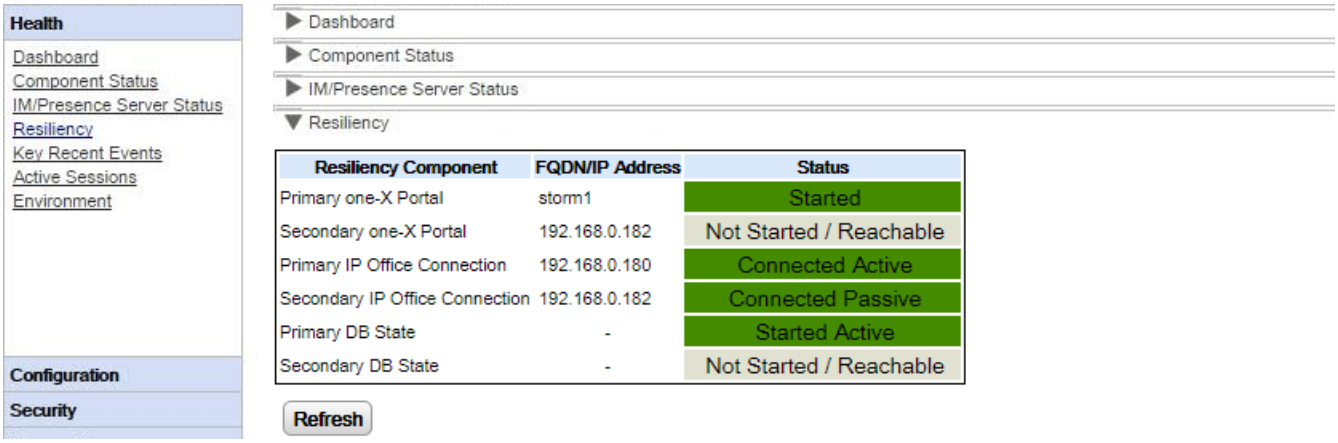
2.1.3 Estado del servidor de MI/presencia

Este menú muestra el estado actual del servidor de mensajería instantánea utilizado como servicio de componente por one-X Portal para IP Office. Para conocer los distintos procesos de mantenimiento relacionados con MI y Presencia, consulte Mensajería instantánea 76.



2.1.4 Resiliencia

Este menú se muestra en los servidores del portal de la red IP Office Server Edition Seleccione. Muestra el estado actual del portal y de los servicios de IP Office en los servidores primarios y secundario cuando se utiliza IP Office Server Edition resilience[14].



Por ejemplo, la captura de pantalla anterior muestra un sistema donde los servidores primarios y secundarios de IP Office están en ejecución y el servidor del portal primario está en ejecución pero el servicio del portal secundario no se ha iniciado. Cuando el servicio del portal está iniciado, el estado del portal secundario cambiará a ***Iniciado*** y el **DB secundario** a ***Iniciado en pasivo***.

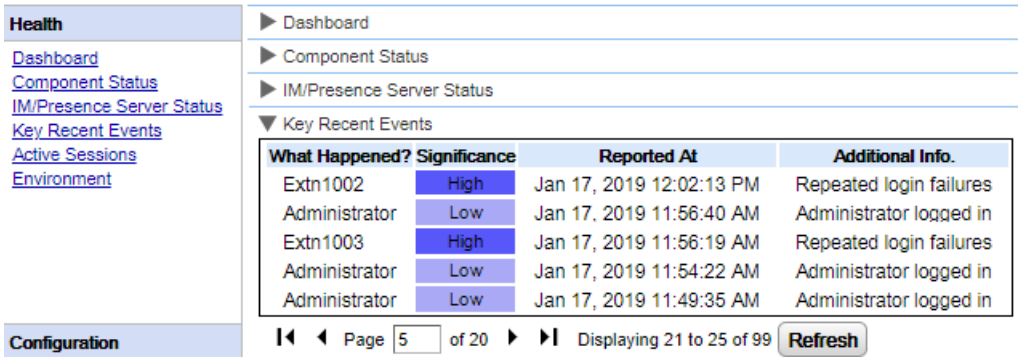
Los términos que se utilizan en la pantalla de estado tienen los siguientes significados. Los términos pueden combinarse:

- **Iniciado**
  El servicio está funcionando.
- **Detenido** o **No iniciado**
  El servicio no está en ejecución.
- **Conectado**
  El servidor del portal tiene una conexión al servicio.
- **No accesible**
  El servidor que aloja el servicio se detectó pero no existe conexión ya que el servicio en ese servidor no se ha iniciado.
- **Activo**
  El servicio actualmente está en uso como respaldo para usuarios del portal.
- **Pasivo**
  El servicio está en ejecución pero actualmente no está en uso como respaldo para usuarios del portal.

2.1.5 Eventos clave recientes

El menú **Eventos clave recientes** muestra los últimos 20 eventos registrados por la aplicación one-X Portal para IP Office. Pueden ser acciones realizadas por el servicio one-X Portal para IP Office y también acciones de administración tales como el inicio o cierre de sesión de administrador, cambios de la contraseña del administrador, cambios de proveedor y restauraciones de configuración.

La lista también incluye los intentos de conexión fallidos del usuario si ocurren más de 10 fallas en un período de 5 minutos. Los intentos de conexión fallidos se basan en el nombre de usuario. Esto no incluye los inicios de sesión fallidos a Avaya Communicator.

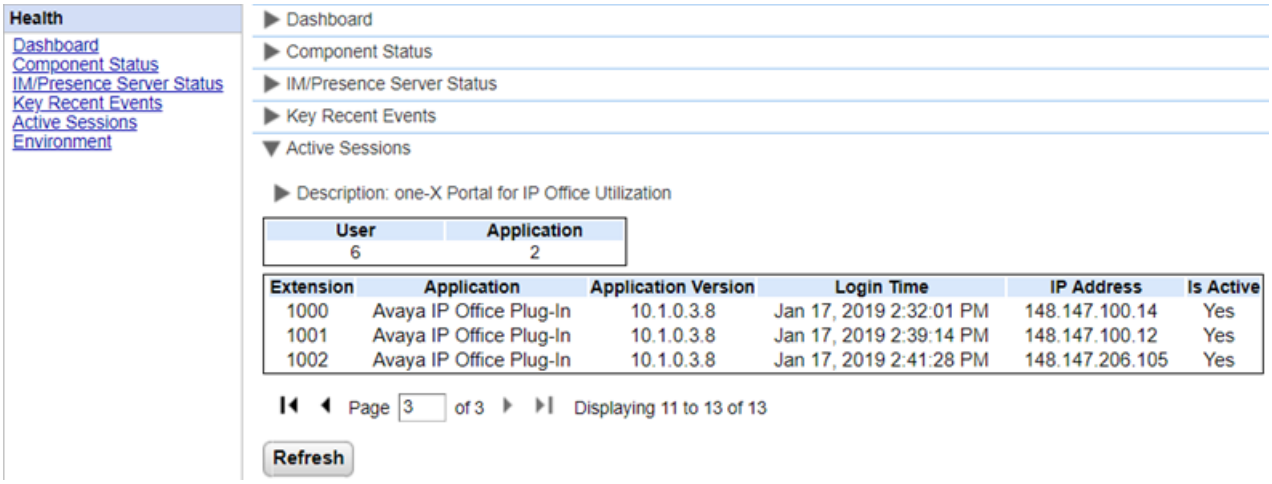


Para ver eventos clave recientes:

1. Seleccione **Estado** y, a continuación, **Eventos clave recientes**. Haga clic en **Actualizar**.
2. Haga clic en **Obtener todo** para recuperar los registros de eventos de la base de datos de one-X Portal para IP Office.
3. Utilice los controles de página para navegar por los registros.
4. La opción **Eliminar** elimina el registro de estado, pero no afecta el componente. Las casillas de verificación y la opción **Eliminar selección** pueden utilizarse para eliminar varios registros.

2.1.6 Sesiones activas

El menú **Sesiones activas** muestra la cantidad de sesiones actuales del explorador conectadas al servidor one-X Portal para IP Office.

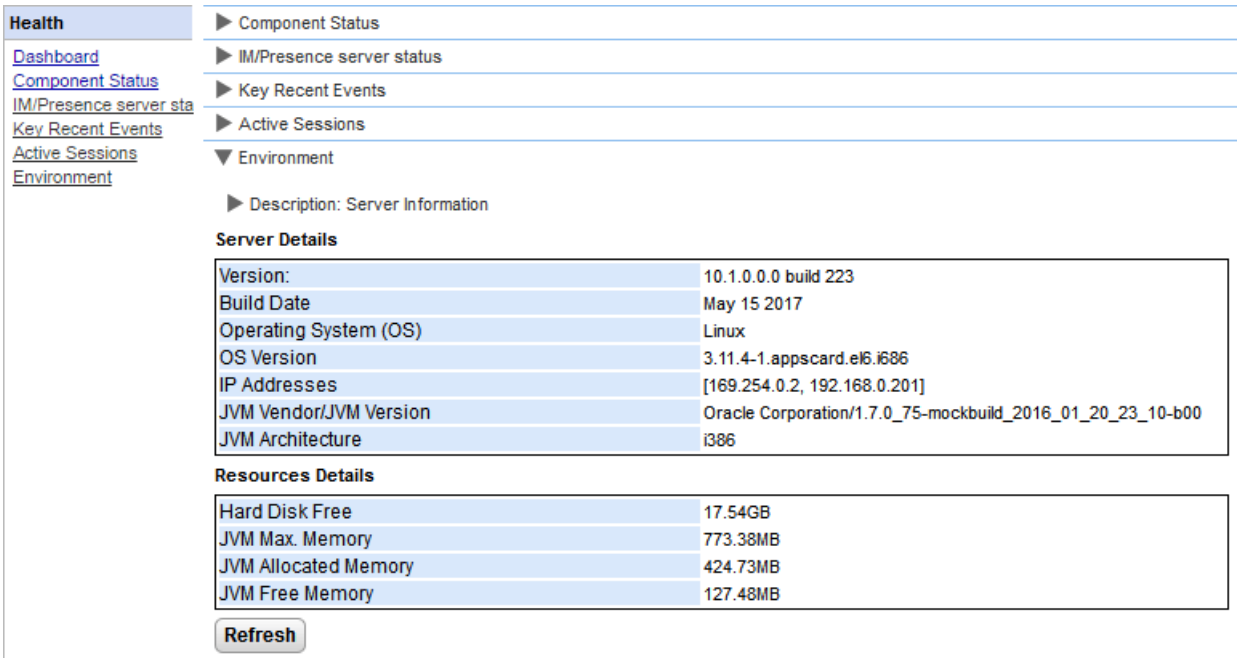


Para ver las sesiones activas:

1. Seleccione **Estado** y, a continuación, **Sesiones activas**.
2. Haga clic en **Actualizar** para actualizar los detalles.

2.1.7 Entorno

El menú **Entorno** muestra información sobre la computadora servidor one-X Portal para IP Office. La información disponible varían según el tipo de servidor del portal.



Para ver la información del entorno:

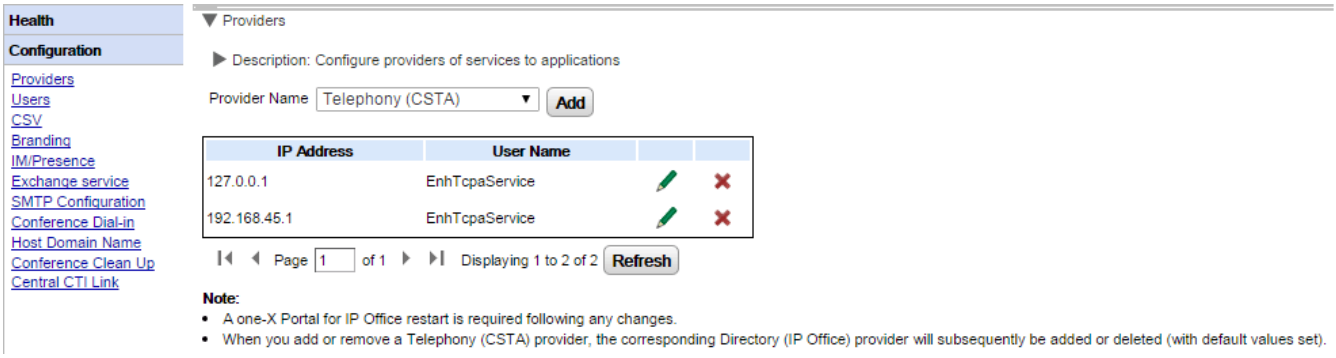
1. Seleccione **Estado** y, a continuación, **Entorno**.
2. Haga clic en **Actualizar**.

2.2 Configuración

Esta sección le permite ver y comprobar distintas opciones de configuración.

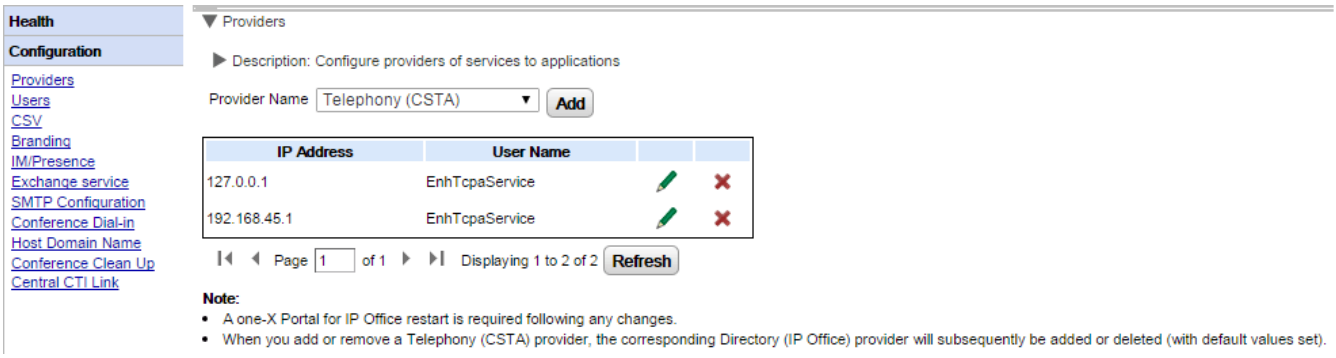
2.2.1 Proveedores

Este menú muestra los proveedores de servicio configurados en el servidor one-X Portal para IP Office. El menú **Proveedores** permite editar qué unidades de IP Office y servidores de LDAP se asignan a los proveedores.



2.2.1.1 Proveedor de telefonía (CSTA)

Los valores de configuración que figuran a continuación se muestran para un proveedor de telefonía (CSTA). Estos valores sólo deben modificarse si el usuario tiene experiencia en la instalación y el funcionamiento de one-X Portal para IP Office.

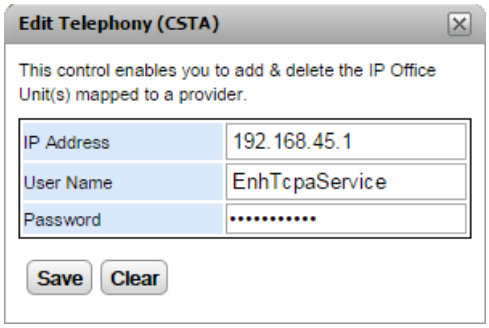


Para agregar un proveedor de CSTA nuevo, haga clic en **Agregar**. Aparece la configuración del proveedor. Tenga en cuenta que al agregar un proveedor de CSTA nuevo, también se agrega automáticamente un proveedor de DMSL nuevo a la misma dirección. Agregar un proveedor nuevo solamente sería necesario en una red que no utilice configuración centralizada 32.

Para editar un proveedor de CSTA existente, haga clic en el icono de edición que se encuentra junto a la entrada existente. Aparece la configuración del proveedor. Para agregar

Configuración del proveedor de CSTA

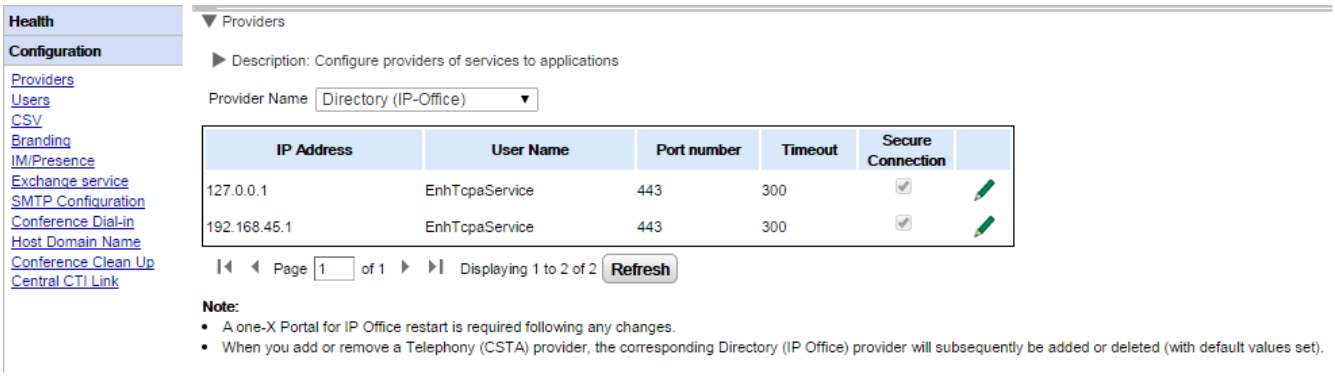
Cualquier cambio en la configuración del proveedor requiere que reinicie el servicio del portal 52.



- **Dirección IP**
  La dirección IP del sistema IP Office.
- **Nombre de usuario**
  El nombre que estableció el usuario del servicio de TCPA en la configuración de seguridad del sistema IP Office. El usuario predeterminado es ***EnhTcpaService***.
- **Contraseña**
  La contraseña establecida para el usuario de servicio de TCPA.

2.2.1.2 Proveedor de directorio (IP Office)

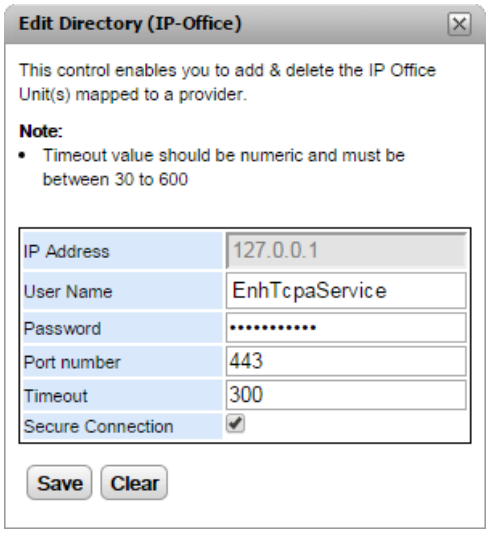
Los valores de configuración que figuran a continuación se muestran para un proveedor de directorios (IP-Office). Estos valores sólo deben modificarse si el usuario tiene experiencia en la instalación y el funcionamiento de one-X Portal para IP Office.



Para agregar un proveedor de directorio nuevo, use las opciones para agregar un proveedor de CSTA 18. Para editar un proveedor existente, haga clic en el icono de edición que se encuentra junto a la entrada existente.

Configuración del proveedor de directorio

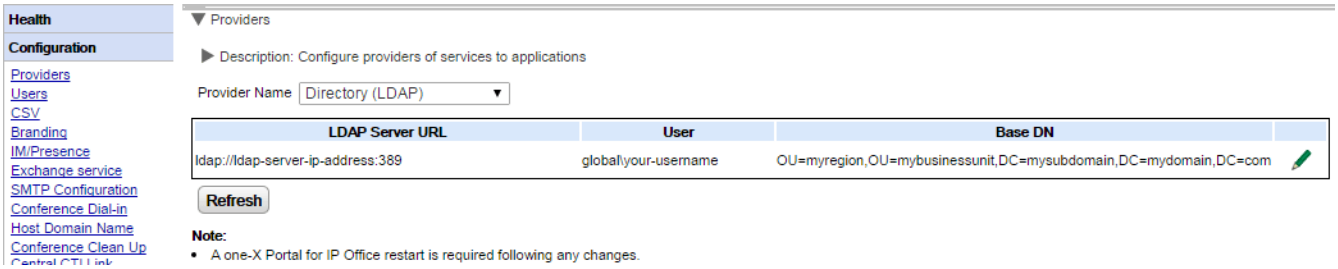
Cualquier cambio en la configuración del proveedor requiere que reinicie el servicio del portal 52.



- **Dirección IP**
  La dirección IP del sistema IP Office.
- **Nombre de usuario**
  El nombre que estableció el usuario del servicio de TCPA en la configuración de seguridad del sistema IP Office. El usuario predeterminado es ***EnhTcpaService***.
- **Contraseña**
  La contraseña establecida para el usuario de servicio de TCPA.
- **Número de puerto**
  El número de puerto en el que el sistema IP Office acepta conexiones.
- **Tiempo de espera**
  El valor de tiempo de espera entre 30 y 600 segundos.
- **Conexión segura**
  Configurar para conectar con el servicio de directorio de sistema telefónico.

2.2.1.3 Proveedor de DSML (LDAP)

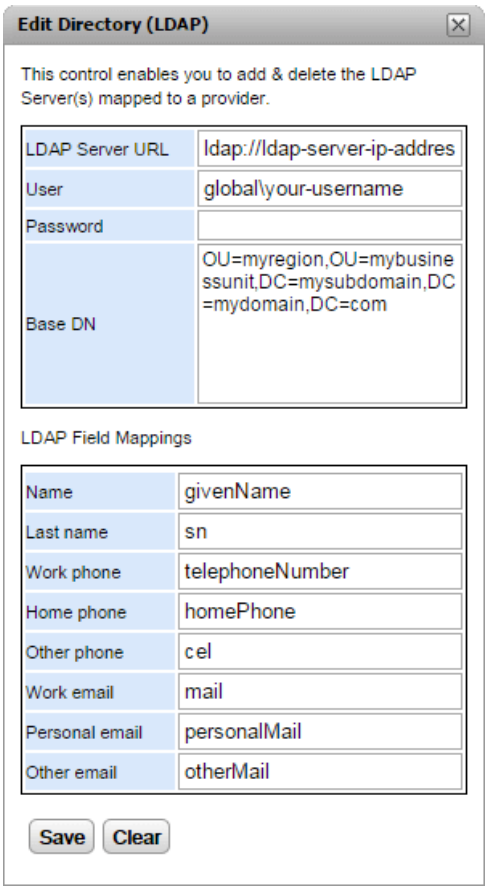
Los valores de configuración que figuran a continuación se muestran para un proveedor de **directorios (DSML LDAP)**.



Para editar el proveedor, haga clic en el icono de edición .

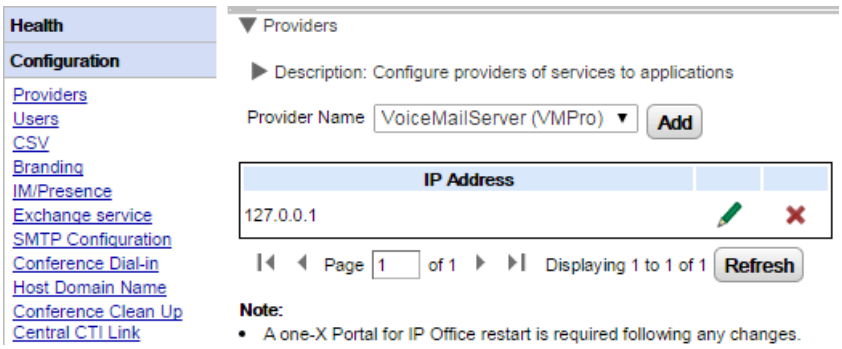
Configuración del proveedor de LDAP

Cualquier cambio en la configuración del proveedor requiere que reinicie el servicio del portal 52.



2.2.1.4 Proveedor de correo de voz

Los valores de configuración que aparecen a continuación se muestran para un proveedor de **VoiceMailServer**.



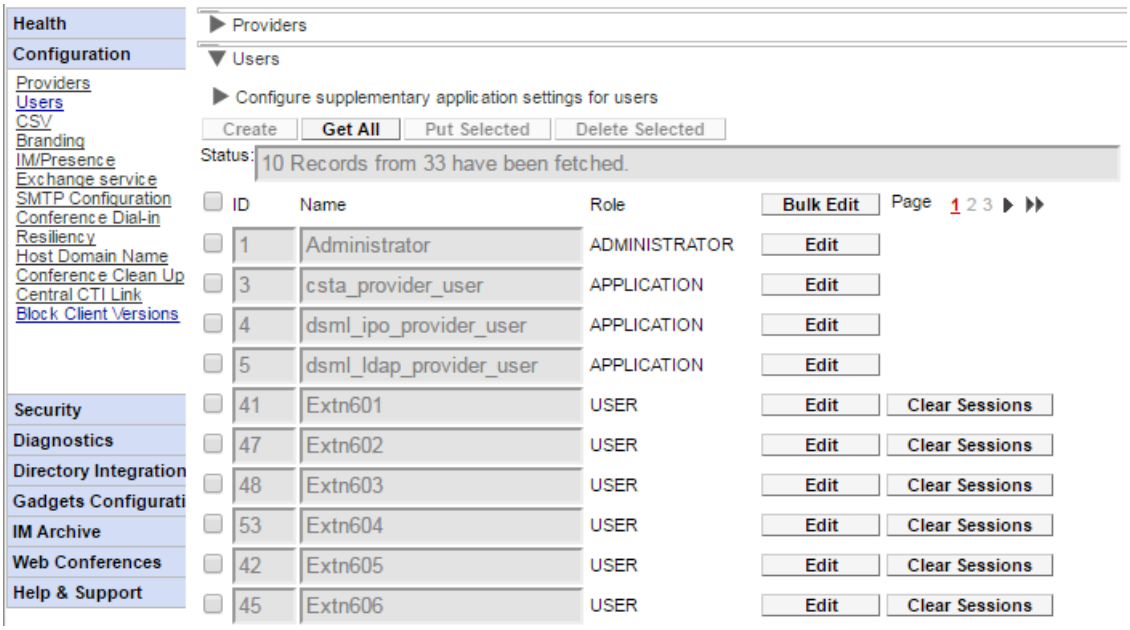
Para editar el proveedor, haga clic en el icono de edición .

Cualquier cambio en la configuración del proveedor requiere que reinicie el servicio del portal 52.

2.2.2 Usuarios

Puede ver los usuarios de IP Office en el menú **Usuarios**. Enumera todos los usuarios de IP Office, y no sólo los habilitados para el funcionamiento de one-X Portal para IP Office. Tenga en cuenta que durante el funcionamiento normal, el servidor del portal solamente vuelve a sincronizar la lista de usuarios conocidos con el sistema telefónico cada 5 minutos.

Puede editar algunas de las configuraciones de usuario almacenadas en one-X Portal para IP Office; para ello, consulte Edición de configuraciones de usuario 66. Puede editar las configuraciones de usuario almacenadas en el IP Office. <<<El botón 'Eliminar' ahora es el botón 'Borrar sesión'>>>

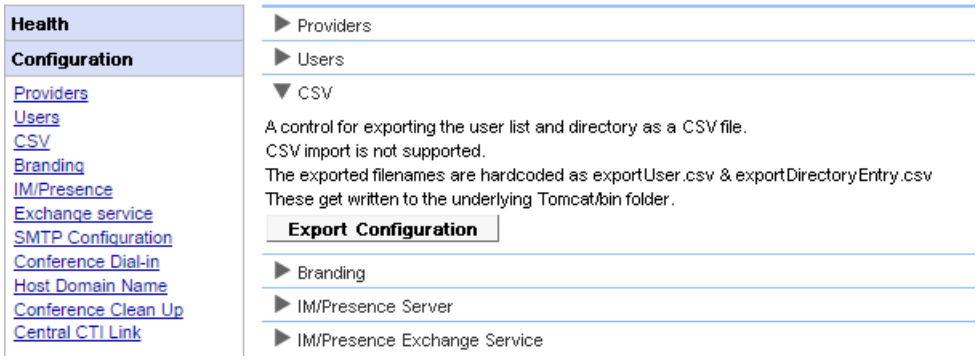


Para ver los usuarios:

1. Haga clic en **Configuración** y seleccione **Usuarios**.
2. Haga clic en **Obtener todo**.
3. El botón **Borrar sesiones** junto a cada usuario puede utilizarse para desconectar a cualquier cliente actualmente conectado que esté ejecutando ese usuario.

2.2.3 CSV

Este menú le permite exportar la información de usuario y los directorios del sistema que utiliza el servidor one-X Portal para IP Office a archivos con formato .csv. Los archivos se exportan a la subcarpeta ***/bin*** del directorio de la aplicación (***C:\Program Files (x86)\Avaya\onexportal\Tomcat\Server\\bin*** de forma predeterminada). Todos los archivos existentes se sobrescriben.

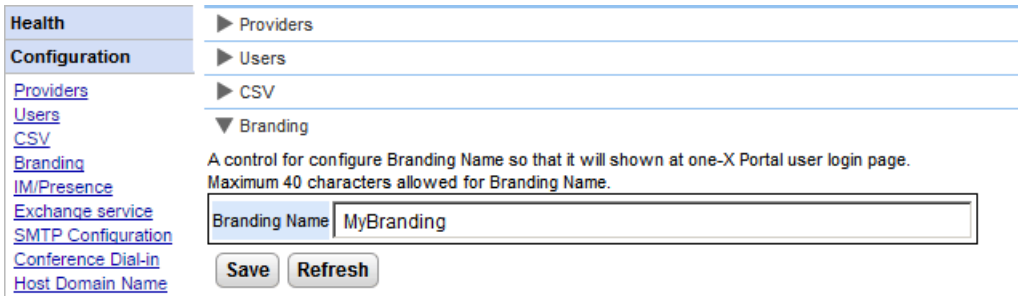


Para exportar:

1. Seleccione **Configuración** y, a continuación, **CSV**.
2. Haga clic en **Exportar configuración**.
3. Se crean dos archivos en la subcarpeta ***/bin*** del directorio de la aplicación. Para los servidores basados en Windows, la ruta por defecto es ***C:\Program Files (x86)\Avaya\onexportal\Tomcat\Server\\bin***. Para los servidores basados en Linux, por defecto es una ruta similar a ***/opt/Avaya/oneXportal/10.1.0_136//apache-tomcat/bin***.
   - ***exportUser.csv***
   - ***exportDirectoryEntry.csv***

2.2.4 Marca

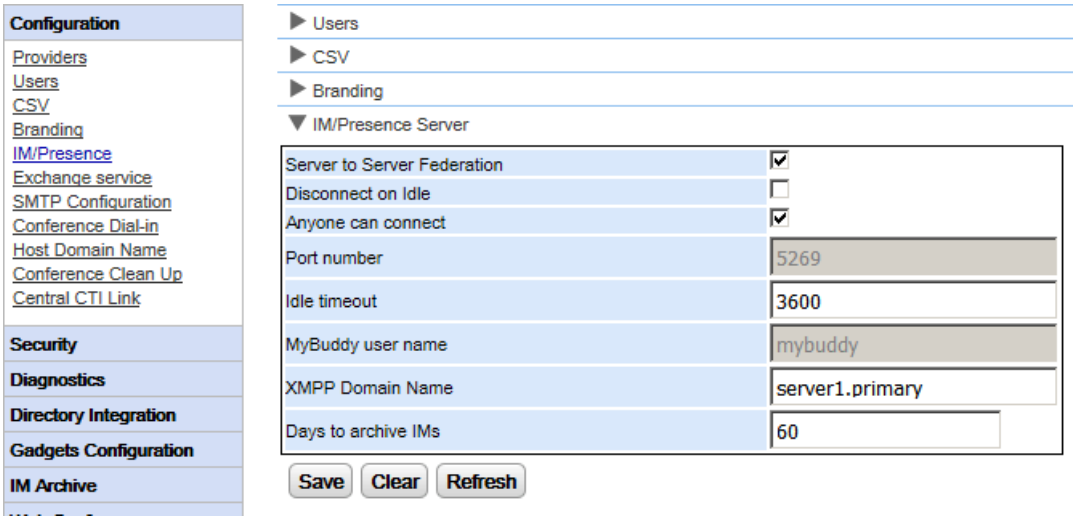
Este menú le permite especificar un texto para que luego se muestre en las páginas de one-X Portal para IP Office una vez que el usuario haya iniciado sesión.



El texto se visualiza en la barra de título de one-X Portal para IP Office tal como se muestra a continuación.

2.2.5 MI/Presencia

El portal incluye un componente que actúa como servidor de mensajería instantánea/presencia. El servidor de MI/Presencia se puede configurar aparte. Consulte Mensajería instantánea/Presencia 76.



Para configurar el servidor de MI/Presencia:

1. Haga clic en **Configuración** y seleccione **Servidor de MI/Presencia**.
2. Seleccione la configuración de servidor requerida:

- **Federación servidor a servidor**
  Si se selecciona, el servidor de presencia del portal puede intercambiar información de presencia con otros servidores de presencia.
- **Desconectar cuando la sesión esté inactiva**
  Si se selecciona, las conexiones de servidor a servidor se desconectan cuando no hay actividad durante el período de **Tiempo de espera en inactividad**.
- **Cualquiera se puede conectar**
  Permite que cualquiera se conecte a los servicios de MI/Presencia.
- **Número de puerto**
  Está establecido como fijo en ***5269***.
- **Tiempo de espera en inactividad**
  El tiempo de espera, en segundos, que se utiliza si se selecciona la opción **Desconectar cuando la sesión esté inactiva**.
- **Nombre de usuario de MyBuddy**
  Este campo está establecido como fijo en ***mybuddy***. Puede requerirse el valor al momento de integrar los detalles de presencia con otros servicios de MI/Presencia.
- **Nombre de dominio de XMPP**
  Establece el nombre de dominio DNS que se utiliza para las funciones de MI/Presencia:
  - El nombre de dominio de XMPP debe ser un nombre de dominio que DNS pueda resolver. Puede establecer el nombre de dominio de XMPP en cualquier momento. El nombre de dominio debe ser accesible desde Internet si desea utilizar presencia fuera de su red LAN; por ejemplo, con one-X Mobile.
  - Avaya recomienda utilizar un DNS dividido de modo que el nombre del servidor fuera de su red LAN sea resuelto en la dirección IP pública de la NAT o firewall mientras que, dentro de la red, se resuelve en la dirección IP privada del servidor de la red LAN.
  - Si no puede establecer un nombre de dominio DNS que se pueda resolver, puede utilizar la dirección IP del servidor de one-X Portal para IP Office para MI/Presencia solo interna. En este caso, one-X Portal para IP Office no puede federar con servidores remotos.
  - Para servidores basados en Linux (IP Office Server Edition, IP Office Application Server y Unified Communications Module), debe utilizar los menús de Web Control del servidor para configurar los parámetros de red de modo que el enlace de correo electrónico de configuración automática utilice el nombre FQDN en lugar de la dirección IP del servidor. En Web Control, diríjase a Configuración > Sistema > Nombre del host para cambiar la configuración de la red. Si cambia el nombre de dominio de cualquier otra manera, puede que los enlaces del correo electrónico no funcionen adecuadamente.
- **Días para archivar MI**
  Este campo configura cuánto tiempo el servidor debería conservar los mensajes en el archivo de MI antes de eliminarlos. La configuración predeterminada es 182 días (6 meses). Si es necesario, puede desactivar el archivado de MI 83 mediante la consola de administrador de XMPP. El servidor de MI/presencia debe estar disponible (consulte Estado del servidor de MI/Presencia 13) para cambiar esta configuración.

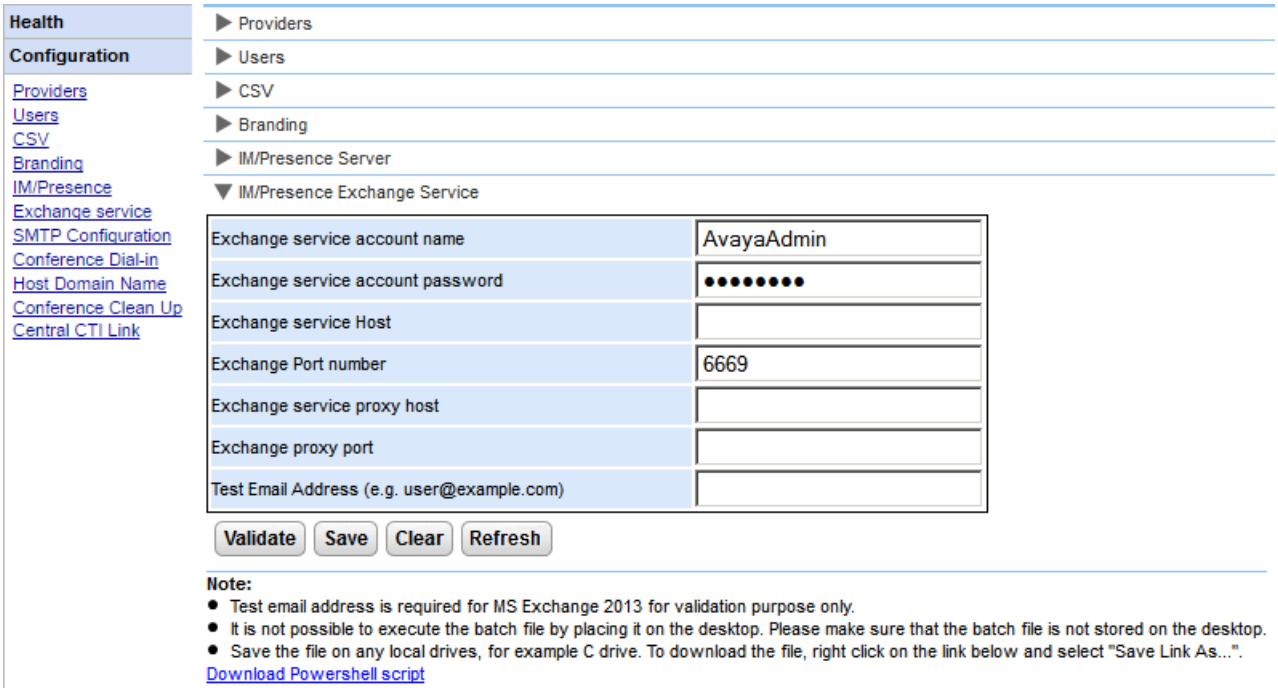
Página930 de 3226.

3. Haga clic en **Guardar**.

2.2.6 Servicio Exchange

one-X Portal para IP Office se puede configurar con el servidor Exchange para validar la información de minería de calendario y de presencia de los usuarios. Solamente Microsoft Exchange Server 2007, 2010 y 2013 se pueden configurar con one-X Portal para IP Office.

En esta sección se ofrece únicamente un resumen de las opciones de configuración. Consulte el manual *Implementar one-X Portal para IP Office* para obtener los detalles completos de la integración del servidor Microsoft Exchange.

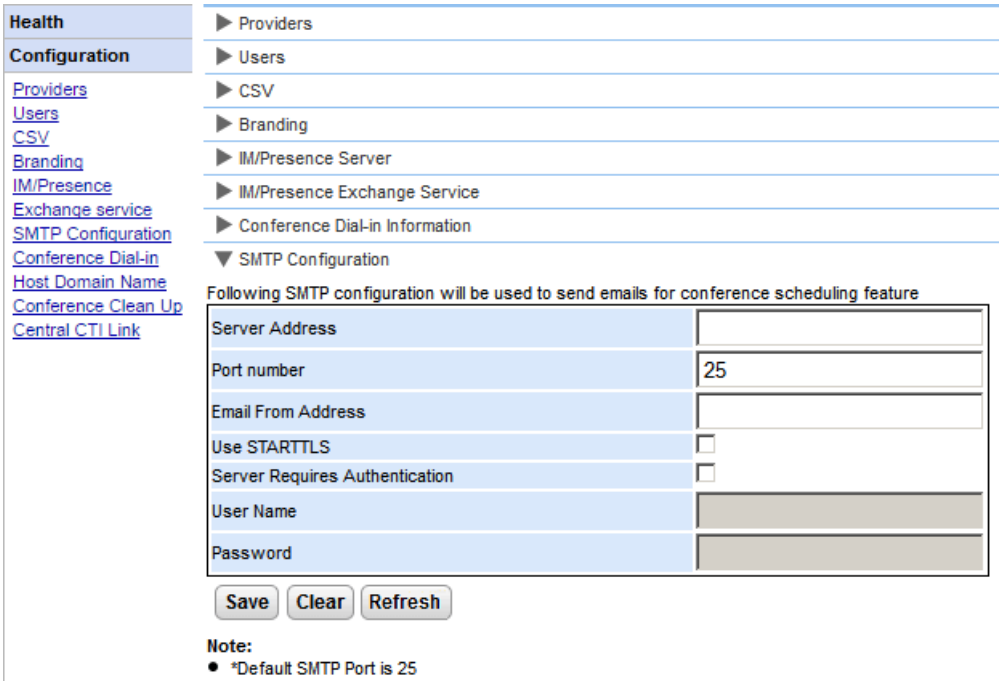


Para configurar servicios de Exchange:

1. Haga clic en **Configuración**, en el panel de navegación izquierdo.
2. Haga clic en **Servicio Exchange**.
   a. Escriba ***AvayaAdmin*** en el campo **Nombre de cuenta para servicio Exchange**. Asegúrese de que este nombre sea el mismo que la cuenta de ***AvayaAdmin*** que creó en el servidor Exchange.
   b. Ingrese la contraseña que se estableció para **AvayaAdmin** en **Contraseña de cuenta para servicio Exchange**.
   c. Ingrese la dirección IP del host del servicio Exchange en **Host de servicio Exchange**.
   d. Ingrese el número de puerto del servicio Exchange en **Número de puerto para Exchange**.
   e. Ingrese el nombre de dominio del servidor proxy que se utiliza para conectarse al servidor Exchange en **Host del proxy para servicio Exchange**.
   f. Ingrese el número de puerto del servidor proxy para el servicio Exchange en **Puerto proxy para Exchange**.
   g. Establezca una **Dirección de correo electrónico de prueba** utilizando una dirección de correo electrónico válida.
3. Haga clic en **Validar configuración del servicio Exchange** para verificar si los detalles de intercambio proporcionados son válidos.
4. Haga clic en **Guardar**.

2.2.7 Configuración SMTP

Las invitaciones a la conferencia para el participante pueden enviarse por mensajería instantánea y también por correo electrónico. En el caso del correo electrónico, la configuración de correo electrónico de conferencia debe realizarse del siguiente modo. La dirección de correo electrónico que se utiliza para cada participante individual se establece en la configuración del sistema telefónico.

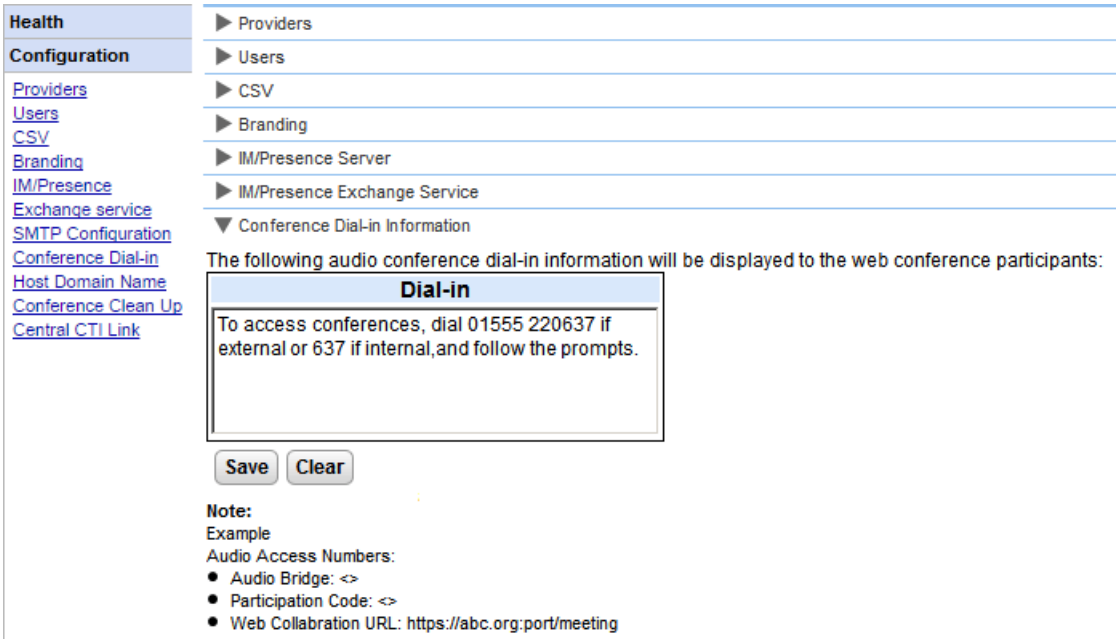


Para establecer el texto fijo de notificación de conferencia:

1. Seleccione **Configuración** y, a continuación, **Configuración SMTP**.
2. Establezca los detalles de correo electrónico SMTP que debe utilizar el servidor:
   - **Dirección del servidor**
     La dirección IP del servidor SMTP del cliente.
   - **Número de puerto**
     El puerto de escucha SMTP del servidor. El valor predeterminado es 25.
   - **Dirección del remitente**
     La dirección que será utilizada por el servidor. Algunos servidores de correo electrónico solo transmiten mensajes de direcciones reconocidas o direcciones con el mismo dominio.
   - **Usar STARTTLS**
     Seleccione este campo para activar la encriptación TLS/SSL. El cifrado permite la integración de correo de voz a correo electrónico con proveedores de correo electrónico alojado que solo permiten SMTP en un transporte más seguro.
   - **El servidor requiere autenticación**
     Si el servidor requiere una cuenta de usuario para recibir y enviar mensajes de email, ingrese los detalles de una cuenta configurada en ese servidor para ser usada por IP Office.
     - **Nombre de usuario**
       El nombre de cuenta que se utilizará si se selecciona El servidor requiere autenticación.
     - **Contraseña**
       La contraseña de cuenta que se utilizará si se selecciona El servidor requiere autenticación.
3. Haga clic en **Guardar**.

2.2.8 Acceso telefónico a conferencias

Cuando un usuario programa una conferencia, el servidor envía a los participantes invitados una notificación de conferencia a través de correo electrónico y mensajería instantánea. Esa notificación contiene los detalles de la conferencia establecidos por el usuario (número de puente, código del participante, URL de colaboración web). Además, puede incluir un texto fijo determinado mediante el menú **Acceso telefónico a conferencias**.



Para establecer el texto fijo de notificación de conferencia:

1. Seleccione **Configuración** y, a continuación, **Acceso telefónico a conferencias**.
2. Ingrese el texto fijo que debe incluirse en todas las notificaciones de conferencia.
3. Haga clic en **Guardar**.

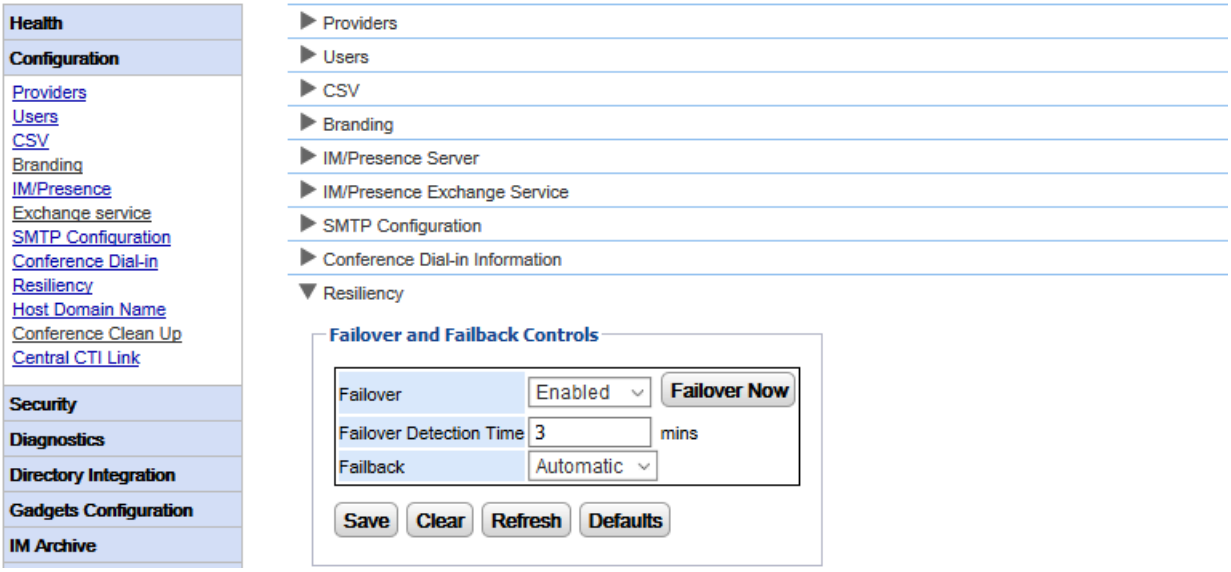
2.2.9 Resistencia

Este menú está disponible en servidores de portal basados en Linux que admiten una red IP Office Server Edition Seleccione. Ofrece ajustes adicionales para el servidor del portal que son necesarios para su participación en la resistencia de dicho servidor. Consulte Resistencia 57.

- En sistemas anteriores que no estaban originalmente en modo Select pero se pasaron a modo IP Office Server Edition Seleccione recientemente, quizás sea necesario reiniciar los servicios del portal para que la configuración de resiliencia esté disponible. De manera similar, es posible que sea necesario reiniciar los servicios del portal después de configurar por primera vez la resistencia del portal en la configuración del sistema IP Office.

Configuración del servidor primario

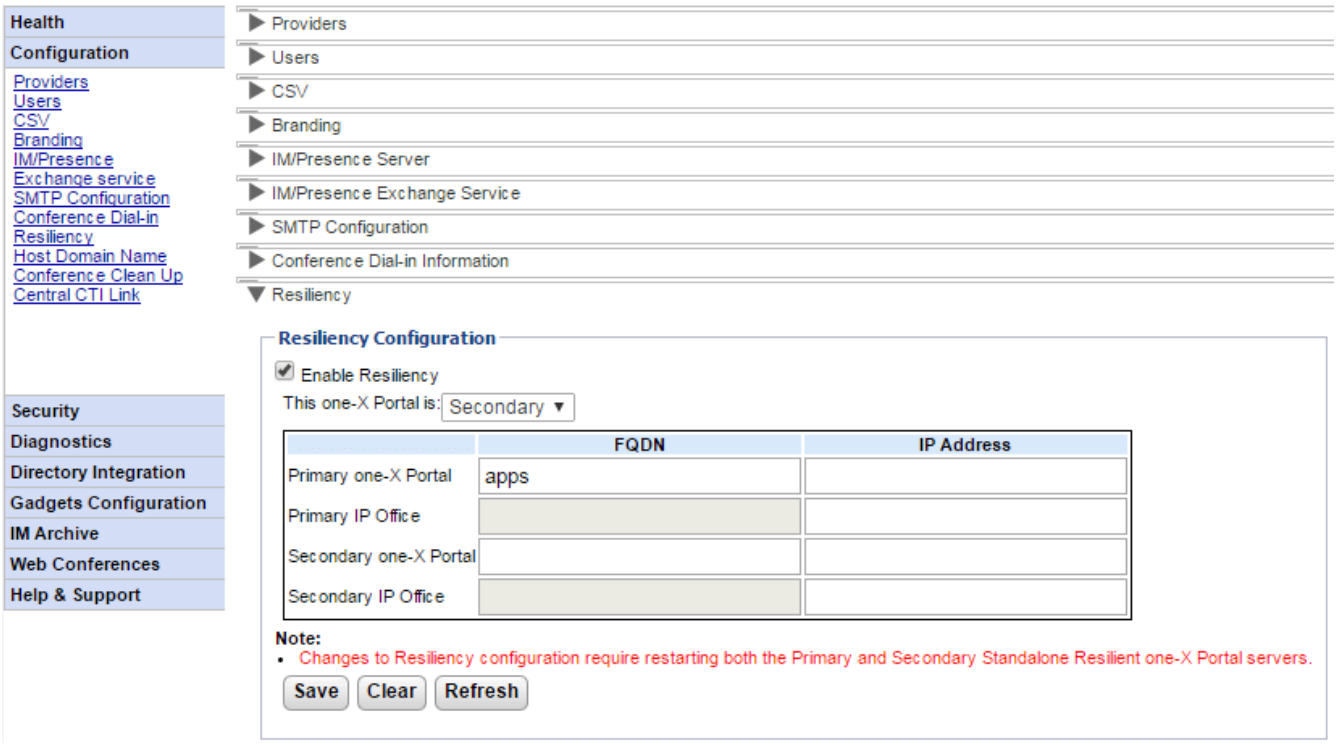
Las opciones de configuración que se muestran en el servidor primario son:



- **Conmutación por error**
  Seleccione si el servidor debe admitir la conmutación por error. Si se activa esta opción, se debe establecer el nombre de dominio del servidor del portal secundario en la forma de un nombre de dominio de host 30.
  - **Conmutación por error ahora**
    Este control se puede usar para iniciar manualmente el proceso de conmutación por error.
- **Tiempo de detección de conmutación por error**
  Establece el tiempo, en minutos, hasta la conmutación por error cuando se detectan problemas potenciales. La configuración predeterminada (3 minutos) impide que se inicie una conmutación por error debido a reinicios de mantenimiento normales de los servicios.
- **Conmutación por recuperación**
  Establece si el proceso de conmutación por recuperación debe iniciar automáticamente cuando fuera posible. Si se configura en manual, es necesario reiniciar los servicios del portal para finalizar la conmutación por recuperación.

Configuración del servidor de aplicaciones

La configuración también aparece en un servidor de aplicaciones. Cuando ese servidor se usa en una red IP Office Server Edition Seleccione, o puede actuar como servidor del portal para el servidor primario o secundario y reemplazar el servicio integrado del portal en ese servidor.



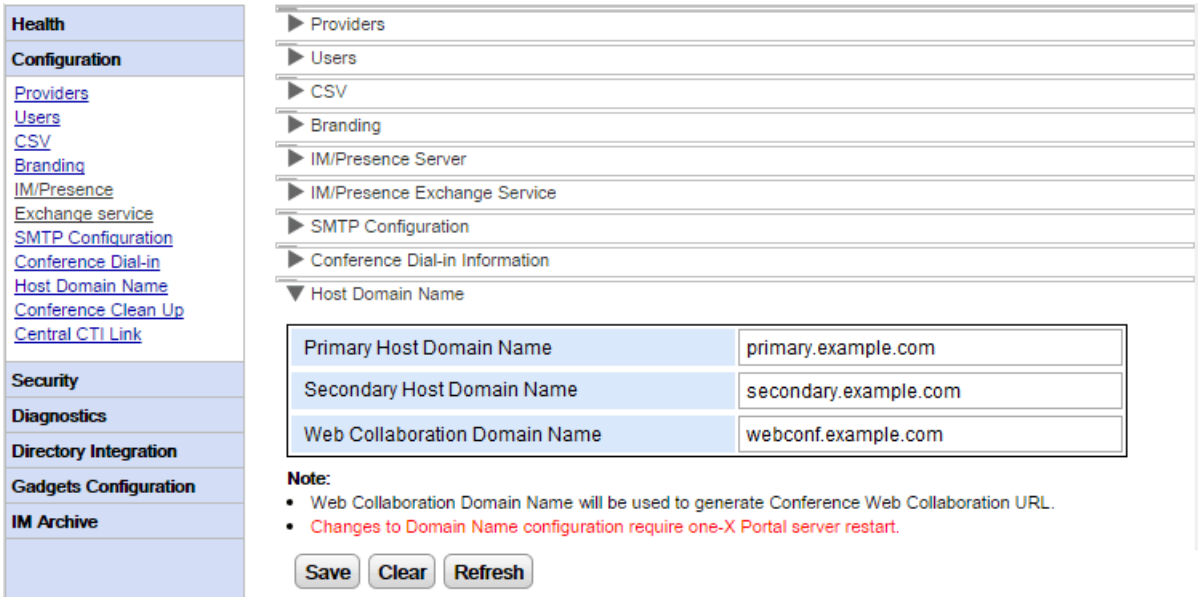
- **Habilitar resistencia**
  Si está seleccionada, la opción activa la resiliencia del portal, muestra los campos adicionales requeridos para definir las direcciones de los otros servidores en la configuración de resistencia y el rol de los servidores. Si no se activa la resistencia, el servicio del portal que tiene lugar en un servidor secundario se detiene automáticamente y no es posible reiniciarlo.
  - **Este one-X Portal:**
    Define el rol de este servidor.
    - **Primario**
      Seleccionar si este servidor va a actuar como servidor primario del portal.
    - **Secundario**
      Seleccionar si este servidor va a actuar como servidor de respaldo/reserva si el portal primario no está disponible.
- **FQDN/Dirección IP**
  Use esta tabla para introducir los nombres completos de dominio o direcciones IP de todos los portales y servidores IP Office del conjunto de resistencia.

2.2.10 Nombre de dominio de host

El menú**Configuración | Nombre de dominio del host** se usa para establecer el nombre de dominio utilizado para acceder a los servicios del portal y entre servidores del portal. La cantidad de nombres de dominio requeridos dependen del tipo de servidor de portal.

También se utiliza para establecer la URL del servicio de colaboración web. La URL de colaboración web se usa como predeterminada para invitaciones a conferencia cuando se programa una conferencia.

Tenga en cuenta que se si cambian los nombres de dominio, se debe reiniciar el servicio del portal para que los cambios surtan efecto.

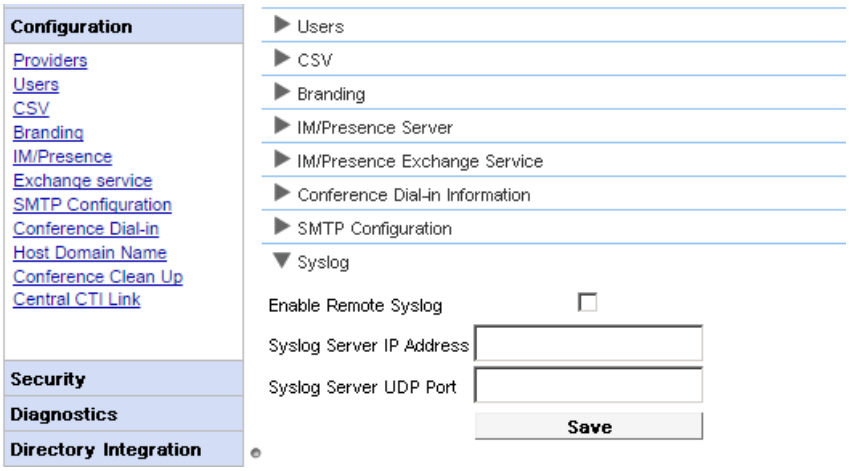


2.2.11 Syslog

Se muestra solamente para servidores basados en Windows. En el caso de los servidores basados en Linux, los informes Syslog se administran a través de los menús de Web Manager de IP Office del servidor.

Este menú permite activar los informes Syslog. El servidor admite informes de:

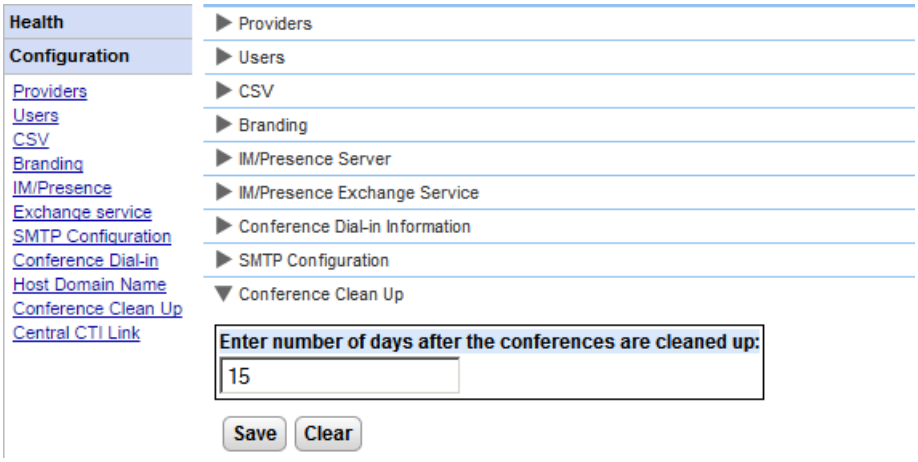
- Inicios de sesión de usuario y administrador, lo que incluye intentos de inicio de sesión fallidos.
- Inicios y detenciones del componente OpenFire utilizado por la aplicación del portal.



- **Activar Syslog remoto**
  Si se selecciona esta opción, se activa el envío de informes Syslog a los detalles de servidor remoto especificados.
- **Dirección IP del servidor Syslog**
  Establece la dirección IP de destino o el nombre de dominio del servidor que puede recibir los informes Syslog.
- **Puerto UDP del servidor Syslog**
  Establece el puerto en el que el servidor remoto escucha los informes Syslog.

2.2.12 Limpieza de conferencia

Este menú permite configurar la cantidad de días durante los cuales el servidor conservará los detalles de conferencia. Esta opción no es compatible con el servidor basado en Windows.



2.2.13 Enlace de CTI central

Los servidores del portal IP Office Server Edition pueden usar el modo CTI centralizado. En este modo, el servicio del portal solo se debe vincular a un sistema de IP Office basado en Linux para brindar servicios a todos los sistemas IP Office de la red. Esto incluye que se utilice IP Office Application Server con IP Office Server Edition. Esta opción no está disponible para los servidores basados en Windows o en UCM ni para IP Office Application Server compatible con IP500 V2.

En el modo de Enlace de CTI central, el servicio del portal brinda servicios de llamadas automáticamente a todos los sistemas IP Office de la red. Obtiene entradas de directorio del sistema de todos los sistemas y automáticamente de sistemas agregados o quitados de la red. Además, el portal obtiene información automáticamente del servidor central de correo de voz.

- **Enlace de CTI central**
  Esta configuración se usa para activar o desactivar el modo de CTI centralizado. Tenga en cuenta que el servicio de one-X Portal para IP Office se debe reiniciar si se cambia la configuración.
  - **Si se activa:**
    Cuando se activa esta configuración, el servicio del portal usa el modo de CTI centralizado. Esto significa lo siguiente:
    - El portal se conecta solo con un sistema de IP Office. Los proveedores de CSTA y DSML se crean solo para ese sistema. Sin embargo, las conexiones con ese sistema se usan para obtener información y brindar servicios a todos los demás sistemas de IP Office de la red.
    - El enlace al sistema IP Office también se utiliza para detectar la configuración del servidor de correo de voz y crear automáticamente el proveedor necesario.
    - Si también está habilitadoresiliencia de IP Office Server Edition 57, los proveedores de CSTA se crean para el sistema de IP Office primario y secundario.
    - Cada sistema IP Office individual que detecta el servidor del portal se muestra en el menú **Estado de los componentes** 13.
    - El portal obtiene la información del servidor IP Office y los directorios del sistema de parte del sistema de IP Office primario.
    - Los registros del directorio personal se siguen obteniendo desde el sistema IP Office host de cada usuario.
  - **Si se desactiva:**
    Cuando esta configuración no está activada, ocurre lo siguiente:
    - Los proveedores de CSTA y DSML se deben configurar manualmente cada sistema IP Office de la red. Esto se hace durante la instalación o mediante los menús de **Proveedores** 17. Sin embargo, el proveedor de correo de voz se aprovisiona automáticamente en función de información del sistema IP Office conectado.
    - Esta es la configuración predeterminada para el sistema actualizado a la versión 10 de IP Office.

Aprovisionamiento automático

Los sistemas actualizado de la versión 9.1 muestran la configuración original de **autoaprovisionamiento** y la utilizan en lugar de **Enlace de CTI central**. Si se habilita el **Aprovisionamiento automático**, se usa el proveedor de CSTA inicial para crear automáticamente proveedores adicionales y mantener proveedores CSTA y DSML para los demás sistemas de la red. En la versión 10.0, el proveedor de correo de voz también está configurado automáticamente mediante la información del sistema telefónico.

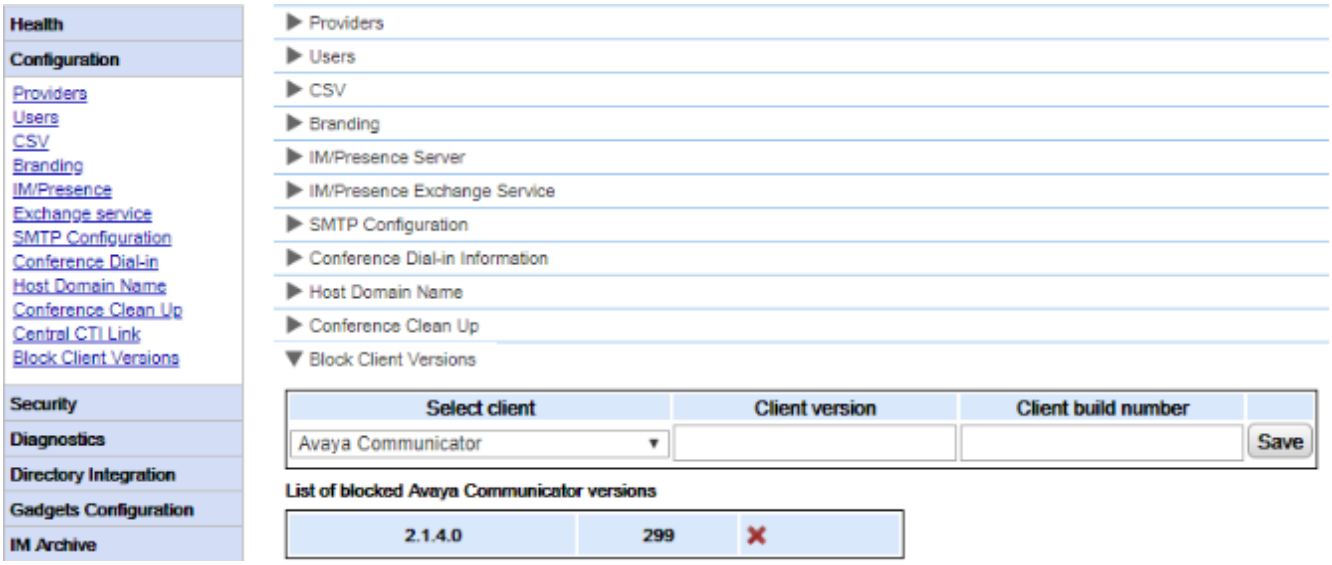
Los sistemas que utilizan **autoaprovisionamiento** se pueden convertir mediante **Enlace de CTI central** si se hace clic en el botón **Convertir al enlace de CTI central**. Este proceso no se puede revertir.

2.2.14 Bloquear versiones del cliente

Este menú puede utilizarse para crear una lista de versiones del cliente que no serán compatibles con el servidor del portal. Para realizar esto, agregue la versión y compilación del cliente a las listas de clientes bloqueados.

Los clientes bloqueados no pueden iniciar sesión. Los clientes que ya están conectados seguirán trabajando hasta que cierren sesión.

Para cada cliente, pueden bloquearse un máximo de 15 combinaciones de versiones/compilaciones.



Para agregar un nuevo cliente bloqueado:

1. Utilice el menú desplegable **Seleccionar cliente** para seleccionar al cliente.
2. Ingrese los valores de número **Versión del cliente** y **Compilación del cliente**. Deben configurarse ambos valores.
3. Haga clic en **Guardar**.

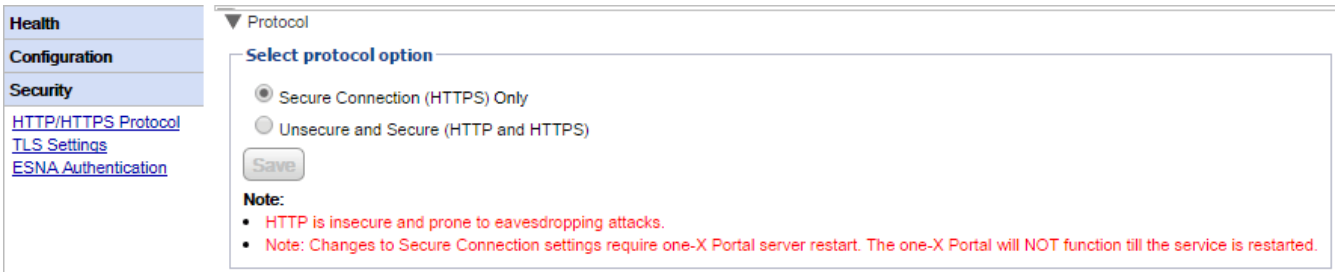
Para eliminar un cliente bloqueado:

1. Haga clic en el icono de cruz.

2.3 Seguridad

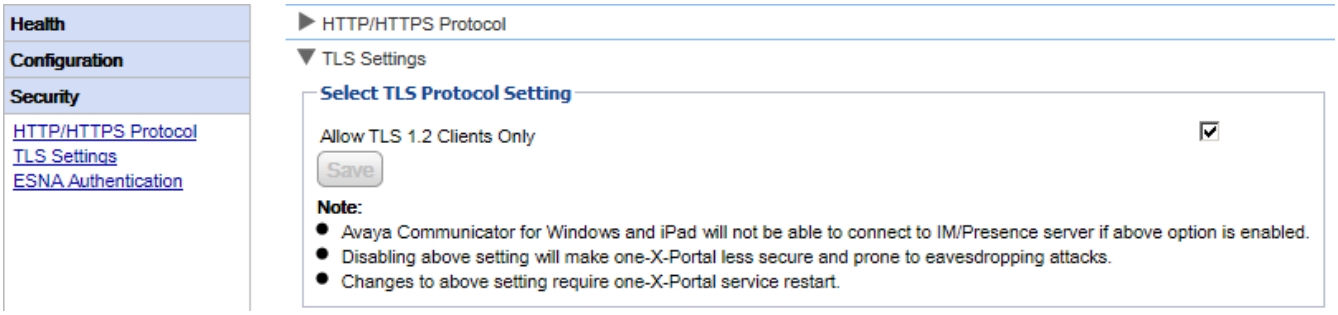
2.3.1 Protocolo HTTP/HTTPS

De manera predeterminada, la instalación del servidor admite únicamente acceso HTTPS encriptado; es decir, puerto 9443 en un servidor Linux y puerto 8443 en un servidor Windows. Este menú también se puede utilizar para habilitar el acceso HTTP en el puerto 8080.



2.3.2 Configuración TLS

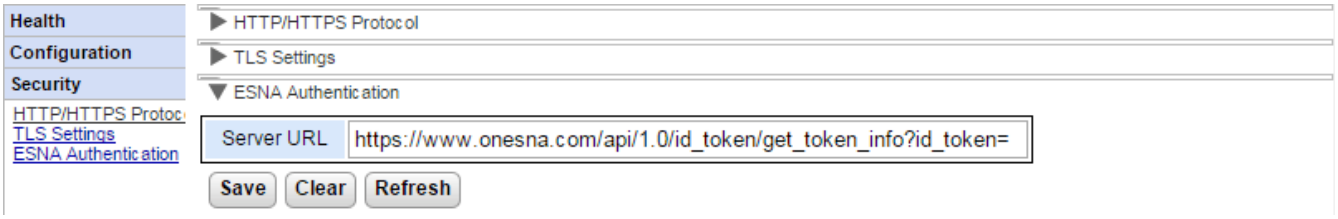
El servidor del portal admite la conexión de usuarios y aplicaciones mediante TLS. Esto se puede restringir a las conexiones que utilizan TLS 1.2.



- **Permitir solo clientes TLS 1.2**
  Si está activado, la compatibilidad TLS provista por el portal se restringe a TLS 1.2. Si se cambia la configuración, deberá reiniciar el servicio del portal [52] para que surta efecto el cambio.
  - Tenga en cuenta que las aplicaciones de cliente Avaya Communicator actuales no admiten TLS 1.2 y, por lo tanto, no podrán conectarse si esta opción está habilitada.

2.3.3 Autenticación ESNA

Los usuarios que se conectan mediante una cuenta ESNA deben autenticarse a través de los servidores propios de ESNA.

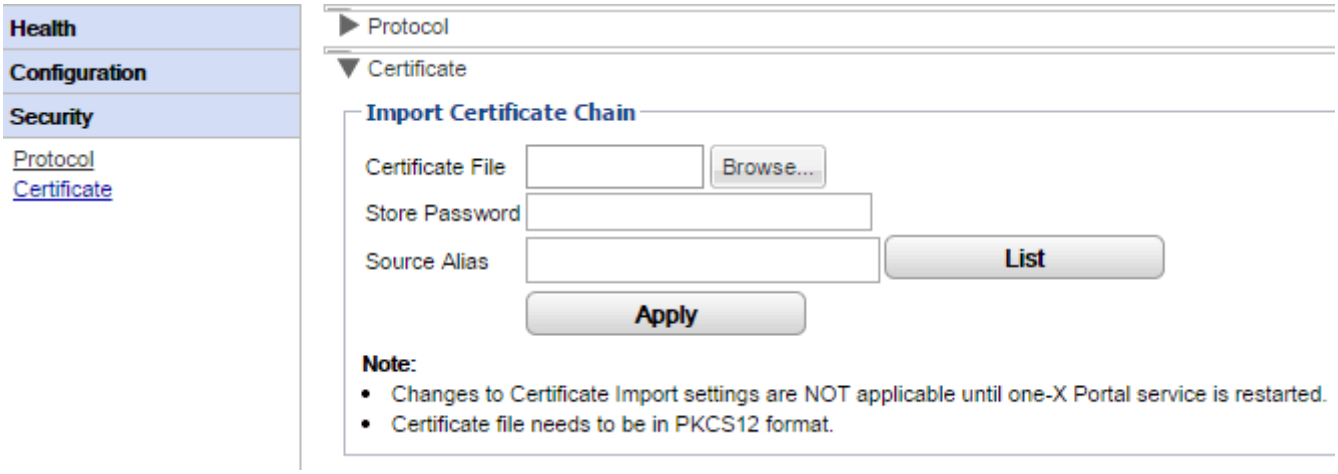


- **URL del servidor**
  Este campo configura la URL del servidor para las solicitudes de autenticación de usuario redireccionadas a ESNA.

2.3.4 Certificado

Solamente para servidores basados en Windows. En el caso de los servidores basados en Linux, los certificados se controlan a través de los menús de Web Manager de IP Office del servidor.

Este menú permite al portal importar un certificado de acceso cifrado. Esto es necesario para aplicaciones que desean utilizar una conexión TLS encriptada con el portal, por ejemplo, Avaya Communicator.

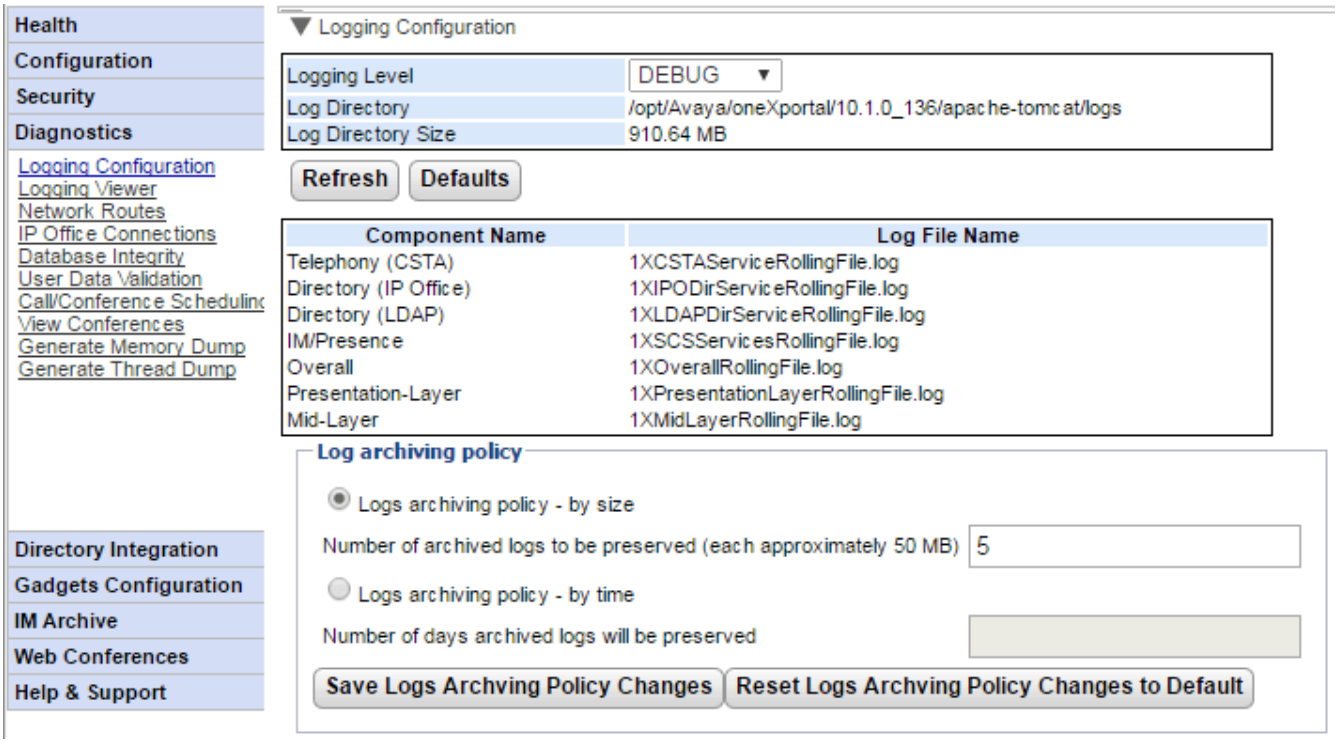


2.4 Diagnóstico

Esta sección permite ejecutar distintas comprobaciones de diagnóstico.

2.4.1 Configuración de registros

one-X Portal para IP Office es compatible con una amplia variedad de métodos de información de registro, y es necesario seleccionar el nivel de registro.



- **Nivel de registro maestro**
  Este campo se utiliza para seleccionar el nivel mínimo de eventos que se registran o para inhabilitar cualquier registro con solo seleccionar ***Desactivar***.
- **Directorio de registro**
  El directorio donde el servidor guarda los archivos de registro. No variable.
- **Tamaño del directorio de registro**
  El tamaño total actual de los archivos de registro.
- **Actualizar**
  Cuando se hace clic, se actualiza la información que se muestra.
- **Predeterminado**
  Cuando se hace clic, el nivel de registro maestro vuelve a su valor predeterminado. La configuración predeterminada es ***ERROR*** excepto en los servidores de Unified Communications Module, donde el valor predeterminado es ***Desactivado***.
- **Descripciones del archivo de registro:**
  En esta tabla, se muestran los archivos de registro que usan los distintos componentes de one-X Portal para IP Office.
  - **Telefonía (CSTA):** *1XCSTAServiceRollingFile.log*
    Este registro captura información de telefonía. Esto incluye obtener información de usuario y licencias de las unidades de IP Office
  - **Directorio (IP-Office):** *1XIPODirServiceRollingFile.log*
    Este registro captura información de directorios de IP Office.
  - **Directorio (LDAP):** *1XLDAPDirServiceRollingFile.log*
    Este registro captura información de directorios de LDAP.
  - **MI/Presencia:** *1XSCSServicesRollingFile.log*
    Este registro captura información de IP Office MI y Presencia.
  - **General:** *1XOverallRollingFile.log*
    Es un archivo de registro general de todos los tipos de eventos registrados.
  - **Capa de presentación:** *1XPresentationLayerRollingFile.log*
    Este registro captura información de la actividad del navegador del usuario/

Página941 de 3226.

- **Capa intermedia:** *1XMidLayerRollingFile.log*
  Este registro captura la interacción entre los diversos componentes de one-X Portal para IP Office, incluidas las unidades de IP Office.

- **Política de archivo de registros**
  Esta configuración permite definir cómo controlará la conservación de archivos de registro el servidor. Por defecto se conservan los últimos 5 archivos de registro.

  - **Política de archivo de registros - por tamaño**
    Si se selecciona esta opción, se usa la configuración cantidad de archivos de registro para determinar qué archivos se conservan. Cuando se crea un archivo nuevo (los archivos se renuevan automáticamente cuando alcanzan aproximadamente los 50 MB), el archivo más antiguo se borra automáticamente si se ha excedido la cantidad de archivos que se deben conservar.

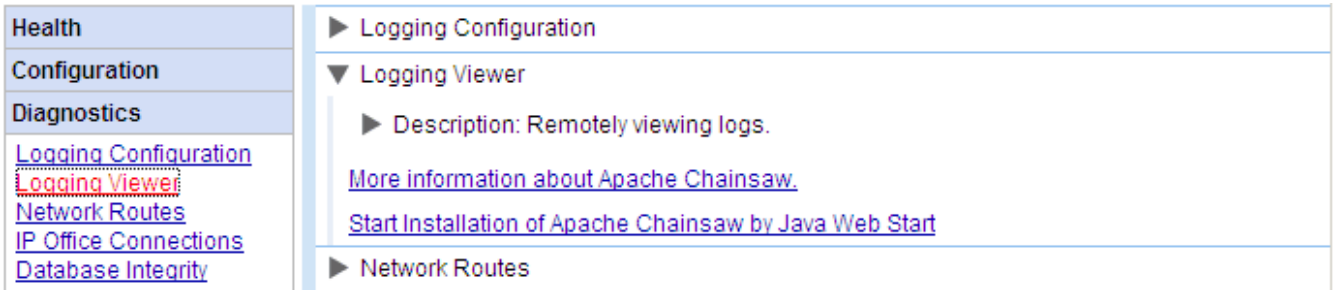
    - **Cantidad de registros archivados para conservar**
      Establece la cantidad de archivos que se debe conservar si se selecciona **Política de archivo de registros - por tamaño**. La configuración predeterminada es 5 archivos.

  - **Política de archivo de registros - por tiempo**
    Si se selecciona esta opción, se usa la antigüedad del archivo en días para determinar qué archivos se conservan. Los archivos más antiguos se borran automáticamente.

    - **Cantidad de días que se conservarán los registros almacenados**
      Establece la cantidad de días que se debe conservar un archivo de registro si se selecciona **Política de archivo de registros - por tiempo**. La configuración predeterminada es 5 días.

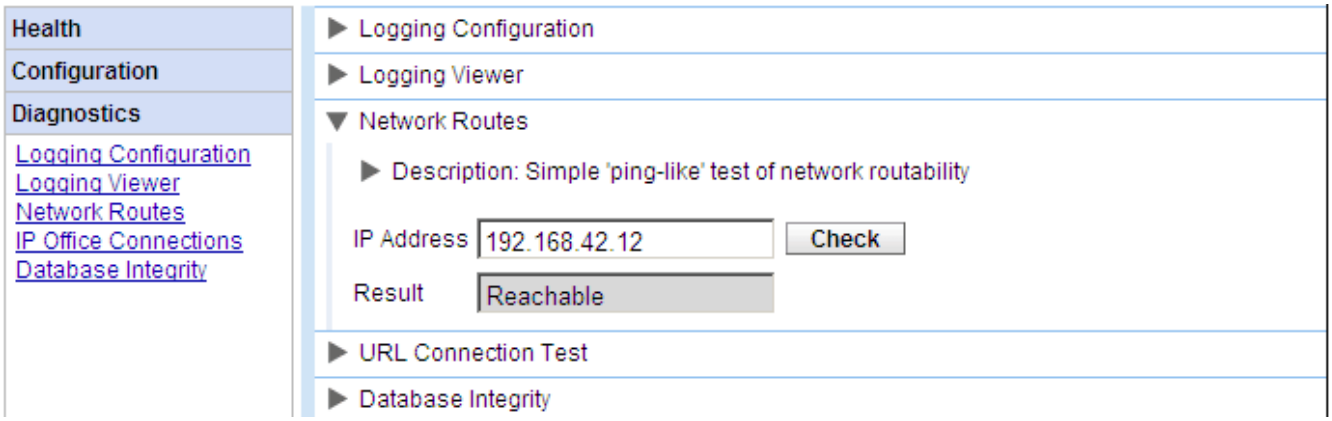
2.4.2 Visor de registros

Además del registro en archivos, la información de mensajes de registro proporcionada por los componentes de one-X Portal para IP Office también puede verse a través de una aplicación de registro remoto que admite el formato Log4j. El menú **Diagnóstico | Visor de registros** ofrece enlaces para obtener información e instalar Apache Chainsaw 89, que es una aplicación de registro apropiada.



2.4.3 Rutas de red

Este menú puede utilizarse para evaluar la ruta del servidor one-X Portal para IP Office a una dirección de IP Office. Utiliza el puerto de TCP 7 (servicio "Echo service") en la dirección IP de destino. Cabe destacar que esto no funciona con unidades de control de IP Office, para las que deben utilizarse las Conexiones de IP Office 38.

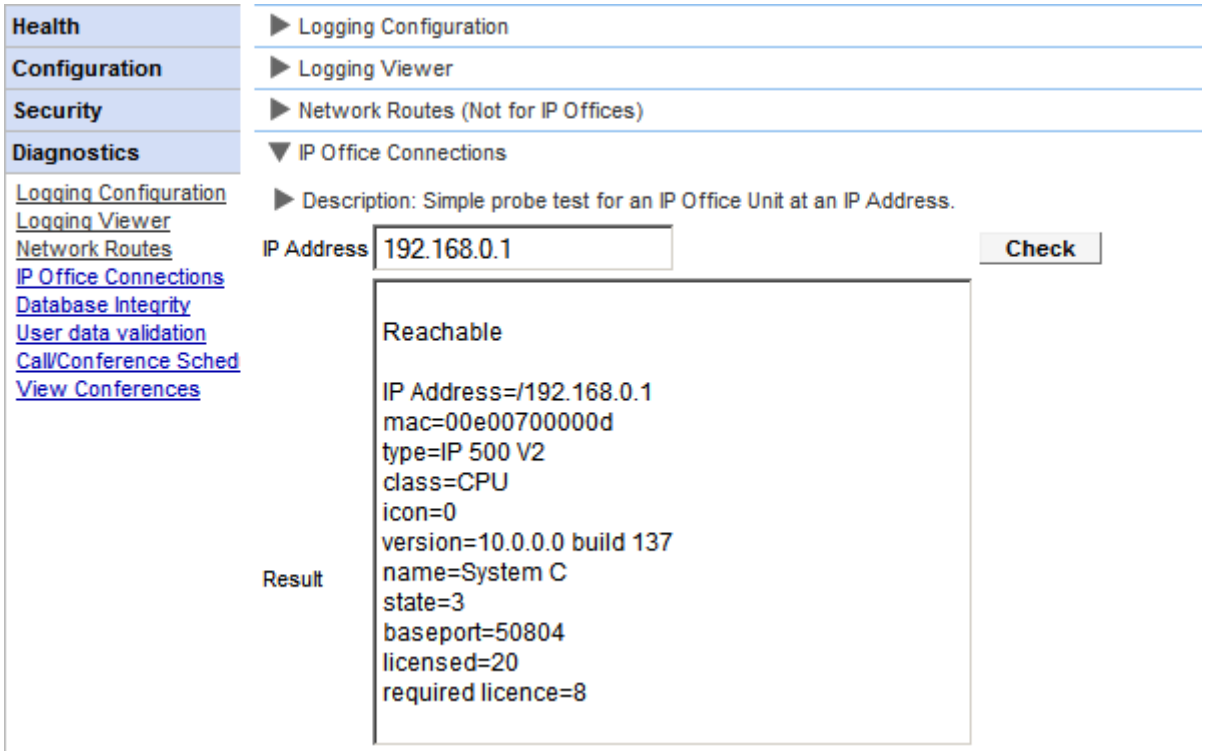


Para comprobar una ruta de red:

1. Seleccione **Diagnóstico** y, a continuación, **Rutas de red**.
2. Ingrese la **Dirección IP** de la unidad de destino y haga clic en **Verificar**.
3. El servidor one-X Portal para IP Office informará si la unidad de destino es ***Accesible*** o ***No accesible***.

2.4.4 Conexiones de IP Office

Este menú puede utilizarse para verificar la conexión entre el servidor one-X Portal para IP Office y una unidad de IP Office en particular. La verificación de la conexión emplea el método de búsqueda estándar que utilizan las aplicaciones IP Office como IP Office Manager (conexión al puerto 50804 de la unidad de control de IP Office).

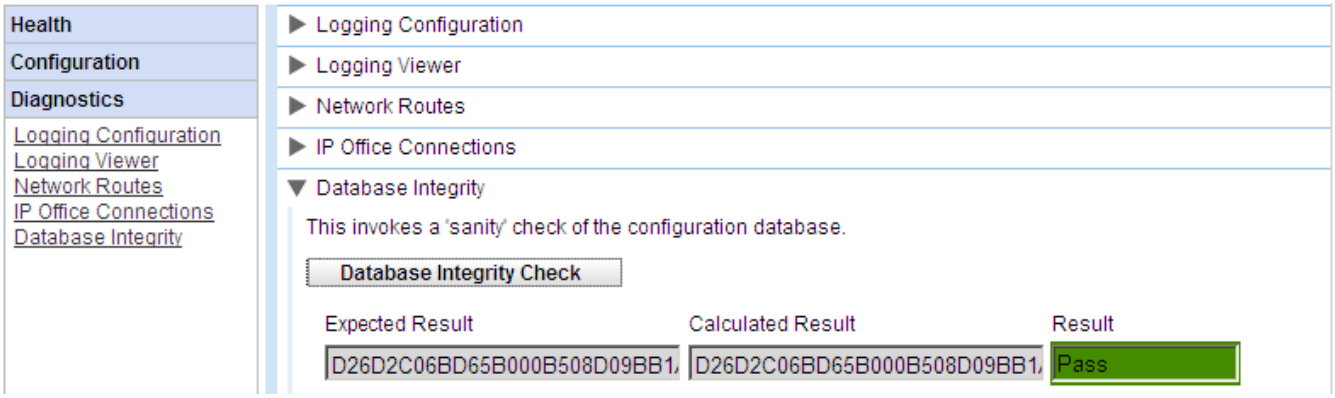


Para realizar la prueba de conexión de IP Office:

1. Seleccione **Diagnóstico** y, a continuación, **Conexiones de IP Office**.
2. Ingrese la **Dirección IP** de la unidad de IP Office de destino y haga clic en **Verificar**.
3. Si es posible acceder a IP Office, los resultados incluirán información básica sobre el sistema IP Office.

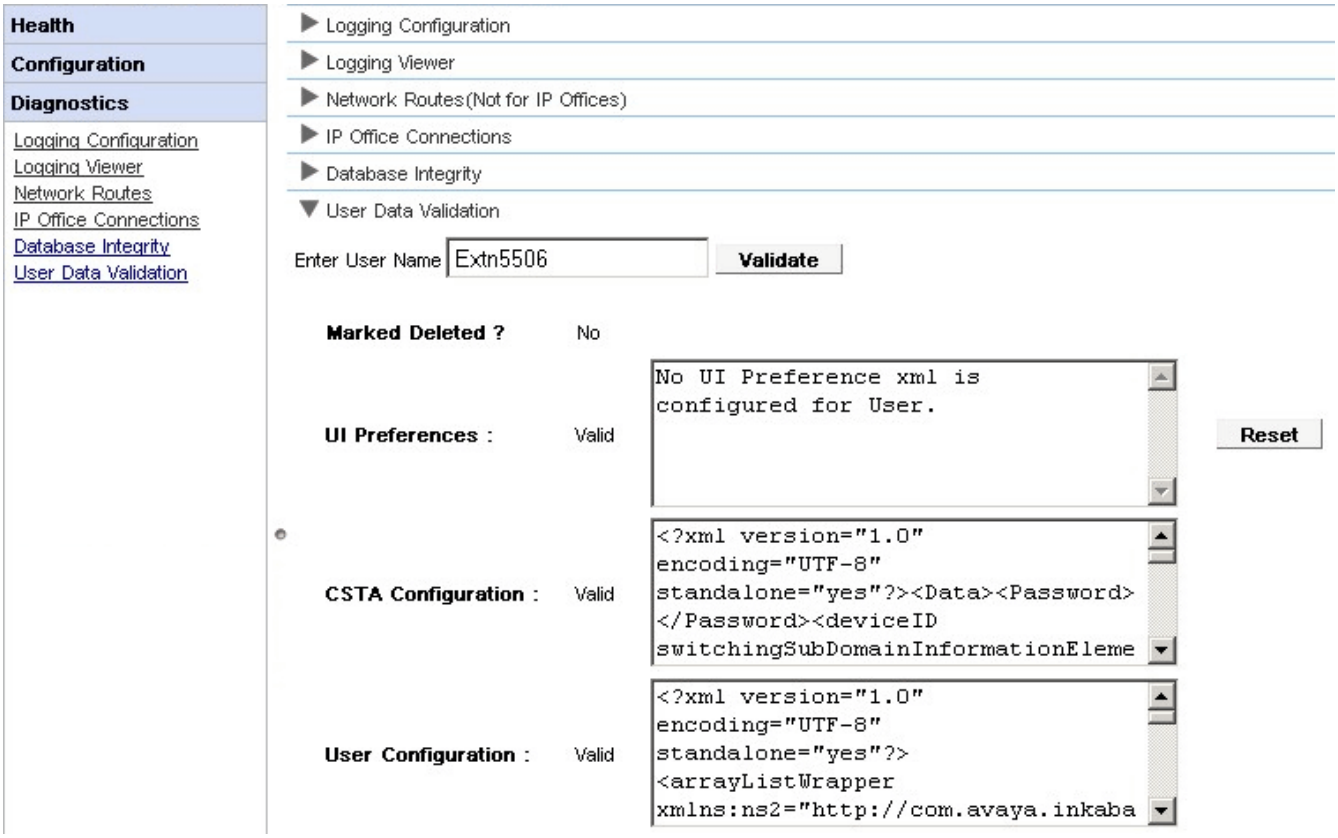
2.4.5 Integridad de base de datos

Este menú puede utilizarse para verificar la estructura de la base de datos. Mostrará el resultado **Aprobado** si las tablas y los campos de la base de datos son los correspondientes para la versión de one-X Portal para IP Office. No verifica los datos dentro de los campos. Si se informa el resultado **Desaprobado**, consulte la sección Solución de problemas 93 para obtener información sobre problemas conocidos y soluciones.



2.4.6 Validación de datos de usuario

El administrador y el grupo de asistencia técnica para redes troncales de Avaya pueden identificar la causa de fallo en el inicio de sesión de usuario o de daño de datos de usuario y restablecer los datos dañados mediante la función de diagnóstico en one-X Portal para IP Office.

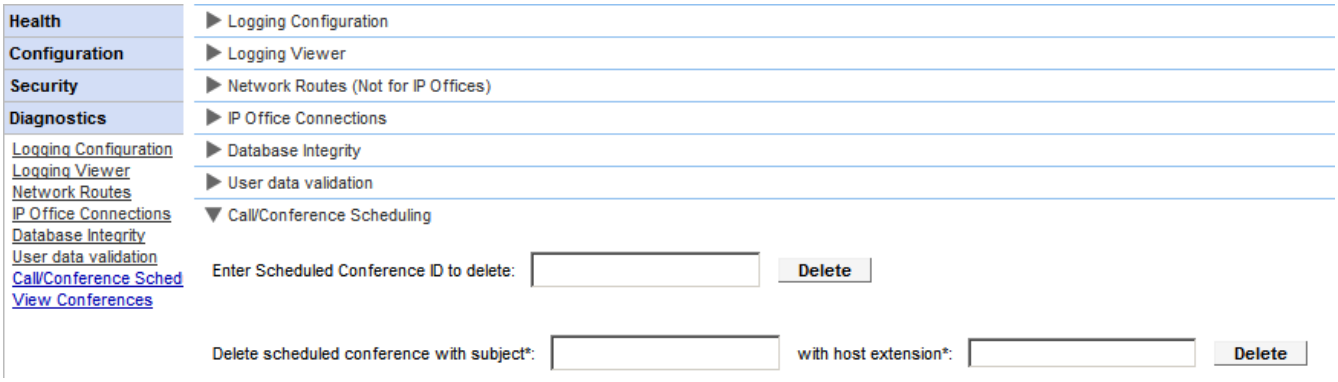


Para ver la validación de datos del usuario:

1. En la interfaz de administrador de one-X Portal para IP Office, haga clic en **Diagnóstico**.
2. Seleccione **Validación de datos de usuario** para ver el formulario correspondiente a la derecha.
3. **Ingrese el Nombre de usuario** de quien se quiere validar los datos. Este campo tiene la opción de completado automático como un menú desplegable.
4. Haga clic en **Validar**. El sistema valida ciertos campos de datos del usuario en la base de datos y muestra el resultado. Los campos validados son:
   - **Marcado como eliminado:** Si el registro del usuario está marcado como eliminado o no.
   - **Preferencias de IU:** Si los datos de preferencia de la IU son válidos o no respecto al XML correspondiente. Hay un botón para **restablecer** los datos si sufrieron daños. Las preferencias de la IU se restauran con la configuración predeterminada de fábrica. El usuario tiene que volver a iniciar sesión para acceder a one-X Portal para IP Office.
   - **Configuración de CSTA:** Si la configuración de CSTA es válida o no respecto al XML correspondiente.
   - **Configuración de usuario:** Si los datos de configuración del usuario son válidos o no respecto al XML correspondiente.

2.4.7 Programación de llamadas/conferencias

Puede eliminar una conferencia futura programada. Si la conferencia es recurrente, se eliminan todas las instancias de la conferencia. Esta opción no se admite en los servidores basados en Windows.

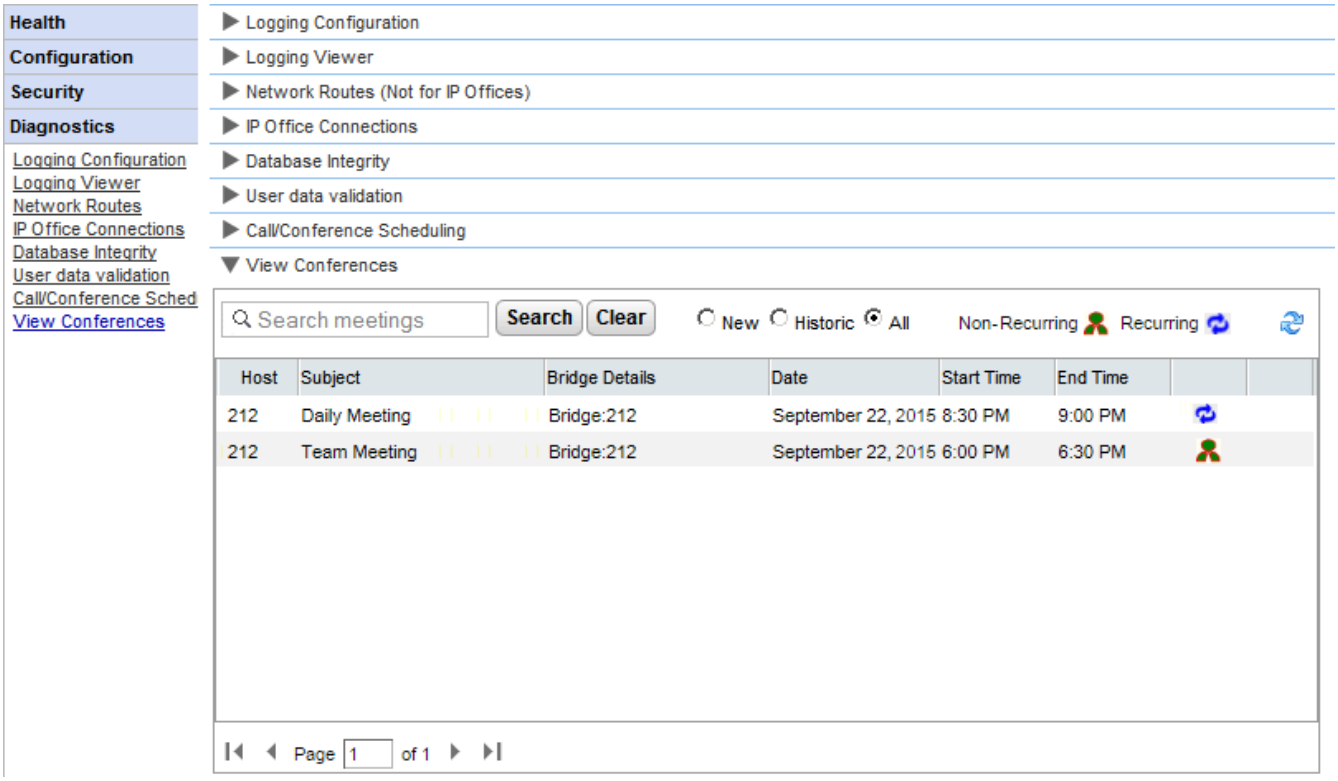


Para eliminar una o varias conferencias programadas:

1. Haga clic en **Diagnóstico** y seleccione **Programación de llamadas/conferencias**.
2. Ingrese la extensión del host y un asunto. Si deja el asunto vacío, se borran todas las conferencias que programó el host.
3. Haga clic en **Eliminar**.

2.4.8 Visualización de conferencias

En este menú, se muestra el calendario para la conferencia programada similar al que ven y utilizan los usuarios individuales de one-X Portal para IP Office. No obstante, la diferencia es que muestra las conferencias programadas para todos los usuarios. Puede utilizar este menú para eliminar una conferencia programada y modificar los detalles de conferencias futuras. Esta opción no se admite en los servidores basados en Windows.



2.4.9 Volcar memoria

Para diagnosticar problemas, Avaya puede solicitar un vuelco de memoria. Este menú crea un archivo de registro del vuelco de memoria del estado de funcionamiento actual del servidor. El archivo se nombra segúna la fecha y la hora, a las que se agrega el sufijo **.hprof**.

La ubicación del archivo depende del tipo de servidor del portal.

- **Servidor basado en Windows:** *C:\Program Files (x86)\Avaya\onexportal\Tomcat\Server\logs*
- **Servidores basados en Linux:**
  - **Unified Communications Module:** */var/log/One-X*
  - **Otros servidores basados en Linux:** */opt/Avaya/oneXportal/<one-X version>/apache-tomcat/logs*

En los servidores basados en Linux, cualquier archivo existente de vuelco de memoria se incluye en los archivos de registro que se pueden descargar de los menús de visualización de control/plataforma web del servidor (**Registros | Descargar**).

2.4.10 Volcar subprocesos

Para diagnosticar problemas, Avaya puede solicitar un vuelco de subprocesos. Este menú crea un archivo de registro del vuelco de subprocesos del estado de funcionamiento actual del servidor. El archivo se denomina ***onex_thread_dump*** junto con la fecha y la hora y el sufijo **.log**.

La ubicación del archivo depende del tipo de servidor del portal.

- **Servidor basado en Windows:** *C:\Program Files (x86)\Avaya\onexportal\Tomcat\Server\logs*
- **Servidores basados en Linux:**
  - **Unified Communications Module:** */var/log/One-X*
  - **Otros servidores basados en Linux:** */opt/Avaya/oneXportal/<one-X version>/apache-tomcat/logs*

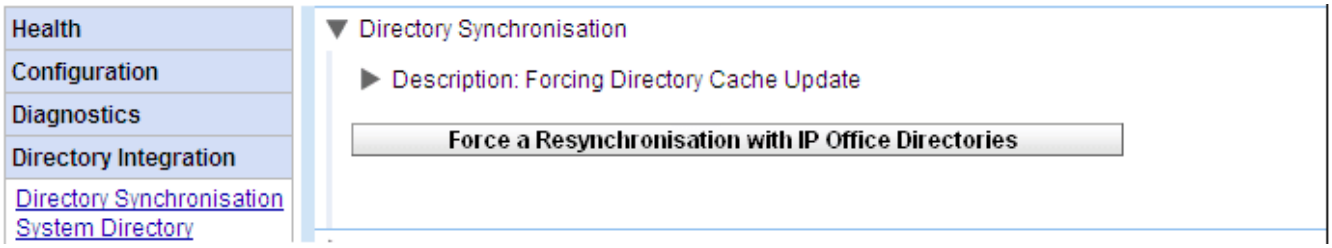
En los servidores basados en Linux, cualquier archivo existente de vuelco de memoria se incluye en los archivos de registro que se pueden descargar de los menús de visualización de control/plataforma web del servidor (**Registros | Descargar**).

2.5 Integración de directorios

Esta sección le permite ver y comprobar la integración de los servidores con los directorios que utilizan.

2.5.1 Sincronización de directorios

Durante el funcionamiento normal, el servidor one-X Portal para IP Office actualiza los registros cada 300 segundos aproximadamente. Sin embargo, se puede utilizar este menú para forzar una actualización del directorio de los usuarios del directorio del sistema y de IP Office.



- **Forzar una resincronización con directorios de IP Office**
  Solicita una actualización de las entradas del directorio del sistema almacenadas en las configuraciones de los sistemas IP Office. Las entradas del **directorio del sistema** también pueden verse y controlarse a través de la opción **Integración de directorios | Directorio del sistema** 44.

2.5.2 Búsqueda de directorios de LDAP

Esta opción también le permite realizar una búsqueda en el directorio externo de la misma manera que los usuarios de one-X Portal para IP Office. Esto le permite evaluar el funcionamiento del Proveedor de LDAP 68.

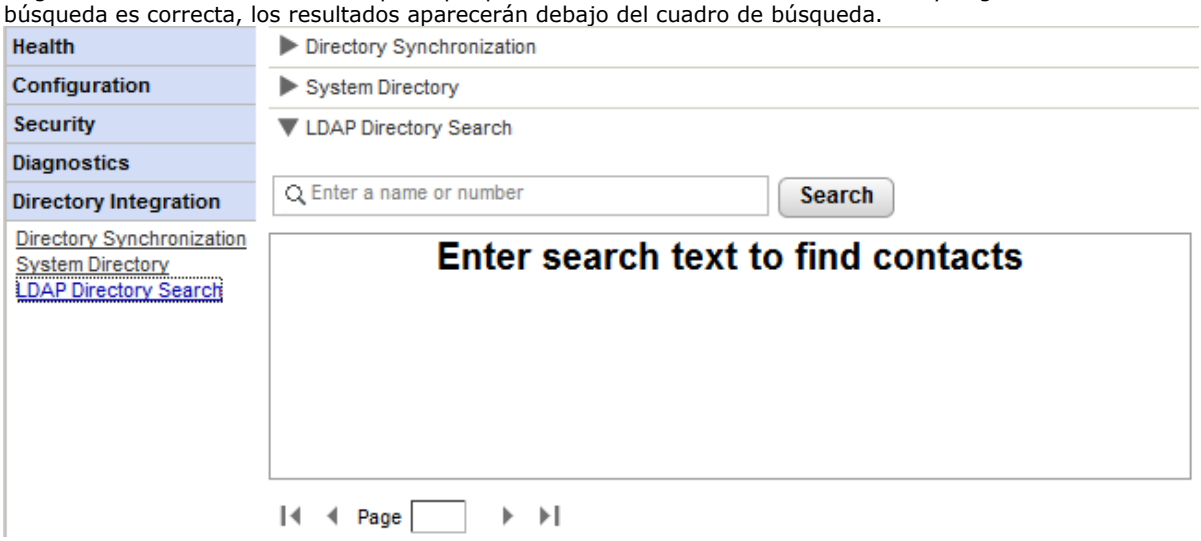
Para buscar en el directorio LDAP:

1. Seleccione **Integración de directorios**.

Página948 de 3226.

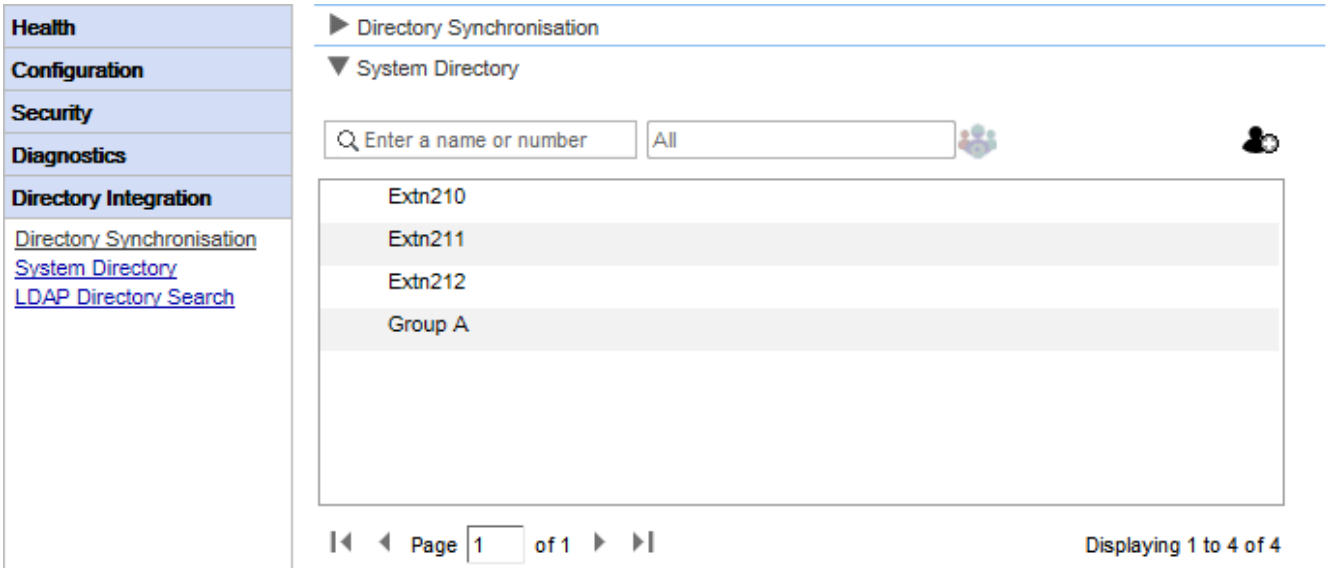
2. Seleccione **Búsqueda de directorios de LDAP**.

3. Ingrese un nombre o un número que sepa que se encuentra en el directorio externo y haga clic en **Buscar**. Si la búsqueda es correcta, los resultados aparecerán debajo del cuadro de búsqueda.



2.5.3 Directorio del sistema

Esta opción le muestra el directorio del sistema como se muestra a los usuarios de one-X Portal para IP Office. Puede realizar una búsqueda en el directorio tal como si utilizase el cliente one-X Portal para IP Office.



Puede utilizar este menú para verificar que el directorio se encuentre como se esperaba y que admita usuarios, grupos y entradas de directorios de cada IP Office.

- **Nota:** El sistema no muestra grupos de búsqueda establecidos como *Fuera de directorio* en la configuración del sistema telefónico.

El servidor one-X Portal para IP Office actualiza los registros del directorio personal y del sistema cada 300 segundos aproximadamente. De ser necesario, puede forzar una actualización por medio de la opción **Sincronización de directorios** 42.

- Para algunos contactos del directorio, one-X Portal para IP Office puede indicar el estado actual de los contactos por medio de diferentes iconos. Para los contactos que tienen varios números de teléfono, el estado toma como base el número de trabajo.

Estado	Icono	Descripción
Disponible		El estado normal para un usuario que muestra el estado de su extensión de trabajo en uso.
Ocupado		El estado normal para un usuario que muestra que su extensión de trabajo se encuentra en una llamada.
No interrumpir		El usuario ha establecido la opción **No interrumpir**. Las llamadas que reciba se dirigirán al correo de voz si está activado, o bien aparecerá el tono de ocupado a menos que la persona que llama figure en la **lista de excepciones de la función No interrumpir del usuario**.
Desconectado		El usuario se ha desconectado de su teléfono. Es probable es que las llamadas que reciba se dirijan al correo de voz, de estar disponible.
Otro		Se utiliza este icono cuando no se conoce o no se puede conocer el estado, es decir, números externos.
Timbre		Se utiliza este icono para un contacto interno que está sonando actualmente.

Agregar y editar contactos del portal

Puede utilizar el icono para agregar un nuevo contacto del directorio del sistema. Cabe señalar que los contactos agregados de esta manera son almacenados por one-X Portal para IP Office y los usuarios solo pueden acceder a ellos a través de one-X Portal para IP Office. De ser necesario, estos contactos pueden tener varios números de teléfono y direcciones de correo electrónico configuradas.

Para eliminar contactos que se hayan agregado de esta manera, haga clic en el contacto y seleccione el icono de eliminación.

2.6 Configuración de gadget

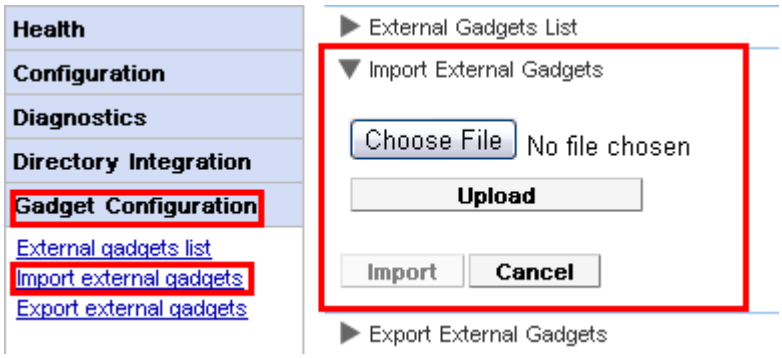
Como administrador de one-X Portal para IP Office puede configurar una lista de gadgets externos en el sistema. Puede habilitar, editar y eliminar los gadgets que el usuario de one-X Portal para IP Office puede agregar. El usuario de one-X Portal para IP Office solamente puede agregar aquellos gadgets externos habilitados por el administrador.

2.6.1 Lista de gadgets externos

Todos los gadgets que están en el sistema aparecen en la **Lista de gadgets externos**. De forma predeterminada, no hay gadgets externos configurados en el one-X Portal para IP Office. Como administrador, usted puede agregar un gadget externo 64 o importar gadgets externos 61 para el usuario.

2.6.2 Importación de gadgets

Puede importar gadgets externos como un archivo XML. Posteriormente, esos gadgets estarán disponibles para que el usuario los seleccione. Consulte Importación de gadgets 61.



Para importar un archivo de gadget:

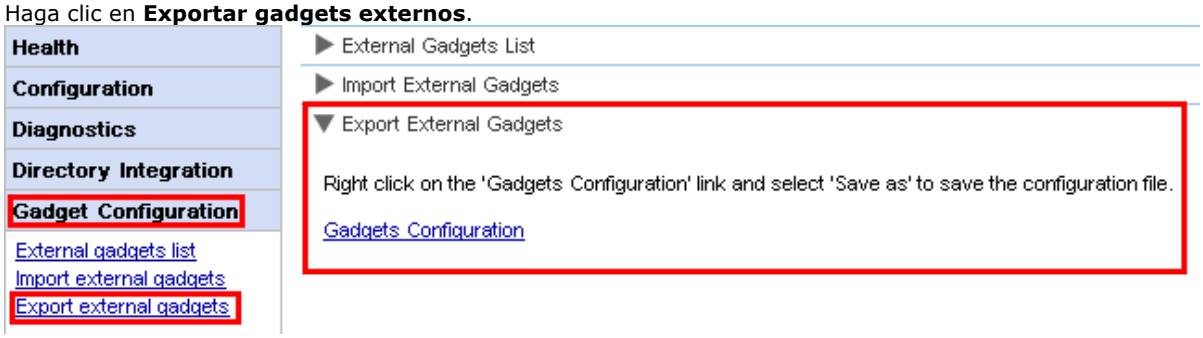
1. Haga clic en **Configuración de Gadget** y seleccione **Importar gadgets externos**.
2. Haga clic en **Elegir archivo** para buscar el archivo de configuración.
3. Haga clic en **Cargar**. El sistema carga el archivo XML en el one-X Portal para IP Office.
4. Haga clic en **Importar** para agregar el gadget de terceros a la *Lista de Gadgets*.
5. La próxima vez que el usuario inicie sesión en one-X Portal para IP Office, el gadget de terceros estará disponible para que el usuario lo agregue a su portal.

2.6.3 Exportación de gadgets

El conjunto actual de gadgets externos en el one-X Portal para IP Office se puede exportar como un archivo de configuración. El archivo de configuración está en formato XML. El archivo de configuración contiene información acerca de los parámetros del gadget. Puede agregar este conjunto de gadgets al one-X Portal para IP Office de otro usuario al importar 61 el archivo de configuración guardado.

Para exportar un gadget de terceros:

1. Haga clic en **Configuración de Gadget**, en el panel de navegación izquierdo.
2. Haga clic en **Exportar gadgets externos**.



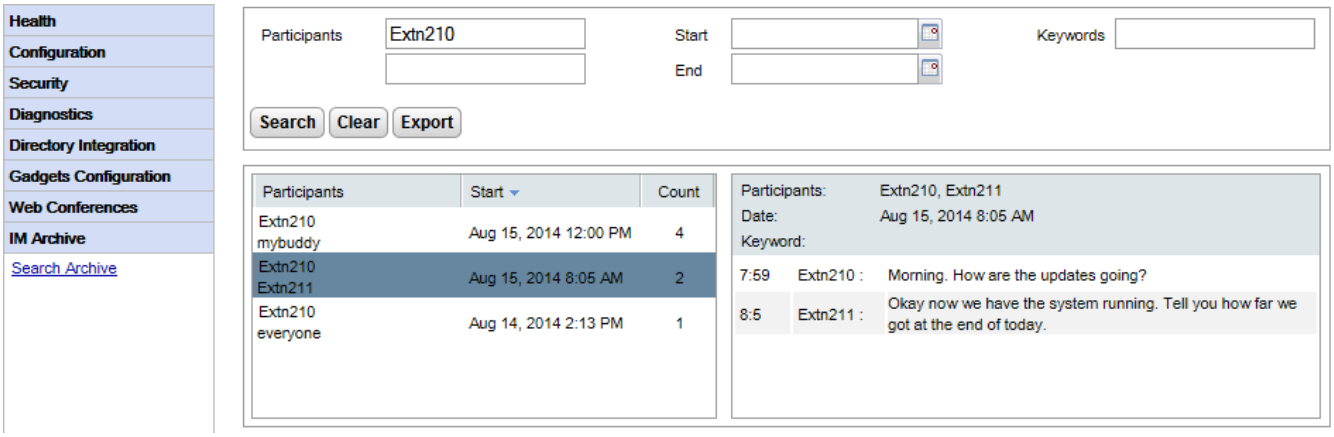
3. Haga clic con el botón secundario en el enlace **Configuración de gadgets**.
4. Seleccione ***Guardar como*** para guardar el archivo de configuración.

2.7 Archivo MI

Como administrador de one-X Portal para IP Office puede buscar las conversaciones de MI de todos los usuarios. Consulte Activación/desactivación de archivado de MI 76.

2.7.1 Buscar archivo

Puede buscar conversaciones de mensajería instantánea entre los usuarios y del sistema a un usuario. Todos los campos en el panel de búsqueda son opcionales. La cantidad de días que el servidor conserva un MI en el archivo se determina mediante la configuración de **Días para archivar MI 77**.



Para buscar en el archivo de MI:

1. En el panel de la izquierda, seleccione el **Archivo de MI**.
2. Haga clic en **Buscar archivo**.
3. Ingrese los criterios de búsqueda y haga clic en Buscar.

Campo	Descripción
Participantes	Escriba el nombre del participante en la conversación de MI.
Palabras clave	Escriba las palabras clave en la conversación de MI.
inicie	Seleccione la fecha desde la que se deben incluir las conversaciones. Si no selecciona una fecha, el sistema muestra desde la conversación más reciente que guardó el sistema.
Fin	Seleccione la fecha hasta la que se deben incluir las conversaciones. Si no selecciona una fecha, el sistema muestra hasta la conversación más reciente.

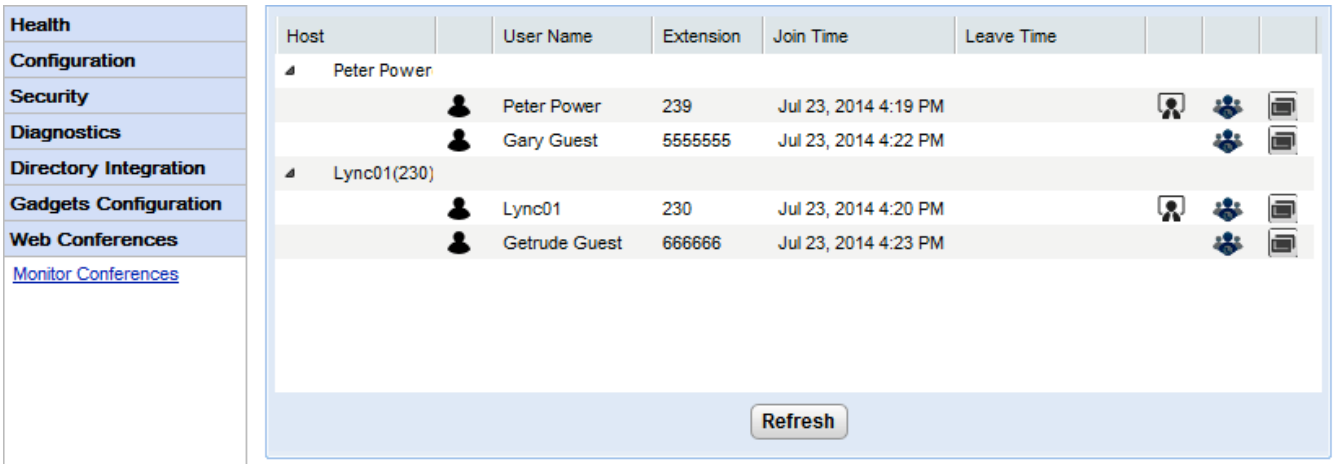
4. Haga clic en la conversación que desea abrir. El sistema muestra la conversación.

2.8 Conferencias web

En los sistemas de portal basados en IP Office Server Edition y IP Office Application Server, el servidor de one-X Portal para IP Office puede mostrar detalles de las conferencias de audio que están en curso.

2.8.1 Control de conferencias

Este menú permite ver detalles de cualquier conferencia de colaboración web que aloje el servidor. Contiene una lista de los miembros de las conferencias, la última fecha en que se unieron y cuál es su participación (presentador, miembro de conferencia de audio, miembro de conferencia web). Este menú no se admite en el servidor de Unified Communications Module.



Para ver conferencias actuales:

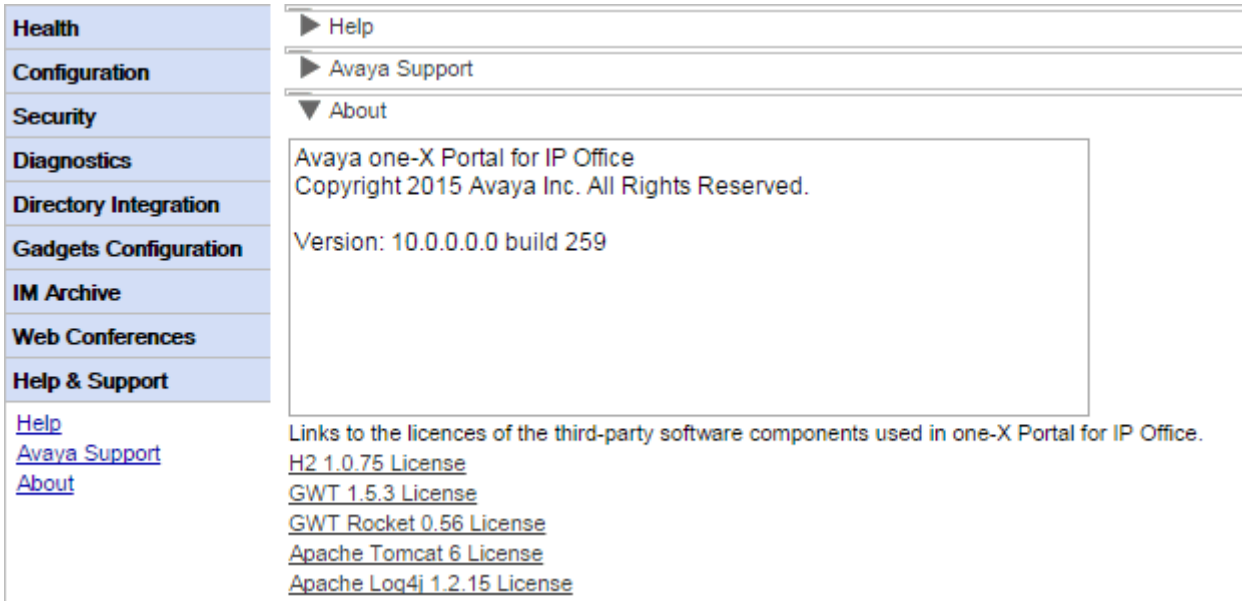
1. Seleccione **Conferencias web** y, a continuación **Control de conferencias**.
2. Aparece una lista de la conferencia web actual.
3. Haga clic en **Host** para expandir la conferencia y ver detalles de los participantes.

2.9 Ayuda y asistencia técnica

Ayuda | Ayuda
Proporciona enlaces a la ayuda para el usuario de one-X Portal para IP Office y a este documento como una forma de ayuda.

Ayuda | Asistencia técnica de Avaya
Carga un enlace al sitio Web de asistencia técnica de Avaya (http://support.avaya.com).

Ayuda | Acerca de
Muestra información de la versión básica para la instalación de one-X Portal para IP Office.



Capítulo 3.
Tareas de mantenimiento

3. Tareas de mantenimiento

3.1 Reiniciar el servicio

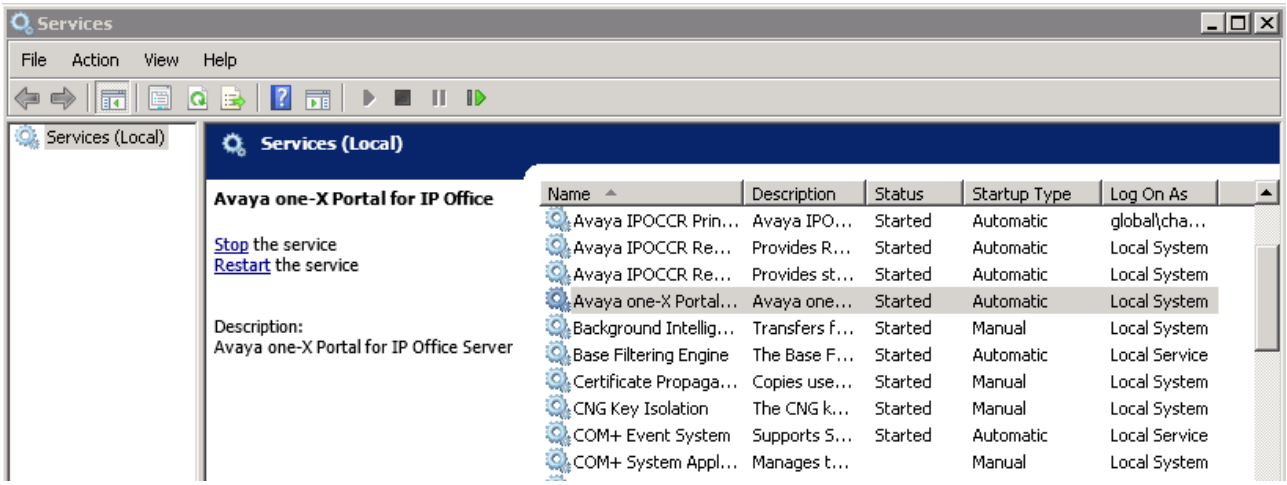
El servicio de one-X Portal para IP Office se puede detener y reiniciar de varias maneras.

Desde los menús del administrador

Puede hacer clic en el icono en la parte superior de los menús del administrador para reiniciar el portal. Tenga en cuenta que este icono aparece automáticamente si realiza cambios que requieren un reinicio.

Servidor basado en Windows

La aplicación one-X Portal para IP Office se instala como un servicio denominado Avaya one-X Portal. Puede iniciarse y detenerse a través del panel de control estándar de Windows Services.



Cabe destacar que cuando se inicia o reinicia el servicio, aunque en pocos segundos Avaya one-X Portal informe por sí mismo que ha sido iniciado, se necesitarán hasta 15 minutos para que la aplicación esté totalmente en funcionamiento. Una forma de controlar el progreso es utilizar Windows Task Manager. Por lo general, cuando one-X Portal para IP Office se inicie, el **uso de PF** aumentará gradualmente a aproximadamente 2.3 GB antes de que one-X Portal para IP Office se haya iniciado.

- **¡No hay servicio!**
  Si no hay servicio, la causa probable es un puerto en conflicto o un problema de Java. Consulte Solución de problemas 93.

Servidor basado en Linux

1. Mediante los menús de administración web para el servidor, seleccione **Solución**.
2. Haga clic en el icono y seleccione **Vista de plataforma**.
3. En la vista de plataforma, el estado del servicio one-X Portal aparece en la pestaña **Sistema**. Para detener el servicio, haga clic en **Detener** o **Forzar detención**. Para iniciar el servicio, haga clic en **Iniciar**.

3.2 Configuración del registro de llamadas

El registro de llamadas que muestra one-X Portal para IP Office se almacena en el sistema telefónico como parte de la configuración del usuario. Se almacenan hasta 30 registros; los registros nuevos reemplazan a los antiguos una vez que se alcanzó el límite. Sin embargo, para las llamadas repetidas hacia o desde el mismo número, se actualiza el registro existente y se incrementa el número del conteo de llamadas.

Para las llamadas entrantes, de modo predeterminado, solo se incluyen en el registro de llamadas las llamadas personales (no de grupo de búsqueda) al usuario, respondidas por el usuario o que no fueron respondidas.

- **Llamadas perdidas**
  Las llamadas que el usuario no responde pero son respondidas por el correo de voz u otro interno no suelen registrarse como llamadas perdidas. Para permitir el registro de llamadas perdidas, la configuración para todo el sistema **Registrar llamadas perdidas respondidas en cobertura** (**Sistema | Telefonía | Registro de llamadas**) debe estar activada en la configuración telefónica de IP Office.
- **Llamadas perdidas del grupo de búsqueda**
  De manera predeterminada, únicamente se registran las llamadas del grupo de búsqueda que el usuario responde. Para permitir el registro de llamadas perdidas del grupo de búsqueda, la configuración para todo el sistema **Registrar llamadas perdidas del grupo de búsqueda** también debe estar activada en la configuración telefónica de IP Office. El usuario además debe estar configurado en los sistemas telefónicos con los grupos de búsqueda para los cuales el registro de llamadas puede incluir llamadas perdidas (**Usuario | Telefonía | Registro de llamadas**).
- **Eliminación automática**
  Los registros de llamadas antiguas se eliminan automáticamente cuando se alcanza el máximo de capacidad del registro de llamadas y es necesario agregar un nuevo registro de llamadas. Además, mediante la configuración del sistema telefónico puede hacer que se eliminen las entradas del registro después de un período determinado. Seleccione **Eliminar entradas después de** (**Usuario | Telefonía | Registro de llamadas**).

Historial de conversaciones telefónicas

Para los usuarios que utilizan un teléfono de la serie 1400, 1600, 9500 o 9600 con un botón **Registro de llamadas** o **Historial**, o un teléfono de la serie M o T, de manera predeterminada, el mismo registro de llamadas que muestra el portal se muestra también en el teléfono. En consecuencia, puede utilizar y editar el registro de llamadas desde el teléfono o desde one-X Portal para IP Office. Ambos se modifican en paralelo.

Los usuarios que utilizan cualquier otro tipo de teléfono que tenga un registro de llamadas, este registro es almacenado por el teléfono y, por ello, no necesariamente coincidirá con el registro de llamadas que se muestra en one-X Portal para IP Office. Por ejemplo, las llamadas realizadas por medio de one-X Portal para IP Office no aparecen en el registro de llamadas del teléfono y viceversa.

En cualquiera de los casos, el registro de llamadas de one-X sólo muestra 255 registros.

3.3 Conmutador de IP Office

3.3.1 Incorporación de una unidad adicional de IP Office

Para agregar una unidad adicional de IP Office en la red comunitaria pequeña (Small Community Network), es necesario asignar la dirección IP al proveedor de telefonía (CSTA) y al proveedor de directorios (IP Office).

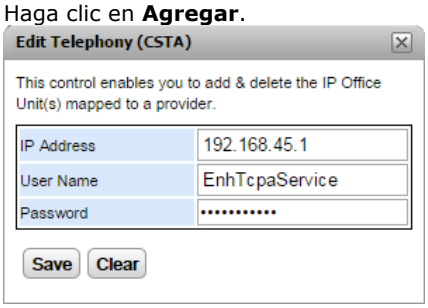
- **Autoaprovisionamiento automático/Modo de CTI centralizado** 32
  Para un servidor de portal basado en Linux que admite una red IP Office Server Edition, el sistema IP Office primario puede informar al servidor acerca de otros sistemas IP Office de la red y el servidor de correo de voz. Luego, crea o quita automáticamente los proveedores adecuados para los otros sistemas. Esto se realiza mediante **la configuración de Enlace de CTI central**, que está activada de forma predeterminada para las nuevas instalaciones. Cuando está activada, la configuración manual de proveedores para sistemas IP Office adicionales no es necesaria. En modo CTI centralizado:
  - Si no se utiliza la resiliencia, el servidor solamente requiere un proveedor DMSL en el sistema IP Office primario.
  - Si se utiliza la resiliencia, el servidor solamente requiere un proveedor DMSL en el sistema IP Office primario y secundario.
  - El servidor solo requiere un proveedor de CSTA para el sistema IP Office primario, a menos que se use la resiliencia del portal, en cuyo caso también se necesita un proveedor de CSTA para el sistema IP Office secundario.

Para agregar otro sistema IP Office:

- **Advertencia**
  Este proceso requiere que reinicie el servicio del portal 52 para que los cambios surtan efecto. Durante el reinicio, el portal no estará disponible para los usuarios por un máximo de 15 minutos.

1. Antes de agregar otra unidad de IP Office a la configuración de one-X Portal para IP Office:
   - Verifique que la unidad de IP Office se haya definido con la configuración de seguridad para el funcionamiento de one-X Portal para IP Office.
   - Verifique que la unidad de IP Office cuente con la licencia para one-X Portal para IP Office.
   - Compruebe que al menos un usuario de la unidad de IP Office esté habilitado para one-X Portal para IP Office.
2. Inicie sesión 8 en los menús de administrador.
3. Verifique que la unidad de IP Office pueda verse desde el servidor one-X Portal para IP Office.
   a. Seleccione **Diagnóstico** y, a continuación, **Conexiones de IP Office**.
   b. Ingrese la **Dirección IP** de la unidad de IP Office de destino y haga clic en **Verificar**.
   c. Si es posible acceder a IP Office, los resultados incluirán información básica sobre el sistema IP Office.
4. Seleccione **Configuración** y, a continuación, **Proveedores**.

5. Haga clic en **Agregar**.



6. Ingrese la **Dirección IP** del sistema IP Office nuevo.
7. Ingrese el nombre de **usuario** y la **contraseña** que coincidan con el usuario de seguridad de TCPA configurado en el sistema IP Office.
8. Haga clic en **Guardar**.

Página960 de 3226.

9. Reinicie el servicio Avaya one-X Portal 52. Cuando el servicio se haya iniciado completamente, vuelva a iniciar sesión en los menús de administrador.
10. Seleccione **Estado** y, a continuación, **Estado de los componentes**.
11. Haga clic en **Obtener todo**. Estarán incluidos los nuevos componentes de CSTA y DSML para la dirección IP de la unidad de IP Office que se agregó recientemente. Su estado debe ser "disponible".
12. Seleccione **Integración de directorios**. Verifique que se hayan incluido los nuevos usuarios del sistema IP Office. De lo contrario, seleccione **Sincronización de directorios | Forzar una resincronización con directorios de IP Office** y espere 5 minutos.
13. Seleccione **Configuración** y, a continuación, **Usuarios**. Haga clic en **Obtener todo**. Verifique que se hayan incluido los nuevos usuarios del sistema IP Office.

3.3.2 Modificación de la información de IP Office

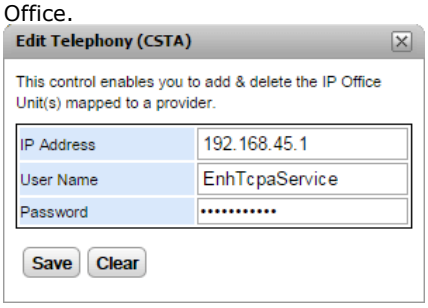
Si se modifica la información (dirección IP, nombre de usuario o contraseña del servicio de TCPA) de una unidad de IP Office asignada, la configuración de IP Office que se encuentra en la sección de proveedores de one-X Portal para IP Office debe actualizarse para que coincida.

- **Advertencia**
  Este proceso requiere que reinicie el servicio del portal 52 para que los cambios surtan efecto. Durante el reinicio, el portal no estará disponible para los usuarios por un máximo de 15 minutos.

Para cambiar los detalles de IP Office:

1. Inicie sesión 8 en los menús de administrador.
2. Si se modificó la dirección IP de la unidad de IP Office, verifique que la unidad pueda verse desde el servidor one-X Portal para IP Office.
   a. Seleccione **Diagnóstico** y, a continuación, **Conexiones de IP Office**.
   b. Ingrese la **Dirección IP** de la unidad de IP Office de destino y haga clic en **Verificar**.
   c. Si es posible acceder a IP Office, los resultados incluirán información básica sobre el sistema IP Office.
3. Seleccione **Configuración** y, a continuación, **Proveedores**.

4. Haga clic en el icono que se encuentra junto al proveedor de CSTA existente al que se asignó la unidad de IP Office.



5. Edite la información que aparece para que coincida con la nueva configuración del sistema IP Office y haga clic en **Guardar**.
6. Reinicie el servicio del portal 52.

3.3.3 Resistencia

Para IP Office versión 10 y posteriores, el servicio del portal también se instala de manera predeterminada en el servidor secundario de IP Office Server Edition. Esto permite al servidor secundario actuar como el servidor del portal para los usuarios cuando, por alguna razón, el servidor primario no está disponible.

- La resiliencia del portal se admite en modo IP Office Server Edition Seleccione. La resiliencia del portal también se puede configurar cuando se usa IP Office Application Server en lugar del servicio de portal del servidor primario o secundario.
    - En sistemas anteriores que no estaban originalmente en modo Select pero se pasaron a modo IP Office Server Edition Seleccione recientemente, quizás sea necesario reiniciar los servicios del portal para que la configuración de resiliencia esté disponible. De manera similar, es posible que sea necesario reiniciar los servicios del portal después de configurar por primera vez la resistencia del portal en la configuración del sistema IP Office.
- Solo se admite la resiliencia entre servidores primarios y secundarios que ejecutan la misma versión de software de portal.
- Durante el funcionamiento normal (con ambos servidores en ejecución y conectados), los cambios del usuario y del administrador realizados al servidor primario se sincronizan automáticamente con el servidor secundario. Sin embargo, durante la resiliencia, los cambios realizados en un servidor no se sincronizan y podrían perderse cuando los servidores regresen al funcionamiento normal.
    - Las conferencias programadas actualmente son una excepción a lo anterior. Las conferencias programadas en el primario no ocurren cuando se ejecuta en conmutación por error. Las conferencias programadas en el secundario se pierden cuando ocurre la conmutación por recuperación.
- Dentro de la vista de la plataforma (panel Web Control) de cada servidor:
    - el servidor del portal activo se muestra 'Disponible' (icono verde).
    - el servidor del portal pasivo se muestra 'Iniciando' (icono ámbar).
- Las aplicaciones del cliente del portal como one-X Portal Call Assistant no se redirigen automáticamente. El usuario debe ingresar la dirección del servidor secundario para poder iniciar sesión.

Cuando se configura la resiliencia del portal:

- **Falla en el portal del servidor primario**
  Si el servicio de portal del servidor primario se detiene por algún motivo, el servicio de portal del servidor secundario queda disponible automáticamente.
    - Los usuarios que habían iniciado sesión en el portal, en el servidor primario pueden iniciar sesión nuevamente en el servidor secundario.
        - Si el servicio primario de IP Office todavía se está ejecutando, esos usuarios del portal se redireccionan automáticamente.
        - Si el usuario no accedió previamente al servidor secundario del portal, es posible que deban aceptar el certificado de seguridad o crear una excepción que interrumpirá la reconexión automática.
    - Lo mismo se aplica a los usuarios que habían iniciado sesión en uno de los clientes del portal, como el complemento de Outlook
    - Los usuarios nuevos que deseen iniciar sesión deberán utilizar la dirección del servidor secundario.
- **Falla en IP Office del servidor primario:**
  Si el servicio de IP Office del servidor primario se detiene por algún motivo, los servicios del portal se transfieren de manera automática al servidor secundario, como anteriormente.
    - Cuando el núcleo de IP Office no está activo, los usuarios que pertenecen a ese núcleo de IP Office no pueden actualizar ni eliminar contactos del gadget de directorio del portal.
- **En caso de falla en la red:**
  Si la conexión de red entre el servidor primario y secundario falla por algún motivo, ambos servidores del portal se activan y permiten el inicio de sesión. Nuevamente, los cambios de administrador y usuario en el servidor del portal secundario no se copian en el primario cuando se recupera la conexión de red. Esto es lo que se denomina "Modo independiente".
- **Recuperación del portal del servidor primario:**
  Cuando el servicio del portal del servidor primario está disponible nuevamente, el servicio del portal en el servidor secundario deja de admitir el inicio de sesión.
    - Los usuarios que hayan iniciado sesión en el servidor secundario del portal se redireccionan automáticamente al servidor primario.
    - Los usuarios que hayan iniciado sesión en uno de los clientes del portal, como el Plug-in de Outlook, se conectan automáticamente al servidor primario.
    - Los usuarios nuevos que deseen iniciar sesión se redireccionan al primario.

- **Recuperación de IP Office del servidor primario:**
  Cuando el servicio de IP Office del servidor primario está disponible de nuevo, la compatibilidad del servicio del portal también regresa al servidor primario, como anteriormente.

Para configurar la resiliencia:

1. **Active el modo de enlace de CTI centralizado**
   Ambos servidores del portal deben estar configurados para usar el modo de enlace de CTI centralizado. Esa es la manera predeterminada para una instalación nueva, pero se debe activar manualmente para los sistemas existentes actualizados a IP Office versión 10 o superior.

   a. El modo de enlace de CTI centralizado se activa mediante el menú **Enlace de CTI central** 32.

   b. Si se cambia la configuración, el servicio del portal se debe reiniciar para que se efectúe el cambio.

   c. La configuración debe estar activada en los dos servidores, el primario y el secundario.

2. **Active la resistencia del servidor del portal**
   El servidor del portal primario se debe configurar para admitir la resistencia a través de los menús de **Configuración de resistencia** 28.

3. **Reinicie los servicios del portal**
   Si se hace algún cambio en los pasos anteriores.

4. **Active el respaldo del portal en las líneas troncales de red**
   Las líneas troncales de SCN entre los servidores IP Office primario y secundario deben tener activada la configuración para el respaldo del portal.

   a. Mediante Manager de IP Office, cargue la configuración desde los sistemas de IP Office de IP Office Server Edition.

   b. En la configuración del servidor primario, ubique la línea de IP Office desde el sistema de IP Office primario hasta el secundario.

   c. En la ficha **Línea** en **Opciones de resiliencia de SCN**, compruebe que **Admite resistencia** y **Hace copia de seguridad de mi one-X Portal** estén seleccionados.

   d. Guarde los cambios en la configuración.

3.4 Gadgets

3.4.1 Búsqueda de URL del gadget

Google proporciona una variedad de gadget que puede agregar a su página Web.

Ejemplo: Para obtener la URL de un gadget de Google:

1. Para obtener la lista de gadget que Google ofrece, vaya a: http://www.google.com/ig/directory?synd=open
2. Seleccione el gadget que desea agregar a su página Web.
3. Haga clic en **Agregar a su página Web**.
4. Haga clic en **Obtener código**. El sistema muestra una cadena similar a la que se muestra más abajo. El texto que está entre comillas (") es la URL para el gadget:


```
<script src="http://www.gmodules.com/ig/ifr?
url=http://www.donalobrien.net/apps/google/currency.xml&amp;up_def_from=USD&amp;up_def_to=EUR&a
mp;synd=open&amp;w=320&amp;h=170&amp;title=Currency+Converter&amp;border=%23ffffff%7C0px%
2C1px+solid+%2382CAFA%7C0px%2C2px+solid+%23BDEDFF%7C0px%2C3px+solid+%
23E0FFFF&amp;output=js"></script>
```

3.4.2 Importación de gadgets

Se pueden agregar gadget de terceros a one-X Portal para IP Office mediante un archivo XML. Puede cargar hasta 50 gadgets por vez. El tamaño del archivo no debe superar los 2 MB.

Para cada gadget, debe especificar los siguientes parámetros:

- URL del gadget, es decir, la fuente del gadget y su contenido
- Nombre del gadget que aparece en la barra de título del gadget
- Iconos de los gadgets en la barra de herramientas. Es conveniente proporcionar iconos de barra de herramientas para todos los gadgets especificados en gadgets.xml.
- Textos de la barra de herramientas de los gadget (el texto de información de la herramienta y el texto que aparece debajo del icono de la barra).

El siguiente es un ejemplo del formato de archivo XML de un gadget:


```
<GadgetsConfigurationImpl>
<gadgetRecords>
<entry>
<key>1</key>
<value>
<categorys>1</categorys>
<categorys>2</categorys>
<created>2012-08-10</created>
<defaultToolbarIcon />
<downToolbarIcon />
<deleted />
<enable>true</enable>
<external>true</external>
<height>300</height>
<id>1</id>
<localizedName><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></localizedName>
<name>Angry Birds</name>
<toolbarText><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></toolbarText>
<tooltip><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></tooltip>
<url>http://www.gmodules.com/ig/ifr?
url=http://www.forumforyou.it/google_gadget_angry_birds.xml&amp;synd=open&amp;w=820&amp;h=680&amp;ti
tle=Angry+Birds&amp;border=%23ffffff%7C3px%2C1px+solid+%23999999&amp;output=js</url>
</value>
</entry>
</gadgetRecords>
</GadgetsConfigurationImpl>
```


Nota: Asegúrese de lo siguiente en el archivo .xml:

1. Coloque cada uno de los gadgets dentro del elemento <entry></entry>.
2. El elemento <key></key> debe ser único y debe coincidir con <id></id>. Esta es una ID del gadget única de uso interno.
3. El elemento <value></value> debe contener información sobre el gadget.
4. El elemento <categorys></categorys> indica la categoría del gadget. Las ID y los códigos de las categorías son los siguientes:

Código	Categoría
1	TODOS
2	COMUNICACIÓN
3	HERRAMIENTAS
4	PRODUCTIVIDAD
5	FINANZAS

Página967 de 3226.

6	TECNOLOGÍA
7	ZOHO

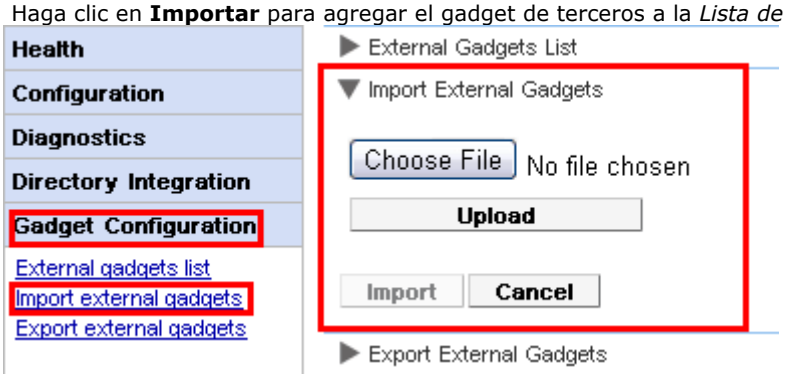
5. Detalles de otros elementos:

Elemento	Descripción
<created>	La fecha en que creó el archivo.
<defaultToolbarIcon>	Especifique el icono de la barra de herramientas predeterminado que el sistema muestra cuando se minimiza el gadget. El sistema muestra el icono en la barra de herramientas del usuario.
<downToolbarIcon>	Especifque la barra de herramientas que el sistema muestra cuando el usuario hace clic en el icono de gadgets.
<enable>	Establezca el valor como true (verdadero) si desea que el usuario vea el gadget.
<external>	Establezca el valor como true (verdadero) para todos los gadgets externos.
<height>	Establezca la altura del gadget en píxeles.
<id>	ID del gadget.
<localizedName>	Especifique el nombre localizado de cada configuración regional.
<name>	Especifique un nombre exclusivo para el gadget.
<toolbarText>	El texto que el sistema muestra en la barra de herramientas del gadget.
<tooltip>	El texto que el sistema muestra en la información sobre herramientas del gadget.
<url>	La URL del gadget. Para más información, consulte Buscar la URL de un gadget externo - Ejemplo 60.

Nota: Aparecerán los mensajes de errores correspondientes si el archivo de configuración no es compatible con ninguno de los criterios arriba mencionados.

Para importar un archivo de gadget:

1. Haga clic en **Configuración de gadget**, en el panel de navegación izquierdo.
2. Haga clic en **Importar gadget externos**.
3. Haga clic en **Elegir archivo** para buscar el archivo de configuración.
4. Haga clic en **Cargar**. El sistema carga el archivo XML en el one-X Portal para IP Office.
5. Haga clic en **Importar** para agregar el gadget de terceros a la *Lista de Gadgets*.



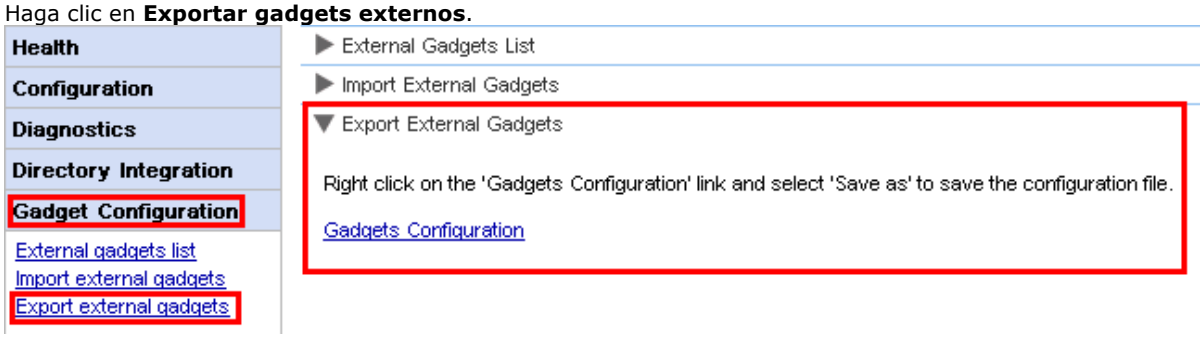
6. La próxima vez que el usuario inicie sesión en one-X Portal para IP Office, el gadget de terceros estará disponible para que el usuario lo agregue a su portal.

3.4.3 Exportación de gadgets

El conjunto actual de gadgets externos en el one-X Portal para IP Office se puede exportar como un archivo de configuración. El archivo de configuración está en formato XML. El archivo de configuración contiene información acerca de los parámetros del gadget. Puede agregar este conjunto de gadgets al one-X Portal para IP Office de otro usuario al importar 61 el archivo de configuración guardado.

Para exportar un gadget de terceros:

1. Haga clic en **Configuración de Gadget**, en el panel de navegación izquierdo.
2. Haga clic en **Exportar gadgets externos**.



3. Haga clic con el botón secundario en el enlace **Configuración de gadgets**.
4. Seleccione ***Guardar como*** para guardar el archivo de configuración.

3.4.4 Agregar un gadget externo

Para agregar un gadget individual, necesita la URL del gadget. Para obtener más información sobre cómo obtener la URL del gadget, consulte Buscar la URL de un gadget externo - Ejemplo 60.

Para agregar un gadget externo:

1. Haga clic en **Configuración de gadget**, en el panel de navegación izquierdo.
2. Haga clic en **Lista de gadgets externos**.
3. Haga clic en **Agregar**. El sistema muestra el cuadro de diálogo **Agregar gadget**.
4. Agregue los detalles del gadget (vea más abajo) y haga clic en **Guardar**. El sistema actualiza el gadget externo que agregó en la base de datos de one-X Portal para IP Office.

Campos del gadget

Nombre del campo	Descripción
Nombre del gadget	El sistema muestra el nombre que especifica en este campo en la barra de título del gadget. Asegúrese de que el nombre del gadget no exceda los 50 caracteres.
URL del gadget	Contiene la URL del gadget. La URL que proporciona debe cumplir con las normas de especificación de la URL de http://www.w3.org/Addressing/URL/url-spec.txt. El sistema utiliza la URL que se especifica para mostrar el gadget.
Nombre del gadget localizado	El sistema muestra el nombre localizado que especifica en este campo en la barra de título del gadget. El sistema muestra el nombre localizado solamente si el usuario de one-X Portal para IP Office selecciona un idioma mientras inicia sesión.
Etiqueta del icono de la barra de herramientas	El sistema muestra el texto que configuró en este campo como la etiqueta del gadget en la barra de herramientas. Si no especifica un texto, el sistema muestra el nombre del gadget completo.
Texto de información de la herramienta del icono de la barra de herramientas	El sistema muestra la información de la herramienta que configuró en este campo para el gadget cuando el usuario se desplaza por el icono del gadget en la barra de herramientas.
Icono de la barra de herramientas	El sistema muestra el icono que configuró en este campo en la barra de herramientas. Asegúrese de que el tipo de imagen sea solamente png, gif o jpeg, la dimensión de la imagen sea de 37*37 píxeles y el tamaño máximo de la imagen sea de 10KB. Si no configura un icono, el sistema muestra la imagen predeterminada.
Icono de la barra de herramientas en el clic del mouse	El sistema muestra el icono que se configuró en este campo cuando hace clic en el icono de la barra de herramientas. Asegúrese de que el tipo de imagen sea solamente png, gif o jpeg, la dimensión de la imagen sea de 37*37 píxeles y el tamaño máximo de la imagen sea de 10KB.
Activado	El sistema habilita el gadget para todos los usuarios de one-X Portal para IP Office.
Altura del gadget	El sistema muestra la altura del gadget a la altura que configuró en este campo. La altura predeterminada de la ventana del gadget está ajustada a 300 píxeles en este campo. Puede configurar la altura de la ventana del gadget solamente cuando agrega un gadget. No puede editar la altura del gadget después de agregar un gadget.

3.4.5 Editar un gadget externo

Puede editar los detalles de un gadget como el nombre del gadget, la URL del gadget, el texto que aparece en la barra de herramientas, información de herramientas, icono que aparece en la barra de herramientas y el icono que aparece en un clic del mouse.

Para editar un gadget externo:

1. Haga clic en **Configuración de Gadget**, en el panel de navegación izquierdo.
2. Haga clic en **Lista de Gadgets externos**.
3. Haga clic en **Obtener todo**. El sistema muestra una lista de los gadget externos que están disponibles en el sistema.
4. Haga clic en **Editar** para editar los detalles del gadget. El sistema muestra el cuadro de diálogo **Editar gadget**.
5. Para obtener detalles de los campos del gadget, consulte Adición de un gadget externo 64. Actualice los cambios que desee realizar y haga clic en **Guardar**.
6. Haga clic en **Ingresar selección**. El sistema actualiza los gadget externos que editó en la base de datos one-X Portal para IP Office.

3.4.6 Habilitar un gadget externo

Cuando se habilita un gadget, todos los usuarios de one-X Portal para IP Office pueden agregar ese gadget.

Para habilitar un gadget externo:

1. Haga clic en **Configuración de gadget**, en el panel de navegación izquierdo.
2. Haga clic en **Lista de gadget externos**.
3. Haga clic en **Obtener todo**. El sistema muestra una lista de los gadget externos que están disponibles en el sistema.
4. Habilite el gadget que los usuarios de one-X Portal para IP Office pueden agregar a la ventana one-X Portal para IP Office.
5. Haga clic en **Ingresar selección**. El sistema actualiza los gadget externos que habilitó en la base de datos one-X Portal para IP Office.

3.4.7 Desactivar un gadget externo

Cuando se desactiva un gadget, los usuarios de one-X Portal para IP Office no podrán agregar ese gadget a la ventana de one-X Portal para IP Office. Si desactiva un gadget que los usuarios ya han agregado a su ventana de one-X Portal para IP Office, el sistema no mostrará el gadget cuando los usuarios inicien sesión la próxima vez.

Para desactivar un gadget externo:

1. Haga clic en **Configuración de Gadget**, en el panel de navegación izquierdo.
2. Haga clic en **Lista de Gadgets externos**.
3. Haga clic en **Obtener todo**. El sistema muestra una lista de los gadget externos que están disponibles en el sistema.
4. Desactive el gadget que no desea que los usuarios de one-X Portal para IP Office agreguen en la ventana de one-X Portal para IP Office.
5. Haga clic en **Ingresar selección**. El sistema actualiza los gadgets externos que deshabilitó en la base de datos one-X Portal para IP Office.

3.4.8 Eliminar un gadget externo

Para eliminar un gadget externo:

1. Haga clic en **Configuración de Gadget**, en el panel de navegación izquierdo.
2. Haga clic en **Lista de gadgets externos**.
3. Haga clic en **Obtener todo**. El sistema muestra una lista de los gadget externos que están disponibles en el sistema.
4. Seleccione el gadget que desea eliminar.
5. Haga clic en **Eliminar**.
6. Haga clic en **Sí** para confirmar que desea eliminar el gadget. El sistema actualiza los gadgets externos que eliminó en la base de datos de one-X Portal para IP Office.

3.5 Usuarios

3.5.1 Incorporación o eliminación de usuarios

El servidor one-X Portal para IP Office está sincronizado con los usuarios que existen en los sistemas IP Office. Los usuarios se agregan y/ o se eliminan a través de la configuración de IP Office.

Los cambios realizados a los usuarios en los sistemas IP Office se actualizarán dentro de one-X Portal para IP Office y otros clientes de Avaya, como movilidad y Avaya Communicator, entre otros, 10 minutos después del momento de sincronización; además, los usuarios deben haber iniciado sesión después de la sincronización.

3.5.2 Edición de la configuración de usuarios

Puede utilizar los menús de administración del portal para ver y editar una serie de opciones de configuración de usuarios.

Para editar configuraciones de usuarios:

1. Seleccione **Configuración** y, a continuación, **Usuarios**.
2. Haga clic en **Obtener todo** y recorra los usuarios.
3. Haga clic en el botón **Editar** que se encuentra junto al usuario que desea editar. Aparecerá la configuración de usuario.

4. Utilice el **Selector de tipo de configuración de usuario** para seleccionar los valores de configuración del usuario que desea ver o editar. De ser necesario, edite los valores.

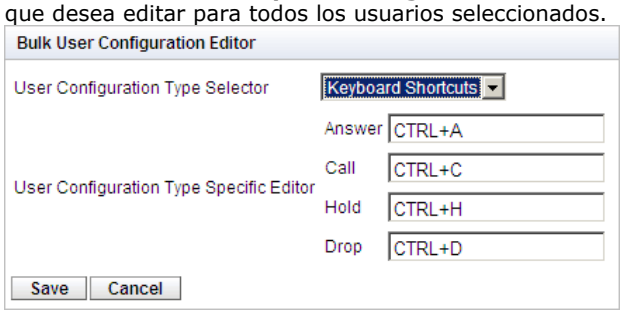
   - **Ventanas emergentes**
     Muestra el enlace para descargar el software de instalación de escritorio del cliente de one-X Portal Call Assistant y Outlook Plug-in.
   - **Posición de estacionamiento**
     Permite la configuración de los números de posiciones de estacionamiento asociados con los botones del estacionamiento del usuario.
   - **Número de puente**
     Permite la configuración del puente del usuario para las conferencias de enlace de encuentro.
   - **Modo de teletrabajador**
     Permite la selección del modo de teletrabajo para el usuario y la configuración del número fijo o de móvil que se utilizará cuando el modo esté activo.
   - **Configuración de MI/Presencia**
     Permite la configuración de las opciones de MI/Presencia. Tenga en cuenta que el usuario, igualmente, debe habilitar las notificaciones a través de su propia sesión de one-X Portal para IP Office.

5. Haga clic en **Guardar**.
6. Para confirmar los valores editados en la base de datos de one-X Portal para IP Office, seleccione la casilla de verificación que se encuentra junto al usuario y haga clic en **Ingresar selección**.

Para realizar edición múltiple de configuraciones de usuarios:

1. Seleccione **Configuración** y, a continuación, **Usuarios**.
2. Haga clic en **Obtener todo** y recorra los usuarios.
3. Seleccione la casilla de verificación que se encuentra junto a cada uno de los usuarios que desea editar.
4. Haga clic en **Edición múltiple**.

5. Utilice el **Selector de tipo de configuración de usuario** para seleccionar los valores de configuración de usuarios que desea editar para todos los usuarios seleccionados.



6. Cuando haya finalizado la edición, haga clic en **Guardar**.
7. Seleccione la casilla de verificación junto a cada uno de los usuarios que editó y haga clic en **Ingresar selección** para volver a enviar los cambios a la base de datos de one-X Portal para IP Office.

3.6 Directorios

3.6.1 Incorporación de una fuente de directorios externos de LDAP

Durante la instalación, se crea un proveedor de LDAP de forma predeterminada pero no se configura para la conexión con un servidor de LDAP (a menos que se seleccione una instalación avanzada y se modifique la configuración del proveedor de LDAP). El proceso que figura a continuación modifica la configuración del proveedor de LDAP para permitir el funcionamiento de LDAP.

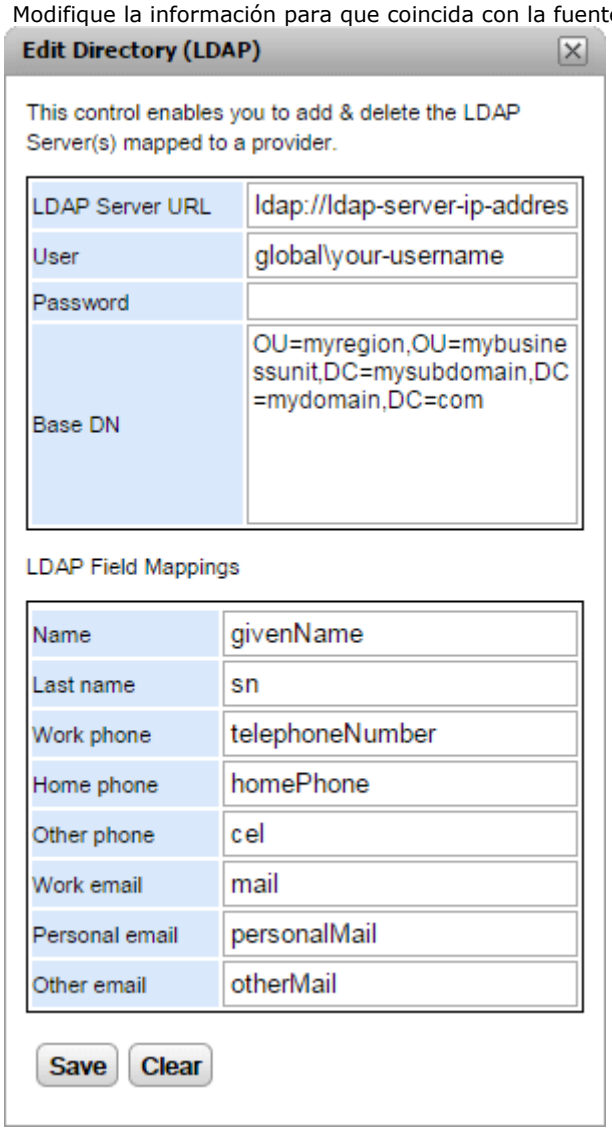
El funcionamiento de LDAP puede evaluarse a través de la opción **Integración de directorios | Búsqueda de directorios de LDAP** 42 en los menús de administrador.

A diferencia de la asistencia de LDAP en IP Office, el servidor one-X Portal para IP Office no importa registros de la fuente de LDAP y luego utiliza esos registros como un directorio. En cambio, cuando un usuario de one-X Portal para IP Office ingresa caracteres en la ficha Directorio externo del gadget Directorio, el servidor one-X Portal para IP Office utiliza la configuración de la fuente de LDAP para realizar una búsqueda en tiempo real de los registros de fuentes de LDAP. Por lo tanto, el servidor one-X Portal para IP Office no necesita actualizar los registros de LDAP con regularidad.

- **Advertencia**
  Este proceso requiere que reinicie el servicio del portal 52 para que los cambios surtan efecto. Durante el reinicio, el portal no estará disponible para los usuarios por un máximo de 15 minutos.

Para agregar un directorio LDAP externo:

1. Inicie sesión en los menús de administrador.
2. Seleccione **Configuración** y, a continuación, **Proveedores**.
3. Desde el menú desplegable **Nombre del proveedor** seleccione ***Directorio (LDAP)***.
4. Haga clic en el icono junto al proveedor de LDAP.
5. Modifique la información para que coincida con la fuente del servidor de LDAP que desea utilizar.



- **URL del servidor de LDAP**
  La URL de la fuente de directorios de LDAP, como por ejemplo ***ldap:\\ldap.example.com***.

- **Usuario/ contraseña**
  El nombre de usuario y la contraseña para acceder al servidor de LDAP.
- **Nombre distintivo de la base**
  También se conoce como **Base de búsqueda**. Define qué conjunto de registros de la fuente de LDAP debe utilizarse para realizar búsquedas. El administrador del servidor de LDAP proporcionará una cadena apropiada, como por ejemplo *ou=Users,dc=global,dc=example,ddc=com*.
- **Asignaciones de campos de LDAP**
  Los nombres de campos (a la izquierda) son los nombres de los campos mostrados en el directorio de one-X Portal para IP Office. Ingrese los nombres del campo que coincida para cada uno en los registros de fuentes de LDAP.

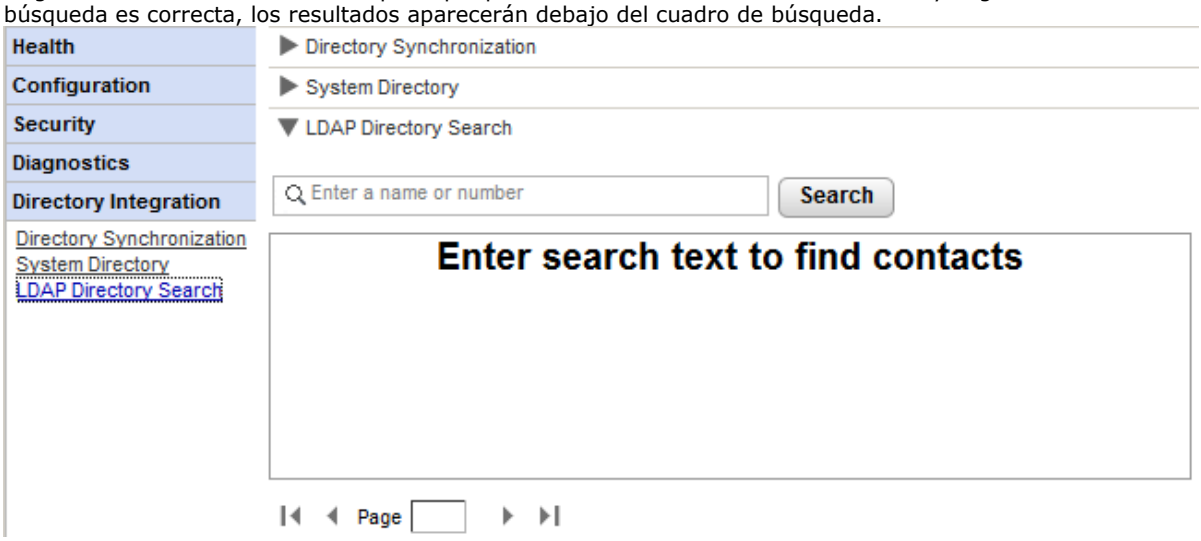
6. Haga clic en **Guardar**.
7. Reinicie el servicio Avaya one-X Portal 52.

3.6.2 Verificación del directorio externo de LDAP

Si ha configurado una fuente de directorios externos de LDAP, puede comprobar el acceso a través de one-X Portal para IP Office desde los menús de administrador.

Para comprobar el directorio LDAP:

1. Seleccione **Integración de directorios**.
2. Seleccione **Búsqueda de directorios de LDAP**.
3. Ingrese un nombre o un número que sepa que se encuentra en el directorio externo y haga clic en **Buscar**. Si la búsqueda es correcta, los resultados aparecerán debajo del cuadro de búsqueda.



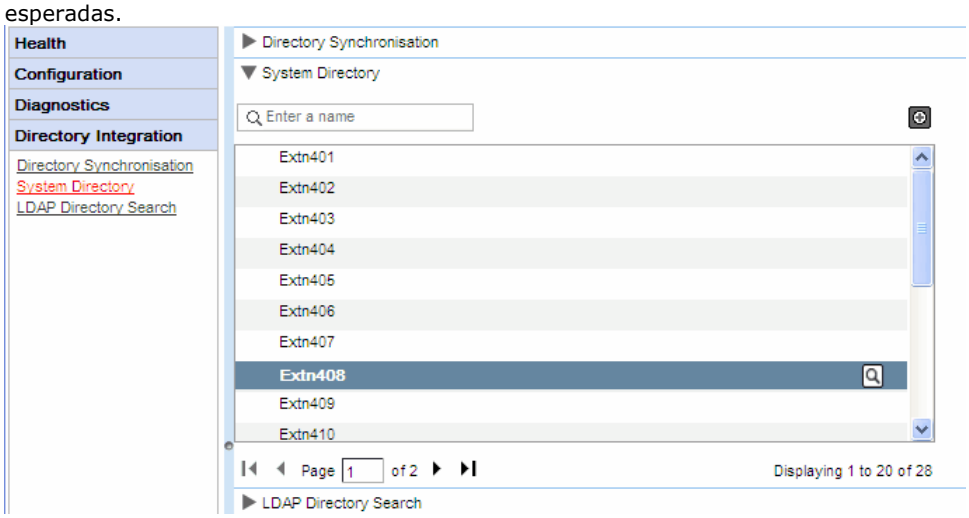
3.6.3 Verificación y actualización del directorio del sistema

El directorio del sistema que se muestra a los usuarios de one-X Portal para IP Office es una combinación de usuarios, grupos y entradas de directorios de todos los sistemas IP Office con los que se configuró one-X Portal para IP Office para su funcionamiento.

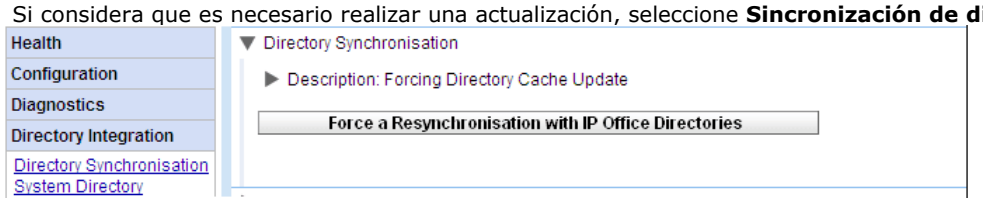
De forma predeterminada, la aplicación one-X Portal para IP Office actualiza los registros del directorio del sistema cada 300 segundos aproximadamente. A través de los menús de administrador de one-X Portal para IP Office es posible ver el directorio del sistema y forzar una actualización.

Para comprobar el directorio del sistema:

1. Seleccione **Integración de directorios**.
2. Seleccione **Directorio del sistema**. Aparecerá el directorio del sistema actual. Verifique que las entradas sean las esperadas.



3. Si considera que es necesario realizar una actualización, seleccione **Sincronización de directorios**.



4. Haga clic en **Forzar una resincronización con todos los directorios de IP Office**.

3.7 Actualización/regreso a versión anterior

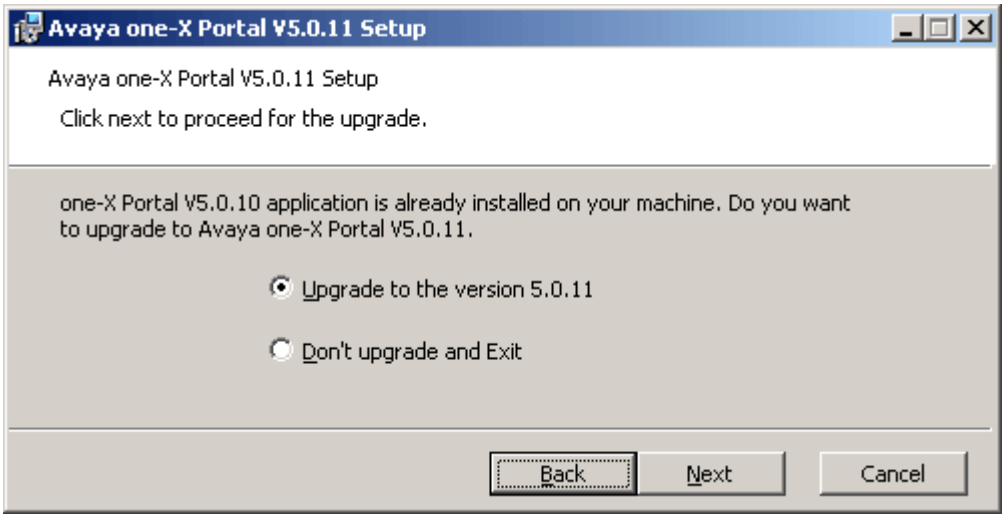
El proceso de esta sección corresponde a los servidores basados en Windows únicamente.

3.7.1 Actualización de one-X Portal para IP Office

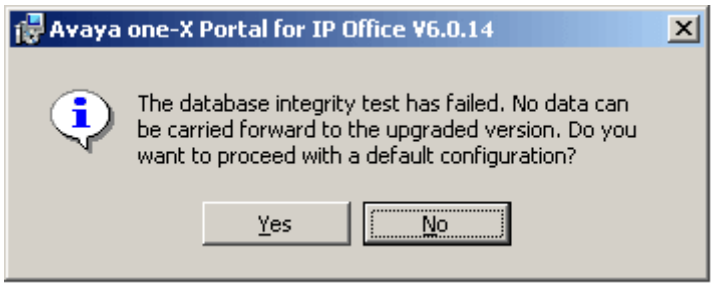
Antes de actualizar one-X Portal para IP Office basado en Windows, asegúrese de haber leído el boletín técnico de Avaya IP Office para la versión de software one-X Portal para IP Office que desea instalar o la versión de software IP Office en la que se incluyó. Este boletín incluye información sobre los requisitos especiales y pasos adicionales que no están incluidos en esta documentación.

Si one-X Portal para IP Office ya se instaló en una computadora del servidor y se está ejecutando el archivo de instalación de una versión posterior, la versión existente se detectará y el sistema le preguntará si desea realizar la actualización. Si opta por hacerlo, el proceso será similar a la instalación de software normal, aunque algunas opciones de instalación estarán inhabilitadas porque la configuración existente no puede modificarse.

- **Advertencia**
  Este proceso requiere que reinicie el servicio del portal 52 para que los cambios surtan efecto. Durante el reinicio, el portal no estará disponible para los usuarios por un máximo de 15 minutos.



- Si la base de datos existente de one-X Portal para IP Office no puede actualizarse, aparecerá una advertencia. Si selecciona Sí, la base de datos existente se reemplazará por la predeterminada. Si selecciona No, deberá volver a ejecutar el instalador para poder volver a la versión anterior 73 de one-X Portal para IP Office que es compatible con la base de datos.



Durante el proceso de actualización, se crea un archivo de copia de seguridad (backup.sql). Ésta no es una copia de seguridad completa del sistema one-X Portal para IP Office y no debe utilizarse para restablecer la configuración.

3.7.2 Regreso a la versión anterior de one-X Portal para IP Office

Si el software de la aplicación one-X Portal para IP Office basado en Windows se actualizó por medio del proceso de actualización 72, también es posible volver a la versión original instalada.

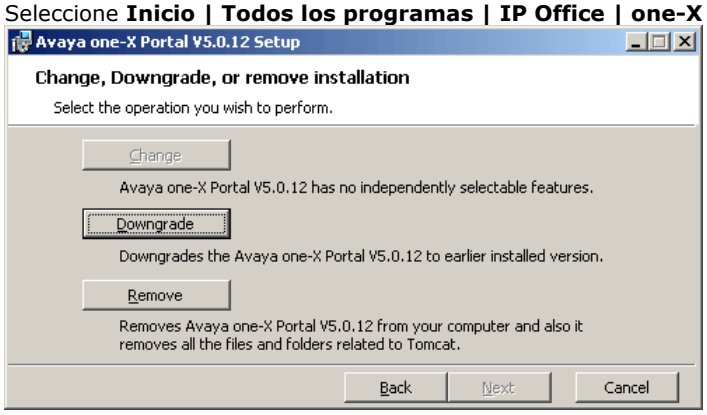
- **Nota:** Tanto la instalación de one-X Portal para IP Office como la última actualización al one-X Portal para IP Office figuran en la lista **Agregar y quitar programas** del Panel de control de Windows. No obstante, es importante señalar que la eliminación de cualquiera de estas opciones eliminará toda la aplicación.

Antes de volver a la versión anterior de one-X Portal para IP Office, asegúrese de haber leído el boletín técnico de Avaya IP Office para las versiones de software de one-X Portal para IP Office. Este boletín incluye información sobre los requisitos especiales y pasos adicionales que no están incluidos en esta documentación.

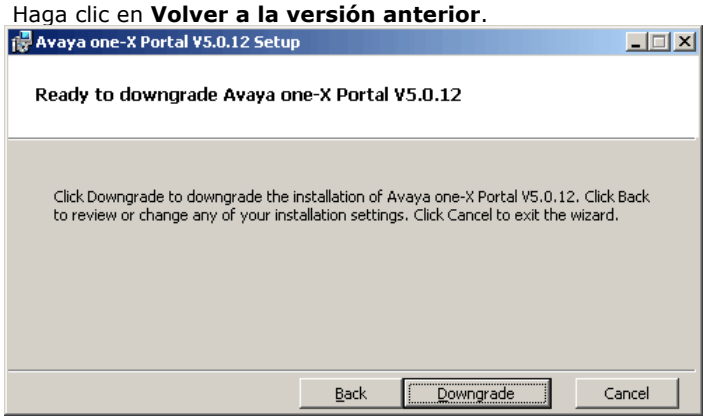
- **Advertencia**
  Este proceso requiere que reinicie el servicio del portal 52 para que los cambios surtan efecto. Durante el reinicio, el portal no estará disponible para los usuarios por un máximo de 15 minutos.

Para volver a una versión anterior de one-X Portal para IP Office:

1. Seleccione **Inicio | Todos los programas | IP Office | one-X Portal | Desinstalar one-X Portal**.



2. Haga clic en **Volver a la versión anterior**.



3. Cuando se haya realizado la acción, Avaya one-X Portal deberá reiniciarse manualmente 52.

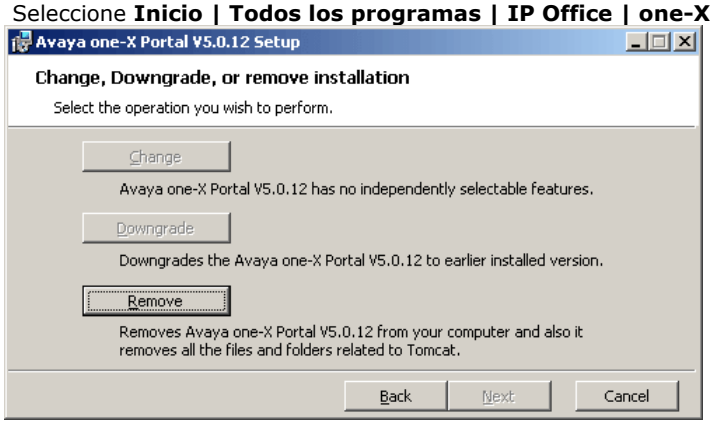
3.7.3 Eliminación de one-X Portal para IP Office

Existen 2 métodos para eliminar la aplicación one-X Portal para IP Office de un servidor de Windows.

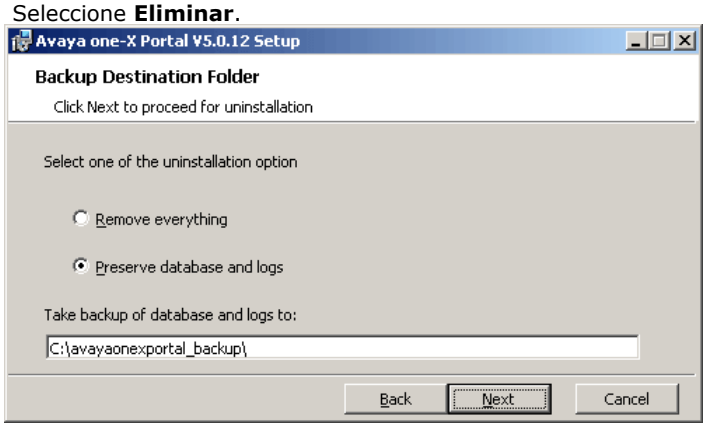
Para desinstalar one-X Portal para IP Office:

Este método de eliminación permite seleccionar si deben conservarse copias de seguridad de la base de datos y archivos de registro.

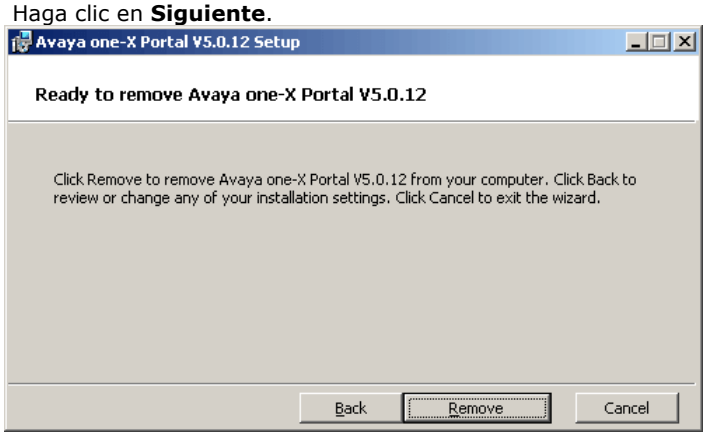
1. Seleccione **Inicio | Todos los programas | IP Office | one-X Portal | Desinstalar one-X Portal**.



2. Seleccione **Eliminar**.



3. Haga clic en **Siguiente**.



4. Haga clic en **Eliminar** para iniciar el proceso de eliminación de archivos.

Para eliminar one-X Portal para IP Office mediante el panel de control de Windows:

La opción **Agregar o quitar programas** del panel de control de Windows puede utilizarse para eliminar one-X Portal para IP Office. Este método realiza copias de seguridad de la base de datos y los archivos de registro en la carpeta ***c:\avayaonexportal_backup*** automáticamente.

1. Inicie el panel de control estándar de Windows.
2. Seleccione **Agregar o quitar programas**.
3. Seleccione **one-X Portal** y, a continuación, haga clic en **Eliminar**.
   - Si one-X Portal para IP Office se actualizó en alguna oportunidad, habrá una entrada de programa tanto para la instalación original de one-X Portal para IP Office como para la actualización más reciente. Seleccione la actualización y la instalación y, a continuación, haga clic en Eliminar. Se eliminará tanto la actualización como la instalación original.

3.8 Mensajería instantánea/Presencia

El servidor one-X Portal para IP Office incluye un servidor XMPP como componente que está activado de manera predeterminada. Este servidor permite que los usuarios se envíen MI entre sí y que compartan su presencia de MI.

El archivado de los mensajes instantáneos también está activado de manera predeterminada, lo que le permite buscar mensajes anteriores del usuario.

- Configuración del servidor de MI 77
- Inicio del servidor de MI 79
- Búsqueda en el archivo de MI 80
- Configurar la duración de generación de archivos MI 77
- Integración de calendario de Exchange 81

Para desactivar el archivado de MI:

1. Activación de la consola de administración de XMPP Server 82
2. Uso del servidor XMPP para desactivar la configuración de archivado de MI 83
3. Desactivación de consola de administración de XMPP Server 83

Para activar el archivado de MI:

1. Activación de la consola de administración de XMPP Server 82
2. Uso del servidor XMPP para activar la configuración de archivado de MI 82
3. Desactivación de consola de administración de XMPP Server 83

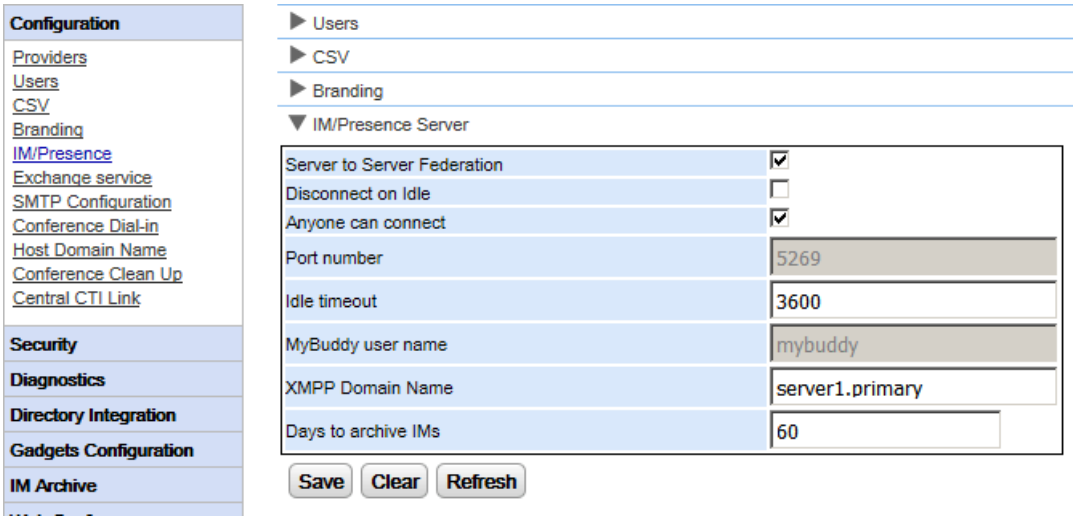
Cambios en la operación de XMPP predeterminada

Antes de las versión 9.1 de IP Office, todos los sistemas de IP Office tenían un grupo de XMPP predeterminado que contenía a cada usuario de IP Office como miembro. Como consecuencia, cada usuario podía ver automáticamente la presencia de MI de otro usuario.

Para la versión 9.1 de IP Office, lo anterior ya no tiene vigencia. El uso compartido de MI/presencia entre los usuarios requiere la configuración manual de grupos de XMPP que contengan a esos usuarios en la configuración del sistema de IP Office (consulte la ayuda o la documentación de IP Office Manager).

3.8.1 Configuración del servidor de MI

El portal incluye un componente que actúa como servidor de mensajería instantánea/presencia. El servidor de MI/Presencia se puede configurar aparte. Consulte Mensajería instantánea/Presencia 76.



Para configurar el servidor de MI/Presencia:

1. Haga clic en **Configuración** y seleccione **Servidor de MI/Presencia**.
2. Seleccione la configuración de servidor requerida:

- **Federación servidor a servidor**
  Si se selecciona, el servidor de presencia del portal puede intercambiar información de presencia con otros servidores de presencia.
- **Desconectar cuando la sesión esté inactiva**
  Si se selecciona, las conexiones de servidor a servidor se desconectan cuando no hay actividad durante el período de **Tiempo de espera en inactividad**.
- **Cualquiera se puede conectar**
  Permite que cualquiera se conecte a los servicios de MI/Presencia.
- **Número de puerto**
  Está establecido como fijo en ***5269***.
- **Tiempo de espera en inactividad**
  El tiempo de espera, en segundos, que se utiliza si se selecciona la opción **Desconectar cuando la sesión esté inactiva**.
- **Nombre de usuario de MyBuddy**
  Este campo está establecido como fijo en ***mybuddy***. Puede requerirse el valor al momento de integrar los detalles de presencia con otros servicios de MI/Presencia.
- **Nombre de dominio de XMPP**
  Establece el nombre de dominio DNS que se utiliza para las funciones de MI/Presencia:
  - El nombre de dominio de XMPP debe ser un nombre de dominio que DNS pueda resolver. Puede establecer el nombre de dominio de XMPP en cualquier momento. El nombre de dominio debe ser accesible desde Internet si desea utilizar presencia fuera de su red LAN; por ejemplo, con one-X Mobile.
  - Avaya recomienda utilizar un DNS dividido de modo que el nombre del servidor fuera de su red LAN sea resuelto en la dirección IP pública de la NAT o firewall mientras que, dentro de la red, se resuelve en la dirección IP privada del servidor de la red LAN.
  - Si no puede establecer un nombre de dominio DNS que se pueda resolver, puede utilizar la dirección IP del servidor de one-X Portal para IP Office para MI/Presencia solo interna. En este caso, one-X Portal para IP Office no puede federar con servidores remotos.
  - Para servidores basados en Linux (IP Office Server Edition, IP Office Application Server y Unified Communications Module), debe utilizar los menús de Web Control del servidor para configurar los parámetros de red de modo que el enlace de correo electrónico de configuración automática utilice el nombre FQDN en lugar de la dirección IP del servidor. En Web Control, diríjase a Configuración > Sistema > Nombre del host para cambiar la configuración de la red. Si cambia el nombre de dominio de cualquier otra manera, puede que los enlaces del correo electrónico no funcionen adecuadamente.
- **Días para archivar MI**
  Este campo configura cuánto tiempo el servidor debería conservar los mensajes en el archivo de MI antes de eliminarlos. La configuración predeterminada es 182 días (6 meses). Si es necesario, puede desactivar el archivado de MI 83 mediante la consola de administrador de XMPP. El servidor de MI/presencia debe estar disponible (consulte Estado del servidor de MI/Presencia 13) para cambiar esta configuración.

Página983 de 3226.

3. Haga clic en **Guardar**.

3.8.2 Configuración de MI del usuario

Dos usuarios de IP Office solamente pueden ver el estado de presencia del otro e intercambiar mensajes instantáneos si son miembros del mismo grupo XMPP en la configuración del sistema IP Office. Cada usuario puede ser miembro de uno o varios grupos XMPP.

Si un nuevo usuario de IP Office se agrega como acción simple (agregar usuario, agregar nuevo usuario a grupo XMPP, guardar configuración), el usuario no se verá en la vista del portal del grupo XMPP. La solución es, entonces, realizar más cambios de configuración al grupo XMPP o reiniciar el servicio del portal.

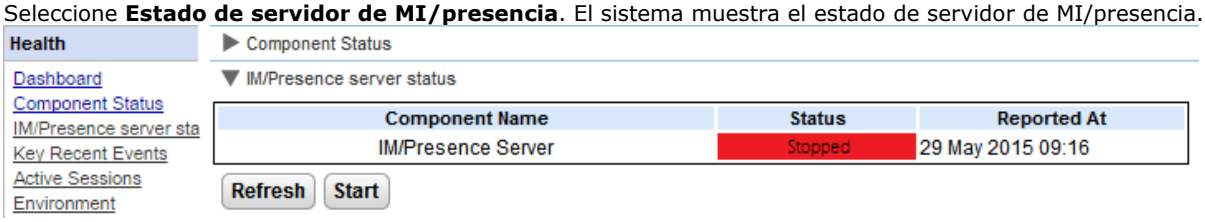
Para evitarlo, debería guardar la configuración entre cada acción (agregar usuario, guardar configuración, agregar nuevo usuario a grupo XMPP, guardar configuración).

3.8.3 Inicio del servidor de MI

Puede comprobar el estado del servidor de MI/Presencia a través del menú Estado del servidor de MI/Presencia 13. Si el servidor de MI/Presencia no se está ejecutando, puede seguir el proceso indicado a continuación para dar comienzo al servicio.

Para iniciar el servidor de MI/Presencia:

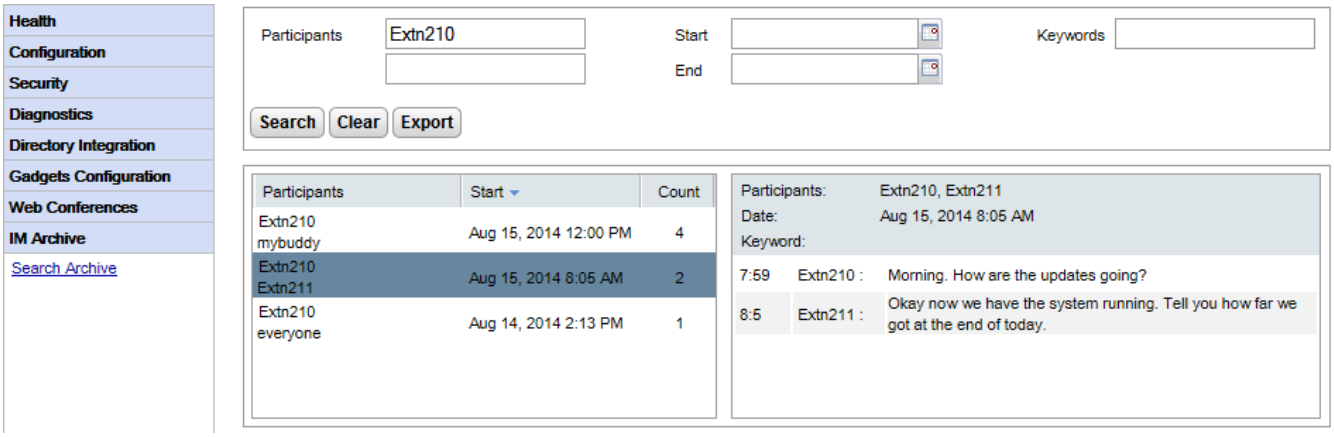
1. Seleccione **Estado**.
2. Seleccione **Estado de servidor de MI/presencia**. El sistema muestra el estado de servidor de MI/presencia.



3. Haga clic en **Iniciar**.
   - Si la base de datos está dañada, el sistema muestra el mensaje *"La base de datos del servidor de MI/Presencia está dañada y debe ser restaurada. ¿Desea restaurar la base de datos?"*
     - Para restaurar la base de datos e iniciar el servidor de MI/Presencia, haga clic en **Sí**. El sistema restaura la base de datos desde la carpeta de respaldo. El sistema respalda automáticamente la base de datos cada ocho horas. No puede iniciar el servidor de MI/presencia sin restaurar la base de datos corrupta.
     - Si selecciona **No**: El sistema muestra *"El servidor de MI/Presencia no se puede iniciar con la base de datos dañada. Las características de MI/Presencia no estarán disponibles"*.

3.8.4 Búsqueda en el archivo de MI

Puede buscar conversaciones de mensajería instantánea entre los usuarios y del sistema a un usuario. Todos los campos en el panel de búsqueda son opcionales. La cantidad de días que el servidor conserva un MI en el archivo se determina mediante la configuración de **Días para archivar MI** 77.



Para buscar en el archivo de MI:

1. En el panel de la izquierda, seleccione el **Archivo de MI**.
2. Haga clic en **Buscar archivo**.
3. Ingrese los criterios de búsqueda y haga clic en Buscar.

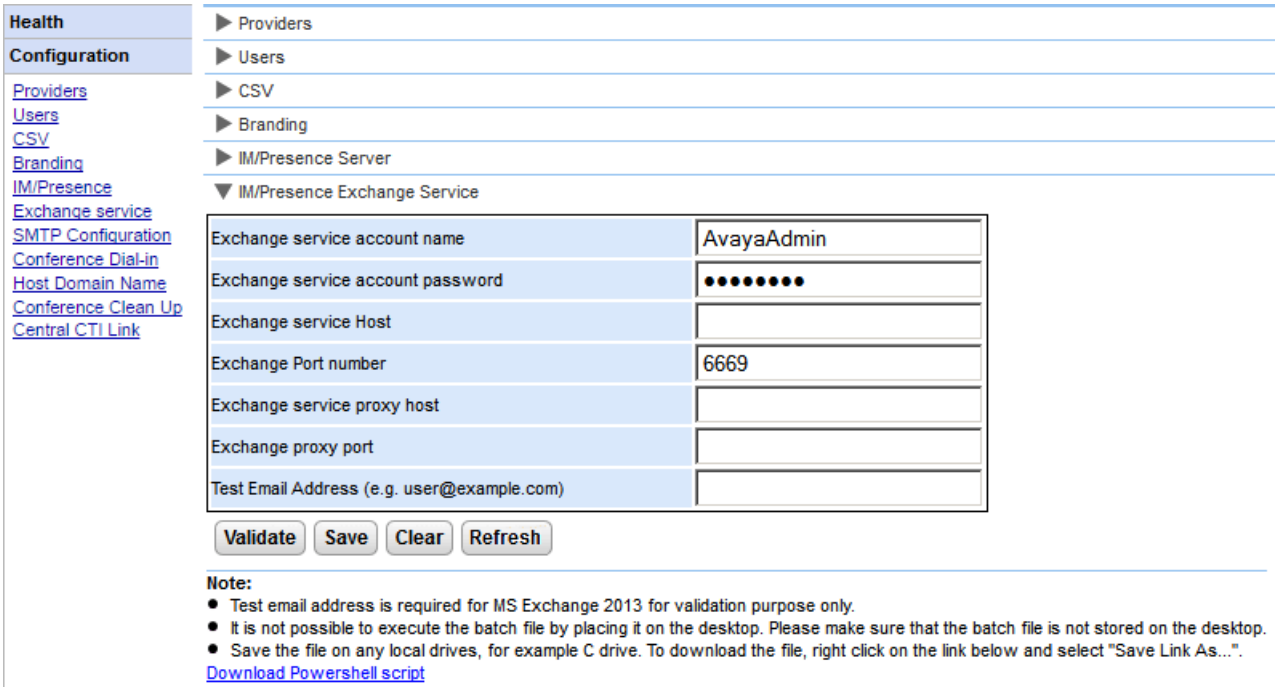
Campo	Descripción
Participantes	Escriba el nombre del participante en la conversación de MI.
Palabras clave	Escriba las palabras clave en la conversación de MI.
inicie	Seleccione la fecha desde la que se deben incluir las conversaciones. Si no selecciona una fecha, el sistema muestra desde la conversación más reciente que guardó el sistema.
Fin	Seleccione la fecha hasta la que se deben incluir las conversaciones. Si no selecciona una fecha, el sistema muestra hasta la conversación más reciente.

4. Haga clic en la conversación que desea abrir. El sistema muestra la conversación.

3.8.5 Integración de calendario de Exchange

one-X Portal para IP Office se puede configurar con el servidor Exchange para validar la información de minería de calendario y de presencia de los usuarios. Solamente Microsoft Exchange Server 2007, 2010 y 2013 se pueden configurar con one-X Portal para IP Office.

En esta sección se ofrece únicamente un resumen de las opciones de configuración. Consulte el manual *Implementar one-X Portal para IP Office* para obtener los detalles completos de la integración del servidor Microsoft Exchange.



Para configurar servicios de Exchange:

1. Haga clic en **Configuración**, en el panel de navegación izquierdo.
2. Haga clic en **Servicio Exchange**.
   a. Escriba ***AvayaAdmin*** en el campo **Nombre de cuenta para servicio Exchange**. Asegúrese de que este nombre sea el mismo que la cuenta de ***AvayaAdmin*** que creó en el servidor Exchange.
   b. Ingrese la contraseña que se estableció para **AvayaAdmin** en **Contraseña de cuenta para servicio Exchange**.
   c. Ingrese la dirección IP del host del servicio Exchange en **Host de servicio Exchange**.
   d. Ingrese el número de puerto del servicio Exchange en **Número de puerto para Exchange**.
   e. Ingrese el nombre de dominio del servidor proxy que se utiliza para conectarse al servidor Exchange en **Host del proxy para servicio Exchange**.
   f. Ingrese el número de puerto del servidor proxy para el servicio Exchange en **Puerto proxy para Exchange**.
   g. Establezca una **Dirección de correo electrónico de prueba** utilizando una dirección de correo electrónico válida.
3. Haga clic en **Validar configuración del servicio Exchange** para verificar si los detalles de intercambio proporcionados son válidos.
4. Haga clic en **Guardar**.

3.8.6 Activación de la consola de administrador de XMPP

Por cuestiones de seguridad, la consola de administrador de XMPP no se encuentra activada de forma predeterminada. Si se la activa para mantenimiento o resolución de problemas, luego debe desactivar la consola del administrador 83 nuevamente.

Para activar la consola del administrador: (Linux)

1. Inicie sesión como usuario root.
2. Introduzca `cd /opt/Avaya/oneXportal/openfire/bin`
3. Ante la solicitud, introduzca: `sh AdminConsoleManager.sh enable`
4. Para reiniciar el servicio, introduzca: `service onexportal restart`

Para activar la consola del administrador: (Windows)

1. Vaya al símbolo del sistema.
2. Vaya al directorio donde está instalado one-X Portal para IP Office, por ejemplo cd `C:\Program Files\Avaya\oneXportal` .
   - **Nota:** La ruta de instalación será distinta en una instalación para 32 o 64 bits
3. Introduzca `cd \openfire\bin`
4. En el símbolo del sistema, escriba: `AdminConsoleManager.bat enable`
5. Reinicie Avaya one-X Portal.

3.8.7 Activación del archivado de MI

Para activar la configuración de archivado de MI en el servidor XMPP:

1. Activar la consola de administrador de XMPP 82.
2. Abra la consola de administrador en un explorador, mediante la introducción de*http://<dirección IP del servidor>:9094*
3. Inicie sesión con el nombre y la contraseña ***admin***.
4. Haga clic en la pestaña **Servidor**.
5. Haga clic en la pestaña **Archivado**.
6. En el panel de la izquierda, seleccione **Configuración de archivado**.
7. Active las siguientes casillas de verificación:
   - **Archivado de estado de conversación**
   - **Archivar chats personales**
   - **Archivar chats grupales**
8. Haga clic en el botón **Actualizar configuración**. El sistema guarda la configuración y muestra el siguiente mensaje: *Se ha guardado la configuración de archivado.*
9. Desactivar la consola de administrador de XMPP 83.

3.8.8 Desactivación de archivo de MI

Para desactivar el archivado de MI:

1. Activar la consola de administrador de XMPP 82.
2. Abra la consola de administrador en un explorador, mediante la introducción de*http://<dirección IP del servidor>:9094*
3. Inicie sesión con el nombre y la contraseña ***admin***.
4. Haga clic en la pestaña **Servidor**.
5. Haga clic en la pestaña **Archivado**.
6. En el panel de la izquierda, seleccione **Configuración de archivado**.
7. Desactive las siguientes casillas de verificación:
   - **Archivado de estado de conversación**
   - **Archivar chats personales**
   - **Archivar chats grupales**
8. Haga clic en el botón **Actualizar configuración**. El sistema guarda la configuración y muestra el siguiente mensaje: *Se ha guardado la configuración de archivado.*
9. Desactivar la consola de administrador 83.

3.8.9 Desactivación de la consola de administrador de XMPP

Por cuestiones de seguridad, la consola de administrador de XMPP no se encuentra activada de forma predeterminada. Si se la activa para mantenimiento o resolución de problemas, luego debe desactivar la consola del administrador nuevamente.

Para desactivar la consola del administrador: (Linux)

1. Inicie sesión como usuario root.
2. Introduzca `cd /opt/Avaya/oneXportal/openfire/bin`
3. Ante la solicitud, introduzca: `sh AdminConsoleManager.sh disable`
4. Para reiniciar el servicio, introduzca: `service onexportal restart`

Para desactivar la consola del administrador: (Windows)

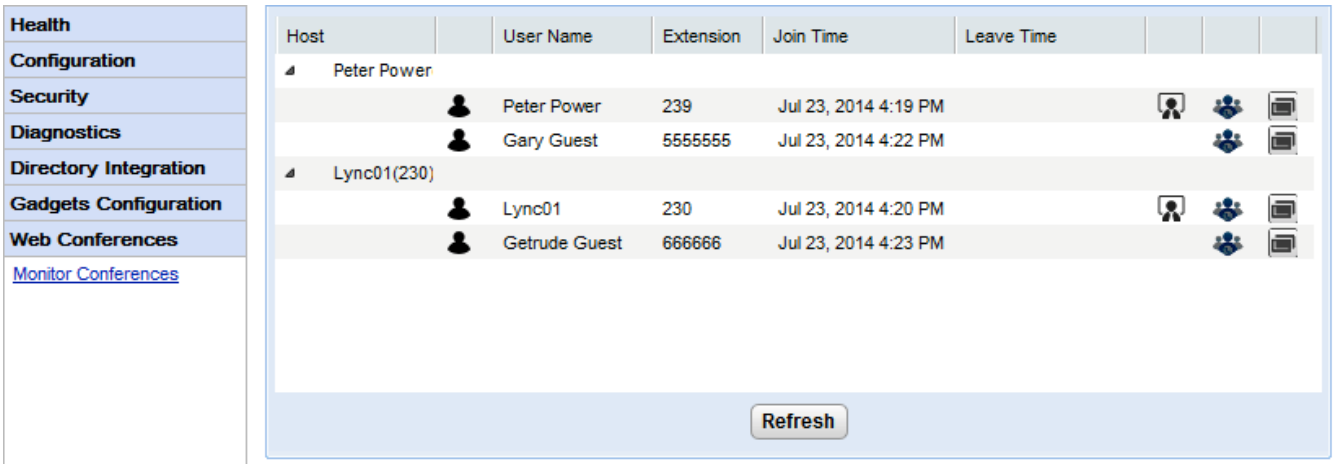
1. Vaya al símbolo del sistema.
2. Vaya al directorio donde está instalado one-X Portal para IP Office, por ejemplo cd `C:\Program Files\Avaya\oneXportal` .
   - **Nota:** La ruta de instalación será distinta en una instalación para 32 o 64 bits
3. Introduzca `cd \openfire\bin`
4. En el símbolo del sistema, escriba: `AdminConsoleManager.bat disable`
5. Reinicie Avaya one-X Portal.

3.9 Conferencias

El portal puede incluir un componente que proporciona soporte para funciones de conferencia: programar conferencias y sesiones de colaboración web, de manera paralela a las conferencias.

3.9.1 Visualización de conferencias

Este menú permite ver detalles de cualquier conferencia de colaboración web que aloje el servidor. Contiene una lista de los miembros de las conferencias, la última fecha en que se unieron y cuál es su participación (presentador, miembro de conferencia de audio, miembro de conferencia web). Este menú no se admite en el servidor de Unified Communications Module.

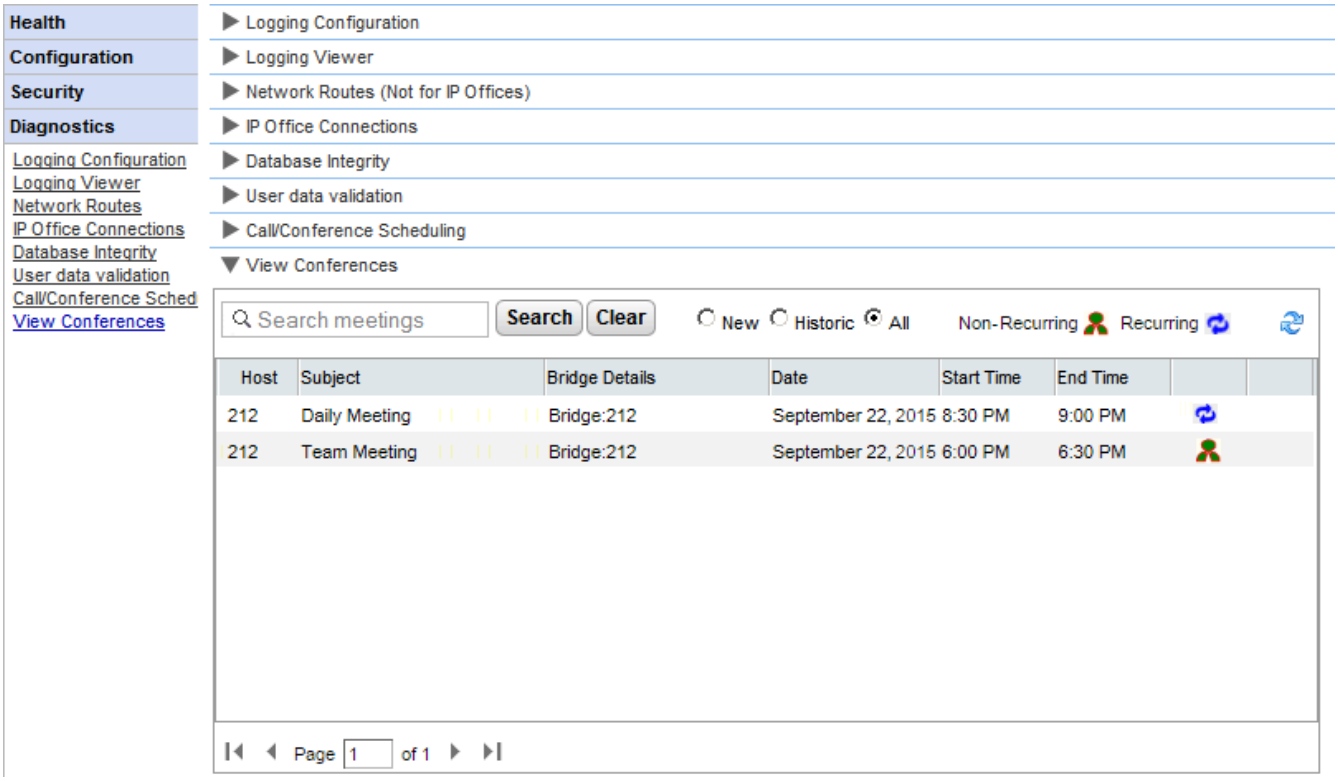


Para ver conferencias actuales:

1. Seleccione **Conferencias web** y, a continuación **Control de conferencias**.
2. Aparece una lista de la conferencia web actual.
3. Haga clic en **Host** para expandir la conferencia y ver detalles de los participantes.

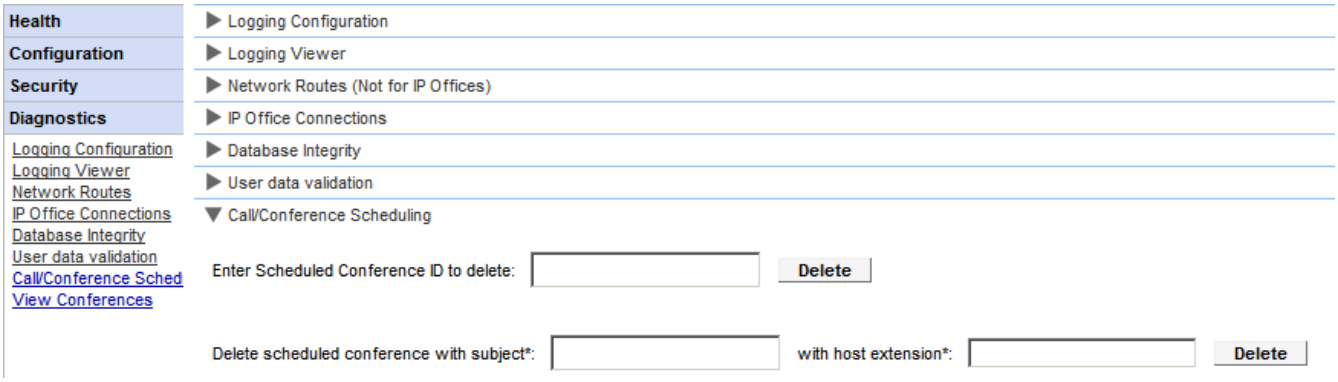
3.9.2 Visualización de conferencias programadas

En este menú, se muestra el calendario para la conferencia programada similar al que ven y utilizan los usuarios individuales de one-X Portal para IP Office. No obstante, la diferencia es que muestra las conferencias programadas para todos los usuarios. Puede utilizar este menú para eliminar una conferencia programada y modificar los detalles de conferencias futuras. Esta opción no se admite en los servidores basados en Windows.



3.9.3 Eliminación de una conferencia programada

Puede eliminar una conferencia futura programada. Si la conferencia es recurrente, se eliminan todas las instancias de la conferencia. Esta opción no se admite en los servidores basados en Windows.

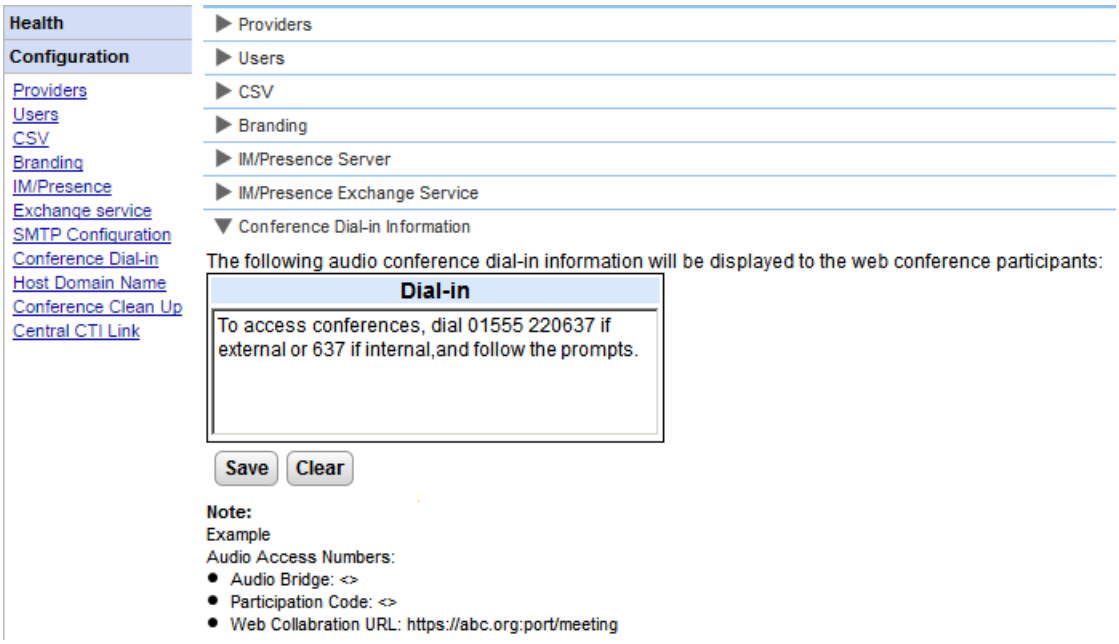


Para eliminar una o varias conferencias programadas:

1. Haga clic en **Diagnóstico** y seleccione **Programación de llamadas/conferencias**.
2. Ingrese la extensión del host y un asunto. Si deja el asunto vacío, se borran todas las conferencias que programó el host.
3. Haga clic en **Eliminar**.

3.9.4 Mensaje de notificación de conferencia

Cuando un usuario programa una conferencia, el servidor envía a los participantes invitados una notificación de conferencia a través de correo electrónico y mensajería instantánea. Esa notificación contiene los detalles de la conferencia establecidos por el usuario (número de puente, código del participante, URL de colaboración web). Además, puede incluir un texto fijo determinado mediante el menú **Acceso telefónico a conferencias**.

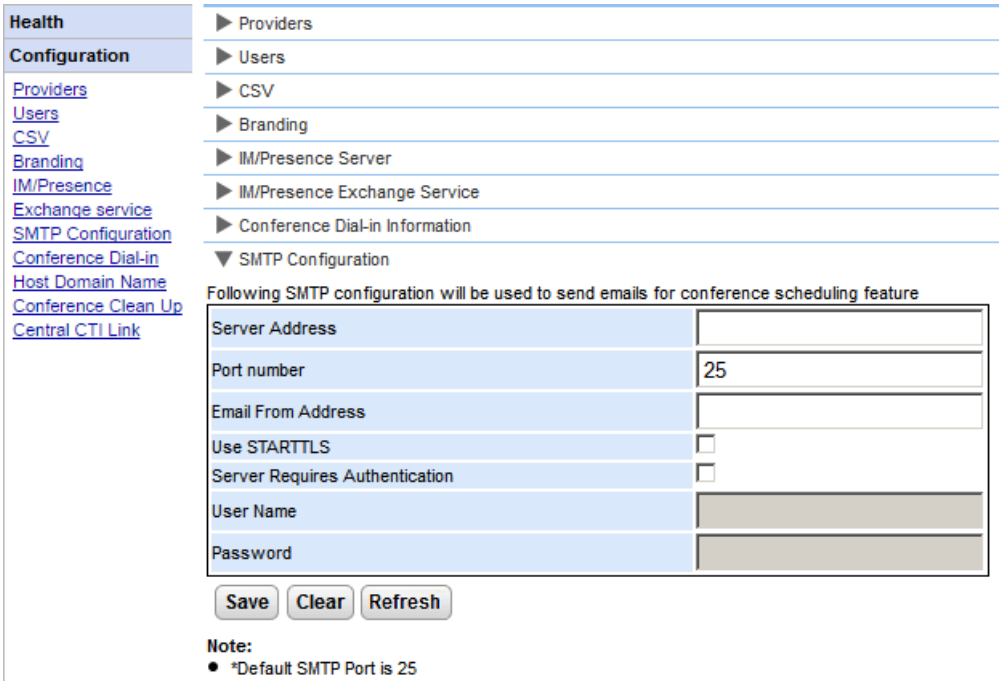


Para establecer el texto fijo de notificación de conferencia:

1. Seleccione **Configuración** y, a continuación, **Acceso telefónico a conferencias**.
2. Ingrese el texto fijo que debe incluirse en todas las notificaciones de conferencia.
3. Haga clic en **Guardar**.

3.9.5 Mensajes de correos electrónico de conferencia

Las invitaciones a la conferencia para el participante pueden enviarse por mensajería instantánea y también por correo electrónico. En el caso del correo electrónico, la configuración de correo electrónico de conferencia debe realizarse del siguiente modo. La dirección de correo electrónico que se utiliza para cada participante individual se establece en la configuración del sistema telefónico.



Para establecer el texto fijo de notificación de conferencia:

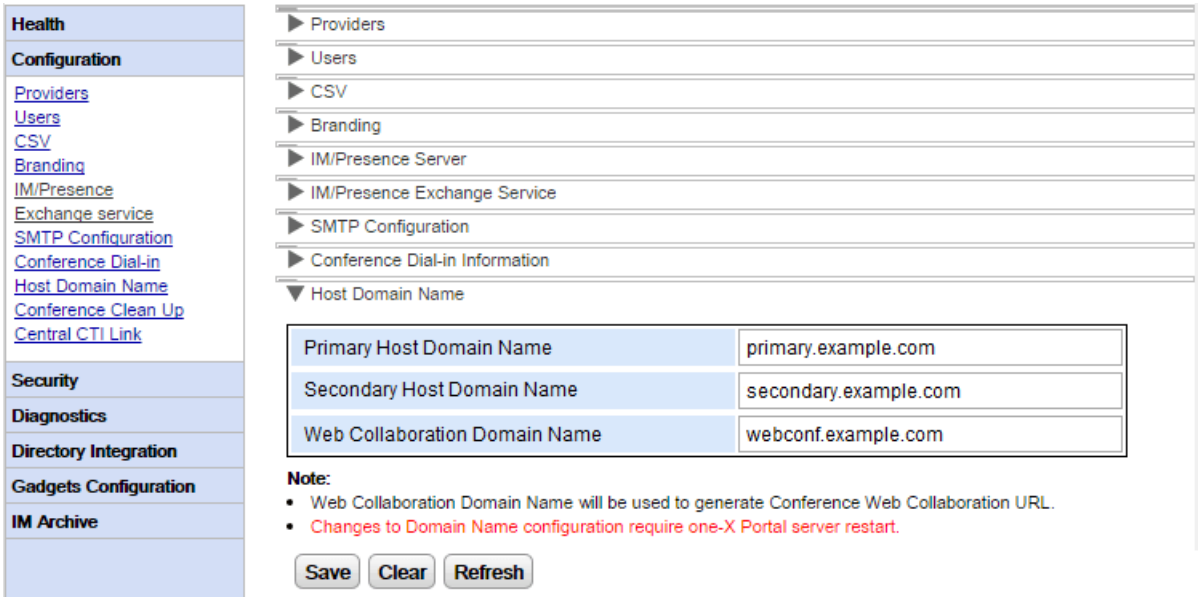
1. Seleccione **Configuración** y, a continuación, **Configuración SMTP**.
2. Establezca los detalles de correo electrónico SMTP que debe utilizar el servidor:
   - **Dirección del servidor**
     La dirección IP del servidor SMTP del cliente.
   - **Número de puerto**
     El puerto de escucha SMTP del servidor. El valor predeterminado es 25.
   - **Dirección del remitente**
     La dirección que será utilizada por el servidor. Algunos servidores de correo electrónico solo transmiten mensajes de direcciones reconocidas o direcciones con el mismo dominio.
   - **Usar STARTTLS**
     Seleccione este campo para activar la encriptación TLS/SSL. El cifrado permite la integración de correo de voz a correo electrónico con proveedores de correo electrónico alojado que solo permiten SMTP en un transporte más seguro.
   - **El servidor requiere autenticación**
     Si el servidor requiere una cuenta de usuario para recibir y enviar mensajes de email, ingrese los detalles de una cuenta configurada en ese servidor para ser usada por IP Office.
     - **Nombre de usuario**
       El nombre de cuenta que se utilizará si se selecciona El servidor requiere autenticación.
     - **Contraseña**
       La contraseña de cuenta que se utilizará si se selecciona El servidor requiere autenticación.
3. Haga clic en **Guardar**.

3.9.6 Establecer la URL de colaboración web

El menú**Configuración | Nombre de dominio del host** se usa para establecer el nombre de dominio utilizado para acceder a los servicios del portal y entre servidores del portal. La cantidad de nombres de dominio requeridos dependen del tipo de servidor de portal.

También se utiliza para establecer la URL del servicio de colaboración web. La URL de colaboración web se usa como predeterminada para invitaciones a conferencia cuando se programa una conferencia.

Tenga en cuenta que se si cambian los nombres de dominio, se debe reiniciar el servicio del portal para que los cambios surtan efecto.

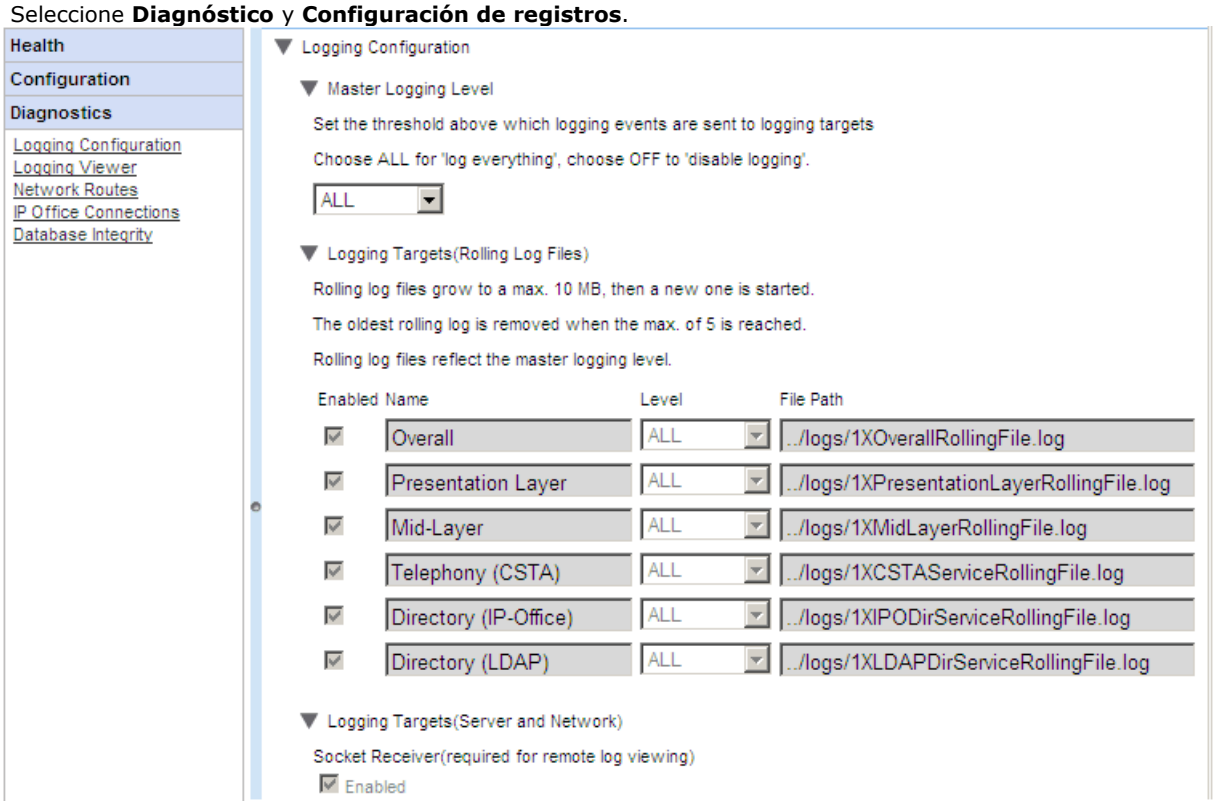


3.10 Registro remoto

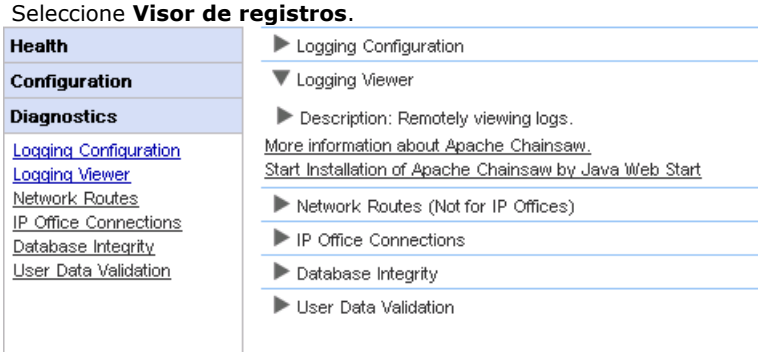
El servidor one-X Portal para IP Office puede configurarse para permitir que las aplicaciones de registro establezcan una conexión con el puerto 4560 para reunir información de registro. La información se encuentra en formato Log4j. La interfaz de administrador del servidor one-X Portal para IP Office incluye enlaces para instalar Apache Chainsaw.

Este proceso parte de la premisa de que la computadora desde la que se ejecuta tiene conexión a Internet. De no ser así, Apache Chainsaw puede descargarse e instalarse por medio de las instrucciones que se detallan en el sitio Web de Apache Chainsaw (http://logging.apache.org/chainsaw).

1. Seleccione **Diagnóstico** y **Configuración de registros**.

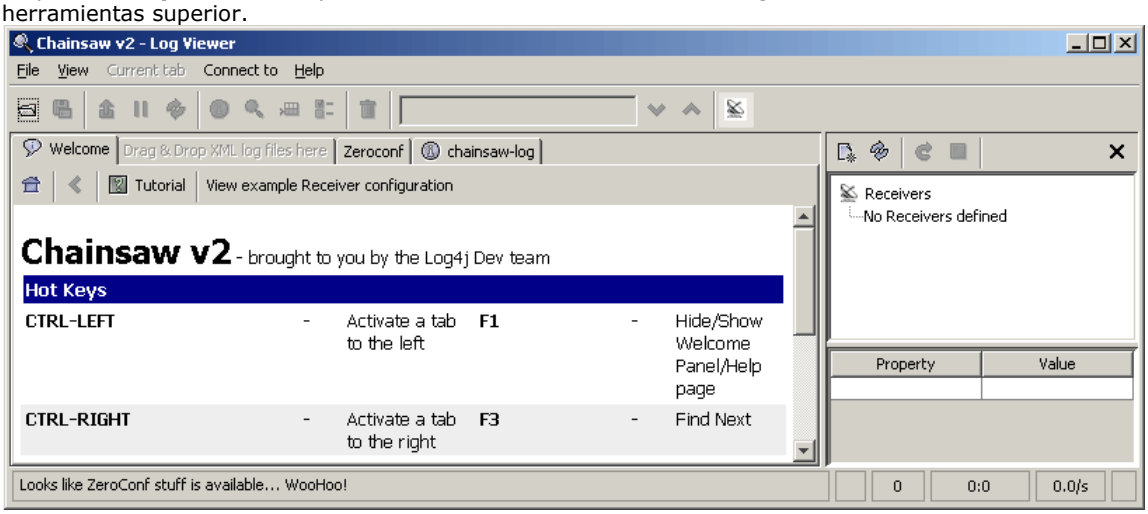


2. Seleccione **Objetivos de registro** y compruebe que esté habilitado **Receptor de conexiones**.
3. Seleccione **Visor de registros**.

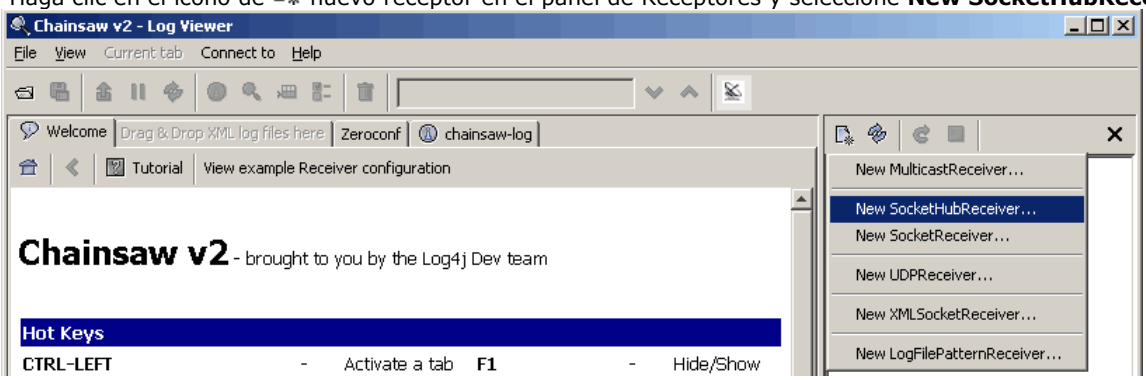


4. Haga clic en **Iniciar instalación de Apache Chainsaw por Java Web Start**.
5. El proceso de descarga e instalación de Chainsaw es automático en gran parte. Chainsaw se iniciará. Si aparece el mensaje ***Warning: You have no Receivers defined... (Advertencia: no se han definido receptores)***, seleccione ***I'm fine thanks, don't worry (No importa)*** y ***Don't show me this again (No volver a mostrar este mensaje)***, y luego haga clic en **OK**.

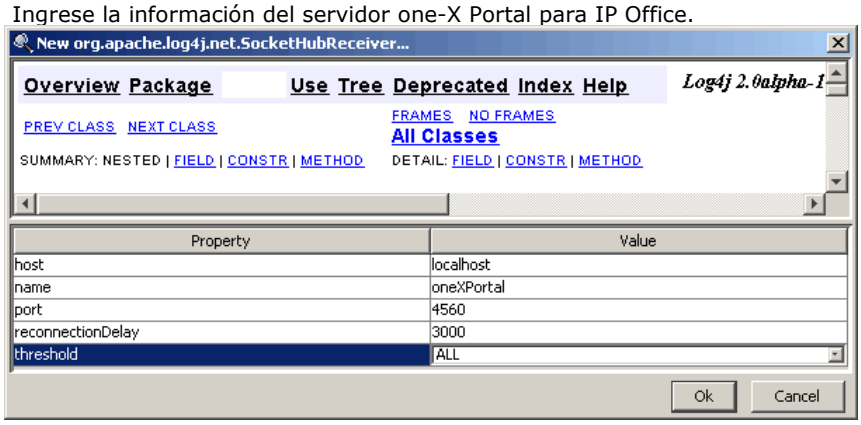
6. El panel **Receptores** debe aparecer a la derecha. De lo contrario, haga clic en el botón de la barra de herramientas superior.



7. Haga clic en el icono de nuevo receptor en el panel de Receptores y seleccione **New SocketHubReceiver**.

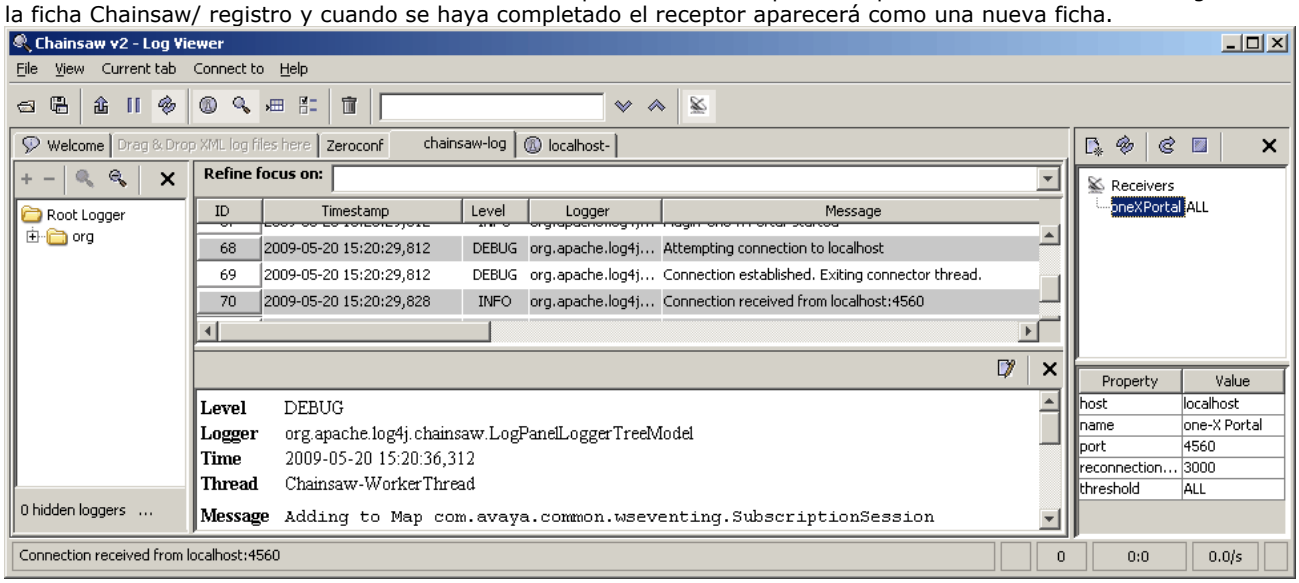


8. Ingrese la información del servidor one-X Portal para IP Office.

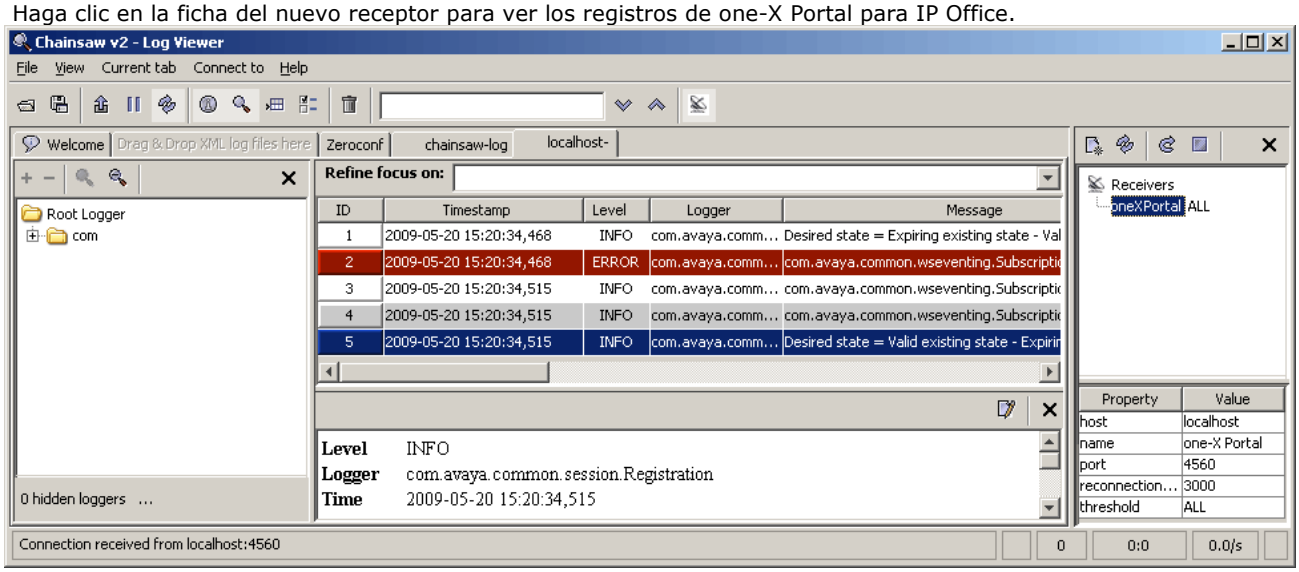


sistema central	Este campo establece la dirección del servidor one-X Portal para IP Office. En el ejemplo anterior, Chainsaw se está ejecutando en la computadora del servidor one-X Portal para IP Office.
nombre	Este campo es sólo de visualización. Ingrese un nombre para la entrada de receptor en Chainsaw.
puerto	Defina el puerto en 4560. Éste es el puerto al que one-X Portal para IP Office envía registros para que las aplicaciones de registro remoto los reúnan.
demora en la reconexión (reconnectionDelay)	Este campo establece cuánto tiempo (en milésimas de segundo) debe esperar el receptor si se sospecha que se ha perdido la conexión antes de volver a intentar establecerla.
límite	Este campo establece el nivel mínimo de mensajes de registro que pueden recibirse, o la opción Todo o Desactivado.

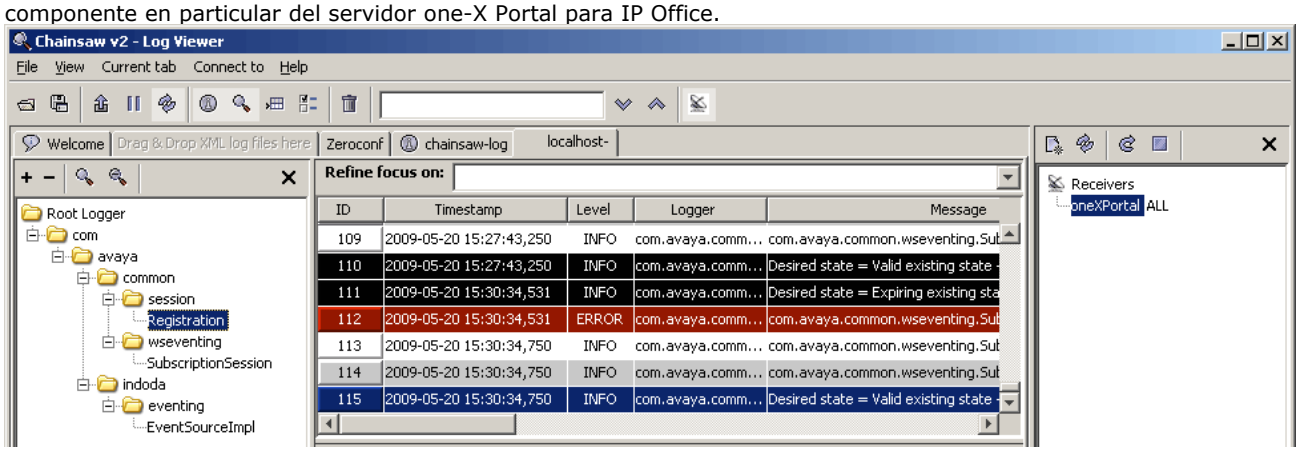
9. Cuando haya completado los campos, haga clic en Aceptar. Después de unos segundos, el receptor debe iniciarse y establecer una conexión con el servidor one-X Portal para IP Office. El proceso aparecerá como eventos de registro en la ficha Chainsaw/ registro y cuando se haya completado el receptor aparecerá como una nueva ficha.



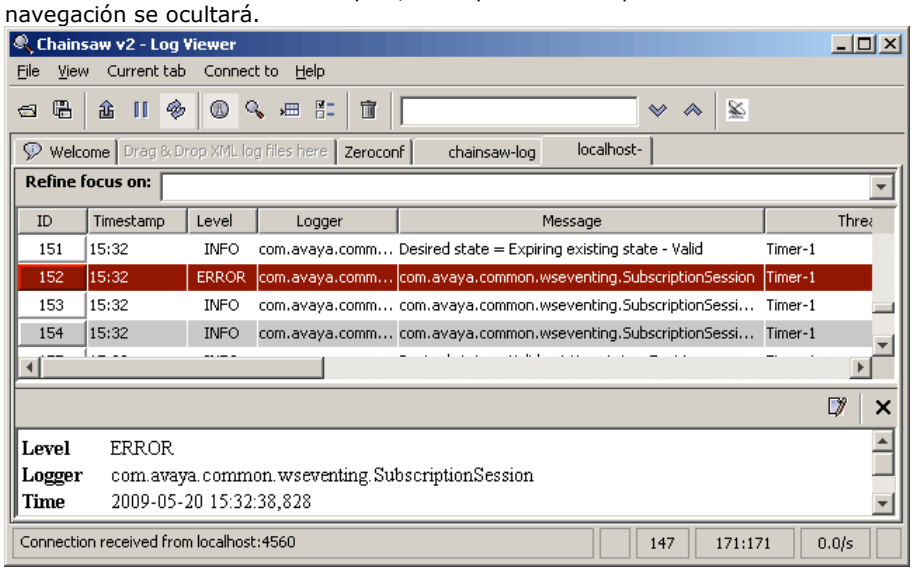
10. Haga clic en la ficha del nuevo receptor para ver los registros de one-X Portal para IP Office.



11. El árbol de navegación que se encuentra a la izquierda puede utilizarse para centrar el visor de registros en un componente en particular del servidor one-X Portal para IP Office.



12. Al hacer clic en el icono de receptor, el panel de receptores se ocultará. Al hacer clic en el icono el árbol de navegación se ocultará.



3.11 Solución de problemas

Problema de incompatibilidad de versiones

Síntomas	• No se puede realizar el control de la integridad de base de datos 38. • Al iniciar one-X Portal para IP Office, la versión que aparece en la página de inicio de sesión es la versión anterior y no coincide con la que aparece en el menú de Windows (**Inicio| Programas | IP Office | Avaya one-X Portal for IP Office | Desinstalar V***X.XX*).
Causa	Habitualmente, el instalador de one-X Portal para IP Office detendrá automáticamente cualquier servidor Web Tomcat relacionado con una instalación anterior de one-X Portal para IP Office. Sin embargo, se observó que en algunos casos no puede detener el servidor Tomcat y de todas formas indica que el proceso de instalación finalizó con éxito. Esto da lugar a una incompatibilidad de versiones entre los componentes.
Solución	1. Quitar one-X Portal para IP Office 74. 2. Elimine manualmente la carpeta de la aplicación one-X Portal para IP Office (de forma predeterminada C:\Program Files (x86)\Avaya\onexportal). Si se informa que la carpeta está bloqueada, debe reiniciar el servidor. 3. Instale la nueva versión de one-X Portal para IP Office.

one-X Portal para IP Office no se inicia

Síntomas	• one-X Portal para IP Office no se inicia. • El mensaje **Prorun Error** (Error de prorun) aparece en los archivos de registro del servidor Tomcat. • Otras aplicaciones Java no se ejecutan en el servidor (por ejemplo, IP Office System Status Application).
Solución	1. Verifique si hay un conflicto de puertos. Si existe alguno, quite la otra aplicación o instale one-X Portal para IP Office utilizando un puerto diferente. 2. Elimine Java por medio de la aplicación **Agregar o quitar programas** de Windows. 3. Quitar one-X Portal para IP Office 74. 4. Instalar one-X Portal para IP Office.

3.12 Incorporación de administradores adicionales

De manera predetermina, los servidores de one-X Portal para IP Office basados en Linux usan la **Autenticación referida**. Esto significa que los derechos de la administración del portal se asignan a los usuarios de seguridad establecidos en la configuración de seguridad del servicio IP Office que se ejecuta en el mismo servidor. De manera predetermina es el usuario **Administrador**; sin embargo, otros usuarios de servicio también pueden configurarse para el acceso de administrador del portal. Si se desactiva la opción de autenticación referida, el portal usa su propia cuenta de administrador local para un servidor basado en Windows, como a continuación.

Los servidores basados en Windows usan una cuenta de **Administrador** local almacenada en la propia configuración del portal (o **Superusuario** para los menús de AFA). El instalador cambia la contraseña predeterminada como parte del proceso de instalación.

En el siguiente proceso, se muestra cómo configurar los derechos de administración del portal para usuarios del servicio de seguridad adicional. Cada usuario del servicio IP Office es miembro de uno o varios grupos de derechos. La configuración del grupo de derechos es la que controla lo que el usuario del servicio puede hacer, lo que incluye su nivel de acceso al servidor one-X Portal para IP Office.

Para ver y modificar la configuración de un grupo de derechos:

1. Mediante Manager de IP Office, seleccione **Archivo | Opciones avanzadas | Configuración de seguridad**.
2. Seleccione el sistema IP Office y haga clic en **Aceptar**.
3. Introduzca el nombre y la contraseña para acceder a la configuración de seguridad de IP Office.
4. Seleccione **Grupos de derechos**.
5. Seleccione la ficha **Externo**. Esta ficha incluye parámetros de configuración para el nivel de acceso al portal que se permite a los miembros del grupo de derechos.
   - **One-X Portal Administrator**
     Acceso a los menús del administrador del portal.
   - **One-X Portal Super User**
     Acceso a los menús de AFA del portal.
6. Seleccione un grupo de derechos específico en la lista para ver qué nivel de acceso posee dicho grupo.
7. Si realiza algún cambio, haga clic en **Aceptar**.
8. Haga clic en para guardar los cambios.

Para cambiar las membresías de un usuario del servicio a un grupo de derechos:

1. Mediante Manager de IP Office, seleccione **Archivo | Opciones avanzadas | Configuración de seguridad**.
2. Seleccione el sistema IP Office y haga clic en **Aceptar**.
3. Introduzca el nombre y la contraseña para acceder a la configuración de seguridad de IP Office.
4. Seleccione **Usuarios del servicio**.
5. Seleccione el usuario del servicio. Los detalles muestran el grupo de derechos al cual pertenece el usuario del servicio.

Capítulo 4.
Menús AFA

4. Menús AFA

one-X Portal para IP Office es compatible con un grupo de menús para copias de seguridad y restauración de la configuración de one-X Portal para IP Office. Esto permite copias de seguridad y restauración utilizando el servidor one-X Portal para IP Office, un servidor FTP o su computadora con explorador como destino de los archivos de copia de seguridad.

Los menús también tienen el propósito de posibilitar la copia de seguridad y restauración entre una instalación antigua y nueva de one-X Portal para IP Office en un nuevo servidor. No obstante, no se admite para la copia de seguridad y restauración entre diferentes versiones de one-X Portal para IP Office, por ejemplo desde 6.1 a 7.0.

El acceso a los menús avanzados de copia de seguridad y restauración es controlado por un usuario y una contraseña independientes de otros accesos de administrador.

- **Servidores basados en Linux**
  Para que el portal se ejecute en un servidor basado en Linux, el portal puede incluirse en las funciones de copia de seguridad y restauración proporcionadas a través de los menús de administración web del servidor Linux. Esas opciones admiten copias de seguridad a HTTP. Servidores HTTPS y SFTP y copias de seguridad programadas.

4.1 Iniciar sesión

Sólo puede haber un usuario en sesión como Superuser (Súper usuario) en cualquier momento.

De manera predetermina, los servidores de one-X Portal para IP Office basados en Linux usan la **Autenticación referida**. Esto significa que los derechos de la administración del portal se asignan a los usuarios de seguridad establecidos en la configuración de seguridad del servicio IP Office que se ejecuta en el mismo servidor. De manera predetermina es el usuario **Administrador**; sin embargo, otros usuarios de servicio también pueden configurarse para el acceso de administrador del portal. Si se desactiva la opción de autenticación referida, el portal usa su propia cuenta de administrador local para un servidor basado en Windows, como a continuación.

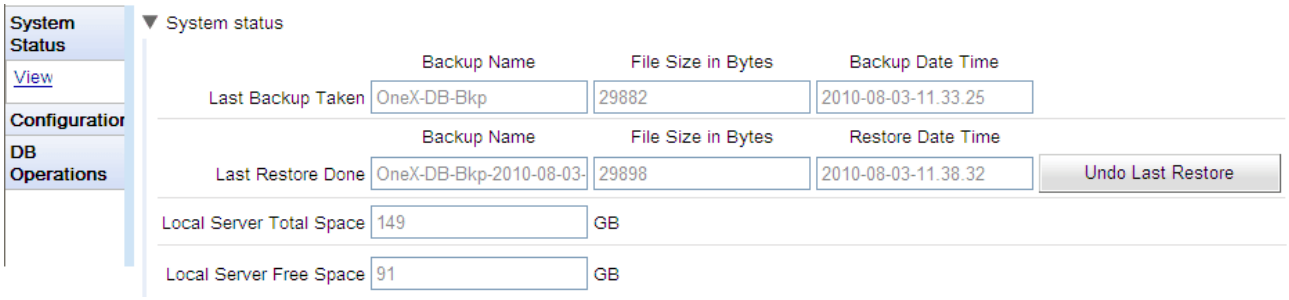
Los servidores basados en Windows usan una cuenta de **Administrador** local almacenada en la propia configuración del portal (o **Superusuario** para los menús de AFA). El instalador cambia la contraseña predeterminada como parte del proceso de instalación.

Para iniciar sesión:

1. Ingrese la dirección del explorador ***http://<nombre del servidor>:<puerto de servidor>/onexportal-afa.html***, donde:
   - ***<nombre del servidor>*** es el nombre o la dirección IP del servidor de one-X Portal para IP Office.
   - ***<puerto del servidor>*** es el número de puerto que usa one-X Portal para IP Office. Será 9443 o 8443 para el acceso HTTPS.
   - Puede utilizar ***http://*** en lugar de ***https://*** y ***8080*** como puerto, si se configuró acceso no seguro. Consulte Protocolo 33.
   - O bien, puede seleccionar **Inicio de sesión de AFA** en el menú de inicio de sesión de usuario común.
2. En el menú de inicio de sesión, ingrese la contraseña:
   - En un servidor basado en Linux, ingrese la contraseña de un usuario de seguridad de IP Office, configurado para el acceso a one-X Portal como superusuario 94. De forma predeterminada, ese usuario es el **Administrador**.
   - En un servidor basado en Windows, ingrese el nombre de ***Superusuario*** y la contraseña asociada.
     - Cuando inicie sesión por primera vez, utilice la contraseña predeterminada ***MyFirstLogin1_0***. Luego de iniciar sesión se le indicará introducir una nueva contraseña para la cuenta ***Superuser (Súper usuario)*** y otra información adicional.
   - **Mostrar nombre**
     Introduzca un nombre a visualizar en los menús de one-X Portal para IP Office.
   - **Contraseña/Confirmar contraseña**
     Introduzca una contraseña que será utilizada para un futuro acceso al ***Superusuario***. Esta contraseña se usa en los servidores basados en Windows y en los servidores basados en Linux que no usen **Autenticación referida**.

4.2 Estado del sistema

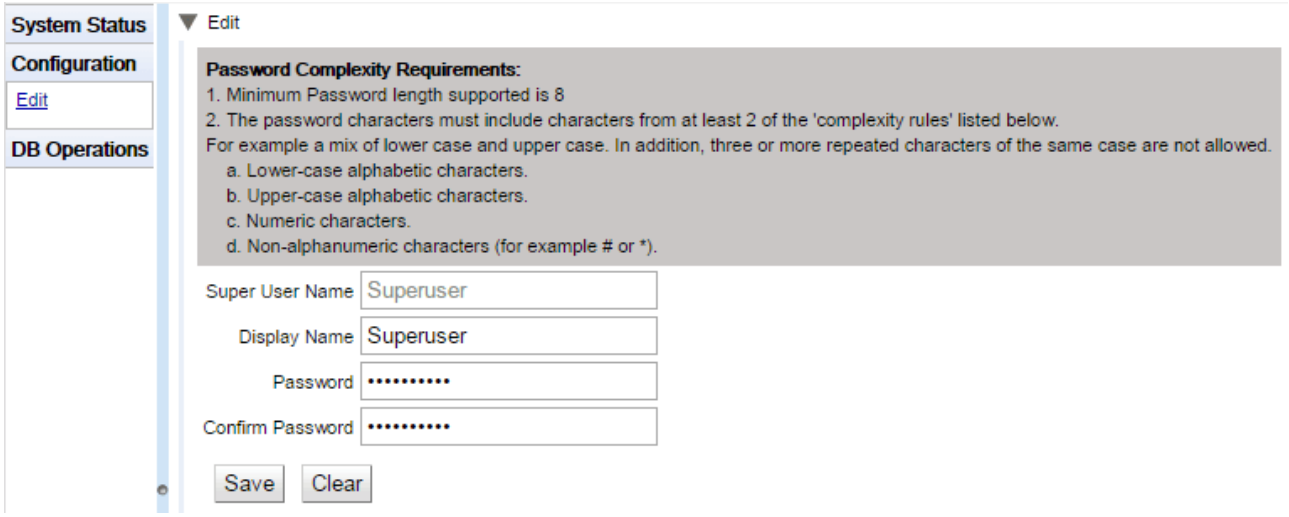
Este menú proporciona un resumen del uso anterior de los menús Superuser (Súper usuario). Permite la restauración de la última operación de restauración anterior.



- **Última copia de seguridad**
  Esta sección proporciona información de la última copia de seguridad utilizando el menú Copia de seguridad. El nombre de archivo de copia de seguridad será un archivo comprimido en formato zip cuyo nombre estará compuesto por el **Nombre de copia de seguridad** y la **Fecha y hora de copia de seguridad**. Por ejemplo, ***OneX-DB-Bkp-2010-08-03-11.33.25.zip***.
- **Última restauración**
  Esta sección proporciona información de la última operación de restauración. Se muestra la hora y fecha de la restauración y el nombre del archivo utilizado para esa operación. Se puede usar el control Deshacer última restauración para deshacer la acción de restauración.
- **Espacio total del servidor local**
  Muestra el espacio aproximado en disco del servidor one-X Portal para IP Office.
- **Espacio libre en servidor local**
  Muestra el aproximado espacio libre en disco restante del servidor one-X Portal para IP Office.

4.3 Configuración

Se utiliza este menú para establecer la configuración básica del acceso del ***Superuser (Súper usuario)***.



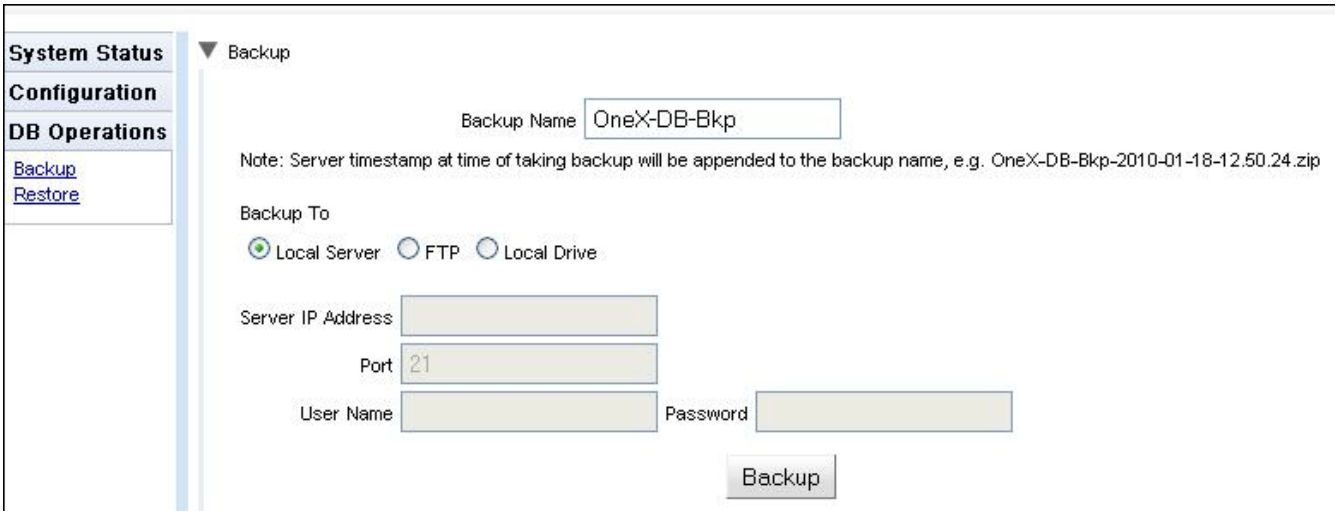
- **Super User Name (Nombre del Súper usuario)**
  Es un nombre fijo y no puede modificarse.
  - **Mostrar nombre**
    Introduzca un nombre a visualizar en los menús de one-X Portal para IP Office.
  - **Contraseña/Confirmar contraseña**
    Introduzca una contraseña que será utilizada para un futuro acceso al ***Superusuario***. Esta contraseña se usa en los servidores basados en Windows y en los servidores basados en Linux que no usen **Autenticación referida**.

4.4 Operaciones de base de datos

Se utilizan estos menús para crear archivos de respaldo y restablecer la configuración de un archivo de respaldo anterior.

4.4.1 Respaldar

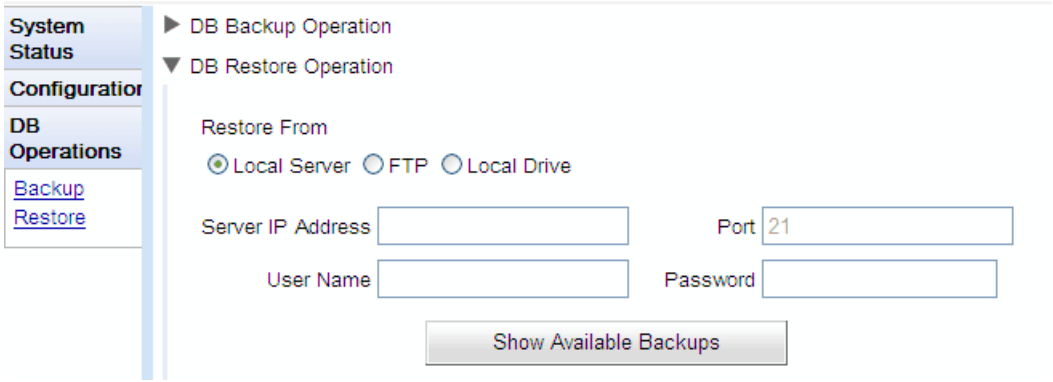
Se utiliza este menú para crear archivos de respaldo.



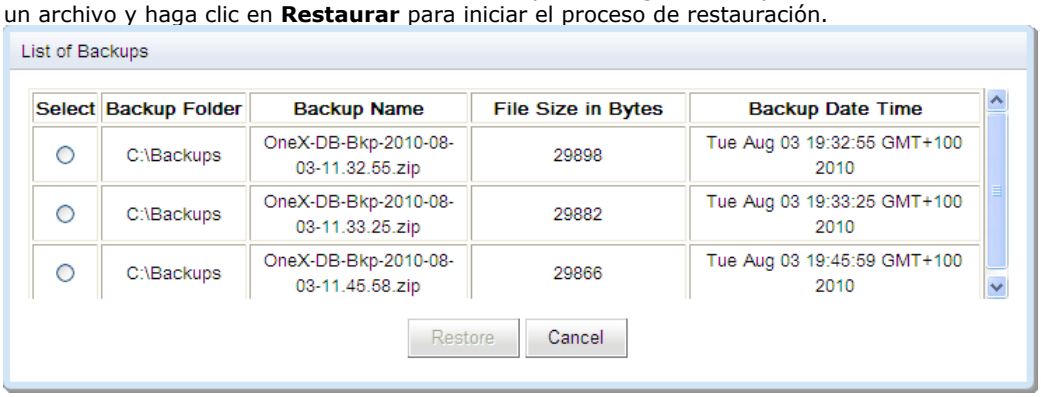
- **Nombre de copia de seguridad**
  Se utiliza este nombre para los archivos comprimidos de la copia de seguridad. La fecha y hora del respaldo se agregan también al nombre de archivo. Por ejemplo, ***OneX-DB-Bkp-2010-08-03-11.33.25.zip***.
- **Hacer copia de seguridad en**
  Se utiliza esta configuración para seleccionar el destino del archivo de la copia de seguridad.
- **Servidor local**
  Si se selecciona esta opción, el archivo de copia de seguridad se crea en la **Carpeta de copia de seguridad**.
- **FTP**
  Si se selecciona esta opción, el archivo de copia de seguridad se crea temporalmente en la **Carpeta de copia de seguridad**. Luego se la envía a la dirección del servidor FTP especificado.
- **Unidad local**
  Si se selecciona esta opción, el archivo de copia de seguridad se crea temporalmente en la **Carpeta de copia de seguridad**. Luego el explorador ofrece la descarga.
- **Configuración de FTP**
  Se utiliza la siguiente configuración si el destino del archivo de copia de seguridad está establecido en **FTP**.
- **Dirección IP del servidor**
  La dirección, inclusive la ruta de archivo, del servidor FTP.
- **Puerto**
  El puerto FTP del servidor. El valor predeterminado normal del puerto es 21.
- **Nombre del usuario** / **Contraseña**
  El nombre del usuario y la contraseña para acceso de archivo al servidor FTP especificado.
- **Copia de seguridad**
  Se utiliza este botón para iniciar una copia de seguridad utilizando la configuración anterior.

4.4.2 Restaurar

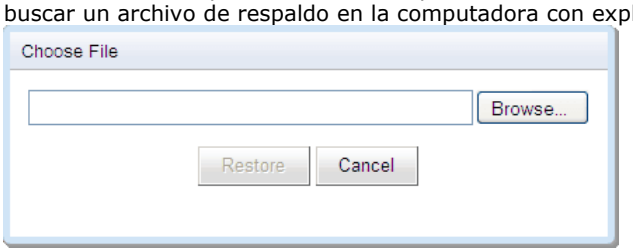
Se utiliza este menú para seleccionar un archivo anterior de copia de seguridad y luego utilizarlo para una operación de restauración. Antes de iniciar la restauración, se realiza una copia de seguridad de la configuración actual y se la almacena en la **Carpeta de copia de seguridad** para utilizarla con el control **Deshacer última restauración** 97. La restauración sólo se admite desde el respaldo de la misma versión de one-X Portal para IP Office.



- **Restaurar desde**
  Se usa esta configuración para seleccionar el destino desde el que se debe seleccionar el archivo de copia de seguridad anterior.
- **Servidor local**
  Si se selecciona esta opción, se selecciona el archivo de copia de seguridad para la restauración desde la **Carpeta de copia de seguridad** configurada.
- **FTP**
  Si se selecciona esta opción, se selecciona el archivo de copia de seguridad para la restauración desde la dirección del servidor FTP especificado.
- **Unidad local**
  Si se selecciona esta opción, se selecciona el archivo de copia de seguridad para la restauración utilizando un menú de exploración de archivos para localizar un archivo en la computadora del explorador.
- **Configuración de FTP**
  Se utiliza la siguiente configuración si el destino del archivo de copia de seguridad está establecido en **FTP**.
- **Dirección IP del servidor**
  La dirección, inclusive la ruta de archivo, del servidor FTP.
- **Puerto**
  El puerto FTP del servidor. El valor predeterminado normal del puerto es 21.
- **Nombre del usuario** / **Contraseña**
  El nombre del usuario y la contraseña para acceso de archivo al servidor FTP especificado.
- **Mostrar copias de seguridad disponibles**
  Se muestra este botón cuando la opción **Restaurar desde** está establecida en **Servidor local** o **FTP**. Si se hace clic en él, se visualiza una lista de archivos de copias de seguridad disponibles en el sitio seleccionado. Seleccione un archivo y haga clic en **Restaurar** para iniciar el proceso de restauración.



- **Seleccionar archivo**
  Este botón está disponible cuando la opción **Restaurar desde** está establecida en **Unidad local**. Le permite buscar un archivo de respaldo en la computadora con explorador.



Capítulo 5.
Historial de documentos

5. Historial de documentos

Fecha	Edición	Resumen de cambios
30 de enero de 2019	14a	Actualización para la versión 11.0.4.0 de IP Office: ○ Controles para Bloquear cliente específico 33. ○ Los Eventos clave recientes 15 ahora incluyen inicios de sesión de usuario fallidos. ○ El tablero ahora muestra la cantidad de usuarios conectados. ○ Los detalles de las Sesiones activas 16 se mejoraron para incluir cliente, versión de cliente, etc.
5 de febrero de 2019	14b	○ La opción para borrar sesiones ahora está disponible en la lista de usuarios.

© 2019 AVAYA Reservados todos los derechos.

Aviso
Si bien se hicieron esfuerzos razonables para asegurar que la información contenida en este document esté completa y sea exacta en el momento de su impresión, Avaya no se responsabiliza por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información contenida en este documento sin la obligación de notificar a ninguna persona u organización dichos cambios.
Para leer toda la información de apoyo técnico, consulte el documento en su totalidad, Avaya Support Notices for Hardware Documentation, documento número 03–600759.
Para leer toda la información de apoyo técnico, consulte el documento en su totalidad, Avaya Support Notices for Software Documentation, documento número 03–600758.
Para encontrar este documento en nuestro sitio web, solo visite http://www.avaya.com/support y busque el número de documento en el cuadro Búsqueda.

Exención de responsabilidad con respecto a la documentación
“Documentación” hace referencia a la información publicada por Avaya en diversos medios, que puede incluir información del producto, instrucciones operativas y especificaciones de rendimiento, que Avaya suele poner a disposición de los usuarios de sus productos. La documentación no incluye material publicitario. Avaya no es responsable de ninguna modificación, incorporación ni eliminación en la version original publicada de la presente documentación a menos que dichas modificaciones, incorporaciones o eliminaciones hayan sido efectuadas por Avaya. El usuario final acuerda indemnizar y eximir de toda responsabilidad a Avaya, agentes de Avaya y empleados con respecto a todo reclamo, acción judicial, demanda y juicio que surgiere de o en relación con modificaciones, incorporaciones o eliminaciones posteriores en esta documentación realizadas por el usuario final.

Exención de responsabilidad con respecto a los vínculos
Avaya no asume la responsabilidad del contenido ni la fiabilidad de los enlaces a los sitios Web incluidos en cualquier punto de este sitio o en documentación proporcionada por Avaya. Avaya no es responsible de la confiabilidad de ninguna información, instrucción ni contenido proporcionado en estos sitios y no necesariamente aprueba los productos, los servicios o la información descritos u ofrecidos por los mismos. Avaya no garantiza que estos vínculos funcionarán todo el tiempo ni tiene control de la disponibilidad de las páginas vinculadas.

Garantía
Avaya ofrece una garantía limitada para sus “productos” de hardware y software. Consulte su contrato de compraventa para establecer las condiciones de la garantía limitada. Asimismo, el idioma de la garantía estándar de Avaya, así como la información relativa al soporte técnico para este producto durante el período de vigencia de la garantía está disponible en el sitio Web: del soporte técnico de Avaya: http://support.avaya.com. Tenga en cuenta que si ha adquirido los productos de un socio de canal autorizado por Avaya fuera de Estados Unidos y Canadá, la garantía es proporcionada por el mencionado socio de canal de Avaya y no por Avaya. “Software” significa programas de computadora en código objeto proporcionado por Avaya o un Channel Partner de Avaya, ya sea como productos independientes o preinstalados en productos de hardware, y cualquier mejora, actualización, corrección de falla o versions modificadas.

Licencias
LOS TÉRMINOS DE LICENCIA DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, SE APLICAN A CUALQUIER PERSONA QUE DESCARGUE, USE Y/O INSTALE SOFTWARE DE AVAYA, ADQUIRIDO A AVAYA INC., CUALQUIER SUBSIDIARIA DE AVAYA, O UN SOCIO DE CANAL AUTORIZADO DE AVAYA (SEGÚN SEA APLICABLE) BAJO UN ACUERDO COMERCIAL CON AVAYA O CON UN SOCIO DE CANAL AUTORIZADO DE AVAYA. A MENOS QUE AVAYA ACUERDE LO CONTRARIO POR ESCRITO, AVAYA NO OTORGA ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE ALGUIEN DISTINTO A AVAYA, UNA SUBSIDIARIA DE AVAYA O UN SOCIO DE CANAL AUTORIZADO DE AVAYA, RESERVÁNDOSE AVAYA EL DERECHO A EJERCER ACCIONES LEGALES EN SU CONTRA O EN CONTRA DE TERCEROS QUE USEN O VENDAN EL SOFTWARE SIN UNA LICENCIA. AL INSTALAR, DESCARGAR O USAR EL SOFTWARE DE AVAYA, O AL AUTORIZAR A TERCEROS A HACERLO, USTED, EN NOMBRE PROPIO Y EN NOMBRE DE LA ENTIDAD PARA LA CUAL ESTÁ INSTALANDO, DESCARGANDO O USANDO EL SOFTWARE (EN ADELANTE REFERIDOS INDISTINTAMENTE COMO “USTED” O “USUARIO FINAL”), ACEPTA OBLIGARSE DE CONFORMIDAD CON LO DISPUESTO POR ESTOS TÉRMINOS Y CONDICIONES Y CREAR UN CONTRATO OBLIGATORIO ENTRE USTED Y AVAYA INC. O LA AFILIADA DE AVAYA APLICABLE (“AVAYA”).

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el que el alcance de la licencia se detalla a continuación. Donde la documentación de la orden no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de sistema designado. La cantidad correspondiente de licencias y unidades de capacidad para la que se otorga la licencia será uno (1), a menos que una cantidad diferente de licencias o unidades de capacidad se especifique en la documentación u otros materiales disponibles para el usuario final. “Procesador designado” significa un dispositivo informático independiente único. “Servidor” significa un Procesador designado que aloja una aplicación de software a la que pueden acceder varios usuarios.

Tipos de licencia
Licencia de sistemas designados (DS). El usuario final puede instalar y utilizar cada copia del software solo en la cantidad de procesadores designados indicada en la orden. Avaya puede exigir que se identifique el procesador designado por tipo, número de serie, tecla de función, ubicación u otra designación específica o que el usuario final lo proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este propósito.

Licencia de usuarios simultáneos (CU). El usuario final puede instalar y utilizar el software en múltiples procesadores designados o uno o más servidores, siempre y cuando sólo las unidades con licencia accedan y utilicen el software en un momento dado. Una “unidad” se refiere a la unidad en la que Avaya, a su exclusivo criterio, fundamenta el precio de sus licencias y puede ser incluso, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o de correo de voz en nombre de una persona o function corporativa (por ejemplo, administrador web o centro de asistencia técnica) o una entrada de directorio en la base de datos administrative utilizada por el software que permite que un usuario se conecte con el software. Las unidades pu8eden vincularse con un servidor específico identificado.

Licencia de la base de datos (DL). El usuario final puede instalar y utilizar cada copia del software en un servidor o en múltiples servidores siempre que cada servidor en el cual el software esté instalado se comunique con no más de una única instancia de la misma base de datos.

Licencia de CPU (CP). El usuario final puede instalar y utilizar cada copia del software hasta la cantidad de servidores que indica la orden, siempre que la capacidad de rendimiento de los servidores no exceda la capacidad de rendimiento especificada para el software. El usuario final no puede instalar nuevamente ni operar el software en servidores con una capacidad de rendimiento más grande sin el consentimiento previo de Avaya y sin pagar una tarifa por la actualización.

Licencia del usuario identificado (NU). El cliente puede: (i) instalar y utilizar el software en un solo procesador designado o servidor por usuario identificado autorizado (se define a continuación); o (ii) instalar y utilizar el software en un servidor siempre y cuando únicamente los usuarios identificados autorizados obtengan acceso a él y lo utilicen. “Usuario identificado” se refiere a un usuario o dispositivo que ha sido expresamente autorizado por Avaya para tener acceso al software y utilizarlo. A entera discreción de Avaya, un “usuario identificado” puede ser incluso, entre otros, designado por nombre, función corporative (por ejemplo, administrador web o centro de asistencia técnica), una cuenta de correo electrónico o de correo de voz a nombre de una persona o función corporativa o una entrada de directorio en la base de datos administrative utilizada por el software que permite que un usuario se conecte con el software.

Licencia Shrinkwrap (SR). El cliente puede instalar y utilizar el software de acuerdo con los terminus y condiciones de los contratos de licencia vigentes, como por ejemplo, las licencias “shrinkwrap” o “clickthrough” que acompañan o se aplican al software (“licencia Shrinkwrap”).

Heritage Nortel Software
“Heritage Nortel Software” significa el software que adquirió Avaya como parte de la compra de Nortel Enterprise Solutions Business en diciembre de 2009. El Heritage Nortel Software actualmente disponible para licencia de Avaya es el software contenido en la lista de productos Heritage Nortel Products ubicada en http://support.avaya.com/LicenseInfo en el vínculo “Heritage Nortel Products”. Para Heritage Nortel Software, Avaya otorga al cliente una licencia para utilizar Heritage Nortel Software proporcionado en virtud del presente documento únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el objetivo especificado en la documentación y solamente como se incorpora, ejecuta o (en caso de que la documentación correspondiente permita la instalación en un equipo que no sea Avaya) para comunicación con equipo Avaya. Los cargos por Heritage Nortel Software se podrían basar en el alcance de activación o el uso autorizado según se especifique en una orden o factura.

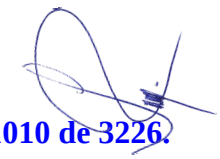
Copyright
Excepto donde se indique expresamente lo contrario, no se debería hacer uso de los materiales de este sitio, de la documentación, del software ni del hardware proporcionados por Avaya. Todo el contenido de este sitio, la documentación y el Producto proporcionados por Avaya, incluida la selección, la disposición y el diseño del contenido, son propiedad de Avaya o de sus licenciantes y están protegidos por las leyes de derecho de autor y otras leyes de propiedad intelectual, incluidos los derechos de su género relacionados con la protección de las bases de datos. No debe modificar, copiar, reproducir, reeditar, cargar, publicar, transmitir ni distribuir de ninguna manera el contenido, en su totalidad o en parte, incluidos los códigos y el software, a menos que posea una autorización expresa de Avaya. La reproducción, transmisión, difusión, almacenamiento y/o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede considerarse un delito penal o civil según la ley vigente.

Virtualización
Cada vAppliance tendrá su propio código de pedido. Tenga en cuenta que cada instancia de vAppliance debe pedirse por separado. Si el cliente usuario final o el socio de canal de Avaya prefieren la instalación de dos vAppliances del mismo tipo, se deben solicitar dos vAppliances del mismo tipo.
Cada Producto tiene su propio código de pedido. Tenga en cuenta que cada instancia de un product debe tener una licencia y pedirse por separado. ""Instancia"" significa una copia única del software. Por ejemplo, si el cliente usuario final o el socio de canal de Avaya prefieren instalar dos instancias del mismo tipo de producto, se deben solicitar dos productos del mismo tipo.
Componentes de terceros
“Componentes de terceros” significa que ciertos programas de software y partes de este incluidos en el producto pueden contener software (incluido el software de código abierto) distribuido según contratos de terceros (“componentes de terceros”), que incluyen condiciones sobre los derechos a utilizar ciertas partes del software (“Términos y condiciones de terceros”). La información con respecto al código fuente de SO Linux distribuido (para aquellos productos que tienen código fuente de SO Linux distribuido) y que identifique a los titulares de derechos de autor de componentes de terceros y las condiciones de terceros que se aplican está disponible en la documentación o en el sitio web de Avaya: http://support.avaya.com/Copyright. Acepta las condiciones de terceros para tales tipos de componentes de terceros.

Nota para el proveedor de servicio
El producto podría utilizar componentes de terceros con términos y condiciones de terceros que no le permitan funcionar como host y podría necesitar licencias independientes para dicho objetivo.

Prevención del fraude telefónico
El fraude telefónico se refiere al uso no autorizado de su sistema de telecomunicaciones por parte de un participante sin autorización (por ejemplo, una persona que no es un empleado, agente ni subcontratista corporativo o no trabaja en nombre de su compañía). Tenga en cuenta que pueden existir riesgos de Fraude telefónico asociados con su sistema y que, en tal caso, esto puede generar cargos adicionales considerables para sus servicios de telecomunicaciones.

Intervención en fraude telefónico de Avaya
En el caso de que sospeche que es víctima de fraude telefónico y que necesite asistencia o soporte técnico, llame a la línea directa de Intervención de Fraude Telefónico del Centro de Servicio Técnico al +1-800-643-2353 para Estados Unidos y Canadá. Para obtener números de teléfono de soporte técnico adicionales, vaya al sitio web de soporte técnico de Avaya: http://support.avaya.com.



Marcas comerciales
Las marcas comerciales, logotipos y marcas de servicio (“Marcas”) que aparecen en este sitio, la Documentación y los Productos proporcionados por Avaya son marcas registradas o no registradas de Avaya, sus subsidiarias y otros terceros. Los usuarios no tienen permiso de usar dichas Marcas sin previo consentimiento por escrito de Avaya o dichos terceros que puedan ser propietarios de la Marca. Ningún contenido de este sitio, la Documentación ni los Productos deben considerarse como otorgamiento, por implicación, impedimento o de alguna otra forma, una licencia ni derecho para usar las Marcas sin la autorización expresa por escrito de Avaya o del tercero correspondiente.

Avaya es una marca registrada de Avaya Inc.

Todas las demás marcas son propiedad de sus respectivos dueños. Linux® es una marca commercial registrada de Linus Torvalds en EE. UU. y en otros países.

Descarga de documentación:
Para obtener las versiones más actualizadas de la documentación, visite el sitio web de soporte técnico de Avaya: http://support.avaya.com.

Contacto con el soporte de Avaya
Visite el sitio web del soporte técnico de Avaya: http://support.avaya.com para obtener avisos y artículos sobre productos o para informar acerca de algún problema con su producto Avaya. Para obtener una lista de números de teléfono y direcciones de contacto de soporte, visite el sitio web de soporte técnico de Avaya: http://support.avaya.com, desplácese hasta el final de la página y seleccione Contacto con el soporte de Avaya.

Índice

4

4560 89

A

Accesible 37
Accesos directos 66
Acerca de 10
Activar
  Gadget externo 65
Actualización 72
Administrador
  Ayuda 49
  Nombre 8
Agregar
  gagdget 64
  IP Office 54
  LDAP 68
  Usuario 66
Apache
  Chainsaw 37, 89
Archivar
  Sesiones de MI 76
Archivos de registro 35
Archivos de registro continuo 35
Asignación de campos 20, 68
Asignar
  IP Office 54, 56
  IP Office (CSTA) 18
  IP Office (Directorio) 19
  Proveedor de correo de voz 21
  Proveedor de LDAP 20
  Proveedores 17
Asistencia técnica de Avaya 10
Ayuda 10
  Acerca de 49
  Asistencia técnica de Avaya 49
  Ayuda 49

B

Base de búsqueda 68
Base de datos
  Control de estado 38
  Verificar 38
Bloqueo de clientes 33
Buscar
  Directorio del sistema 44, 71
  LDAP 42, 70
  Sesiones de MI 47, 80
Búsqueda de directorios
  Directorio del sistema 44, 71
  LDAP 42, 70

C

Calendario 25, 81
Cerrar sesión 8
Chainsaw 37, 89
Cierre de sesión automático 8
Cierre de sesión inmediato 8
Clientes bloqueados 33
Conferencia 48
Conferencia de audio 48
Conferencia web 48
Configuración 10
  CSV 23
  Edición múltiple 66
  Exportar 23
  Marca 23
  MI 77
  Presencia 77
  Proveedores 17
  Usuarios 22
Configuración de registros 89
Contraseña 8
Copias de seguridad 10
Correo de voz
  Proveedor 21
CSTA 18
CSV 10, 23
Cualquiera se puede conectar 77

D

Desconectar cuando la sesión esté inactiva 77
Desinstalar 74
Diagnóstico 10
  Conexiones 38
  Conexiones de IP Office 38
  Configuración de registros 35, 89
  Integridad de base de datos 38
  Rutas de red 37
  Visor de registros 37, 89
Directorio
  Exportar 23
  Resincronizar 42, 71
Directorio (DSML IP Office) 19
Directorio (DSML LDAP) 20
Directorio del sistema 10
  Búsqueda de directorios 44, 71
  Exportar 23
  Resincronizar 42, 71
Directorio externo
  Buscar 42, 70
Directorio personal 66

E

Echo 37
Edición múltiple 22, 66
  Usuario 66
Editar
  Configuración de IP Office 56
  Configuración del usuario 22, 66
  Edición múltiple 66
  Gadget 64
Eliminar
  Gadget 65
  IP Office 56
  one-X Portal para IP Office 74
  Usuario 66
Entorno 10
Estado 10, 38
  Componente 13
  Entorno 16
  Estado de los componentes 13
  Eventos clave recientes 15
  MI 79
  Presencia 79
  Sesiones activas 16
Estado de los componentes 10, 13
Eventos 15
Eventos clave recientes 10, 15
Eventos recientes 15
Excepciones 66

Página1012 de 3226.

Excepciones de NM 66
Exchange 25, 81
Exportar
  Gadgets 46, 63
Exportar configuración 23
exportDirectoryEntry.csv 23
exportUser.csv 23

F

Formato Log4j 89
Forzar una resincronización 42, 71

G

Gadget
  Activar 65
  Desactivar 65
  Editar 64
  Eliminar 65
  Exportar 46, 63
  Importar 61
  URL 60
Gadgets
  Lista de gadgets externos 45

I

Importar
  Gadgets 61
Iniciar servicio 52
Iniciar sesión
  Error 15
Inicio de sesión 8
Inicios de sesión fallidos 15
Integración de directorios 10
  Directorio del sistema 44, 71
  LDAP 42, 70
  Sincronización de directorios 42, 71
Integridad de base de datos 10
IP Office
  Conexiones 10
  Proveedor de CSTA 18
  Proveedor de directorios 19

J

Java Web Start 89

L

LDAP 70
  Asignar 68
  Búsqueda de directorios 10, 42, 70
  Proveedor 20

M

Marca 23
Mensajes 66
Mensajes de correo de voz 66
MI
  Archivo 76
  Buscar sesiones 47, 80
  Configuración 77
  Estado 79
Monitor 48

N

Nivel de registro maestro 35
No accesible 37
Nombre de dominio
  Nombre de dominio de XMPP 77
Nombre de dominio de XMPP 77
Nombre distintivo de la base 68

P

Panel de control 74
Participantes 48
PING 37
Posiciones de estacionamiento 66
Presencia 66
  Configuración 77
  Estado 79
  Exchange 25, 81
Proveedor 10
  Asignar 17
  Correo de voz 21
  CSTA (IP Office) 18
  Directorio (DSML IP Office) 19
  Directorio (DSML LDAP) 20
  DSML (IP Office) 19
  DSML (LDAP) 20
  Ver 17
Proveedor de CSTA (IP Office) 18
Proveedor de DSML (IP Office) 19
Proveedor de DSML (LDAP) 20
Prueba
  Conexión de IP Office 38
  Directorio de LDAP 42, 70
  Directorio del sistema 44, 71
  Directorio externo 42, 70
  Ruta de red 37
Puerto
  4560 89
  7 37
Puerto de TCP 7 37

R

Receptor de conexiones 35, 89
Registro 89
  Configuración 10
  Nivel 35
  Objetivos 35
  Visor 10, 89
Registro de llamadas 66
Registro remoto 89
Regreso a la versión anterior 73
Reiniciar servicio 52
Resincronización 42, 71
Restablecer cómputo de la sesión 8
Rutas 37
Rutas de red 10, 37

S

Servicio
  Reiniciar 52
Servidor
  Información 16
  Versión 16
Sesión del administrador anulada 8
Sesiones 16
Sesiones activas 10, 16
Sincronización 42, 71
Sincronización de directorios 10

T

Teclas de acceso directo 66
Tiempo de espera en inactividad 77

U

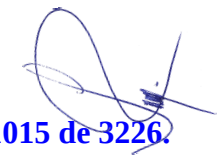
Usuario
  Agregar 66

Página1013 de 3226.

Usuario
Ayuda 49
Edición múltiple 66
Editar configuración 66
Eliminar 66
Exportar 23
Validación de datos 39
Usuarios 10
Activos 16
Editar configuración 22
Resincronizar 42, 71
Ver 22

V

Validación de datos 39
Ver
Conferencia 48
Estado de los componentes 13
Eventos clave recientes 15
Proveedores 17
Versión 16



© 2019 Avaya Inc. Reservados todos los derechos.

Traducido del inglés al español - www.onlinedoctranslator.com

Plataforma IP Office™ 11.0

Implementación de IP Office Essential Edition (IP500 V2)

Contenido

1. Resumen del sistema

1.1 Cambios para.R . . e..le.a.s..e...1..1...0 9
1.2 D..o..c..u..m adicional . . e..n..ta.ción 11
1.3 Equipo .A . . v..a..ila.b..i.li.ty 12
1.4 Reparación 12
1.5 RoHS 12
1.6 Modos de IP Office 13
1.6.1 S..y.s.te.m .. DAKOTA DE Tarjeta. s ..... .13
1.6.2O . . ve.ra ll.C . a..p..a..ciudad 14
1.6.3 horas..a r..d..w..a..re..S. . u..p..p..o..rt.S..u..m metro. a..ry 15
1.6.4 F..e..a..tu.re..S . . u..p..p..o..rt.S..u..m metro. a..ry 16
1.7 El Control.l.U.n.it 18
1.8 Sistema IP500 V2 . . C..o..m. p..o..n..e..n..s 19
1.9 Sistema SD..C . .a. r..d 21
1.10 Licencias 21
1.11 Unidad de control..it.C . . .a. r..d..s 22
1.11.1..IP.5..0..0...B .. Plaza bursátil norte SDRA 22
1.11.2..IP.5..0..0...T . tu hotel k...c. . SDRA 25
1.12 Ex.p..a..n..s..io.n...M . . . o..d..u..le. 26
1.12.1..IP.5..0..0...E . . xte.rn.a l..E . XP.a norte s..io.n...M . impares 27
1.12.2..IP.4..0..0...E . . xte.rn.a l..E . XP.a norte s..io.n...M . impares 28
1.12.3..C . Onormentai c..tin.g...E. x..te.rn.a..l..E x..p..a..n..s..io.n...M. o..d..u..le. 29
1.13 Power Sup pagmentira.s...a..n..d...C . .a b. les 30
1.13.1..P..o..w . . e..r..S..u..p..p..mentiras 30
1.13.2..P..o..w . . e..r..S..u..p..p..ly..C. o. r..d..s 31
1.13.3..P..o..w . . e..r..S..u..p..p..ly..B..a..c..k..u..p 32
1.13.4..C . .a b lin.g...a..n..d...C. poder. 33
1.13.5..G . . ro.u..n.d.ing 35
1.13.6 Protección contra rayos/Conexiones fuera del edificio 36
1.14 Muro y R . . . a..ck..M. o..u..n..tin.g 37
1.14.1..W . .a ll.M . o..u..n..tin.g...K..its 37
1.14.2..R . .a c..k...m . o..u..n..tin.g...K..its 38
1.15 Teléfonos IP Office 39
1.16 VoIP 40
1.16.1..V..o..ice.e...C . . Ometpages r..e..ss.io.n...C. . h..a..n..n.e..ls 41
1.17 Compatible..C . . o..u..n..pruebe..L..o..c..a.le.s 42
1.18 IP Office S..o..ftw . . a..re..A..p..p..lic.a..t.io norte 42
1.18.1..P..ro gram RAM metro energramo A . p..p..l.ic..a.cion.s 43
1.18.2..U s..e..r..A . . p..p..l.ic..a.cion.s 44
1.18.3..V..o..hielo..m . . a..ilA . p..p..l.ic..a.cion.s 44
1.18.4..C . .a ll.L..o..g..g..in.g...A..p..p..lic.a..t.io norte 45
1.18.5..C . .a ll.C . e..n..te.r..A..p..p..lic.a..t.io norte 45
1.18.6..C ..T. I A . p..p..l.ic..a.cion.s 45
1.19 Formación 46
1.20 Sitios web 46
1.21 Emergencia.y...a..n..d...P . .o..w. e..r..F.a ilu.re..P. . o..rts 47

2. Descripción general de la instalación

2.1 Medio ambiente..ta.l..R . . mi.qtu ira metro norte t 51
2.2 Requisitos de espacio . . . e..n..ts 53
2.2.1C . . Onorte r.o..ll . . liendre 53
2.2.2 E..x..te.rn.a..l..E..x..p..a..n..s..io.n...M. . .o.d.u. les 54
2.2.3W . .a ll.M . o..u..n..tin.g 55
2.2.4 R . .a c..k...S pagsa c..e...R. e..q..u..ire.m. . e..n.s 57
2.3 Herramientas y P..a..arts..R. . e..q..u..ir..e..d 59
2.4 Documentación 60
2.5 Desembalaje 60

3. Instalación del software del administrador

3.1 Descarga en..g...l.e...S..o..ftw . . a..re 63
3.2 Instalación del...A . . . d..m en es.tra.to.r..A . p..p..l.ic..a.cion.s 64
3.3 Instalador PC..C . . o..n..n..e..c..tio.n 67
3.4 Iniciando IP .O . ffic.e...M. . a..n..a..g..e..r 68
3.5 Sistema de Arranque . . ..S . ta.tu.s..A . p..p..l.ic..a.ción 69
3.6 Sistema de Arranque .. METRO o..n..ito.r 70
3.7 Iniciando IP .O . ffic.e...W . . e..b...M . a..n..a..g..e..r 71

4. Preparación de la tarjeta SD del sistema

4.1 Actualice la... C.. a.. rd . . ..F. ir..m mercancía 75
4.2 Creando una..O . . fflin.e...C .Onorte fig.u.ra. tio.n...F. ile 76
4.3 Importación y...E..x..p..o..rtin.g...S . . mi. tting.g.s 77
4.4 Agregar un Pr..e..-.B..u..ilt.C . Onorte fig.u.ra. tio.n...F. ile 78
4.5 Adición de un archivo Li.c..e..n..s..e...F..i 78
4.6 Adición de Seg.u.rity..C . . . e..artific..a.te.s 78
4.7 Añadir un 96..0..0...S mi r..ie s....s . c.e..e..n...S..a..v..e..r..F..ile 79
4.8 Añadir música . . norte.H . archivos..antiguos..F 79

5. Instalación de las tarjetas de la unidad de control

5.1 Montaje IP50.0...D . . a..u..g..h..te.r..c.a. r..d..s 83
5.2 Insertar IP.5..0..0...B . . .a segundo . SDRA 84

6. Instalación del sistema físico

6.1 Montaje en pared 87
6.1.1W . .a ll.M . o..u..n..tin.g...K..it.V..3 88
6.2 Montaje en bastidor 89
6.3 Conexión..E . . x..te.rn.a l..E . xp.a..n..s..io.n...M . . impares 91
6.4 Puesta a tierra 93
6.5 Arrancar el..S . . ys.te.m 94
6.6 Comprobación de th..e...L..E..D . . . s 95
6.7 Conexión..P . . .h Onormai . s 97
6.7.1 A..n..a..lo.g...P . . .h Onormai . s 97
6.7.2 ET . .R . . Los telefonos 97
6.7.3D . .S . . D..ig.ita.l..S..ta.tio.n...P..h..o..n..e..s 97
6.7.4 IP./.S . . IP..P..h.o.n.e..s 97
6.7.5 T..C METRO.B . S.T PAGS . h..o..n..e..s 98

7. Configuración inicial usando Manager

7.1 C..o..n..c..n..de.la.red 101
7.2 Con.fig.u.r.inicial 103
7.3 Extensión..N..u..m . . b..e..ring 104
7.4 Desactivar Desactivartu s..e..d...T . r..u..n..ks 105
7.5 Configuración de...D . . yo gita.l..T..ru nostek...c. Cerraduras . o..u..rc.e 107
7.6 Configuración de...T..ru . nortk...p. re.arreglar. 109
7.7 DS16B/30.B . . . P..o..rt.M o..d..e...S mi. le.c..ción 110
7.8 Subiendo..el..e..L..ic.e..n..s..e...F..i.le 111
7.9 Guardar el...C. Onorte fig.u.ra. ción.n 112

8. Configuración inicial mediante IP Office Web Manager

8.1 El Sistemam . . 'pecado itia.l..IP..A . . d..d..res.s 114
8.2 Nuevo sistema..m . . . Instalar 115
8.3 Sistema existente metro 118

Página1018 de 3226.

¿Comentarios sobre este documento? infodev@avaya.com

8.4 Tablero . . . W . iz.a..rd..M. . e..n..u..s..... 119
8.4.1..S..y..s..te.m. . . . Ajustes..... 120
8.4.2..V..o..IP. . . . Ajustes..... 122
8.4.3..V...o..hielo..m . . a..ilS . e..tting..s..... 123
8.4.4..L..hielo norte antando....S mi. tting.g..s..... ... 124
8.4.5..U s..e..rs..a..n..d...E . . . xte.n.s.io.n.s..... 125
8.4.6..G. . r.u.p.s..... 126
8.4.7..L..in.e.s..... 127
8.4.8..En.c.o..m . engrame C . a..todas.las.R.o.u.te.s..... 128
8.4.9..O . u..tg.o..engrame C . a..todas.las.R.o.u.te.s..... 129

9. Seguridad del sistema

9.1 Cambiar.la.e...D. . . e..fa.u..lt.S..e..c..u..rity..S..e..tting.g..s..... 133
9.2 Cambiar.la.e...R. . . e..m . o..te..us..e..r..P. a.s.sw . o..rd..... 135
9.3 Deshabilitar .S..IP. . . ..T . ru.n..k...S..u..p..p..o..rt..... 135
9.4 Deshabilitar .H...3..2..3...T . . mi le.p..h..o..n..e...s. . u..p..p..o..rt..... 135

10. Embarque

10.1 A bordo . . En g..... 139

11. Gestión de tarjetas SD

11.1 Arrancar desde m . . el.e...S CORRIENTE CONTINUA rd.s..... 144
11.2 Creando.a nosta IP . ..O. ffic..e...S CORRIENTE CONTINUA rd..... 146
11.3 Visualización . mi ..C. a..rd..C . o..n..t.n..s..... .. 148
11.4 Respaldo .U..p...a..e....B . . . a..ck.u..p...Fo. ld.e..r..... 149
11.4.1 Copia de seguridad en la carpeta de copia de seguridad mediante IP Office Mana..g.e..r 149
11.4.2 Copia de seguridad en la carpeta de copia de seguridad usando el estado del sistema...A . . pagpágs lic.a..ción..... 149
11.4.3 Copia de seguridad en la carpeta de copia de seguridad usando un sistema..m . . . . Teléfono..... 149
11.4.4 Copia de seguridad en la carpeta de copia de seguridad con IP Office...W . . . . e..b...M. . a..n..a..g..e..r 149
11.5 Restaurando... de . maestro. el mi ..B. a..c..ku pags. Fantiguas mi. r..... 150
11.5.1 Restauración desde la carpeta de respaldo usando IP Office...M. . . a..n..a..g..e..r 150
11.5.2 Restauración desde la carpeta de respaldo usando Syste..m . . . . S..ta.tu.s...A..p..p..lic.a..tio.n..... 150
11.5.3 Restauración desde la carpeta de copia de seguridad utilizando un sistema..m . . . Teléfono..... 150
11.5.4 Restauración desde la carpeta de respaldo usando IP Office...W . . . . e..b...M. . a..n..a..g..e..r 150
11.6 Respaldo .U..p...a..e....O . . . p..tio.n..a..l..S..D. . . Tarjeta 152
11.6.1 Copia de seguridad en la tarjeta SD opcional mediante IP Office...M. . . a..n..a..g..e..r 152
11.6.2 Copia de seguridad en la tarjeta SD opcional mediante Syste..m . . . . S..ta.tu.s...A..p..p..lic.a..tio.n..... 152
11.6.3 Copia de seguridad en la tarjeta SD opcional mediante IP Office...W . . . . e..b...M. . a..n..a..g..e..r 152
11.6.4 Copia de seguridad en la tarjeta SD opcional mediante un sistema.m . . . Teléfono..... 152
11.7 Restaurando...a...C. . o..n..fig.u..ra.tio.n...desde m. . a..n...O . p..t.io nosta l..C . a..rd..... 153
11.7.1 Restauración desde la tarjeta SD opcional mediante IP Office...M . . . a..n..a..g..e..r 153
11.7.2 Restauración desde la SD opcional usando un sistema..m . Teléfono..... 153
11.8 Cargando .S..o..ftw. . . son de . a..n...O . p..tio.n..a..lS ..D ..C . a..rd..... 154
11.8.1 Carga de software desde la SD opcional mediante ... IP Office...M . a..n..a..g..e..r 154
11.8.2 Cargar software desde la SD opcional mediante ...a...S ys.te.m . . . Teléfono..... 154
11.9 Respaldo .U..p...a..a...P . . C..... 155
11.10 Restaurando..g...de . . maestro.. a PAGS. C 155
11.11 Actualizar.en . engrame C . SDRA . o..ftw.a..re 156
11.12 Memoria...C ..a r..d...S..h..u..td.o..w norte R. e..m. o..v.a..l..... 157
11.12...1...S..h..u..td.o..w. . . n...a...C..a..rd. . tu . cantando....IP Office Ma.n..a..g..e..r.... 157
11.12.2 Apagar una tarjeta usando la aplicación de estado del sistema . . norte 157
11.12.3 Apagar una tarjeta mediante IP Office Web Mana..g.e..r..... 157
11.12...4...S..h..u..td.o..w. . . n...a...C..a..rd. . tu. s..ing.g...a...S..y..s..te.m . . T..h..o..n..e..... 157
11.13 Memoria...C ..a. r..d...S..ta.rtu.p..... 158
11.13...1...S..ta.rtu pags.a ..C. a..rd..U . sin.g...IP. ..Office...M . a..n..a..g..e..r..... 158
11.13.2 Puesta en marcha de una tarjeta mediante la aplicación System Status Appli.c..a..t.io norte 158
11.13.3 Puesta en marcha de una tarjeta mediante IP Office Web Mana..g..e..r..... 158
11.13...4...S..ta.rtu pags.a ..C. a..rd..U . sin.g...a...S. ys.te.m PAGS. h..o..n..e..... 158

12. Procesos Adicionales

12.1 Cambio de un sistema IP Office Basic Edition a Standard Mod.e 161
12.2 Automatiz.n..g...l.e...C . . h..a..n..g..e...to..S..ta.n..d..a..rd..M . . o..d..e..... 162
12.3 Conmutación...O. . ff.a...S y..s..te.m 163
12.3.1 Apagar un sistema mediante IP Office Mana..g.e..r..... 163
12.3.2 Apagar un sistema usando la aplicación de estado del sistema norte 164
12.3..3...S..h..u..td.o..w. . . n...a...S..y..s..te.m. . . U..s.ing.g...a...S..y..s..te.m . . T..h..o..n..e..... 164
12.3..4...S..h..u..td.o..w. . . n...a...S..y..s..te.m. . . U..s.ing.g...the...A..U . . X...Btu tto nosta 164
12.3.5 Apagar un sistema mediante IP Office Web Mana..g..e..r..... 164
12.4 Reinicio.g...a...S . . . ys.te.m 165
12.4..1...R mi b o o ejército de asalto ys.te.m . tu pecadegrame IP . ..O. ffic..e...M a..n..a..g..e..r..... 165
12.4.2 Reiniciar un sistema usando IP Office Web Mana..g..e..r..... 166
12.4..3...R mi b o o ejército de asalto ys.te.m . tu pecadegrame el mi ..R. e..s..e..t..B..u..tto.n..... 166
12.4..4...R mi b o o tin.g...a...S . ys.te.m . tu . sin.g...a...S. ys.te.m PAGS. h..o..n..e..... 166
12.5 Cambiando...C . . o..m . p..o..n..e..n..s..... 167
12.5..1...como . para r...L..ik..e...R. . e..p..la.ce metro norte 168
12.5..2...H. ig.h..e..r..C. a..p..a..c..ity..R. e..p..la.ce metro norte 168
12.5..3...B..o..w. e..r..C. a..p..a..c..ity..R e..p..la.c..e..m . e..n.t..... 168
12.5..4...A..a..a..a..g...a...N . e...w...C o..m . p..o..n..e..n..t..... 168
12.5..5...P..e..rm..a norte nosta t..R. e..m . oval..... 169
12.5..6...R mi pags a.c..e..m. n..t..w. tenía. . iffe.re.n..t..T.y..p..e..... 169
12.6 Por defecto g...el...C . . o..n..f.ig tu relación norte 170
12.6.1 Configuración predeterminada mediante IP Office Mana..g.e..r 170
12.6.2 Configuración predeterminada mediante IP Office Web.M . . a..n..a..g..e..r 170
12.6.3 Configuración predeterminada mediante el botón Restablecer n 170
12.6..4...D mi fa tu lting.g...the.e...C . o..n..f.ig tu relación norte tu. cantando...D..e..b..u..g..... 171
12.6.5 Configuración predeterminada usando un teléfono del sistema 172
12.6.6 Configuración predeterminada mediante Boot Load.e..r 172
12.7 Por defecto g...S . mi c..u..rity..S. mi. ajus..... 173
12.7..1...D mi fa tu ltin.g...S mi c..u..rity..U cantando... IP . ..O. ffic.e...M. a..n..a..g..e..r... 174
12.7.2 Configuración predeterminada de seguridad mediante IP Office Web Mana..g.e.r 174
12.7..3...D mi fa tu ltin.g...S mi c..u..rity..u.s..in.g...th.e...R..S ..2.3.2 PAGS. o..rt..... 175
12.7..4...D mi fa tu ltin.g...S mi c..u..rity..U cantando... la... B . .o.o t..L.o.a.d mi. r..... 176
12.8 Cargando .a...C..o..n..fig.u..ra.tio.n..... 177
12.8..1...C r..e..a..t.engrama nosta O. fflin.e...C..o..n..fig.u..ratio.n...F..ile..... 178
12.8.2 Cargar una configuración mediante IP Office Mana..g.e..r..... 179
12.8.3 Cargar una configuración mediante IP Office Web.M . . a..n..a..g..e..r 179

Página1019 de 3226.

¿Comentarios sobre este documento? infodev@avaya.com

12.8.4 Cargar una configuración en una tarjeta SD del sistema..... 179
12.9 Actualización.g. . sistema. . s..... 180
12.9..1...U pagramoa..d..e...U..s..ing.g...th.e...U..p..g..ra . . .dmi ..W. . iz.a..rd..... 181
12.9.2 Actualizar localmente la tarjeta del sistema SD usando Mana..g..e..r 183
12.9..3...U pagramoa..d..engramiu cantando...a..n...O..p..tio.n..a..l..S..D . . . .C.a. r..d..... 184
12.9..4...U pagramoa..d..engramiu cantando... IP..O . ffic..e...W . e..b...M . a..n..a..g..e..r..... 185
12.10 Swappi.n..g...E..x..te.n..s..io norteiu . s..e..rs..... 186
12.11 Fuera de B..u..ild.in gramoT. e..lepagh Onortai . En. s..ta.lla.cio.n.s..... 187
12.11...1...D..S . . Los telefonos..... 188
12.11...2...A..n..a..lo.g...P..h Onortai ..B . a..rrie.r..B..o. x..... 189
12.11...3...D..a c..k...m o..u..n..tin.g...B..a..rrie.r..B. . . o..x..e..s..... 190
12.12 Usando th..e...E x..te.rn..a l..O. u..tp.u..t..P. o. r..t..... 191
12.12...1...P..o..rt.C. . o..n..n..e..c..tio.n..... 191
12.13 SNMP 192
12.13...1...In.s..ta.ll.in.g...la...IP. . ..O. ffic.e...M . IB..F..ile.s 193
12.13...2...E..n..a..b..lin.g...S..N ... METRO P..a..n..d...Po. llin.g...S..u..p..p..o..rt..... 195
12.13...3...E..n..a..b..lin.g...S..N ... METRO P..T..ra pags..S . e..n..d.ing 195
12.14 Refrescando...los.e...S. . ys.te.m ..F. ile.s...de.m . METRO a..n..a..g..e..r..... 196
12.15 Botón Restablecer 197
12.16 Botón AUX 197
12.17 RS232 .P..o..rt.M . .a. in.te.n.a..n..c..... 198
12.18 Borrando...la...C. . o..re..S..o..ftw. . a..re..... 199
12.18.1 Borrado del software principal con el botón de reinicio n..... 199
12.18...2...E..ra cantando....c . o..re..S..o..ftw. a..re...uantando....p. . e..b..u..g..... 200
12.18.3 Borrado del software principal mediante Boot Load.e..r..... 201
12.19 Habilitar.g...IP..O. . . ffic.e...W. e..b...M . a..n..a..g..e..r..... 202

13. Componentes del sistema

13.1 IP500 V2...C..o..n..tro . l...u. . liendre..... .205
13.2 IP500 V2...S..y..s..te.m ... DAKOTA DE Tarjeta. 208
13.3 Base IP500. . ..c . SDRA..... 209
13.3..1...4...-.P..o r..t..E..x..p..a..n..sio.n...c . . a..rd..... 212
13.3..2...A..n..a..lo.g...P..h Onortai 213
13.3..3...A..T METRO C. o..m. b..in.a..t.io norte.C . a..rd..... 214
13.3..4...B..R. . yo..c..o..m. b..in.a..tio.n...C.a. r..d..... 216
13.3..5...U nortefie.d...C . o..m metro u..n..ic..a..ción..s...M. o..d..u..le 217
13.3..6...D . ig.ita.l..s.ta.ción..... 218
13.3..7...E..T. ..R. 6... Ca. r..d..... 219
13.3..8...T..C METRO 8 ..D . ig.ita.lS . ta.ción..... 220
13.3..9...V..C . METRO. 221
13.4 IP500 Tr..n..k..D. . . a..u..g..h..te.r..C. . a..rd.s..... 223
13.4..1...A..n..a..lo.g...T..ru.n..k...C. . . a..rd..... 224
13.4..2...B..R. . . I..T..ru.n..k...Ca. r..d..s..... 226
13.4..3...P..R. I..T..ru.n..k...Ca. r..d..s..... 227
13.5 IP500 Ex.te. . r..n..a..lE. XP.a norte..s..io.n...M . ..d..u..les..... 228
13.5..1...A..n..a..lo.g...T..ru.n..k...1..6..... 229
13.5..2...D..S . 1..6../.3..0..... 231
13.5..3...D..S 1..6..A../.3..0..A. 233
13.5..4...D..S 1..6..B../.3..0..B. , . . D..S.1.6.B . 2../.3..0..B..2..... 236
13.5..5...P..h..o..n..e...1..6../.3..0..... 238
13.6 IP400 Ex. p . a norte..s..io.n...M. . a..d..u..les..... 240
13.6..1...A..n..a..lo.g...T..ru.n..k...1..6..... 241
13.6..2...D. ig.ita.l..S..ta.tio.n...V..2 243
13.6..3...P..h..o..n..e...V. . . 2..... 245
13.7 Montaje...K..its..... 247
13.7..1...IP.5..0..0...W. . . a..llM o..u..n..tin.g...k . su..... 247
13.7..2...R . a c..k...m . o..u..n..tin.g...K..it..... 247
13.7..3...B..a..rr.ie . r...B..o..x...R..a..c..k...M. . o..u..n..tin.g...K..it..... 248
13.8 Teléfonos 249
13.9 Botón Teléfono n...M . . . o..d..u..le 250
13.10 Aplicaciones..... 251
13.10...1...IP...O. . ffic.e...A..p..p..lica. tio.n...S . e..rve r..... 252
13.10...2...IP...O. . ffic.e...M.a norte agramiu. r..... 253
13.10...3...M. e..d..ia METRO a norte agramiu. r..... 253
13.10...4...A..v..a..y..a...IX..W. . o..rk.p..la c..e...C mentnorte..(..E..q..u..in.o..x.)..... 254
13.10...5...IP...O. . ffic.e...W. e..b...C . li.e..n..t..... 254
13.10...6...M. o..n..it.o. r..... 255
13.10...7...o..n..e..-.X PAGS o..rta.l..para.r..IP..O . . ffic.e..... 255
13.10...8...A..v..a..y..a...C..o..m metro. u..n..ic.a.to.r..... .256
13.10...9...S..o..ftC . o..n..s.o..le. 257
13.10...1..0...S..y..s..te.m. . . S..ta.tu.s...A..p..p..lic.a..tio.n..... 257
13.10...1..1...T..A..P . . YO..... 258
13.10...1..2...V..o..hielo..m . . a..ilP . r..... 259
13.10...1..3...W. nu.b ..C . o..lla.b.o..ra.ción..... 260
13.10...1..4...IP..O . . fic.e...p..o..rts..... 260
13.11 Operati.n..g...S..y.s..tem.m . . . . Apoyo..... 261
13.11...1...W. en.d..o..w . s..S . up..p..p.o..rt..... 261
13.11...2...A..n..d..ro. id..S. . up..p..p.o..rt..... 262
13.11...3...A..p..p..le..S . tu pagpagso. r..t..... 262
13.11...4...L..in.u..x..S. . . up..p..p.o..rt..... 262
13.11...5...B..ro..w . s..e..r..S..u..p..p..o..rt..... 263
13.12 Física.l..P . . . o..rts..... 264
13.12...1...C..a b. les..... 265
13.12...2...A..N . A..L..O GRAMO . Puerto..... 267
13.12...3...A...U . . D..IO PAGSO. r..t..... 267
13.12...4...B..R. . I..P..o..rt.(.S . o..)..... 268
13.12...5...B..R. . I..P..o..rt.(.T . o..)..... 269
13.12...6...B..S. . T...P..o..rt.(.R . J..2..1..)..... 270
13.12...7...B..S. . T...P..o..rt.(.R . J..4..5..)..... 270
13.12...8...D..C . I./.P...P. . o..rt..... 271
13.12...9...D..S. . P..o..rts..(.R . J..4..5..)..... 271
13.12...1..0...E..F PAGS . o..rt..... 272
13.12...1..1...E...T..R . . Puerto..... 272
13.12...1..2...E..X PAGS UN. S..IO norte . . P..o..rt..... 273
13.12...1..3...E..X.T . . O PAGS . . Puerto..... 273
13.12...1..4...L..A..N . . . Puerto..... 274
13.12...1..5...P..F... PAGS . o..rt..... 275
13.12...1..6...PH . . O norteiu (..CORREOS. T..)..P..o. r..t..... 276
13.12...1..7...P..R. . I..P..o..rt 277
13.12...1..8...R..S. 2..3..2...P..o..rt.(.D. . TE.) 278
13.13 Licencias..... 279
13.13...1...S..y..s..te.m. . . E..d..itio.n...L..hielo norte S..e..s..... 279
13.13...2...U pagramoa..d..e...L..ic..e..n..s..e..s..... 280
13.13...3...T..ru.n..k...L..hielo..n..cantar..... 280
13.13...4...T..e..le.p..h..o..n..e../.E..n..d..p..o..in. t..L..ic.e..n..se 281
13.13...5...U s..e..r..L. helados..... 282
13.13...6...V..o..hielo..m . . a..ilP. ro..L..ic.e..n..se. 284
13.13...7...T..ria.l..L..hielo . . norte S..e..s..... 285
13.13...8...C..TILLINGIS helados..... 285
13.13...9...O . el..e..r..L..hielo norte S..e..s..... 285
13.14 Hardware. . /.S . o..ftwson. ..C o..m . p..a..tib.i.li.ty 286
13.14...1...C..onortetr.o..lU. n..its..a..n..d...C..o..n.t.ro..l.U. . . n..it..C.o..m. p..o..n..e..n..ts.. 287

Página1020 de 3226

13.14...2...S..e..rv.e..r..P. ..latfo r..m. 289
13.14...3...P..h..o..n.e..s..... 290
13.14...4...A..p..p..lic.a..t.io . . norte s..... 295
13.15 Niveles PCS 296
13.16 TAA 296

14. Declaraciones de seguridad

14.1 Rayo...P..ro.te.c..tio.n../.H..a..z..a..rd..S . . . mmm.b o. ls..... 298
14.2 Trunk Int.e.rfa.c..e...M . . a..d..u..les..... 299
14.3 Más adentro para r..m . a..t.io norte a norte d PAGS rod.d..u..c..t..U pags d.a te. s..... 300
14.4 Port Safe..ty..C.la.s..if.ic.a.tion..... 300
14.5 CEM grave. . c..tiv.e..... 301
14.6 Regulación..In.s..tru.c..tio.n..s...for.u..U . s..e..... 302
14.6..1...A..u..s..tra.lia..... 302
14.6..2...C . a nosta d.a 302
14.6..3...C . h. en un..... 303
14.6..4...J..a..p..a..n..... 304
14.6..5...E..u..ro . pags mi . a norte u . nión..... 304
14.6..6...N mi .w . . Z.e.a.la.n.d..... 304
14.6..7...F..C . c....N . o..t.if.ic.a..ción..... 305
14.6..8...C . Ometpags lia.n..c..e...w con..F..C ..C..R . u..les..... 307

15.Historial del documento

Índice 315

Capítulo 1.

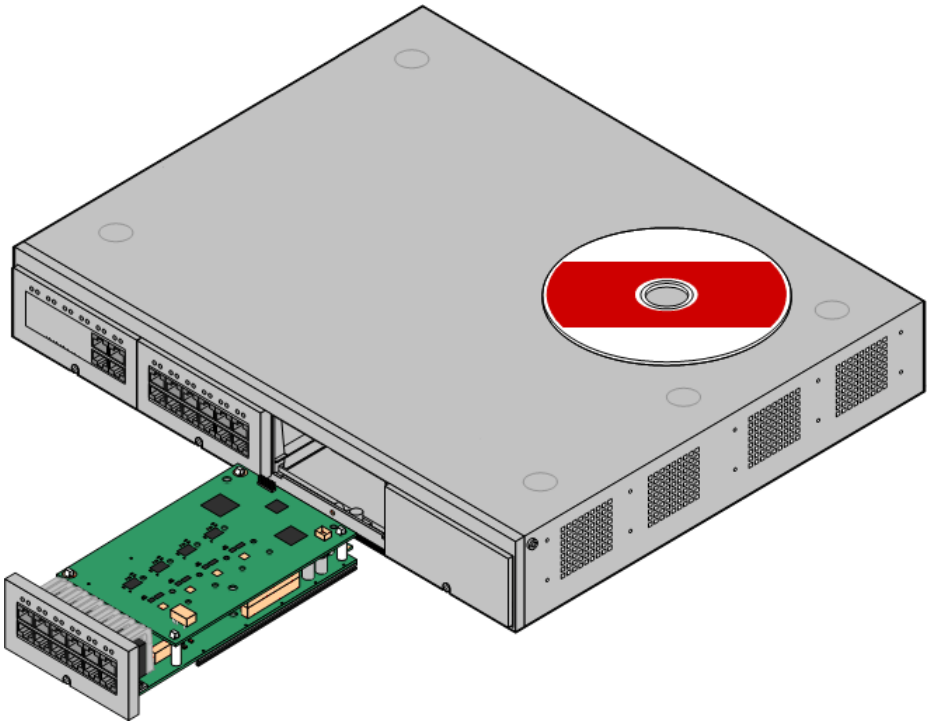
Resumen del sistema

1. Resumen del sistema

Este documento está destinado a ayudar con la instalación de un sistema IP Office que se ejecuta en el modo estándar de IP Office (IP Edición esencial de OfficeoEdición preferida de IP Office) utilizando una unidad de control IP500 V2.

Esta documentación no cubre la instalación de los sistemas IP Office Basic Edition, IP Office Basic Edition - Norstar Mode o IP Office Basic Edition - PARTNER® Mode, cada uno de los cuales tiene su propia documentación de instalación por separado. Tampoco cubre la adición de un sistema IP500 V2 como sistema de expansión IP500 V2 en una red Server Edition o IP Office Select. Sin embargo, las notas de compatibilidad de hardware para IP500 V2 en este manual siguen siendo aplicables a menos que se indique lo contrario.

- Los instaladores familiarizados con la instalación de versiones anteriores deben consultar elCambios para la versión 11.0 9 sección.



- IP Office es un sistema de comunicaciones de voz y datos convergentes. Por lo tanto, sólo debe ser instalado por personas con experiencia en telefonía y redes de datos IP.
- Los instaladores deben estar capacitados en los sistemas IP Office. A través de suUniversidad Avaya 46 (AU), Avaya ofrece una variedad de cursos de capacitación que incluyen capacitación específica sobre implementación e instalación de IP Office. También proporciona esquemas de certificación para que los instaladores logren varios niveles de acreditación de IP Office.
- Es responsabilidad del instalador asegurarse de que todo el trabajo de instalación se realice de acuerdo con las normas y los requisitos locales y nacionales. También es su responsabilidad establecer con precisión los requisitos del cliente antes de la instalación y asegurarse de que la instalación cumpla con esos requisitos.
- Debe leer y comprender esta documentación antes de la instalación. También debe obtener y leer los boletines técnicos de Avaya correspondientes a las versiones recientes de software y hardware para asegurarse de estar familiarizado con cualquier cambio en el equipo y el software de IP Office.
- Avaya IP Office IP500 V2 también se conoce como "IPO IP500 V2 Cntrl Unit", "IP Office IP 500 v2", "IPO IP500 v2", "IP 500 V2", "IP500 V2", "IPO 500v2 System Unit Assembly" o "IP Office 500 v2". A lo largo de esta documentación se utiliza el término IP500 V2.

1.1 Cambios para la versión 11.0

El siguiente es un resumen de los principales cambios que afectan la instalación de IP500 V2 con la versión 11.0 de IP Office:

- **Uso de IP Office Web Manager para la configuración inicial** 114
  Usando el acceso del navegador web, la configuración inicial del sistema ahora se puede realizar a través de una serie de asistentes de menú. Estos menús reemplazan la pantalla del tablero de IP Office Web Manager.
- **Cliente web de IP Office** 254
  El cliente web de IP Office, anteriormente disponible en R10.1 solo para comentarios de los clientes, ahora es completamente compatible y se ha mejorado con una gama de funciones de control de llamadas, video y conferencias. Este es un cliente WebRTC que puede usar cualquier usuario configurado para one-X Portal for IP Office a través del navegador Chrome (Windows y macOS) que se ejecuta en un IP Office Application Server. También se puede instalar en PC con Windows como un cliente pesado. Hay disponible una extensión de Chrome que permite hacer clic para marcar los números que se muestran en el navegador.
- **Teléfonos SIP J169/J179**
  Estos nuevos teléfonos SIP de Avaya ahora son compatibles. Estos proporcionan funciones de IP Office similares a las que se muestran en los teléfonos de las series 1400, 1600, 9500 y 9600. Ambos teléfonos son físicamente similares y admiten 24 botones programables a través de una pantalla con 8 botones físicos de doble LED. El J169 tiene una pantalla en escala de grises, el J179 una pantalla a color.
  - **Módulo de botones JBM24**
    Los teléfonos J169 y J179 admiten hasta 3 de estos módulos de botones. Cada módulo proporciona al teléfono 24 botones programables de doble LED adicionales.
  - **Módulo inalámbrico J100**
    El J179 tiene una ranura para módulos opcionales adicionales. El módulo inalámbrico J100 permite que el J179 se conecte a la red del cliente a través de WiFi. Esto permite que el teléfono se use en lugares donde una conexión Ethernet por cable no está disponible o no se desea.
- **Teléfonos de la serie Vantage K100**
  Estos teléfonos SIP de Avaya son compatibles. El teléfono consta de un dispositivo de tableta Android integrado en un teléfono de escritorio. El teléfono está disponible en formato modular:
  - **Teléfono Vantage K165**
    Un teléfono de escritorio con tableta Android con un puerto para auriculares de telefonía RJ11. Esta versión del teléfono no incluye una cámara integrada.
  - **Teléfono Vantage K175**
    Este teléfono es similar al K165 pero también incluye una cámara integrada para admitir videollamadas.
  - **Módulo de microteléfono con cable J1B1**
    Utilizable con ambos teléfonos K100, este módulo agrega un auricular de teléfono estándar.
  - **Módulo de auricular Bluetooth J1B2**
    Utilizable con ambos teléfonos K100, este módulo agrega un auricular Bluetooth al teléfono de escritorio.
- **Cliente del lugar de trabajo de Avaya IX** 254
  Esta es una aplicación de comunicaciones unificadas compatible con una amplia gama de sistemas operativos tanto en PC como en dispositivos móviles.

Service Pack 1

Como parte de R11.0 Service Pack 1, ahora también se admiten los siguientes:

- **Teléfonos de la serie H200**
  Una gama de teléfonos de hostelería destinados a entornos hoteleros y similares: H229, H239 y H249.
- **Teléfono K155 Vantage**
  Similar al K175 pero con una pantalla más pequeña para permitir la inclusión de un teclado de marcación telefónica regular.

Paquete de servicio 2

Como parte de R11.0 Service Pack 2, ahora también se admiten los siguientes:

- **Modo de control compartido de Avaya IX Workplace Client**
  La aplicación Avaya IX Workplace Client en PC con Windows y macOS se puede utilizar en el modo de control del teléfono de escritorio. En ese modo, la aplicación se puede utilizar para realizar y contestar llamadas en el teléfono de escritorio asociado del usuario.

Paquete de características 4

Como parte de R11.0 Feature Park 4 (11.0.4.0), ahora también se admiten los siguientes:

- **Firmware de la serie J100 40.0**
  El paquete de servicios incluye el firmware SIP J100 Series 4.0. Ese firmware habilita el soporte para lo siguiente:
  - **Bluetooth J179**
    El firmware actualizado admite la conexión de auriculares Bluetooth a teléfonos J179 que tienen instalado el módulo inalámbrico J100 opcional.

¿Comentarios sobre este documento? infodev@avaya.com

- **Módulo de botones JEM24**
  Este tipo de módulo de botones es compatible con los teléfonos J169/J179. El JEM24 tiene 24 botones de doble LED con pantalla de etiqueta de botón adyacente. Un solo JEM24 admite 72 espacios para botones programables. Estos están organizados en 3 páginas, a las que se accede mediante el botón de desplazamiento de página del módulo. Cuando se conectan varios módulos JEM24 (hasta 3) a un teléfono, cada módulo solo admite una sola página de 24 ranuras de botones programables. Los módulos de botones JEM24 y JBM24 no se pueden combinar en el mismo teléfono.

- **Cliente Avaya IX Workplace en Vantage**
  El cliente Avaya IX Workplace Client ahora es compatible como una aplicación de marcación en los teléfonos Vantage K165/K175.

Paquete de características 4 - Paquete de servicio 2 (R11.0.4.2)

Como parte de este paquete de servicios, ahora también se admiten los siguientes:

- **Teléfono J159**
  Estos teléfonos ahora son compatibles (usando J100 R4.0.3 o firmware superior).

- **Cambio de marca de equinoccio**
  Esta versión es compatible con los clientes Equinox R4.3, que ahora se denominan Avaya IX Workplace Client.

Ya no es compatible

Las siguientes opciones ya no son compatibles con IP Office R11.0 y versiones posteriores:

- **Teléfonos de la serie T3**
  Los teléfonos de la serie T3 (VoIP y no VoIP) no son compatibles.

- **IP DECT**
  La solución IP DECT más antigua (anterior a R4) no es compatible. Aún se admite IP DECT R4.

- **Registrador de contactos para IP Office**
  El servicio Contact Recorder for IP Office (para IP500 V2, proporcionado por un servidor de aplicaciones de IP Office) ya no es compatible. El reemplazo, Media Manager, introducido en R10.1 incluye opciones para ayudar a migrar cualquier archivo de Contact Recorder for IP Office existente a Media Manager.

- **Softphone de vídeo de IP Office**
  La versión macOS de esta aplicación ya no es compatible. La versión de Windows ya no era compatible.

- **Reportero de contacto integrado**
  Esta aplicación no es compatible.

- Con el lanzamiento de la versión 11.0 de IP Office, Avaya ya no es compatible directamente con los sistemas y aplicaciones relacionadas de las versiones 10.0 y R9.1 de IP Office.

1.2 Documentación adicional

Este manual solo cubre la instalación básica del sistema necesaria para dar como resultado un sistema IP500 V2 configurable. Las aplicaciones de IP Office y los productos auxiliares, incluidos los teléfonos IP, están fuera del alcance de este manual.

Si esas aplicaciones y productos van a ser parte de la instalación del sistema, se debe obtener, leer y comprender la documentación separada para esos productos antes de la instalación.

- **!Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín técnico de IP Office relacionado con la versión del software de IP Office que pretende instalar. El boletín contiene información importante que puede no haber sido incluida en este manual. Los boletines técnicos de IP Office están disponibles en elSoporte de Avaya sitio web*(http://soporte.avaya.com)*.

Para descargar documentación:

1. Navegar a***https://soporte.avaya.com***.
2. Seleccione**Soporte por producto**y entonces**Documentos**.
3. Entrar***Oficina de PI***en el**Introduzca el nombre del producto**y seleccione la opción correspondiente de la lista que se muestra.
4. Usa el**Elija Liberar**desplegable para seleccionar la versión de IP Office necesaria.
5. Seleccione el tipo de documentos necesarios de la lista y haga clic en**INGRESAR**.

1.3 Disponibilidad de equipos

Los códigos SAP y los detalles de artículos específicos dentro de esta documentación son solo para referencia. Los artículos disponibles en cualquier lugar específico deben confirmarse con la lista de precios local de Avaya IP Office para ese lugar. La lista de precios local también puede incluir elementos adicionales relacionados con los requisitos de instalación de ese lugar.

Esta documentación cubre el equipo compatible con IP Office 11.0. Eso incluye equipos compatibles pero que ya no están disponibles como nuevos de Avaya.

1.4 Reparación

Los sistemas IP Office no contienen ningún componente reparable o reparable por el usuario. Si se sospecha que hay una unidad defectuosa, se debe reemplazar toda la unidad.

Las unidades de control de IP Office no deben abrirse bajo ninguna circunstancia exceptoinserción de tarjetas base IP500 82.

1.5 RoHS

RoHS es una directiva de la Unión Europea para la eliminación de ciertas sustancias peligrosas de equipos eléctricos y electrónicos. Se ha introducido o se está introduciendo una legislación similar en varios otros países. Avaya ha decidido hacer que su gama global de productos cumpla con los requisitos de RoHS.

Las acciones tomadas varían:

- En algunos casos, el equipo ha sido descontinuado y ya no está disponible en Avaya.
- En algunos casos, el stock nuevo fabricado cumple con RoHS y mantiene su código SAP existente.
- En otros casos, el equipo ha sido reemplazado por una nueva alternativa compatible con RoHS con nuevos códigos SAP.
- Los códigos SAP dentro de este documento son para equipos que cumplen con RoHS a menos que se indique lo contrario.

1.6 Modos de IP Office

Los sistemas IP Office pueden ejecutarse en varios modos. Para la versión 10.0 de IP Office, solo se admiten los siguientes modos para las unidades de control IP500 V2:

Modos de la edición básica de IP Office

Los siguientes modos operativos se denominan colectivamente como modo básico de IP Office.

- **Edición básica de IP Office**
  Este es el modo de funcionamiento predeterminado para las unidades de control IP500 V2.
- **Edición básica de IP Office - Modo Norstar**
  Este modo funciona igual que el modo IP Office Basic Edition. Este modo se vende en lugares de Medio Oriente y África del Norte.
- **Edición básica de IP Office - Modo PARTNER®**
  Este modo funciona igual que el modo IP Office Basic Edition. Este modo se vende en locales de América del Norte.

Modos estándar de IP Office

Los siguientes modos operativos se denominan colectivamente como modo estándar de IP Office.

- **Edición esencial de IP Office**
  Para la versión 11.0 de IP Office, los sistemas IP500 V2 se ejecutan en este modo si**Edición esencial**la licencia se agrega a la configuración. Los sistemas configurados en este modo sin una licencia no admitirán ninguna función de telefonía.
- **Edición preferida de IP Office**
  Este modo es similar a IP Office Essential Edition pero agrega soporte para la aplicación Voicemail Pro. Este modo se habilita agregando un**Edición preferida (Voicemail Pro)**licencia a un sistema ya licenciado para**Edición esencial**.

Otros modos

- **Edición del servidor**
  Este modo de IP Office no está cubierto por esta documentación. Utiliza servidores de IP Office que se ejecutan en servidores Linux, incluidos servidores virtuales. Consulte la documentación separada de Server Edition. Los sistemas IP500 V2 físicos se pueden usar en una red Server Edition como un sistema de expansión IP500 V2. Por lo tanto, las notas de compatibilidad de hardware para la unidad de control IP500 V2 en este manual siguen siendo aplicables para el uso de Server Edition a menos que se indique lo contrario.

- **Seleccionar IP Office**
  Este modo habilitó capacidad y funciones adicionales para una red Server Edition. Todos los sistemas de la red deben configurarse como sistemas IP Office Select. Nuevamente, las unidades de control IP500 V2 se pueden emplear como sistemas de expansión en una red IP Office Select.

1.6.1 Tarjetas SD del sistema

La unidad de control IP500 V2 debe estar equipada con una tarjeta System SD. El modo predeterminado del sistema está determinado por el tipo de tarjeta SD del sistema presente. Al usar IP Office Manager y agregar licencias, se puede cambiar el modo del sistema.

Las diferentes tarjetas SD del sistema son:

- **Tarjeta SD de ley U de IP Office**
  Un sistema equipado con este tipo de tarjeta utiliza de forma predeterminada telefonía U-Law e IP Office Basic Edition.***Sistema de llaves*** operación. Destinado a locales de América del Norte.
- **Tarjeta SD de ley A de IP Office**
  Un sistema equipado con este tipo de tarjeta tiene por defecto telefonía A-Law e IP Office Basic Edition***Sistema PBX*** operación. Destinado a lugares fuera de América del Norte.

1.6.2 Capacidad total

La siguiente tabla es solo un resumen. El soporte para tipos particulares de extensiones, troncales y puertos de usuario también depende de otros factores, como las variaciones de soporte local. Por ejemplo, los troncales BRI no se admiten en las configuraciones regionales de América del Norte.

		Oficina de PI Edición básica - SOCIO® Modo	Oficina de PI Edición básica -Norstar Modo	Oficina de PI Edición básica	Oficina de PI Básico Edición Oficina de PI Privilegiado Edición
Extensiones	Extensiones máximas	100[1]	100[1]	100[1]	384
Bañador	Máximo de troncales	64	64	64	[5]
	- Troncales analógicos máximos	32	32	32	204
	- Máximo de canales BRI[3]	–	12	12	32
	- Máximo de canales PRI[4]	24	30	30	240
	- Máximo de canales SIP[2]	20	20	20	[5]
	- Máximo de canales IP H323	–	–	–	[5]

1. 100 Extensiones en modo de numeración de extensiones de 3 dígitos. 48 extensiones en modo de numeración de extensión de 2 dígitos.

   - Para los modos de IP Office Basic Edition, el sistema asume que la unidad de control base siempre está completa con hasta 32 extensiones, ya sea reales, fantasma o una combinación, a las que asigna números de extensión en secuencia.

     oHace esto antes de asignar números de extensión a cualquier extensión real en la expansión externa adjunta. módulos hasta el límite de extensión del sistema. Si no se ha excedido el límite de extensión del sistema, los números de extensión restantes se asignan a extensiones fantasma adicionales.

     oPara los puertos DS, la unidad de control solo puede albergar hasta 3 tarjetas DS8 más una tarjeta Combo con 6 puertos DS y 2 Puertos de teléfonos analógicos. Esto significa que con los módulos de expansión externos, el máximo de extensiones DS que se pueden lograr es 98 en el modo de numeración de extensiones de 3 dígitos, 46 en el modo de numeración de extensiones de 2 dígitos.

2. En todos los modos, también se requieren recursos de hardware de compresión de voz para la compatibilidad con SIP.

3. Los sistemas en modo IP Office Basic Edition no admiten troncales BRI y PRI en el mismo sistema. También están restringidos a 12 canales BRI, independientemente del hardware BRI instalado. Los sistemas de modo estándar de IP Office admiten troncales BRI y PRI en el mismo sistema.

4. Los sistemas en modo IP Office Basic Edition están limitados a 1 tarjeta PRI de puerto único.

5. La capacidad depende de las licencias, los recursos de compresión de voz y el ancho de banda disponible.

1.6.3 Resumen de soporte de hardware

Tenga en cuenta que incluso cuando se indica como compatible, la disponibilidad y el soporte del equipo pueden estar sujetos a restricciones locales. La siguiente tabla es un resumen de la versión 11.0 de IP Office, consulteCompatibilidad de hardware y software[286] para obtener un resumen más histórico y una lista de teléfonos compatibles.

	IP Office básico Modos de edición	estándar de IP Office modos
Unidad de control IP500 V2	✓	✓
Tarjetas base IP500		
Tarjeta de estación digital IP500	✓ 3	✓ 3
Teléfono analógico IP500 2/8	✓ 4	✓ 4
Tarjeta IP500 TCM8	✓ 4	✓ 4
Tarjetas IP500 VCM 32/64	–	✓ 2
Expansión de 4 puertos IP500	–	✓ 1
Combo IP500 BRI[2][4]	✓ 2	✓ 2
Combinación de cajero automático IP500[2]	✓ 2	✓ 2
Combinación de cajero automático IP500 V2[2]	✓ 2	✓ 2
IP500 ETR6[1][6]	✓ 3	–
Módulo de comunicaciones unificadas[6]	–	✓
Tarjetas de la hija del tronco		
Tarjeta de troncales analógicas	✓	✓
Tarjeta de troncales analógicas V2	✓	✓
Tarjetas troncales BRI[4]	✓	✓
Tarjeta Troncal PRI[4][5]	✓ 1	✓ 4
Módulos de expansión		
Número de módulos[3]	8	12
Emisora Digital 16/30	✓	✓
Estación Digital 16A/30A	✓	✓
Estación Digital 16B/30B	✓	✓
Teléfono 16/8/30	✓	✓
Troncal analógico 16	✓	✓
Tipos de teléfono		
Teléfonos ETR*(puertos ETR)*	✓	–
Teléfonos BST*(puertos BST)*	✓	✓
Teléfonos DS*(puertos DS)*	✓	✓
Teléfonos IP H323*(LAN)*	–	✓
Teléfonos IP SIP*(LAN)*	–	✓
DECT R4*(LAN)*	–	✓
DMS DECT*(puertos BST)*	✓	✓
Tipos de correo de voz		
Correo de voz integrado	✓	✓
Buzón de voz profesional	–	✓

1. La tarjeta ETR6 solo es compatible con los sistemas IP500 V2 en los modos IP Office Basic Edition - PARTNER® Mode o IP Office Basic Edition U-Law.
2. Solo se admiten 2 tarjetas de combinación en una unidad de control, independientemente del tipo de tarjeta de combinación.
3. Se pueden agregar módulos de expansión externos siempre que no se exceda el límite total de extensiones y troncales. En los sistemas en modo IP Office Basic Edition, se admite un máximo de un módulo Analog Trunk 16.
4. Los sistemas en modo IP Office Basic Edition no admiten una combinación de troncales BRI y PRI y solo admiten un máximo de 12 canales BRI.
5. Los sistemas en modo IP Office Basic Edition solo admiten una tarjeta PRI de un solo puerto.

1.6.4 Resumen de compatibilidad de funciones

La siguiente tabla es solo un resumen general. Para obtener detalles más específicos, consulte la documentación de instalación para la aplicación específica.

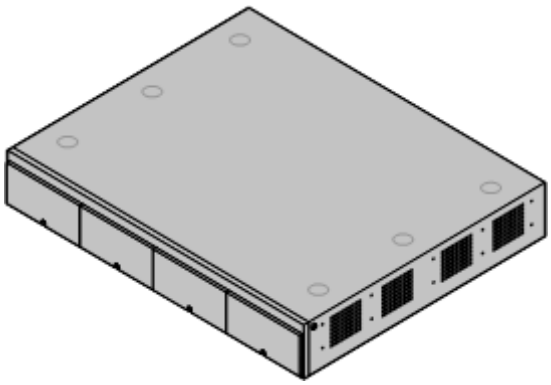
		Edición básica de IP Office			Oficina de PI Básico Edición	Oficina de PI Privilegiado Edición
		COMPAÑERO Modo	Norstar Modo	Modo rápido		
Administración Aplicaciones	Administrador basado en teléfono	✓	✓	✓	–	–
	Administrador web de IP Office	✓	✓	✓	✓	✓
	Gerente de IP Office	✓	✓	✓	✓	✓
	Supervisar (Supervisión del sistema)	✓	✓	✓	✓	✓
	Aplicación de estado del sistema	✓	✓	✓	✓	✓
Aplicaciones	Portal one-X para IP Office	–	–	–	–	✓
	Cliente web de IP Office					✓
	one-x móvil					✓
	Comunicador de Avaya					✓
	SoftConsole	–	–	–	✓	✓
	TAPI (primera parte)	–	–	–	✓	✓
	TAPI (tercero)	–	–	–	✓	✓
	Buzón de voz profesional	–	–	–	–	✓
	Administrador de medios	–	–	–	–	✓

		Edición básica de IP Office			Oficina de PI Básico Edición	Oficina de PI Privilegiado Edición
locales		Canadá, México, Unido estados	Bahréin, Egipto, Kuwait, Marruecos, Omán, Pakistán, Catar, Arabia Saudita Arabia, Sudáfrica, Pavo, Arabes unidos Emiratos.	argentino, Australia, Bahréin, Bélgica, Brasil, Canadá, Chile, China, Colombia, Checo, Dinamarca, Egipto, Finlandia, Francia, Alemania, Grecia, Hong Kong, Hungría, Islandia, India, Irlanda, Italia, Corea, Kuwait, Malasia, México, Marruecos, Países Bajos, Nuevo Zelanda, Noruega, Omán, Pakistán, Perú, filipinas, Polonia, Portugal, Katar, Rusia, Arabia Saudita Arabia, Singapur, Sudáfrica, España, Suecia, Suiza, Taiwán, Pavo, Arabes unidos emiratos, Unido Reino, Unido estados, Venezuela.	Argentina, Australia, Bahrein, Bélgica, Brasil, Canadá, Chile, China, Colombia, República Checa, Dinamarca, Egipto, Finlandia, Francia, Alemania, Grecia, Hong Kong, Hungría, Islandia, India, Irlanda, Italia, Japón, Corea, Kuwait, Malasia, Mediterráneo, México, Marruecos, Países Bajos, Nueva Zelanda, Noruega, Omán, Pakistán, Perú, Filipinas, Polonia, Portugal, Catar, Rusia, Arabia Saudita, Singapur, Sudáfrica, España, Suecia, Suiza, Taiwán, Turquía, Emiratos Árabes Unidos Emiratos, Reino Unido, Estados Unidos, Venezuela.	
Mensaje de voz Idiomas	**Correo de voz integrado**	· **Arábica**,**cantonés**,**danés**,**Holandés**,**Inglés del Reino Unido)**, **Inglés (Estados Unidos)**,**finlandés**,**Francés**,**Francés (Canadá)**, **Alemán**,**hebreo**,**italiano**,**japonés**,**coreano**, **mandarín**,**noruego**,**Polaco**,**portugués**, **Portugués (Brasil)**, **ruso**,**español**,**Español (Argentina)**,**español (latín)**,**Español (México)**, **sueco**,**turco**.				
	Buzón de voz profesional	–	–	–	–	Como anteriormente más:**Griego**, **húngaro**. Menos: **Arábica**, **español (México)**.

1.7 La Unidad de Control

La base de cualquier sistema IP Office es la unidad de control. Almacena la configuración del sistema y controla el funcionamiento del sistema. Cada unidad de control se puede personalizar insertando variostarjeta base 22sobre el cualtarjetas de la hija del baúl 25también se puede agregar.Módulos de expansión externos 26también se puede conectar para agregar extensiones adicionales y puertos troncales.

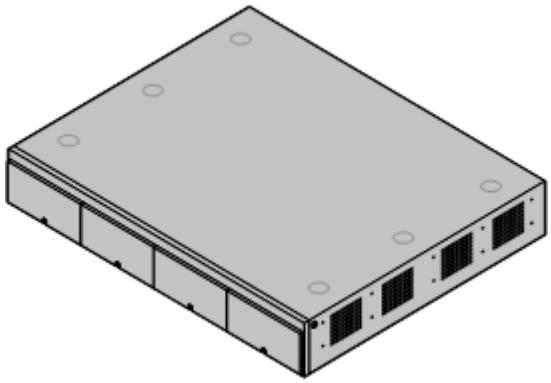
La versión 11.0 de IP Office es compatible con las siguientes unidades de control de IP Office. Otros tipos anteriores de unidades de control de IP Office no son compatibles con la versión 11.0 de IP Office y no están cubiertos por esta documentación.



- **Unidad de control IP500 V2** 205
  Esta unidad de control tiene cuatro ranuras frontales para tarjetas base IP500. Tiene una fuente de alimentación interna y utiliza una tarjeta SD del sistema obligatoria. Incluye un conmutador LAN ethernet de 2 puertos (administrado por capa 3) en la parte posterior.
  - El tipo de tarjeta SD del sistema instalado en el sistema determina su valor predeterminadomodo de operación 13del sistema.
    - **Edición básica de IP Office**
    - **Edición básica de IP Office - Modo PARTNER®**
    - **Edición básica de IP Office - Modo Norstar**
    - **Edición esencial de IP Office**

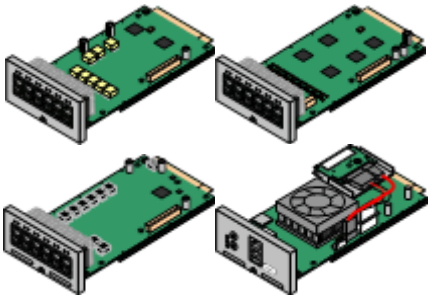
1.8 Componentes del sistema IP500 V2

Los siguientes son los componentes típicos de un sistema basado en una unidad de control IP500 V2.

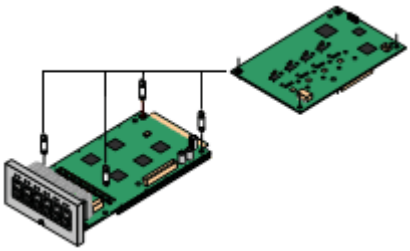


- **Unidad del sistema IP Office IP500 V2** 205
  La unidad de control contiene la configuración principal y realiza el enrutamiento y conmutación de llamadas telefónicas y tráfico de datos. Cada unidad de control incluye 4 ranuras para tarjetas base opcionales para admitir puertos de extensiones telefónicas y troncales.
  - **Tarjeta SD Avaya** 21
    Esta tarjeta contiene el firmware y otros archivos utilizados por el sistema cuando se inicia. Una tarjeta SD de Avaya System es obligatoria para el correcto funcionamiento del sistema. La tarjeta también proporciona almacenamiento para el correo de voz incorporado, si se usa.

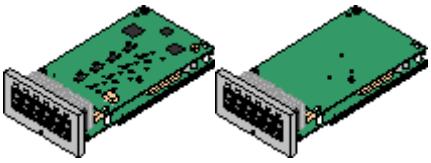
- **Claves de licencia** 209
  Varias funciones y aplicaciones requieren licencias en la configuración del sistema. Estos se ingresan cargando un archivo PLDS XML que contiene todas las licencias del sistema. El archivo y sus licencias son específicos del número de serie único de la tarjeta SD del sistema instalada en el sistema.



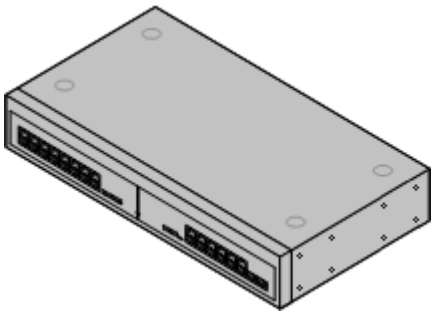
- **Tarjetas base IP500** 22
  La unidad de control IP500 V2 tiene ranuras para hasta 4 tarjetas base IP500. Estos se pueden usar para agregar puertos para extensiones analógicas, extensiones digitales, canales de compresión de voz y otros recursos.
  - **Tarjeta base de estación digital IP500** 218
  - **Tarjeta base de teléfono analógico IP500** 213
  - **Tarjeta base IP500 VCM** 221
  - **Tarjeta base de expansión de 4 puertos IP500** 212
  - **Tarjeta base IP500 TCM8** 220
  - **Tarjeta base IP500 ETR6** 219
  - **Módulo de comunicaciones unificadas** 217



- **Tarjetas auxiliares de troncales IP500** 25
  Muchas de las tarjetas base IP500 pueden equiparse con una tarjeta secundaria IP500 para admitir varios tipos de conexiones troncales.
  - **Tarjeta de troncales analógicas IP500** 24
  - **Tarjeta de troncales analógicas IP500 V2** 224
  - **Tarjeta de troncales IP500 BRI** 226
  - **Tarjeta de troncales PRI IP500** 227



- **Tarjetas combinadas IP500** 22
  Estas tarjetas son tarjetas base y secundarias previamente emparejadas. Proporcionan 6 puertos de estación digital, 2 puertos de teléfono analógico, 10 canales de compresión de voz y 4 puertos de troncales analógicas o 4 canales BRI (2 puertos). La tarjeta secundaria de troncales no se puede quitar ni reemplazar con otro tipo.
  - **Tarjeta combinada IP500 BRI** 216
  - **Tarjeta combinada de cajero automático IP500** 214
  - **Tarjeta combinada de cajero automático IP500 V2** 214

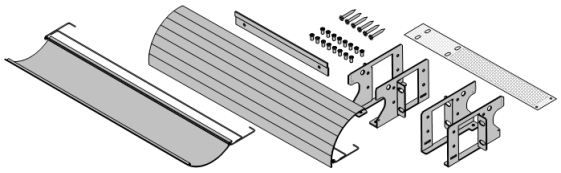


- **Módulos de expansión externos IP500** 26
  Se pueden agregar puertos adicionales utilizando varios módulos de expansión externos IP500.
  - Los sistemas que se ejecutan en los modos estándar de IP Office admiten 8 módulos de expansión externos como estándar. Si está equipado con una tarjeta base de expansión de 4 puertos IP500, se admiten hasta 12 módulos de expansión externos.

- **Fuentes de alimentación** 36
  La unidad de control IP500 tiene una fuente de alimentación interna. Cada módulo de expansión externo se suministra con una fuente de alimentación externa. Es posible que también se requieran unidades de fuente de alimentación adicionales para teléfonos IP y algunos complementos de teléfono.

- **Cables de alimentación** 33
  Según la ubicación, es necesario pedir cables de alimentación diferentes para cada unidad de control, módulo de expansión externo y cualquier teléfono o dispositivo que use unidades de fuente de alimentación externas.

- **cabos** 33
  El sistema está diseñado principalmente para la conexión a un sistema de cableado estructurado mediante cableado UTP CAT3. Este enfoque permite que el tráfico telefónico y de datos comparta la misma infraestructura de cableado y simplifica los movimientos de equipos.



- **Juegos de montaje** 37
  La unidad de control se puede utilizar de forma independiente, con módulos de expansión externos apilados encima. Con kits de montaje en rack opcionales, la unidad de control y los módulos de expansión externos también se pueden montar en rack. Como alternativa, con un kit de montaje en pared opcional, la unidad de control IP500 se puede montar en la pared. Los módulos de expansión externos IP500 también se pueden montar en la pared.

- **Protectores contra sobretensiones y cajas de barrera** 36
  Cuando la instalación incluya ampliaciones en otros edificios, se requiere equipo de protección adicional. Este equipo también puede ser necesario en áreas donde el riesgo de rayos es alto.

- **Los telefonos** 39
  Los sistemas IP Office admiten una variedad de teléfonos digitales e IP de Avaya, además de teléfonos analógicos.

- **DVD de aplicaciones** 42
  Las aplicaciones de IP Office se pueden pedir en varios DVD. Además, se pueden descargar desde la sección IP Office de la Soporte de Avaya sitio web(*http://soporte.avaya.com*).

1.9 Tarjeta SD del sistema

El sistema IP Office requiere unTarjeta SD del sistema Avaya 208para operar. Esta tarjeta lleva la firmware y varios otros archivos que el sistema carga cuando se enciende. Una vez que el sistema está operativo, la tarjeta SD del sistema contiene una copia de la configuración del sistema, el archivo de licencias y, si se utilizan, los archivos de correo de voz integrados. La tarjeta se inserta en la ranura System SD en la parte posterior de la unidad de control antes de iniciar el sistema.

Si el sistema utiliza un archivo XML PLDS para la concesión de licencias, el número de serie de la clave de funciones de la tarjeta SD se utiliza como el valor único con el que se emiten y validan las licencias.

Configuración del nivel de software original del sistema

Para una nueva unidad de control de IP Office, la versión del software de IP Office que carga desde la tarjeta SD del sistema cuando se enciende por primera vez se convierte en su nivel de software base o original. Ese valor se escribe en la memoria permanente de las unidades de control y no se puede cambiar.

Por lo tanto, es importante asegurarse de que la tarjeta SD del sistema se haya cargado con la versión correcta del software antes de encender el sistema por primera vez. Esto se hace usando IP Office Manager paracargar el nivel requerido de software en la tarjeta SD 75.

1.10 Licencias

El sistema IP Office requiere licencia para algunas funciones, consulteLicencias 279.El archivo de licencia se puede cargar manualmente oprecargado en la tarjeta SD del sistema 78.

¿Cómo se licencia el sistema?

- Se carga en el sistema un archivo XML que contiene el conjunto completo de licencias PLDS. El archivo de licencia es único para el número de serie de la clave de función de la tarjeta SD del sistema instalada en el sistema.
    - El ID de host PLDS utilizado para el archivo de licencia debe coincidir con el que se muestra en los 12 dígitos.**Identificación PLDS**impreso en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra con**FK**o**FK SN**. Para esas tarjetas agregue el prefijo***11***para obtener la identificación PLDS de la tarjeta.

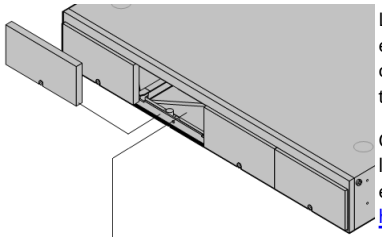
Requisitos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una**Edición esencial**licencia del sistema para la versión específica de IP Office que desea ejecutar.

1.11 Tarjetas de la unidad de control

Se admiten las siguientes tarjetas de unidad de control.

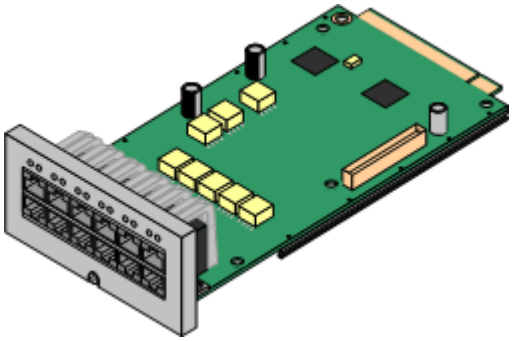
1.11.1 Tarjetas base IP500



La centralita IP500 V2 dispone de 4 slots para la inserción de tarjetas base IP500. Las ranuras están numeradas del 1 al 4 de izquierda a derecha. Normalmente se pueden usar en cualquier orden, sin embargo, si se excede la capacidad de un tipo de tarjeta en particular, la tarjeta en la ranura más a la derecha se desactivará.

Cada tarjeta base incluye un panel frontal integral con puertos para conexiones de cable. Por lo general, los primeros 8 puertos de la izquierda son para la conexión de dispositivos de extensión. Los 4 puertos de la izquierda se utilizan para la conexión de troncales si un[tarjeta hija troncal](#) 25se añade a la tarjeta base.

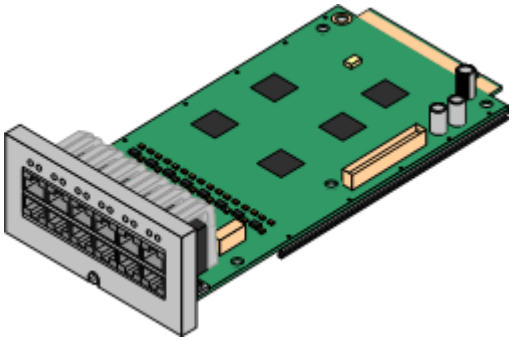
Tarjeta base de estación digital IP500 218



Esta tarjeta proporciona 8 puertos DS (estación digital) para la conexión de teléfonos digitales Avaya.

- La tarjeta se puede equipar con un[Tarjeta auxiliar de troncales IP500](#) 25que utiliza los puertos de la tarjeta base para la conexión troncal.
- **Máximo:**3 por unidad de control.
  - Las conexiones para los teléfonos 4100, 7400, M-Series y T-Series utilizan la tarjeta IP500 TCM8 Digital Station.

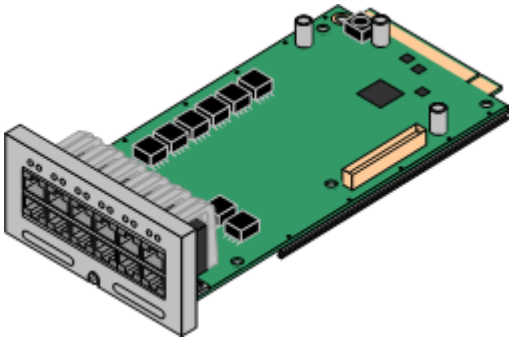
Tarjeta base de teléfono analógico IP500 213



La tarjeta está disponible en dos variantes, que admiten 2 u 8 puertos de teléfono analógico.

- La tarjeta se puede equipar con un[Tarjeta auxiliar de troncales IP500](#) 25que utiliza los puertos de la tarjeta base para la conexión troncal.
- **Máximo:**4 por unidad de control.
  - Los puertos de teléfono analógico no incluyen un condensador de llamada. Cuando este sea un requisito, la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
  - Si está equipada con una tarjeta secundaria de troncales analógicas IP500, durante un corte de energía, el puerto de teléfono 8 se conecta al puerto de troncales analógicas 12.

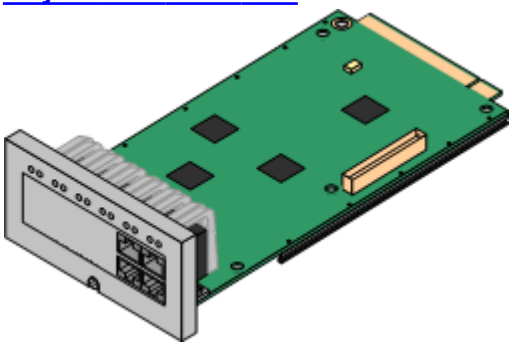
Tarjeta de estación digital IP500 TCM8 220



Esta tarjeta proporciona 8 puertos BST (estación digital) para la conexión de teléfonos Avaya 4100, 7400, M-Series y T-Series.

- La tarjeta se puede equipar con un[Tarjeta auxiliar de troncales IP500](#) 25que utiliza los puertos de la tarjeta base para la conexión troncal.
- **Máximo:**4 por unidad de control por unidad de control IP500 V2.

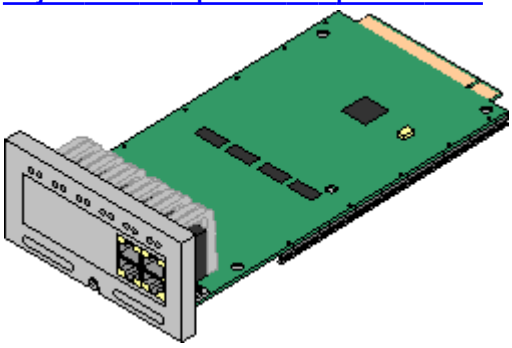
Tarjeta base IP500 VCM 221



Esta tarjeta está disponible en variantes que admiten 32 o 64 canales de compresión de voz para uso con llamadas VoIP.

- La tarjeta se puede equipar con unTarjeta auxiliar de troncales IP500 25que utiliza los puertos de la tarjeta base para la conexión troncal.
- **Máximo:**2 por unidad de control.

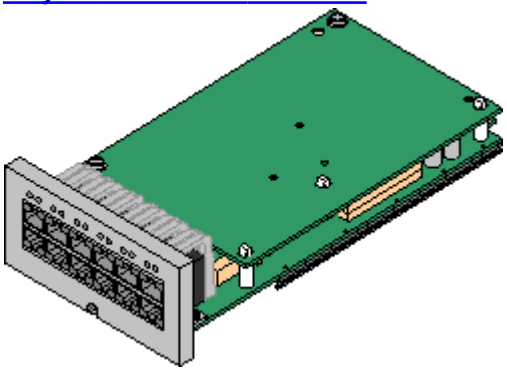
Tarjeta base de expansión de 4 puertos IP500 212



Esta tarjeta agrega 4 puertos de expansión adicionales para módulos de expansión externos. La tarjeta se suministra con cuatro cables de interconexión amarillos de 2 m.

- Esta tarjeta no acepta ninguna tarjeta auxiliar de troncales IP500.
- **Máximo:**1 por unidad de control (solo ranura derecha 4).
- **Módulos de expansión compatibles:**Se admiten los siguientes módulos de expansión externos:
  - Módulo troncal analógico IP500
  - Módulo IP500 BRI So
  - Módulo de estación digital IP500
  - Módulo de estación digital IP500
  - Módulo de estación digital IP500
  - Módulo telefónico IP500

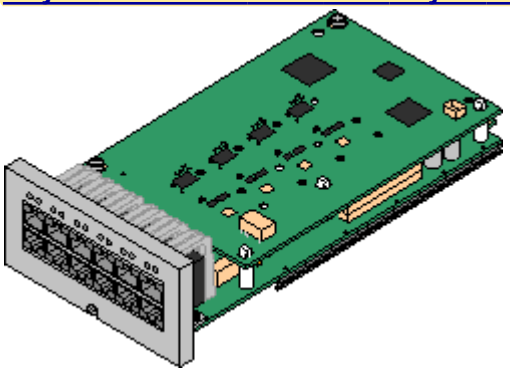
Tarjeta combinada IP500 BRI 216



Esta tarjeta proporciona 6 puertos de estación digital (1-6), 2 puertos de extensión analógica (7-8) y 2 puertos troncales BRI (9-10, 4 canales). La tarjeta también incluye 10 canales de compresión de voz.

- **Máximo:**2 tarjetas combinadas por unidad de control IP500 V2, independientemente del tipo.
  - Las tarjetas combinadas IP500 están preinstaladas con una tarjeta secundaria de troncales que no se puede quitar ni cambiar por otra tarjeta secundaria de troncales de tipo/capacidad.
  - IP Office Basic Edition: los sistemas Norstar Mode e IP Office Basic Edition están limitados a un máximo de 12 canales BRI utilizando una combinación BRI o tarjetas auxiliares de troncales BRI.

Tarjeta combinada IP500 ATM/Tarjeta combinada IP500 ATM V2 214

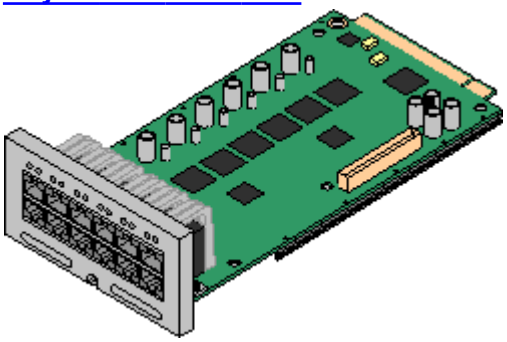


Esta tarjeta proporciona 6 puertos de estación digital (1-6), 2 puertos de extensión analógica (7-8) y 4 puertos de troncal analógica (9-12). La tarjeta también incluye 10 canales de compresión de voz.

- **Máximo:**2 tarjetas combinadas por unidad de control IP500 V2, independientemente del tipo.
  - Las tarjetas combinadas IP500 están preinstaladas con una tarjeta secundaria de troncales que no se puede quitar ni cambiar por otra tarjeta secundaria de troncales de tipo/capacidad.
  - Los puertos de teléfono analógico no incluyen un condensador de llamada. Cuando este sea un requisito, la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
  - Durante un corte de energía, el puerto telefónico 8 se conecta al puerto troncal analógico 12.

Tarjeta base IP500 ETR6

219

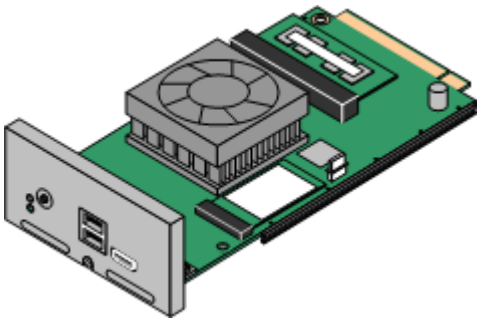


Esta tarjeta solo es compatible con una unidad de control IP500 V2 que se ejecuta en IP Office Basic Edition - Modo PARTNER® o IP Office Basic Edition. Proporciona 6 puertos ETR para la conexión de teléfonos ETR. 2 Los puertos de extensión analógica también se proporcionan para uso de emergencia solo con una tarjeta de troncal analógica.

- La tarjeta se puede equipar con una tarjeta auxiliar de troncales IP500 que utiliza los puertos de la tarjeta base para la conexión de troncales.
- **Máximo:**3 por unidad de control IP500 V2.
- Los puertos de teléfono analógico no incluyen un condensador de llamada. Cuando este sea un requisito, la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
- Si está equipado con una tarjeta secundaria de troncales analógicas IP500, durante un corte de energía, los puertos de teléfono 7 y 8 se conectan al puerto de troncales analógicas 12. Sin embargo, durante el funcionamiento normal, los puertos de teléfonos analógicos 7 y 8 no se pueden utilizar.

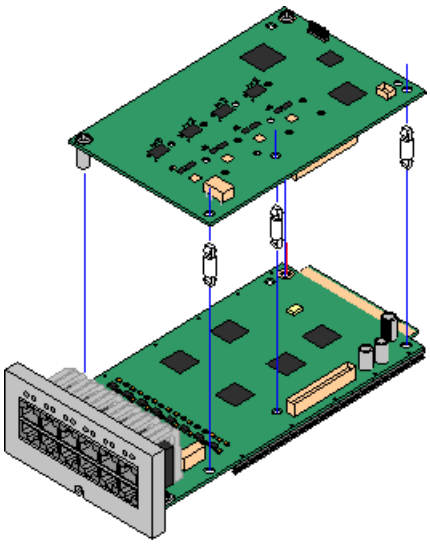
Módulo de comunicaciones unificadas

217



Esta tarjeta actúa como un servidor Linux integrado para las aplicaciones one-X Portal for IP Office y/o Voicemail Pro.

1.11.2 Tarjetas de troncales IP500

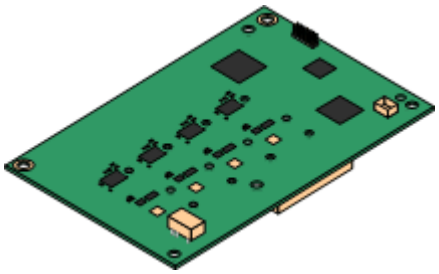


Muchos[Tarjetas base IP500](#) 223 se puede equipar con tarjetas secundarias de troncales IP500 para admitir la conexión de troncales a la tarjeta base.

Cada tarjeta secundaria se suministra con los pilares de separación necesarios para la instalación y una etiqueta para identificar la presencia de las tarjetas secundarias en el frente de la tarjeta base después de la instalación.

- Las tarjetas combinadas IP500 están preinstaladas con una tarjeta secundaria de troncales que no se puede quitar ni cambiar por otro tipo de tarjeta secundaria de troncales.

Tarjeta de troncales analógicas IP500/Tarjeta de troncales analógicas IP500 V2 224

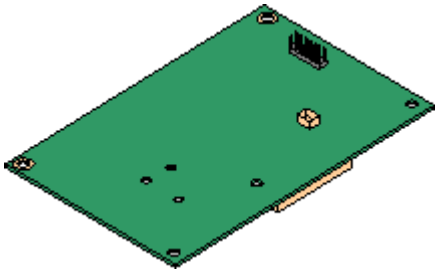


Estas tarjetas permiten que la tarjeta base admita 4 troncales analógicas de inicio en bucle.

  - Los puertos de teléfono analógico no incluyen un condensador de llamada. Cuando este sea un requisito, la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
  - Si la tarjeta base está equipada con puertos telefónicos analógicos, durante un corte de energía, el puerto telefónico 8 se conecta al puerto troncal analógico 12.

- **Máximo:**4 por unidad de control. La tarjeta de troncales analógicas IP500 V2 solo es compatible con IP500 V2.

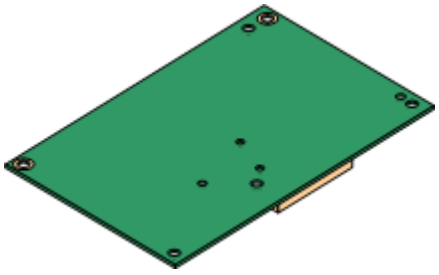
Tarjeta de troncales IP500 PRI-U 227



Esta tarjeta permite que la tarjeta base admita hasta 2 conexiones de troncales PRI. La tarjeta está disponible en variantes de puerto único y doble. La tarjeta se puede configurar para troncales E1 PRI, T1 bit robado, T1 PRI o E1R2 PRI. También está disponible una variante T1(J) para uso en Japón.

- **Máximo:**4 por unidad de control.
- El sistema IP Office admite 8 canales B sin licencia en cada puerto IP500 PRI-U instalado. Se requieren canales B adicionales, hasta la capacidad de los puertos instalados y el modo PRI seleccionado[IP500 Universal PRI (canales adicionales)](#) 280 licencias añadidas a la configuración. Estos canales adicionales consumen las licencias según los canales adicionales configurados como en servicio desde el puerto 9 de la ranura 1 hacia arriba. Los canales D no se ven afectados por las licencias.

Tarjeta de troncales IP500 BRI 226

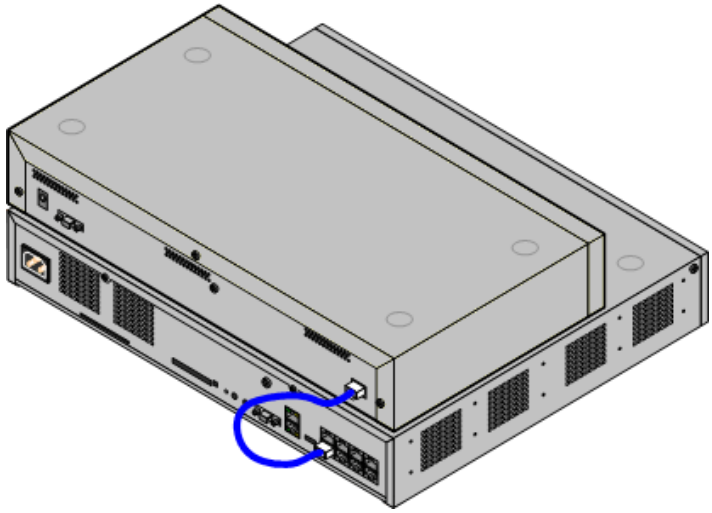


Esta tarjeta permite que la tarjeta base admita hasta 4 conexiones de troncales BRI, cada troncal proporciona 2 canales digitales B+D. La tarjeta está disponible en variantes de 2 puertos (4 canales) y 4 puertos (8 canales).

- **Máximo:**4 por unidad de control.
- **Conexión S-Bus**: La tarjeta se puede cambiar del modo A troncal al modo So. Este modo requiere resistencias de terminación adicionales y una conexión de cable cruzado ISDN, consulte[Puerto BRI (So)](#) 268.
  - IP Office Basic Edition: los sistemas Norstar Mode e IP Office Basic Edition están limitados a un máximo de 12 canales BRI utilizando una combinación BRI o tarjetas auxiliares de troncales BRI.

1.12 Módulos de expansión externos

Estos módulos se pueden usar para agregar puertos adicionales a los sistemas IP Office. El número de módulos de expansión externos admitidos depende del tipo de unidad de control. Cada módulo utiliza un externounidad de fuente de alimentación 30 suministrado con el módulo. Un lugar específicocable de alimentación 31para la fuente de alimentación debe pedirse por separado.



Sistema IP500 con módulo de expansión externo

- Los sistemas que se ejecutan en los modos estándar de IP Office admiten 8 módulos de expansión externos como estándar. Si está equipado con una tarjeta base de expansión de 4 puertos IP500, se admiten hasta 12 módulos de expansión externos.
  - Cada módulo de expansión externo se suministra con un cable de interconexión de expansión azul de 1 metro (3'3''). este cable deber utilizarse cuando se conecta a puertos de expansión en la parte trasera de una unidad de control.
  - Cuando se conecta a puertos de expansión en una tarjeta de expansión de 4 puertos IP500, se puede usar un cable de interconexión de expansión amarillo de 2 metros (6'6") en lugar del cable azul estándar. Se suministran 4 cables amarillos con la tarjeta de expansión de 4 puertos IP500 tarjeta.

- **!Importante: alimentación del módulo de expansión externo**
  Para ser detectados y operados correctamente, los módulos de expansión externos deben iniciarse antes que la unidad de control de IP Office. Normalmente esto se logra conectando todos los módulos de expansión a la misma regleta que la unidad de control. La unidad de control aplica un breve retraso a su propio proceso de inicio para garantizar que los módulos de expansión se encienden al mismo tiempo que se detectan.

Módulos de expansión externos IP500

Los módulos de expansión incluyen una fuente de alimentación externa (PSU) y un cable de interconexión azul de 1 m. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

Variante	País	Código SAP
Teléfonos digitales (no IP)		
Estación digital IPO 500 16 231	Todos	700449499
Estación digital IPO 500 30 231	Todos	700426216
Estación digital IPO 500 16A (RJ21) 233	Todos	700500699
Estación digital IPO 500 30A (RJ21) 236	Todos	700500698
Estación digital IPO 500 16B 236	Todos	700501585
Estación digital IPO 500 30B 236	Todos	700501586
Teléfonos analógicos		
Teléfono IPO 500 16 238	Todos	700449507
IPO 500 Teléfono 30 238	Todos	700426224
Otros		
Troncal analógica IPO 500 16 229	A NOSOTROS	700449473

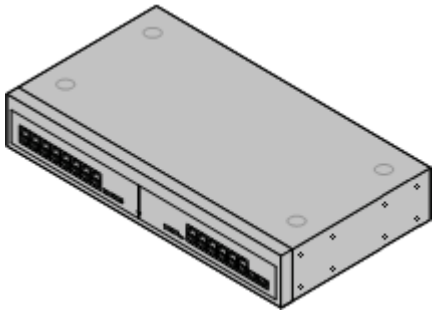
1.12.1 Módulos de expansión externos IP500

Los siguientes módulos de expansión externos IP500 son compatibles con la versión 11.0 de IP Office. Cada módulo utiliza un externo unidad de fuente de alimentación 30 suministrado con el módulo. Un lugar específicocable de alimentación 31para la fuente de alimentación debe pedirse por separado.

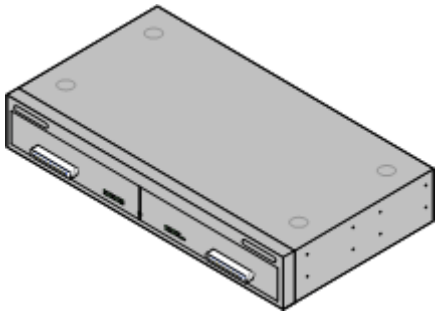
El módulo externo se puede apilar encima de la unidad de control. También se pueden montar en la pared o en un bastidor utilizando uno de losJuegos de montaje de IP Office 247.

- Los sistemas que se ejecutan en los modos estándar de IP Office admiten 8 módulos de expansión externos como estándar. Si está equipado con una tarjeta base de expansión de 4 puertos IP500, se admiten hasta 12 módulos de expansión externos.

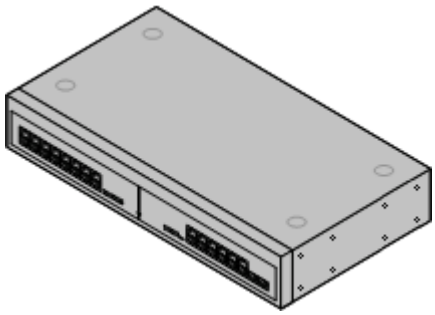
- **Módulos de estación digital IP500** 231
  Proporciona, según la variante, 16 o 30 RJ45 adicionalesSD soportado 271puertos para Teléfonos digitales Avaya DS 39.



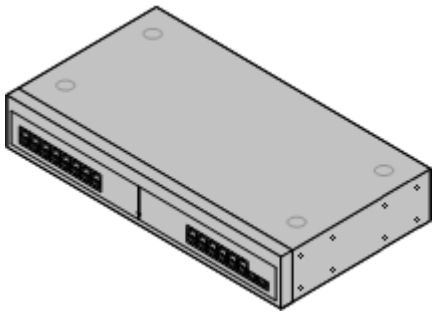
- **Módulos de estación digital A IP500** 233
  Proporciona, según variante, puertos RJ21 para la conexión de 16 o 30 adicionalesTeléfonos digitales Avaya BST 39.Solo compatible con IP500 V2.



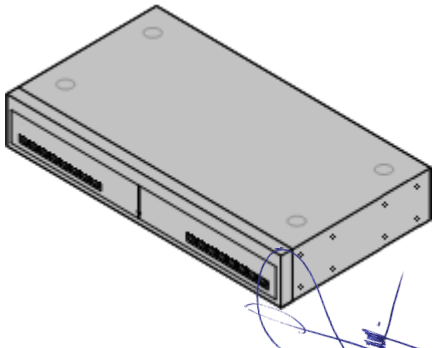
- **Módulos B/B2 de estación digital IP500** 236
  Proporciona, según la variante, 16 o 30 puertos RJ45 adicionales. Estos se pueden utilizar comoSD 271puertos para compatiblesTeléfonos digitales Avaya DS 39o BST 270puertos para compatiblesTeléfonos digitales Avaya BST 39.Sin embargo, el módulo solo puede admitir un tipo de puerto en cualquier momento. Para la versión 10.1 de IP Office, los módulos DS16B/DS30B fueron reemplazados por los modelos DS16B2/DS30B2.



- **Módulos telefónicos IP500** 238
  Proporciona, según la variante, 16 o 30 adicionalesTELÉFONO Conexión 276puertos para de teléfonos analógicos.



- **Módulo troncal analógico IP500** 229
  Proporciona 16 adicionalesCOSA ANÁLOGA 267Puertos para conexión de troncales analógicas. Admite troncales de inicio en bucle y de inicio en tierra.
  - El uso con troncales de inicio desde tierra requiere que el módulo de troncales y la unidad de control de IP Office estén conectados a tierra.
  - En IP Office Basic Edition - Modo PARTNER®, IP Office Basic Edition - Modo Norstar e IP Office Basic Editions, solo se admite 1 módulo de troncal analógica.

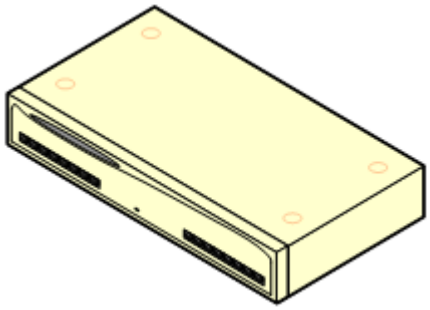


1.12.2 Módulos de expansión externos IP400

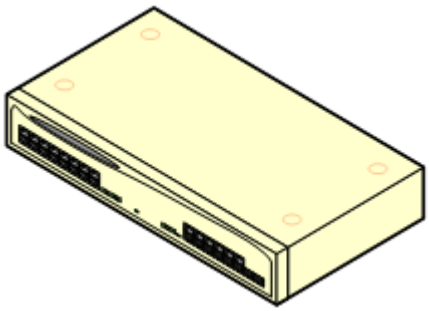
Los siguientes módulos de expansión externos IP400 son compatibles con la versión 11.0 de IP Office y se pueden usar con unidades de control IP500 V2. Cada módulo utiliza un externounidad de fuente de alimentación 30suministrado con el módulo. Un lugar específicocable de alimentación 31para la fuente de alimentación debe pedirse por separado.

Si se van a montar en bastidor, estas unidades utilizan el kit de montaje en bastidor IP400. Si se montan en rack, estas unidades utilizan el KIT DE MONTAJE EN RACK IPO IP500. No se pueden montar en la pared.

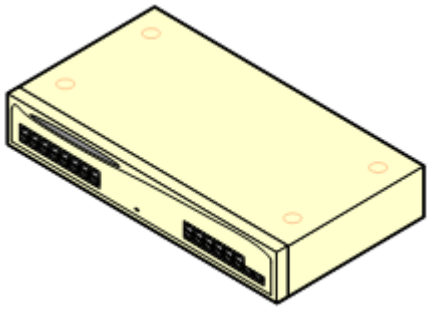
- **Módulo troncal analógico IP400 (ATM16)** 241
  Proporciona 16 adicionalesCOSA ANÁLOGA 267Puertos para conexión de troncales analógicas. Admite troncales de inicio en bucle y de inicio en tierra.
  - Disponible en una serie de variantes para diferentes lugares.
  - El uso con troncales de inicio desde tierra requiere que el módulo de troncales y la unidad de control de IP Office estén conectados a tierra.



- **Módulo de estación digital IP400 V2** 243
  Proporciona, según la variante, 16 o 30 adicionalesSD 271puertos para soportadoTeléfonos digitales Avaya 39.Reemplaza el módulo de Estación Digital anterior.



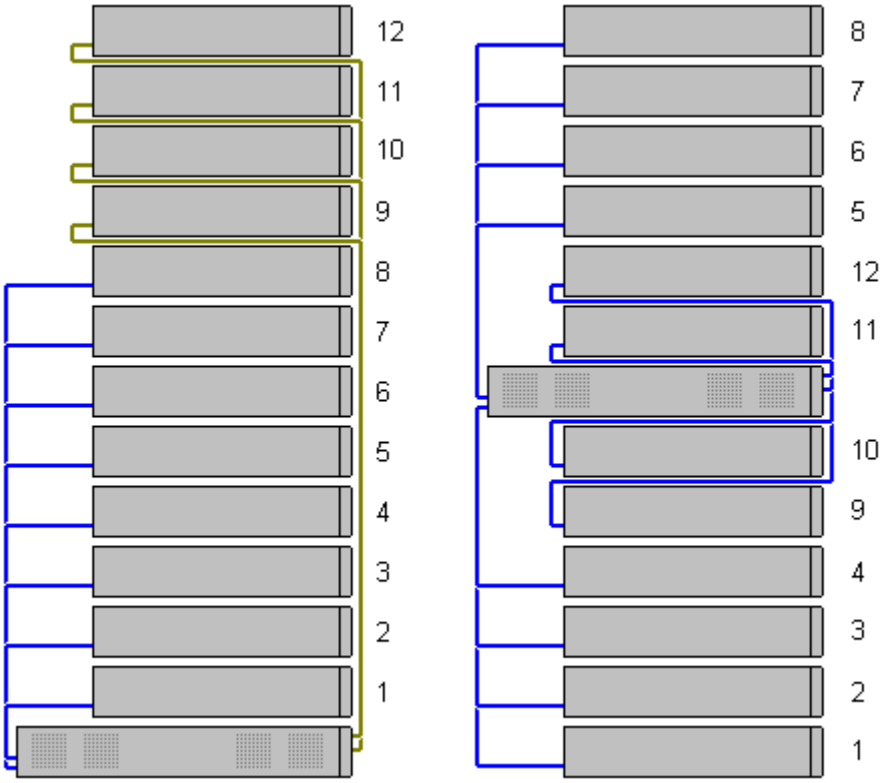
- **Módulo telefónico IP400 V2** 245
  Proporciona, según la variante, 16 o 30 adicionalesTELÉFONO 276puertos para teléfonos analógicos. Reemplaza el módulo Teléfono anterior. Con IP Office 3.1, Phone V2 admite una gama más amplia de opciones de indicación de mensaje en espera (MWI) que los módulos Phone V1.



1.12.3 Conexión de módulos de expansión externos

Los puertos de expansión integrales en una unidad de control están ubicados en la parte posterior de la unidad. Se pueden agregar 4 puertos de expansión adicionales al frente de la unidad de control instalando una tarjeta de expansión de 4 puertos IP500.

- Cada módulo de expansión externo se suministra con un cable de interconexión de expansión azul de 1 metro (3'3"). este cable deber utilizarse cuando se conecta a puertos de expansión en la parte trasera de una unidad de control.
- Cuando se conecta a puertos de expansión en una tarjeta de expansión de 4 puertos IP500, se puede usar un cable de interconexión de expansión amarillo de 2 metros (6'6") en lugar del cable azul estándar. Se suministran 4 cables amarillos con la tarjeta de expansión de 4 puertos IP500 tarjeta.



1.13 Fuentes de alimentación y cables

Todas las unidades de control de IP Office y los módulos de expansión externos tienen una fuente de alimentación interna o se suministran con una fuente de alimentación externa.

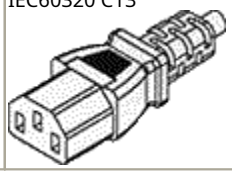
1.13.1 Fuentes de alimentación

Las unidades de control IP500 V2 tienen una fuente de alimentación interna y, por lo tanto, solo requieren una fuente de alimentación adecuada.cable de alimentación específico del lugar 31y una toma de corriente que incluye un interruptor. Tenga en cuenta que si el cable de alimentación incluye un cable de tierra, la toma de corriente debe estar conectada a una tierra de protección.

Todos los módulos de expansión externos se suministran con una unidad de fuente de alimentación (PSU) externa. Estas fuentes de alimentación incluyen un cable integral de 1,5 metros para la conexión a la unidad de control o al módulo de expansión. Acable de alimentación 31para la conexión de la fuente de alimentación a la toma de corriente no está incluida, ya que esto varía según el lugar. El cable de alimentación adecuado debe pedirse por separado o adquirirse localmente.

- **!Importante: alimentación del módulo de expansión externo**
  Para ser detectados y operados correctamente, los módulos de expansión externos deben iniciarse antes que la unidad de control de IP Office. Normalmente esto se logra conectando todos los módulos de expansión a la misma regleta que la unidad de control. La unidad de control aplica un breve retraso a su propio proceso de inicio para garantizar que los módulos de expansión se encienden al mismo tiempo que se detectan.

Se requieren unidades de fuente de alimentación adicionales para los módulos de botones del teléfono y también se pueden requerir para los teléfonos IP de Avaya.

Área	Escribe	Usado en:	tipo de conector
Control de IP Office Unidades y Externo Expansión Módulos	**60W conectado a tierra** fuente de alimentación	Módulo troncal analógico, teléfono IP500 30, estación digital IP500 30, estación digital IP500 16A, estación digital IP500 30A.	IEC60320 C13 

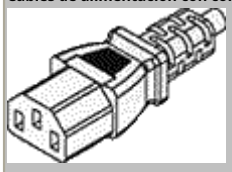
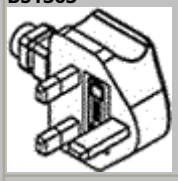
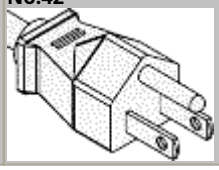
- Los teléfonos IP de Avaya pueden usar fuentes de alimentación IEEE 802.3af Power over Ethernet (PoE). Consulte el Manual de instalación del teléfono IP de IP Office para obtener detalles completos.

1.13.2 Cables de alimentación

Cada unidad de control y módulo de expansión requiere una toma de corriente conmutada de 110-240 V CA, 50-60 Hz. La conexión desde esa toma de corriente requiere un cable de alimentación específico para el lugar que no se suministra con la unidad y se debe pedir por separado. Tenga en cuenta que si el cable de alimentación incluye un cable de tierra, la toma de corriente debe estar conectada a una tierra de protección.

Los cables de alimentación no deben fijarse a la superficie del edificio ni atravesar paredes, techos, suelos ni aberturas similares. Se deben tomar medidas de instalación para evitar daños físicos al cable de alimentación, incluido el enrutamiento adecuado del cable de alimentación y la provisión de una toma de corriente cerca del equipo fijo o la ubicación del equipo cerca de una toma de corriente.

Para los lugares que no se detallan a continuación, se debe obtener localmente un cable de alimentación adecuado.

Tipo de cable de alimentación	Tipo de enchufe de toma de corriente	locales	Códigos SAP
Cables de alimentación con conexión a tierra (IEC60320 C13) 	**CEE7/7 (Schuko)**	Europa y Sudáfrica.	700289762
	BS1363 	República Checa, Irlanda, Unidos Reino.	700289747
	NEMA5-15P/CS22.2 No.42 	Norte central y sur America.	700289770

1.13.3 Respaldo de fuente de alimentación

Se recomienda encarecidamente el uso de una fuente de alimentación ininterrumpida (UPS) con cualquier sistema telefónico. Incluso en sitios que rara vez pierden energía eléctrica, es posible que esa energía deba desconectarse ocasionalmente para el mantenimiento de otros equipos. Además, la mayoría de los UPS también brindan un elemento de acondicionamiento de energía, lo que reduce los picos y sobretensiones.

La capacidad de los sistemas UPS y la carga total del equipo que se espera que admita el UPS generalmente se cotizan en VA. Cuando la carga del equipo se indique en vatios, multiplíquela por 1,4 para obtener la carga de VA.

El cálculo de cuánta capacidad de UPS se requiere depende de varias opciones.

- **¿Qué equipo colocar en el SAI?**
  Recuerde incluir las PC del servidor, como el correo de voz. Se recomienda que la carga total en un UPS nuevo nunca supere el 75 % de la capacidad, lo que permitirá el uso de equipos futuros.
- **¿Cuántos minutos de soporte de UPS se requieren?**
  El tiempo de ejecución real del UPS es variable, depende del porcentaje de la capacidad del UPS que representa la carga total del equipo. Por ejemplo, un SAI con una capacidad de 1000 VA solo puede soportar una carga de 1000 VA (100 %) durante 5 minutos. Esta relación no es lineal, un mismo SAI puede soportar una carga de 500VA (50%) durante 16 minutos. Por lo tanto, cuanto menor sea el porcentaje de capacidad máxima utilizada, mayor será el tiempo de funcionamiento del SAI, por ejemplo, hasta 8 horas.
- **¿Qué tan frecuentes son las pérdidas de energía?**
  También debe incluir la asignación para el tiempo de recarga de UPS. Para la mayoría de los UPS, la relación entre el tiempo de descarga y el tiempo de recarga total es de 1:10.
- **¿Cuántas tomas de salida proporciona el SAI?**
  Es posible que se requieran varias unidades de UPS para garantizar que cada elemento del equipo compatible tenga su propio enchufe de alimentación.

Valores de ejemplo

El factor dominante en el consumo de energía de un sistema IP Office son los teléfonos conectados a la unidad de control y cualquier módulo de expansión externo. Esto no incluye los teléfonos IP que requieren sus propias fuentes de alimentación separadas. Si el sistema utiliza alguna PC de servidor, los requisitos de esas PC también deben incluirse en la evaluación. De manera similar, se debe considerar el soporte para sistemas adjuntos como DECT.

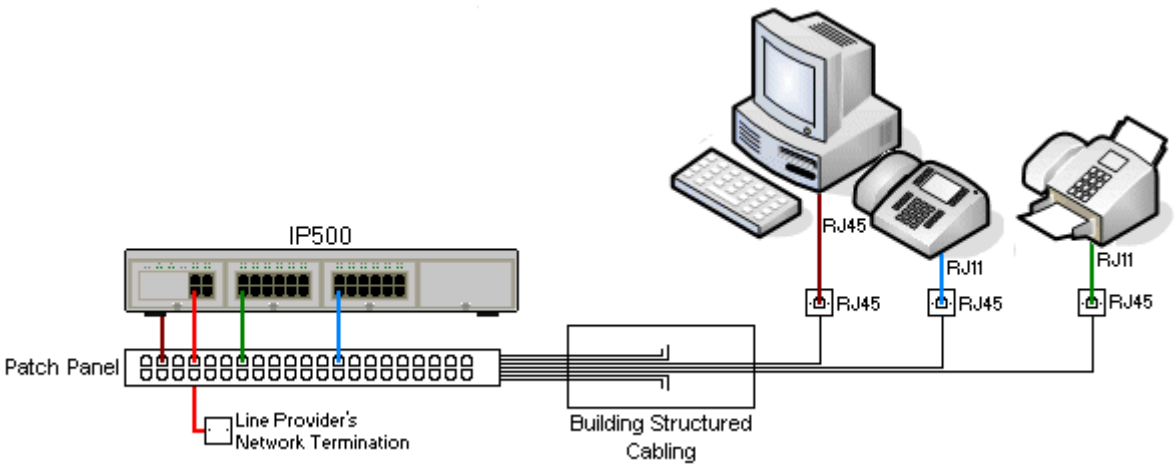
Las siguientes son las cifras del peor de los casos probadas que se encuentran utilizando unidades de control completamente equipadas y módulos de expansión externos:

- **Unidad de control IP500 V2:**115W.
- **Estación digital IP500 16 Módulo de expansión externo:**31W.
- **Módulo de expansión externo IP500 Digital Station 30:**56W.
- **Estación digital IP500 DS16A Módulo de expansión externo RJ21:**34W.
- **Estación digital IP500 DS30A Módulo de expansión externo RJ21:**60W.
- **Teléfono IP500 16 Módulo de expansión externo:**25W.
- **Módulo de expansión externo IP500 Phone 30:**45W.
- **Módulo troncal analógico IP500 16 Módulo de expansión externo:**8.8W.

1.13.4 Cableado y cables

Los sistemas IP Office están diseñados principalmente para su uso dentro de un sistema de cableado estructurado RJ45 que utiliza cableado de par trenzado sin blindaje (UTP) CAT3 y enchufes RJ45.

Un sistema de cableado estructurado es aquel en el que los cables van desde un panel de conexión central RJ45 en la sala de comunicaciones/datos hasta los enchufes RJ45 individuales en las ubicaciones de los usuarios. Todos los hilos de cada cable entre el panel de conexión y el enchufe del escritorio están conectados directamente. Esta disposición permite que los dispositivos conectados en el panel de conexiones se intercambien para que coincidan con el tipo de dispositivo que debe conectarse en el enchufe del usuario. Por ejemplo, convertir un enchufe de usuario en un puerto de teléfono y otro enchufe de usuario en un puerto LAN de computadora, sin necesidad de volver a cablear los cables entre el panel de conexión y la ubicación del usuario.



- **Instalaciones tradicionales de cableado IDC Punchdown**
  Cuando sea necesario, el conector RJ45 del extremo remoto puede quitarse de los cables de IP Office y conectarse a los sistemas de cableado tradicionales mediante conectores de bloque perforado. Este tipo de instalación debe ser realizada por un técnico de cableado con experiencia.

- **Conexiones troncales**
  La mayoría de los puertos troncales de IP Office utilizan conectores RJ45 para aceptar un cable RJ45 a RJ45. Sin embargo, la conexión en el extremo del proveedor de la línea puede requerir el uso de un tipo de enchufe diferente para que coincida con el equipo del proveedor de la línea.

- **Conectores telefónicos RJ11**
  Muchos teléfonos utilizan enchufes RJ11 y se suministran con cables RJ11 a RJ11. Los enchufes RJ11 se pueden insertar en los enchufes RJ45 y, en muchos casos, la conexión funcionará. Sin embargo, esto no se recomienda ni se admite, ya que el bloqueo de la conexión no es realmente positivo y puede desconectarse. UnCable RJ45 a RJ11 [271]está disponible para estas conexiones.

Cables IP Office estándar

Los siguientes son cables estándar de Avaya disponibles para usar con los sistemas IP Office. La longitud máxima se aplica si el cable estándar de Avaya se reemplaza por un cable alternativo.

Cable	Descripción	Código SAP	Estándar Longitud	Máximo Longitud
Cable DTE de 9 vías 278	Se conecta al puerto RS232 DTE de la unidad de control. Enchufe tipo D de 9 vías a enchufe tipo D de 9 vías.	–	2m/6'6''.	2m/6'6''.
Cableado estructurado Cable de línea DS 271	Se conecta desde enchufes RJ45 a teléfonos analógicos y DS con enchufe RJ11.	TT700047871	4m/13'2''.	Ver tabla abajo.
Cable troncal BRI/PRI 269	Conecta los puertos troncales BRI/PRI al punto de terminación de red del proveedor de línea. RJ45 a RJ45. Rojo.	700213440	3m/9'10''.	–
Interconexión de expansión Cable 273	Conecta la unidad de control a los módulos de expansión. RJ45 a RJ45. Azul. Se puede reemplazar por un cable de interconexión amarillo (2 m (6'6") - 700472871) suministrado con elExpansión de 4 puertos IP500 212tarjeta al usar esa tarjeta.	700213457	1m/3'3''.	1m/3'3''.
Cable de LAN 274	Se conecta desde puertos LAN de IP Office a dispositivos IP. RJ45 a RJ45. Gris.	700213481	3m/9'10''.	100m/328'.

La siguiente tabla detalla las distancias totales máximas de cable para DS y extensiones analógicas que utilizan diferentes grosores de cable. El cableado debe ser un cable de par trenzado sin blindaje de categoría 1 o superior.

Teléfono	Par trenzado sin blindaje (UTP) - 50nf/Km		
	AWG22 (0,65 mm)	AWG24 (0,5 mm)	AWG26 (0,4 mm)
Serie 1400	1200m/3937'	1000m/3280'.	670m/2200'
Serie 9500	1200m/3937'	1000m/3280'	670m/2200'
BST	580m/1900'	365m/1200'	228m/750'
Teléfonos analógicos	1000m/3280'	1000m/ 3280'	400m/1312'
Teléfonos ETR	305m/1000'	305m/1000'	122m/400'

1.13.5 Puesta a tierra

Todas las unidades de control de IP Office y módulos de expansión externosdebe estar conectado a una tierra funcional . Cuando la unidad esté conectada a una toma de corriente mediante un cable de alimentación con conductor de tierra, la toma de corriente debe estar conectada a una toma de tierra de protección.

El uso de conexiones a tierra reduce la probabilidad de problemas en la mayoría de los sistemas de telefonía y datos. Esto es especialmente importante en edificios en los que se interconectan varios elementos de equipo mediante cables largos, por ejemplo, redes telefónicas y de datos.

En algunos casos, como las troncales de puesta en tierra, además de ser una medida de protección, es un requisito funcional para el funcionamiento del equipo. En otros casos, puede ser un requisito normativo local o un paso de protección necesario, por ejemplo, áreas de alto riesgo de rayos.

- **ADVERTENCIA**
  Durante la instalación, no asuma que los puntos de tierra están correctamente conectados a tierra. Pruebe los puntos de tierra antes de confiar en ellos para conectar a tierra el equipo.

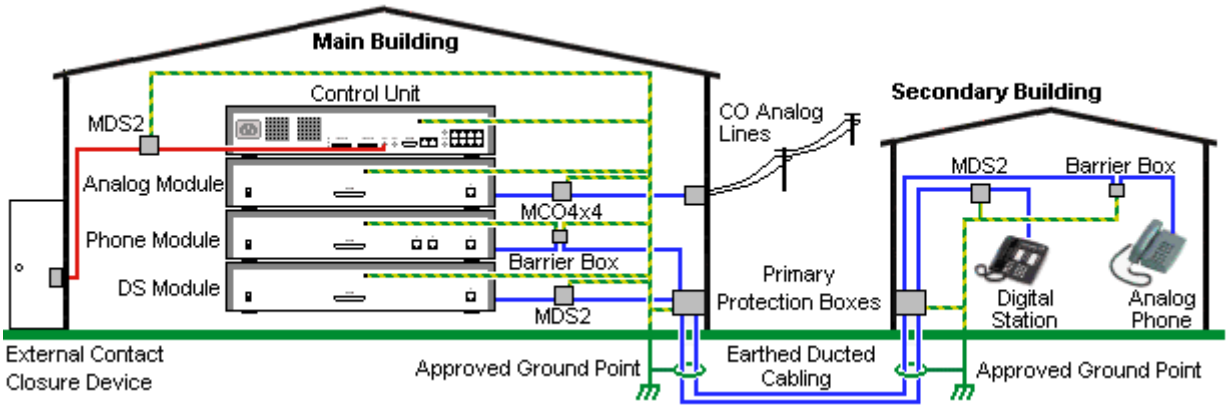
El punto de conexión a tierra en las unidades de control de IP Office y los módulos de expansión externos están marcados con un o símbolo. Terrestre las conexiones a estos puntos deben usar un cable sólido de 14 AWG con un manguito verde para una conexión a tierra funcional o un manguito verde y amarillo para una conexión a tierra protectora.

- **Equipo de protección adicional**
  Además de la conexión a tierra, se requerirá equipo de protección adicional en las siguientes situaciones. Referirse a "Instalaciones Telefónicas Fuera de Edificio 36".
  - En cualquier módulo de expansión externo Digital Station o Phones conectado a una extensión ubicada en otro edificio.
  - En la República de Sudáfrica, en todos los módulos de expansión externos de troncales analógicas (ATM16) y en cualquier unidad de control que contenga tarjetas de troncales analógicas (ATM4/ATM4U).

1.13.6 Protección contra rayos/Conexiones fuera del edificio

Los siguientes son los únicos escenarios admitidos en los que las extensiones y los dispositivos cableados fuera del edificio principal se pueden conectar al sistema IP Office. En estos escenarios, se debe instalar protección adicional, en forma de puesta a tierra protectora y protectores contra sobretensiones.

- **ADVERTENCIA**
  La instalación de protección adicional no elimina el riesgo de daños. Simplemente reduce las posibilidades de daño.



- Solo se admiten puertos en módulos de expansión externos de IP Office. No se admite la conexión fuera del edificio a puertos en tarjetas base en la unidad de control.
- Los cables de diferentes tipos, por ejemplo, líneas troncales, extensiones telefónicas, conexiones a tierra y de alimentación, deben mantenerse separados.
- Todo el cableado entre edificios debe estar encerrado en conductos conectados a tierra. Idealmente, este conducto debe estar enterrado.
- Se debe prever una Caja de Protección Primaria en el punto de entrada de los cables al edificio. Esta debe ser una protección de tres puntos (punta, anillo y tierra). Por lo general, esta sería la protección del tubo de gas proporcionada por la compañía telefónica local. El cable de tierra debe ser lo suficientemente grueso para manejar todas las líneas afectadas por un golpe indirecto al mismo tiempo.

Tipo de conección	Tipo de dispositivo de protección	Requisito
Extensiones de teléfonos analógicos Teléfonos Módulo de expansión externo (MACETA 276 o TELÉFONO 276 puertos solamente.	**Caja de barrera de IP Office** 189 Admite una sola conexión. Máximo de 16 en cualquier módulo de expansión.	· La conexión del módulo de expansión al teléfono debe realizarse mediante un protector contra sobretensiones en cada extremo y mediante el punto de protección principal de cada edificio. · Los módulos de expansión externos, la unidad de control y los dispositivos IROB de IP Office deben estar conectados al punto de conexión a tierra de protección en su edificio. · La conexión entre edificios debe realizarse a través de conductos puestos a tierra, preferiblemente subterráneos. El cable no debe quedar expuesto al exterior en ningún punto.
Extensiones de teléfono DS	**ITW Linx MDS2** 188 Admite hasta 4 conexiones. Este dispositivo se conocía anteriormente como Avaya 146E.	
Extensiones de teléfono BST	Ninguna	Actualmente no es compatible.
Troncales analógicos	**ITW Linx MCO4x4** 188 Admite hasta 4 líneas de dos hilos. Este dispositivo se conocía anteriormente como Avaya 146C.	Para instalaciones en la República de Sudáfrica, la instalación de protección contra sobretensiones en troncales analógicas es un requisito. Para otras ubicaciones donde se considera que el riesgo de caída de rayos es alto, se recomienda una protección adicional de las troncales analógicas entrantes.
Interruptor de salida externa	**ITW Linx MDS2** 188 Admite hasta 4 conexiones. Este dispositivo se conocía anteriormente como Avaya 146E.	Las conexiones desde un puerto IP Office Ext O/P a un dispositivo de retransmisión externo deben realizarse a través de un protector contra sobretensiones. Cuando use el MDS2 en el puerto Ext O/P, use solo las tomas de Línea 1 y Equipo 1, no use las tomas de Línea 2 o Equipo 2.

La gama de dispositivos towerMAX es suministrada por ITWLinx (http://www.itwlinx.com).

1.14 Montaje en pared y bastidor

Todas las unidades de control de IP Office están diseñadas para ser independientes. En los sistemas con módulos de expansión externos, la unidad de control y los módulos están diseñados para apilarse.

Con kits de montaje opcionales adicionales, algunos sistemas pueden montarse en la pared o en un bastidor.

Unidad de control/expansión	Montaje en pared	Estante Montar
Unidad de control IP500 V2	✓	✓
Módulos de expansión externos IP500	✓	✓

1.14.1 Juegos de montaje en pared

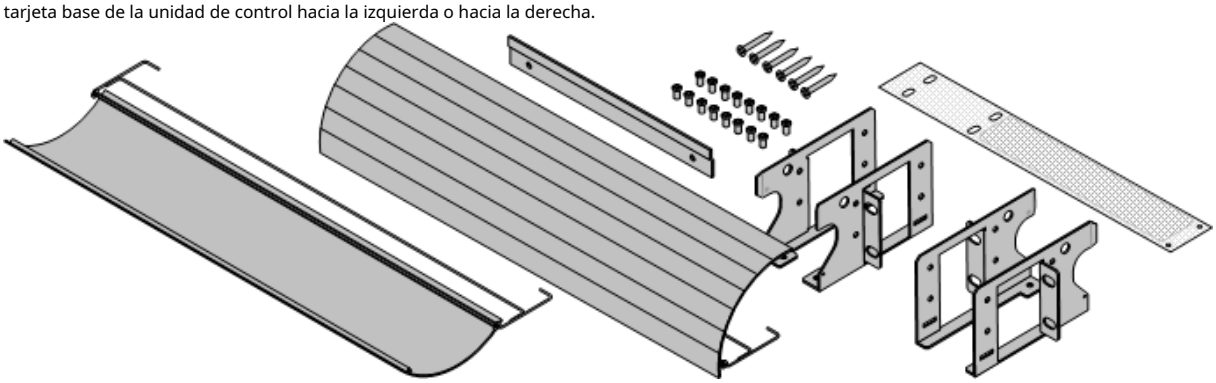
Las unidades de control IP500 V2 y los módulos de expansión externos IP500 pueden montarse en la pared o en un bastidor. Para hacer esto, se requiere un kit de montaje en pared además de las fijaciones de pared adecuadas.

Además de los existentes Requisitos medioambientales 51 para un sistema IP Office, se aplican los siguientes requisitos adicionales al montar una unidad en la pared:

- La superficie de la pared debe ser vertical, plana y libre de vibraciones. No se admite la unión a paredes temporales.
- Solo deben usarse los tornillos proporcionados con el kit de montaje para fijar los soportes a la unidad de control oa los módulos de expansión.
- La instalación debe ser realizada por una persona de servicio.
- Asegúrese de que el sistema se haya apagado y que se haya desconectado la alimentación de todas las unidades. Apague el sistema usando un comando de apagado y luego desconecte la alimentación. No quite simplemente la energía.
- Se requiere una superficie de montaje de madera contrachapada adecuada de al menos 1 m x 1 m x 19 mm (39" x 39" x 0,75"). Si también se va a montar una caja de expansión, se requiere una superficie de montaje de madera contrachapada de al menos 1,2 mx 1,2 mx 19 mm (48" x 48" x 0,75").
- Se debe usar un mínimo de 6 tornillos de cabeza plana de 45 mm de largo y 5 mm/6 mm (1,75" n.° 10/n.° 12) para asegurar la madera contrachapada a los montantes de la pared.
- Se deben usar los tornillos para madera de 20 mm de largo y 4 mm (#8 ¾") para asegurar los soportes a la superficie de montaje de madera contrachapada

El siguiente kit está disponible actualmente:

- **KIT DE MONTAJE EN PARED IPO IP500 V3***(Código SAP 700503160)*
  Este kit se puede utilizar para montaje en pared y en rack de unidades de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora enrutamiento de cables en la parte delantera y trasera de la unidad. Para unidades de control montadas en la pared, permite orientar las ranuras de la tarjeta base de la unidad de control hacia la izquierda o hacia la derecha.

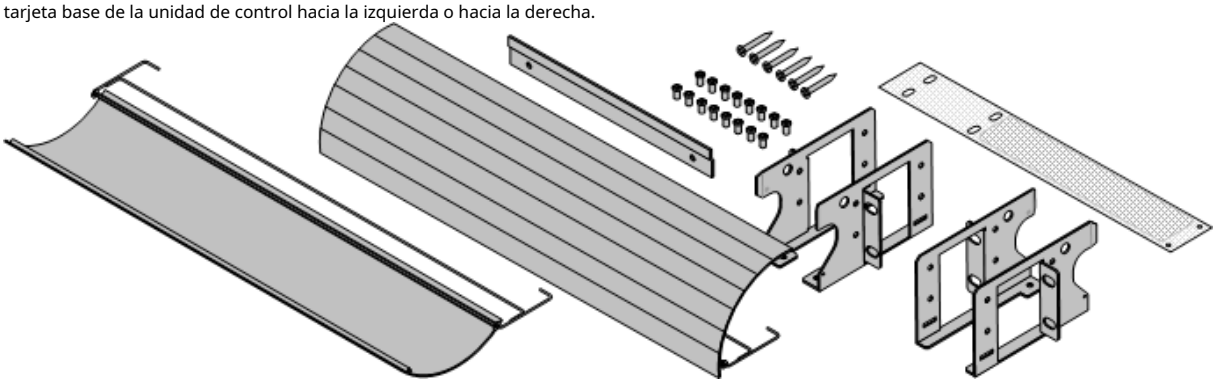


1.14.2 Juegos de montaje en bastidor

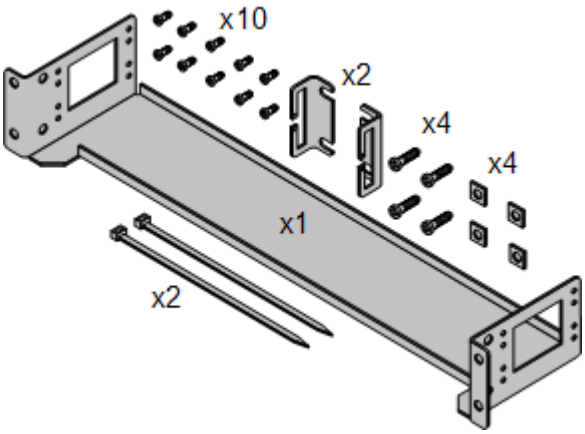
Todas las unidades de control de IP Office y los módulos de expansión externos se pueden montar en rack en sistemas de rack estándar de 19". Cada unidad requiere un espacio de ranura de 2U dentro del rack. El montaje en rack requiere un kit para cada unidad de control y módulo de expansión externo.

Cuando los sistemas se monten en rack, se debe considerar el efecto de las condiciones dentro del gabinete del rack. Por ejemplo, la temperatura del estante puede estar por encima de la temperatura ambiente y el flujo de aire dentro del estante está restringido. losRequisitos medioambientales 51 para las unidades individuales de IP Office siguen siendo aplicables dentro del gabinete del bastidor.

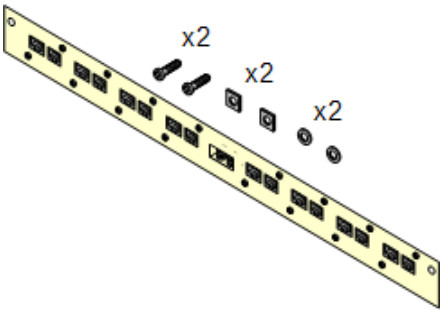
- **KIT DE MONTAJE EN PARED IPO IP500 V3***(Código SAP 700503160)*
  Este kit se puede utilizar paramontaje en pared y en rack de unidades de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora enrutamiento de cables en la parte delantera y trasera de la unidad. Para unidades de control montadas en la pared, permite orientar las ranuras de la tarjeta base de la unidad de control hacia la izquierda o hacia la derecha.



- **KIT DE MONTAJE DE RACK IPO IP500***(Código SAP 700429202)*
  Este kit contiene todos los componentes necesarios para el montaje en rack de una sola unidad de control IP500 V2 o módulo de expansión externo IP500. Esto incluye tornillos para la fijación de los soportes al módulo, pernos para asegurar el módulo en el rack y soportes pasacables.



Kit de montaje en bastidor de caja de barrera



- **Kit de montaje en bastidor de caja de barrera***(SAP 700293905)* Las cajas de barrera se deben utilizar paraextensiones telefónicas analógicas fuera del edificio 36.Este soporte permite montar en rack hasta 8 cajas de barrera de IP Office y simplifica la cantidad de conexiones al punto de protección a tierra en el rack. Este kit debe usarse cuando se usan más de 3 cajas de barrera y admite un máximo de 16 cajas de barrera para un solo módulo de expansión externo.

1.15 Teléfonos IP Office

La versión 11.0 de IP Office es compatible con los siguientes teléfonos y complementos de teléfono. La disponibilidad puede depender de la ubicación y puede estar sujeta a restricciones locales. Para soporte telefónico histórico, consulteCompatibilidad de hardware/software 290.

Punta y anillo mejorados (puertos ETR)

Estos teléfonos solo son compatibles con una tarjeta ETR6 en sistemas IP500 V2. Solo se admiten en los sistemas IP Office Basic Edition - PARTNER® Mode e IP Office Basic Edition que ejecutan una configuración regional de América del Norte y U-Law.

- **Serie ETR:**ETR6, ETR6D, ETR18, ETR18D, ETR34D*(Los teléfonos ETR 34D están limitados a un máximo de 2 por tarjeta y 4 en total)*

Teléfonos digitales Avaya DS (puertos DS)

Estas estaciones digitales se conectan a IP Office a través deSD 271puertos Son compatibles con todos los modos de IP Office.

- **Serie 1400:**1403, 1408, 1416
- **Serie 9500:**9504, 9508

Los siguientes teléfonos con puerto DS adicionales solo se admiten en los modos estándar de IP Office:

- **Serie 2400:**2402, 2410, 2420.

Teléfonos digitales BST de Avaya (puertos BST)

Estas estaciones digitales se conectan al sistema IP Office IP500 V2 a través de puertos BST.

- **Serie 4100:**4135, 4136, 4145, 4145EX, 4146, 4146EX: conexión a puertos IP Office BST a través de un sistema Digital Mobility Solution.
- **Serie 7400:**7420, 7430, 7434, 7439, 7440, 7444, 7449: conexión a los puertos BST de IP Office a través de un sistema Digital Mobility Solution.
- **UCA:**Unidad de audioconferencia
- **Serie M:**M7100, M7100N, M7208, M7208N, M7310, M7310N, M7324, M7324N.
- **Serie T:**T7000, T7100, T7208, T7316, T7316E, T7406, T7406E

Teléfonos Analógicos

Los teléfonos y dispositivos analógicos se conectan aTELÉFONO 276puertos con el sistema IP Office. Sin embargo, debido a la variedad de analógicos teléfonos y dispositivos disponibles no se da garantía de funcionamiento. Es responsabilidad del instalador y del mantenimiento de IP Office probar y verificar el funcionamiento del equipo analógico propuesto.

- **Serie 6200:**6211, 6219, 6221*(América del norte)*.
- **Serie B100:**B149, B159, B169*.
- **Intercuarzo Géminis:**9330-AV, 9335-AV, 9281-AV*(Europa, Oriente Medio, África, Asia-Pacífico)*.

Teléfonos IP

Los teléfonos IP (SIP y H323) se conectan al sistema IP Office a través de la LAN o WAN RJ45. Estos dispositivos requieren una licencia de Avaya IP Endpoint y recursos de compresión de voz.

H323:

- **Serie 1600:**1603IP/SW, 1608, 1608-I, 1616, 1616-I
- **Serie 3600:**3641, 3645
- **Serie 3700:**3701, 3711 - Conexión a través de estaciones base DECT. 3720, 3725, 3730, 3735, 3740, 3745, 3749 - Conexión a través de estaciones base DECT R4.
- **Serie 9600:**9608, 9608G, 9611G, 9620L, 9620C, 9621G, 9630G, 9640, 9640G, 9641G, 9641GS, 9650, 9650C.

SORBO:

- **Serie 1000:**1010, 1040
- **Serie 1100:**1120E, 1140E
- **Serie 1200:**1220, 1230
- **Serie B100:**B169*, B179, B199.
- **Serie D100:**Estos teléfonos DECT (hasta 8) utilizan una estación base que se conecta al sistema IP Office mediante una troncal SIP y aparecen en IP Office como extensiones SIP.
- **E129:**Un teléfono SIP simple, el E129 admite la operación de respuesta automática, manos libres y auriculares.
- **H175:**Videoteléfono SIP.
- **H200:**H229, H239, H249.
- **Serie J100:**J129, J139, J159, J169, J179.
- **Serie K100:**K155*, K165, K175.

* El B169 es un teléfono DECT que se conecta a una estación base DECT. La estación base se conecta a IP Office. Existen estaciones base analógicas y SIP.

1.16 VoIP

IP Office es un sistema de telefonía convergente, es decir, combina aspectos de los sistemas telefónicos PABX tradicionales y los sistemas de telefonía y datos IP. Esto funciona en varios niveles.

- Los usuarios de teléfonos individuales pueden controlar el funcionamiento de su teléfono a través de aplicaciones que se ejecutan en su PC.
- El tráfico de datos se puede enrutar desde la interfaz LAN a una interfaz troncal de telefonía, por ejemplo, una conexión ISP de acceso telefónico.
- El tráfico de voz se puede enrutar a través de enlaces de datos internos y externos. Esta opción se conoce como voz sobre IP (VoIP).

El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas de clientes y/o teléfonos IP H.323 o SIP para usuarios. En cualquier caso, se deben considerar los siguientes factores:

- La unidad de control de IP Office debe estar equipada con canales de compresión de voz 41. Estos se utilizan cuando un dispositivo IP (troncal o extensión) necesita comunicarse con un dispositivo que no es IP (troncal o extensión) o con un dispositivo que utiliza un códec diferente.
- Una evaluación de la red es un requisito obligatorio para todos los sistemas que utilizan VoIP. Para problemas de soporte con VoIP, Avaya puede solicitar acceso a los resultados de la evaluación de la red y puede rechazar el soporte si no están disponibles o no son satisfactorios.

Una evaluación de la red incluiría una determinación de lo siguiente:

- Una auditoría de red para revisar el equipo existente y evaluar sus capacidades, incluida su capacidad para satisfacer las necesidades de voz y datos actuales y planificadas.
- Una determinación de los objetivos de la red, incluido el tipo de tráfico dominante, la elección de tecnologías y el establecimiento de objetivos de calidad de voz.
- La evaluación debería dejarle la confianza de que la red implementada tendrá la capacidad para el tráfico de datos y voz previsto, y puede admitir H.323, DHCP, TFTP y búferes de fluctuación en aplicaciones H.323.
- Un resumen de los objetivos esperados de la evaluación de la red es:

Prueba	Objetivo mínimo de evaluación
Latencia	Menos de 150 ms.
Paquete perdido	Menos de 3%.
Duración	Supervise las estadísticas una vez cada minuto durante una semana completa.

1.16.1 Canales de compresión de voz

Las llamadas hacia y desde dispositivos IP pueden requerir la conversión al formato de códec de audio que utiliza el dispositivo IP. Para los sistemas IP Office, esta conversión se realiza mediante canales de compresión de voz. Estos son compatibles con los códecs de audio IP comunes G.711, G.723 y G.729a. Para IP Office versión 8.0 y superior, las tarjetas combinadas IP500 VCM e IP500 también son compatibles con G.722.

Para las unidades de control IP500 V2, los canales se pueden agregar usandoTarjetas VCM IP500 221yTarjetas combinadas IP500 214.

Los canales de compresión de voz se utilizan de la siguiente manera:

Tipo de llamada	Uso del canal de compresión de voz
Dispositivo IP a dispositivo no IP	Estas llamadas requieren un canal de compresión de voz durante la duración de la llamada. Si no hay ningún canal disponible, la indicación de ocupado se devuelve a la persona que llama.
Dispositivo IP a dispositivo IP	Los tonos de progreso de llamada (por ejemplo, tono de marcado, tono de marcado secundario, etc.) no requieren canales de compresión de voz con las siguientes excepciones: • La confirmación del código corto, la activación del ARS y los tonos de entrada del código de cuenta requieren un canal de compresión de voz. • Los dispositivos que utilizan G723 requieren un canal de compresión de voz para todos los tonos, excepto para la llamada en espera. Cuando se conecta una llamada: • Si los dispositivos IP utilizan el mismo códec de audio, no se utiliza ningún canal de compresión de voz. • Si los dispositivos usan diferentes códecs de audio, se requiere un canal de compresión de voz para cada uno.
Dispositivo no IP a dispositivo no IP	No se requieren canales de compresión de voz.
Música en espera	Esto se proporciona desde el bus TDM de IP Office y, por lo tanto, requiere un canal de compresión de voz cuando se reproduce en un dispositivo IP.
Recursos de la conferencia y dispositivos IP	Los recursos de conferencia son administrados por el chip de conferencia que se encuentra en el bus TDM de IP Office. Por lo tanto, se requiere un canal de compresión de voz para cada dispositivo IP involucrado en una conferencia. Esto incluye servicios que usan recursos de conferencia como escucha de llamadas, intrusión, grabación de llamadas y monitoreo silencioso.
Localización de llamadas al dispositivo IP	IP Office 4.0 y versiones posteriores solo usan G729a para llamadas de buscapersonas, por lo tanto, solo requieren un canal, pero también solo admiten búsquedas a dispositivos compatibles con G729a.
Servicios de correo de voz y Dispositivos IP	Las llamadas a los servidores de correo de voz de IP Office se tratan como llamadas de datos desde el bus TDM. Por lo tanto, las llamadas desde un dispositivo IP al correo de voz requieren un canal de compresión de voz.
Llamadas de fax	Estas son llamadas de voz pero con un rango de frecuencia ligeramente más amplio que las llamadas de voz habladas. IP Office solo admite fax a través de IP entre sistemas IP Office con la opción Transporte de fax seleccionada. Actualmente no es compatible con T38.
Llamadas de fax T38	Cada llamada de fax T38 utiliza un canal VCM. Dentro de una red comunitaria pequeña, una llamada de fax T38 se puede convertir en una llamada a través de líneas SCN H323 utilizando el protocolo de soporte de transporte de fax de IP Office. Esta conversión utiliza 2 canales VCM. Para utilizar la conexión de fax T38, el**Clasificación de equipos**de una extensión analógica conectada a una máquina de fax se puede configurar***Máquina de fax***. Además, una nueva función de código corto **Marcar fax**está disponible.

Medición del uso del canal

La aplicación de estado del sistema se puede usar para mostrar el uso del canal de compresión de voz. Dentro de**Recursos**sección muestra el número de canales en uso. También muestra con qué frecuencia ha habido canales insuficientes disponibles y la última vez que ocurrió tal evento.

En las tarjetas IP500 VCM, el uso del canal también se indica mediante los LED (1 a 8) en la parte frontal de laTarjeta VCM IP500 221.

1.17 Regiones de país admitidas

Cuando la configuración de un sistema nuevo o predeterminado se abre por primera vez en IP Office Manager, el valor establecido en el**Lugar**El campo siempre debe verificarse y cambiarse si es necesario.

La configuración regional del sistema establece factores tales como los patrones de timbre predeterminados y la configuración de visualización de la persona que llama. La configuración regional también controla el idioma que un servidor de correo de voz intentará usar para las indicaciones de manera predeterminada.

- Los países soportados son:***Argentina*,*Australia*,*Baréin*,*Bélgica*,*Brasil*,*Canadá*,*Chile*,*Porcelana*, *Colombia*,*República Checa*,*Dinamarca*,*Egipto*,*Finlandia*,*Francia*,*Alemania*,*Grecia*,*Hong Kong*, *Hungría*,*Islandia*,*India*,*Irlanda*,*Italia*,*Japón*,*Corea*,*Kuwait*,*Malasia*,*Mediterráneo*,*México*, *Marruecos*,*Países Bajos*,*Nueva Zelanda*,*Noruega*,*Omán*,*Pakistán*,*Perú*,*Filipinas*,*Polonia*,*Portugal*, *Katar*,*Rusia*,*Arabia Saudita*,*Singapur*,*Sudáfrica*,*España*,*Suecia*,*Suiza*,*Taiwán*,*Pavo*, *Emiratos Árabes Unidos*,*Estados Unidos*,*Venezuela***.**

1.18 Aplicaciones de software de IP Office

Las aplicaciones de IP Office están disponibles en varios DVD. Estos se pueden pedir a un costo nominal para cubrir el procesamiento y la entrega del pedido. También se pueden instalar paquetes de instalación independientes para las aplicaciones de IP Office.descargado 63desde el sitio web de soporte de Avaya enhttp://soporte.avaya.com .

Título	Discos	Descripción	Código SAP
Juego de DVD para administradores y usuarios de IP Office versión 11.0	2	Estos DVD contienen paquetes de instalación para todas las principales aplicaciones de usuario y administración de IP Office. También contienen documentación para IP Office. · **DVD 1:**Contiene el conjunto de aplicaciones de administrador de IP Office, la documentación de IP Office, las aplicaciones de usuario de IP Office, IP Office Voicemail Pro. · **DVD 2:**Contiene la aplicación one-X Portal for IP Office.	700513659
Conjunto de DVD Voicemail Pro ScanSoft TTS	2	Contiene motores de texto a voz para usar con las funciones TTS de Voicemail Pro. Admite los mismos idiomas que las indicaciones pregrabadas de Voicemail Pro, excepto el húngaro.	700478068
DVD de instalación de IP Office versión 11.0 Server Edition	2	DVD de instalación para servidores Server Edition y IP Office Application Server. El segundo DVD contiene material de código abierto utilizado para el primer DVD.	700513657
DVD virtualizado de IP Office Server Edition	1	DVD de instalación para servidores Server Edition virtualizados y IP Office Application Server virtualizado.	700513658
Juego de DVD TTS de IP Office Linux Server	3	Contiene motores de texto a voz para usar con las funciones TTS de Voicemail Pro basadas en Linux.	700502693

- Es aceptable hacer copias de los DVD de Avaya IP Office enumerados anteriormente. Sin embargo, el contenido debe permanecer intacto, inalterado y sin cambios ni adiciones. Avaya no acepta ninguna responsabilidad por daños o problemas que surjan del uso de dichas copias.

1.18.1 Aplicaciones de programación

Las siguientes aplicaciones se utilizan para programar y mantener un sistema IP Office. Por lo general, se ejecutan en una PC conectada al sistema IP Office a través de su interfaz LAN. Todas estas aplicaciones se proporcionan en el DVD de aplicaciones de administrador de IP Office y no requieren ninguna licencia.

Debido a la naturaleza de las aplicaciones, si se instalan en una PC en el sitio del cliente, esta debe ser una PC segura o la PC de un usuario de confianza. Si también se instala una PC servidor de correo de voz con el sistema IP Office, la misma PC se puede usar para las aplicaciones de programación y mantenimiento.

Para los encargados del mantenimiento, estas aplicaciones también se pueden ejecutar de forma remota si existe una ruta para las conexiones de datos a la IP Office del cliente desde la ubicación del encargado del mantenimiento.

- **Versión del administrador de IP Office**
  Es importante descargar e instalar la versión correcta del paquete de administración de IP Office, incluido IP Office Manager.
  - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincida con la versión de IP Office requerida en el sistema. Esto establece la versión del software cargado cuandorecreando la tarjeta SD del sistema 75.
  - Para el mantenimiento del sistema, la versión de IP Office Manager utilizada establece la versión del software cargado en un sistema cuandoactualizando el sistema 180.
  - Para la configuración del sistema, IP Office Manager es compatible con versiones anteriores. IP Office Manager versión 11.0 es compatible con versiones anteriores para configurar sistemas que ejecutan software a partir de la versión 6.0 de IP Office y en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión superior del software.
    - **Admin Lite no compatible**
      Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).
- **!Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín técnico de IP Office relacionado con la versión del software de IP Office que pretende instalar. El boletín contiene información importante que puede no haber sido incluida en este manual. Los boletines técnicos de IP Office están disponibles en elSoporte de Avaya sitio web*(http://soporte.avaya.com)*.

Aplicaciones

- **Gerente de IP Office** 253
  Esta herramienta se utiliza para acceder a todas las partes de la configuración de IP Office. Se pueden definir diferentes niveles de acceso para controlar qué partes de la configuración puede ver y modificar el usuario de IP Office Manager. IP Office Manager también se utiliza para actualizar los archivos de software utilizados por un sistema IP Office.
  - **Admin Lite no compatible**
    Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).
- **Administrador web de IP Office** 71
  Se puede acceder a la configuración de un sistema IP500 V2 a través del navegador web usando las mismas cuentas de usuario de servicio que se usan para IP Office Manager. Actualmente, para los sistemas de modo estándar de IP Office, IP Office Web Manager solo se puede usar para configurar usuarios, grupos y usuarios de servicios (cuentas de seguridad) y para realizar acciones básicas de mantenimiento. Por lo tanto, aún se requiere IP Office Manager para la instalación y el mantenimiento completos del sistema.
- **Aplicación de estado del sistema** 257
  Esta aplicación se puede utilizar para inspeccionar el estado actual de las líneas y extensiones de IP Office y para ver registros de alarmas y eventos recientes. Se ejecuta como una aplicación Java.
- **MIB de SNMP** 192
  No es una aplicación como tal. Mediante el uso de archivos MIB de SNMP de IP Office, el estado del sistema de IP Office será monitoreado por aplicaciones SNMP de terceros, como Castlerock y HP OpenView. Cuando se configura para la operación SNMP, IP Office también puede enviar alertas sobre posibles problemas. Los sistemas IP Office también admiten el envío de las mismas alertas a direcciones de correo electrónico SMTP o Syslog.
  - Las alarmas configurables para la salida a través de SNMP también se pueden enviar a correo electrónico SMTP o Syslog.
- **Supervisar (SysMon)** 259
  Monitor es una herramienta que puede mostrar un seguimiento de toda la actividad en el sistema IP Office en detalle. Como consecuencia, la interpretación de las trazas de Monitor requiere un alto nivel de conocimiento del protocolo de datos y telefonía. Sin embargo, a pesar de eso, todos los instaladores y mantenedores de IP Office deben comprender cómo ejecutar Monitor cuando sea necesario, ya que Avaya puede solicitar copias de los seguimientos de Monitor para resolver problemas de soporte.

1.18.2 Aplicaciones de usuario

IP Office es compatible con una serie de aplicaciones que funcionan en paralelo con los teléfonos de los usuarios. Estas aplicaciones se instalan desde el DVD de aplicaciones de IP Office. El servidor one-X Portal for IP Office también se puede instalar como parte de la instalación del DVD de la aplicación IP Office.

Algunos de ellos requieren que se ingresen licencias en la configuración del sistema IP Office para habilitar funciones o establecer la cantidad de usuarios simultáneos.

- **Portal one-X para IP Office** [255]
  Esta aplicación se instala en una PC servidor conectada a IP Office. Los usuarios pueden acceder al portal one-X desde su propia PC usando un navegador web. La aplicación permite al usuario controlar sus teléfonos, acceder a mensajes de correo de voz, registros de llamadas y directorios telefónicos.

  - **Cliente web de IP Office**
    Este es un cliente WebRTC compatible con un navegador. Permite al usuario realizar, contestar y controlar llamadas de audio y video desde su PC. Lo pueden utilizar los usuarios configurados para one-X Portal for IP Office. Requiere un servidor de aplicaciones de IP Office con el servicio de puerta de enlace WebRTC configurado.

- **SoftConsole** [257]
  Esta es una aplicación con licencia. Está destinado a operadores de sistemas telefónicos o recepcionistas. Muestra los detalles de las llamadas y les permite ver rápidamente el estado del destino requerido por la persona que llama y transferir la llamada. El usuario de SoftConsole puede acceder a una variedad de detalles sobre el estado de los usuarios y grupos en el sistema IP Office. Se pueden licenciar hasta 4 usuarios simultáneos de SoftConsole.

- **Cliente del lugar de trabajo de Avaya IX** [254]
  Esta es una aplicación de comunicaciones unificadas que se ejecuta en dispositivos Windows, macOS, iOS y Android.

- **Comunicador de Avaya** [256]
  Esta es una aplicación con licencia que se ejecuta en varios dispositivos Windows, iPad y Android. Dependiendo de la configuración, un usuario puede usarlo junto con su propio teléfono para controlar las llamadas o puede usarlo como su teléfono.

- **one-x móvil**
  Se trata de un conjunto de clientes soportados en dispositivos de telefonía móvil Apple iOS y Android. Estos permiten al usuario acceder al directorio de IP Office, contactos personales y mensajes, y realizar y recibir llamadas a través del sistema telefónico.

- **Colaboración web** [260]
  Comparta documentos y mensajes en una conferencia. Web Collaboration proporciona al usuario funciones para compartir documentos, aplicaciones y su escritorio en una conferencia de colaboración web. Esto se ejecuta en paralelo con una conferencia de audio organizada por el sistema IP Office. Los usuarios internos con licencia para la colaboración web pueden usar WebRTC para transmitir audio a través de la conferencia de colaboración web en lugar de tener que realizar una llamada telefónica paralela a la conferencia de audio.

- **TAPI Link Lite** [258]
  La Interfaz del programa de aplicaciones de telefonía de Microsoft (TAPI) permite que las aplicaciones compatibles con TAPI interactúen con los teléfonos de IP Office mediante la instalación de un controlador TAPI de IP Office. TAPILink Lite no requiere ninguna licencia ingresada en la configuración del sistema IP Office. Permite que las aplicaciones compatibles con TAPI, como Outlook, realicen y respondan llamadas. La parte de voz de las llamadas sigue siendo a través del teléfono físico del usuario.

1.18.3 Aplicaciones de correo de voz

IP Office es compatible con una variedad de aplicaciones para grabar y reproducir mensajes de correo de voz.

- **Correo de voz integrado**
  Embedded Voicemail admite la operación básica del buzón de correo de voz, asistentes automáticos simples y anuncios de grupos de búsqueda. Para las unidades de control IP500 V2, Embedded Voicemail se proporciona mediante la tarjeta SD de Avaya instalada de forma predeterminada.

- **Buzón de voz profesional** [259]
  Esta aplicación de correo de voz se ejecuta en una computadora servidor conectada a IP Office. Requiere varias licencias ingresadas en la configuración de IP Office para controlar las funciones que ofrece y la cantidad de conexiones simultáneas. El funcionamiento de Voicemail Pro se puede personalizar para proporcionar servicios especiales. La aplicación puede instalarse en un servidor de Windows o ser proporcionada por un servidor de aplicaciones de IP Office (que también puede ejecutar one-X Portal para IP Office y Media Manager).

- **Administrador de medios** [263]
  Voicemail Pro se puede utilizar para la grabación manual y automática de llamadas. Esas grabaciones se colocan en buzones. Media Manager permite que esas grabaciones se redirijan a una tienda separada donde los detalles de cada grabación se mantienen en una base de datos de búsqueda. Esto permite que las grabaciones se archiven, busquen y reproduzcan por separado de los mensajes del buzón. Esta aplicación requiere la entrada de licencias adicionales en la configuración de IP Office. Esta aplicación requiere un servidor de aplicaciones de IP Office que incluya un disco duro adicional para el almacenamiento de grabaciones.

1.18.4 Aplicaciones de registro de llamadas

Existe una amplia gama de aplicaciones de terceros para proporcionar registro de llamadas y contabilidad para sistemas telefónicos. Para respaldar estos, IP Office proporciona una salida SMDR.

- **Salida SMDR**
  Para la versión 5.0 y posteriores de IP Office, la unidad de control de IP Office envía directamente registros SMDR a una dirección IP específica. Esto se configura mediante IP Office Manager.

1.18.5 Aplicaciones de centro de llamadas

IP Office es compatible con una serie de soluciones de centros de contacto.

- **Centro de contacto de IP Office**
  Este conjunto de aplicaciones admite una variedad de módulos que permiten enrutar las llamadas a los agentes en función de una variedad de factores.
- **Selección del centro de contacto de Avaya**
  Esta es una gran solución de centro de contacto para hasta 250 agentes.

1.18.6 Aplicaciones CTI

- **TAPI Link Pro**
  Utilizando el mismo software que TAPILink Lite, TAPILink Pro proporciona todas las características y funcionalidades de TAPILink Lite, pero además proporciona operación CTI de terceros. Esto significa que un solo servidor puede controlar y monitorear cualquier número de dispositivos telefónicos. Esto requiere la entrada de una licencia CTI Link Pro. TAPILink Pro también brinda la capacidad de monitorear y controlar grupos. Esto permite que una aplicación sea notificada cuando una llamada ingresa a una cola y también puede redirigirla a otra ubicación.
- **Controlador TAPI WAV**
  Proporciona soporte basado en software para procesamiento de voz. La compra de la clave de licencia CTI Link Pro RFA también habilita 4 puertos de procesamiento de voz; se pueden comprar puertos adicionales en incrementos de 4 puertos. El controlador TAPI-WAV solo se usa con TAPI 2.1; para TAPI 3.0, IP Office es compatible con la interfaz del proveedor de servicios multimedia (MSP), definida por Microsoft en TAPI 3.0.
- **DevLink Pro**
  Proporciona un flujo de eventos en tiempo real además de la interfaz SMDR provista en IP Office SMDR (consulte a continuación). El flujo de eventos en tiempo real toma la forma de un registro de llamada, que se emite cada vez que cambia el estado de cualquier punto final de una llamada (por lo general, hay dos puntos finales en una llamada, pero en algunas circunstancias, como llamadas en conferencia, llamadas intrusas allí). quizás más).

1.19 Entrenamiento

Avaya University ofrece una amplia gama de cursos de capacitación para IP Office y sus aplicaciones asociadas. Esto incluye los cursos necesarios para que los revendedores de IP Office se conviertan en socios de canal autorizados de Avaya y para que las personas obtengan la certificación de IP Office.

Los detalles de los cursos se pueden encontrar en el sitio web de la Universidad de Avaya (http://www.avaya-learning.com). El sitio se puede utilizar para verificar la disponibilidad del curso y para reservar un curso. También incluye cursos en línea y evaluaciones de cursos en línea. El sitio requiere que los usuarios establezcan un nombre de usuario y una contraseña para realizar un seguimiento de su registro de entrenamiento personal.

1.20 Sitios web

Puede encontrar información de apoyo a IP Office en varios sitios web.

- **Avaya** *(http://www.avaya.com)*
  El sitio web oficial de Avaya. La página principal también brinda acceso a sitios web individuales de Avaya para diferentes países.
- **Portal empresarial de Avaya** *(http://partner.avaya.com)*
  Este es el sitio web oficial de todos los Business Partners de Avaya. El sitio requiere el registro de un nombre de usuario y contraseña. Una vez accedido, el portal del sitio se puede personalizar individualmente para qué productos y tipos de información desea ver y recibir notificaciones por correo electrónico.
- **Soporte de Avaya** *(http://soporte.avaya.com)*
  Contiene documentación y otros materiales de soporte para los productos de Avaya, incluido IP Office. Las copias de las imágenes del CD de IP Office están disponibles en este sitio y los archivos .bin del software principal actualizado.
- **Base de conocimientos de IP Office de Avaya** *(https://ipofficekb.avaya.com)*
  Acceso a una versión en línea actualizada regularmente de las guías de usuario y manuales técnicos de IP Office.
- **Universidad Avaya** *(http://www.avaya-learning.com)*
  Este sitio brinda acceso a la gama completa de cursos de capacitación de Avaya. Eso incluye cursos en línea, evaluaciones de cursos y acceso a detalles de cursos presenciales. El sitio requiere que los usuarios se registren para brindarle acceso a los detalles de su registro de capacitación.
- **Comunidad Avaya** *(http://www.aucommunity.com)*
  Este es el foro de discusión oficial para los usuarios de productos de Avaya. Sin embargo, no incluye ningún área separada para la discusión de temas de IP Office.
- **Matriz de compatibilidad de productos de Avaya** *(https://secureservices.avaya.com/compatibilitymatrix/menus/product.xhtml)*
- **Documentos de matriz de puertos de productos de Avaya** *(https://support.avaya.com/helpcenter/getGenericDetails?detalleId=C201082074362003)*
- **Otros sitios web que no son de Avaya**
  Existen varios foros web de terceros que analizan IP Office. Estos pueden actuar como una fuente útil de información sobre cómo se usa IP Office. Algunos de estos foros requieren que seas miembro y te registres. Estos no son foros oficiales de Avaya y Avaya no controla ni sanciona su contenido.
  - **Consejos técnicos** *(http://www.tek-tips.com)*
  - **Información de IP Office** *(http://www.ipofficeinfo.com)*
  - **Grupos de Yahoo** *(http://groups.yahoo.com/group/ipoffice)*
  - **Tecnología PBX** *(http://www.pbxtech.info/forumdisplay.php?f=8)*

1.21 Puertos de emergencia y fallas de energía

Los sistemas IP Office proporcionan 2 tipos de puertos de falla de energía de extensión analógica. En todos los casos, estos solo funcionan con troncales analógicas de inicio de bucle. Todos los teléfonos conectados a estos puertos deben estar claramente etiquetados como extensiones de corte de energía de acuerdo con los requisitos normativos nacionales y locales correspondientes.

Conmutación de puertos de falla de energía

Durante el funcionamiento normal, estos puertos se pueden utilizar para conexiones telefónicas analógicas normales. Durante un corte de energía, los puertos se conectan directamente a un puerto troncal analógico.

Este tipo de puerto de falla de energía lo proporcionan las siguientes tarjetas:

- **Tarjeta de teléfono analógico IP500 8**
  Cuando una tarjeta base IP500 Analog Phone 8 está equipada con una tarjeta secundaria IP500 Analog Trunk, durante un corte de energía, el puerto de extensión 8 se conecta al puerto de troncales analógicas 12.
- **Tarjeta combinada IP500 ATM/Tarjeta combinada IP500 ATM V2**
  En esta tarjeta, durante un corte de energía, el puerto de extensión 8 se conecta al puerto de troncal analógico 12.

Puertos de falla de energía solo de emergencia

Durante el funcionamiento normal, estos puertos no se pueden utilizar. Durante un corte de energía, los puertos se conectan directamente a un puerto troncal analógico.

- **Tarjeta secundaria de troncales analógicas IP500/Tarjeta secundaria de troncales analógicas IP500 V2**
  Independientemente de la tarjeta IP500 que la aloje, durante un corte de energía, los pines 4 y 5 del puerto 12 se conectan a los pines 7 y 8.

- **Tarjeta IP500 ETR6**
  En esta tarjeta, durante el funcionamiento normal, los puertos de extensión 7 y 8 no se pueden utilizar. Sin embargo, si la tarjeta está equipada con una tarjeta secundaria de troncales analógicas IP500, durante un corte de energía, los puertos de extensión 7 y 8 se conectan al puerto de troncales analógicas 12.

Capitulo 2.

Descripción general de la instalación

2. Descripción general de la instalación

Este proceso de instalación es un esquema simple. Se pueden completar muchos pasos antes de la instalación real en el sitio del cliente.

Resumen del proceso de instalación

1. **Prepárese para la instalación** 50

   una. **Requisitos medioambientales** 51
   Verifique que el área de instalación cumpla con los requisitos ambientales del sistema.

   b. **Requisitos de espacio** 53
   Verifique que el área de instalación cumpla con los requisitos de espacio del sistema.

   C. **Herramientas y piezas necesarias** 59
   Compruebe que dispone de las herramientas y piezas adicionales necesarias.

   d. **Documentación** 60
   Asegúrese de haber obtenido y leído toda la documentación pertinente.

   mi. **Desembalaje** 60
   Verifique que se haya entregado todo el equipo requerido y que no haya daños.

2. **Instalación del software de administración** 62
   Para la instalación del sistema, necesita una PC con el software de administrador de IP Office instalado. Esto debe incluir una copia de IP Office Manager que coincida con el nivel de software de IP Office requerido.

   una. **Descarga del software** 63

   b. **Instalación de las aplicaciones del administrador** 64

3. **Preparación de la tarjeta SD del sistema** 74
   Actualice la tarjeta SD del sistema a la versión requerida del software IP Office. Además, agregue cualquier otro archivo disponible, como el archivo de licencia, la configuración preconstruida, el archivo de música en espera.

   - **!ADVERTENCIA: Instalación de unidades de control PCS14 y anteriores**
     PC 296 14 o unidades inferiores deben instalar primero la versión 8.1(65) (o superior 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1. Se debe tener cuidado para asegurarse de que no se realicen llamadas antes de la actualización a la Versión 10.0, de lo contrario, el sistema requerirá una licencia de actualización 10.0 a pesar de ser "nuevo". El PCS de la unidad de control está impreso en la etiqueta en la parte posterior de la unidad de control.

4. **Instale las tarjetas de la unidad de control** 82
   Conecte las tarjetas secundarias de troncales a sus tarjetas base IP500 e inserte las tarjetas base en la unidad de control.

5. **Instalar el sistema** 86

   una. **Montaje en pared** 87
   Si se monta en la pared, fije los soportes y coloque la unidad en la pared.

   b. **Montaje en bastidor** 89
   Si se monta en un bastidor, fije los soportes y coloque la unidad de control en el bastidor.

   C. **Conectar los módulos de expansión externos** 91
   Conecte los módulos de expansión externos a la unidad de control.

   d. **Poner a tierra el sistema** 93
   Conecte los cables de tierra necesarios a la unidad de control y a los módulos de expansión externos.

   mi. **Iniciar el sistema** 94
   Inserte la tarjeta SD del sistema y encienda el sistema.

   F. **Conexión de teléfonos** 97
   Conecte los teléfonos digitales de Avaya.

6. **Configuracion inicial**
   Una vez que se inicia el sistema físico, se puede configurar. Esto se puede hacer usando cualquiera Administrador de IP Office Administrador 100 O web de IP Office 114.

2.1 Requisitos ambientales

La ubicación prevista debe cumplir con los siguientes requisitos. Si se instala en un sistema de bastidor, estos son los requisitos para el interior del bastidor:

1.oTemperatura: Funcionamiento 5°C a 40°C (Almacenamiento -40°C a 70°C).

2.oHumedad relativa: En funcionamiento 10 % a 90 % (Almacenamiento 5 % a 95 %).

3.oVerifique que no haya materiales inflamables en el área.

4.oComprobar que no hay posibilidad de inundación.

5.oVerifique que no sea necesario mover primero ninguna otra maquinaria o equipo.

6.oComprobar que no se trata de un ambiente excesivamente polvoriento.

7.oCompruebe que es poco probable que la zona sufra cambios bruscos de temperatura y humedad.

8.oVerifique la proximidad de campos magnéticos fuertes, fuentes de radiofrecuencia y otras interferencias eléctricas.

9.oCompruebe que no haya productos químicos o gases corrosivos.

10oVerifique que no haya vibración excesiva o potencial de vibración excesiva, especialmente en cualquier superficie de montaje.

11oComprobar que en caso de instalación de teléfonos en otro edificio, se disponga de los protectores y tomas de tierra adecuados (verInstalación telefónica fuera del edificio 36).

12oVerificar que exista iluminación adecuada para la instalación, programación del sistema y mantenimiento futuro.

13oVerifique que haya suficiente espacio de trabajo para la instalación y el mantenimiento futuro.

14oAsegúrese de que las actividades probables cerca del sistema no causen ningún problema, por ejemplo, el acceso y el mantenimiento de cualquier otro equipo en el área.

15.oCuando haya orificios de ventilación en cualquiera de las unidades de IP Office, dichos orificios no deben cubrirse ni bloquearse.

dieciséis.oLa superficie debe ser plana y horizontal para instalaciones independientes o montadas en bastidor.

Montaje en bastidor

1. Posicionamiento del estante: asegúrese de cumplir con las instrucciones de seguridad del fabricante del estante. Por ejemplo, verifique que las patas del estante se hayan bajado y que se hayan utilizado los soportes de fijación para evitar que se vuelque.

2. Ambiente de funcionamiento elevado: si se instala en un conjunto de bastidor cerrado o de varias unidades, la temperatura ambiente de funcionamiento del entorno del bastidor puede ser superior a la temperatura ambiente de la habitación. Por lo tanto, se debe considerar la instalación del equipo en un entorno compatible con la temperatura ambiente máxima (Tma) especificada por el fabricante.

   · oTemperatura de funcionamiento: 5 °C (40 °F) a 40 °C (104 °F).

   · oHumedad de funcionamiento: 10 % a 95 % sin condensación.

3. Flujo de aire reducido: la instalación del equipo en un bastidor debe ser tal que la cantidad de flujo de aire necesaria para el funcionamiento seguro del equipo no se vea comprometida. Se debe mantener una ventilación adecuada. Las ranuras de ventilación laterales de la unidad de control IP500 no deben cubrirse ni bloquearse.

4. Carga mecánica: el montaje del equipo en el bastidor debe ser tal que no se logre una condición peligrosa debido a una carga mecánica desigual.

5. Sobrecarga del circuito: se debe considerar la conexión del equipo al circuito de suministro y el efecto que la sobrecarga de los circuitos podría tener en la protección contra sobrecorriente y el cableado de suministro. Se deben tener en cuenta las clasificaciones de la placa de identificación del equipo al abordar esta inquietud.

6. Conexión a tierra confiable: se debe mantener una conexión a tierra confiable de los equipos montados en rack. Debe prestarse especial atención a las conexiones de suministro distintas de las conexiones directas al circuito derivado (p. ej., uso de regletas).

7. ⚠ Solo se deben usar los tornillos proporcionados con el kit de montaje para fijar los soportes a la unidad de control.

Montaje en pared

Además de los requisitos anteriores, los siguientes se aplican a las unidades de IP Office que admiten montaje en pared.

1. Las unidades solo deben montarse en superficies de pared permanentes.

2. La superficie debe ser vertical y plana.

3. La orientación de la unidad debe ser como se muestra en la sección sobreMontaje en pared IP500 87.

4. Se deben utilizar los kits de montaje en pared adecuados de Avaya.

INSTRUCCIONES DE SEGURIDAD IMPORTANTES

Al usar su equipo telefónico, siempre se deben seguir las precauciones básicas de seguridad para reducir el riesgo de incendio, descarga eléctrica y lesiones personales, incluidas las siguientes:

1. No utilice este producto cerca del agua, por ejemplo, cerca de una bañera, un lavabo, un fregadero o un lavadero, en un sótano húmedo o cerca de una piscina.
2. Evite usar un teléfono (que no sea de tipo inalámbrico) durante una tormenta eléctrica. Puede haber un riesgo remoto de descarga eléctrica por un rayo.
3. No use el teléfono para reportar una fuga de gas en las inmediaciones de la fuga.
4. Utilice únicamente el cable de alimentación y las baterías que se indican en este manual.

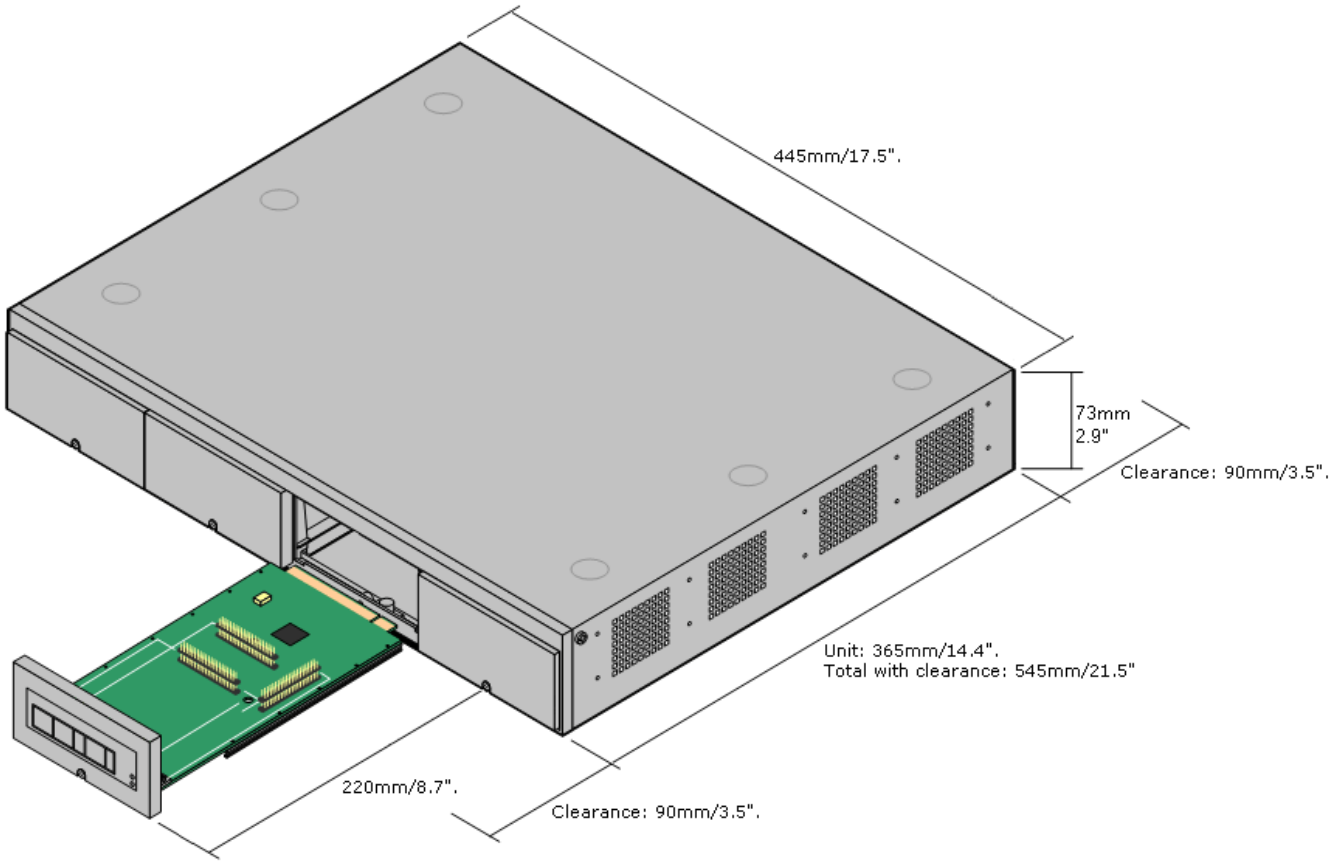
2.2 Requisitos de espacio

Las unidades de control y los módulos de IP Office están diseñados para instalarse en una pila independiente o en un sistema de rack de 19". La instalación en rack requiere unkit de montaje en bastidor 37para cada unidad de control y módulo de expansión.

- **Separación de cables**
  Se debe dejar espacio en la parte delantera y trasera de todos los módulos para el acceso de los cables. En los sistemas IP500 V2, deje un espacio libre mínimo de 90 mm (3,5 pulgadas).
- **Liquidación adicional**
  Se debe tener cuidado para asegurar que el posicionamiento de los módulos no interrumpa el flujo de aire y otros factores que puedan afectarRequisitos medioambientales 51.Esto es especialmente importante en las unidades de control IP500 V2 que tienen ranuras de ventilación laterales.
- **Acceso a cables**
  Los cables de alimentación no deben fijarse a la superficie del edificio ni atravesar paredes, techos, suelos ni aberturas similares. Se deben tomar medidas de instalación para evitar daños físicos al cable de alimentación, incluido el enrutamiento adecuado del cable de alimentación y la provisión de una toma de corriente cerca del equipo fijo o la ubicación del equipo cerca de una toma de corriente.

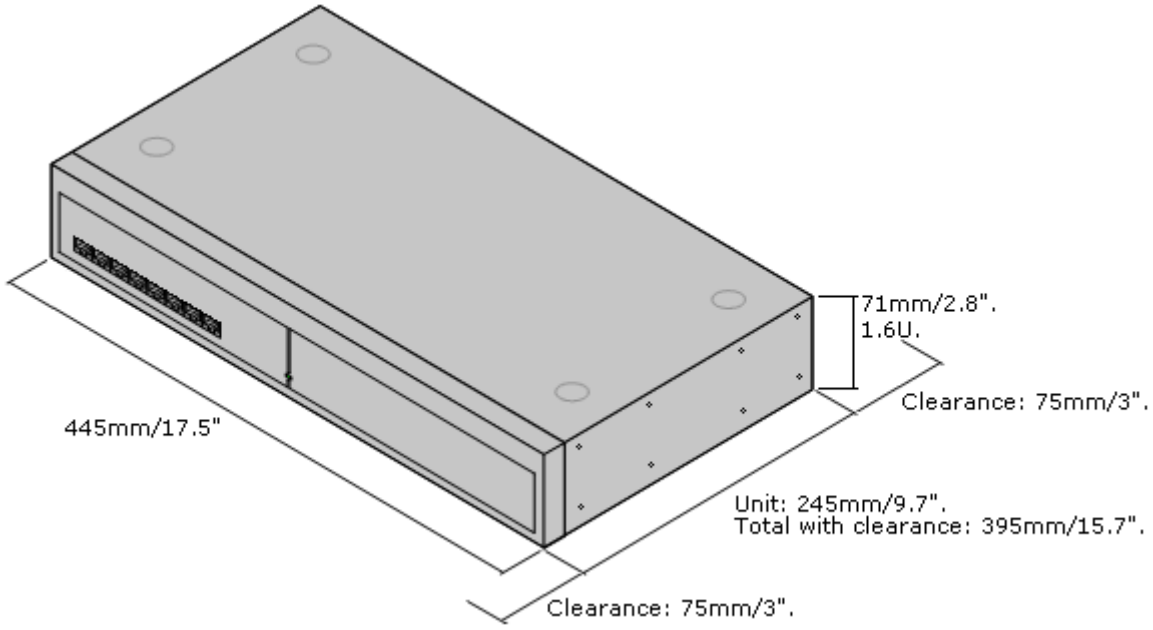
2.2.1 Unidad de control

Las ranuras de ventilación de la parte trasera y los laterales no deben taparse ni bloquearse.



2.2.2 Módulos de expansión externos

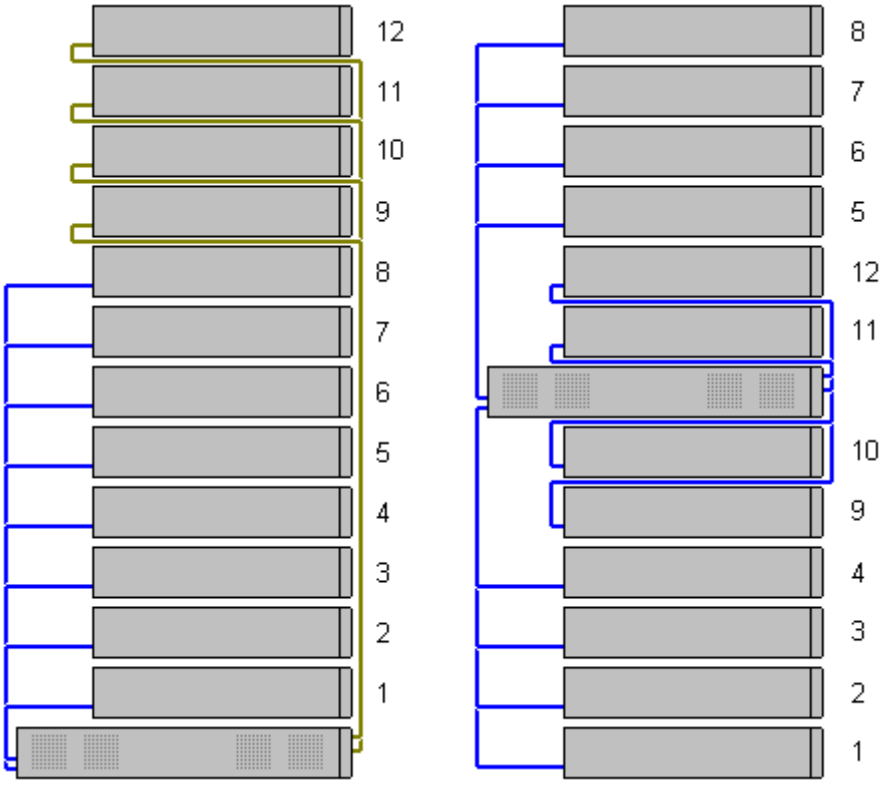
Las siguientes dimensiones se aplican a todos los módulos de expansión externos de IP Office.



Para sistemas independientes, los módulos de expansión externos se pueden apilar sobre la unidad de control. Para eso, y para los sistemas montados en rack, el siguiente diagrama muestra las opciones recomendadas para acomodar la longitud del cable de interconexión del módulo.

Los puertos de expansión integrales en una unidad de control están ubicados en la parte posterior de la unidad. Se pueden agregar 4 puertos de expansión adicionales al frente de la unidad de control instalando una tarjeta de expansión de 4 puertos IP500.

- Cada módulo de expansión externo se suministra con un cable de interconexión de expansión azul de 1 metro (3'3''). este cable deber utilizarse cuando se conecta a puertos de expansión en la parte trasera de una unidad de control.
- Cuando se conecta a puertos de expansión en una tarjeta de expansión de 4 puertos IP500, se puede usar un cable de interconexión de expansión amarillo de 2 metros (6'6") en lugar del cable azul estándar. Se suministran 4 cables amarillos con la tarjeta de expansión de 4 puertos IP500 tarjeta.



2.2.3 Montaje en pared

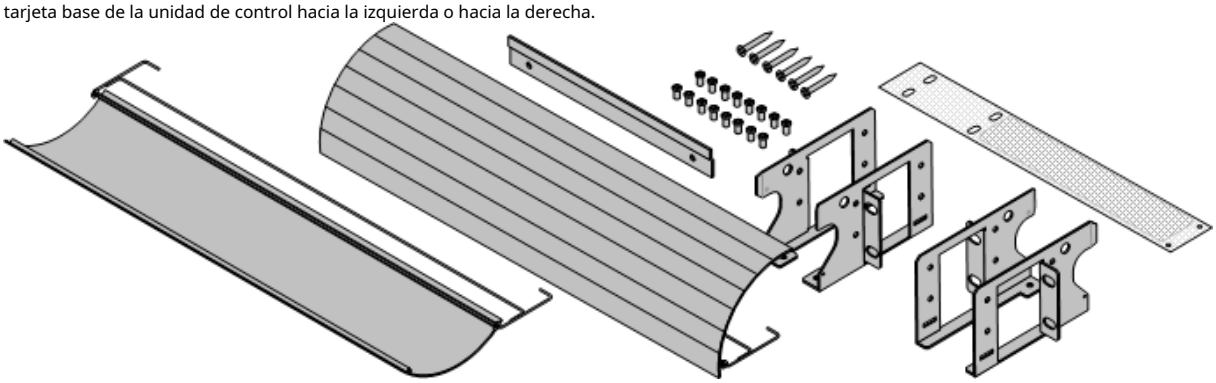
Las unidades de control IP500 V2 y los módulos de expansión externos IP500 pueden montarse en la pared o en un bastidor. Para hacer esto, se requiere un kit de montaje en pared además de las fijaciones de pared adecuadas.

Además de los existentesRequisitos medioambientales 51para un sistema IP Office, se aplican los siguientes requisitos adicionales al montar una unidad en la pared:

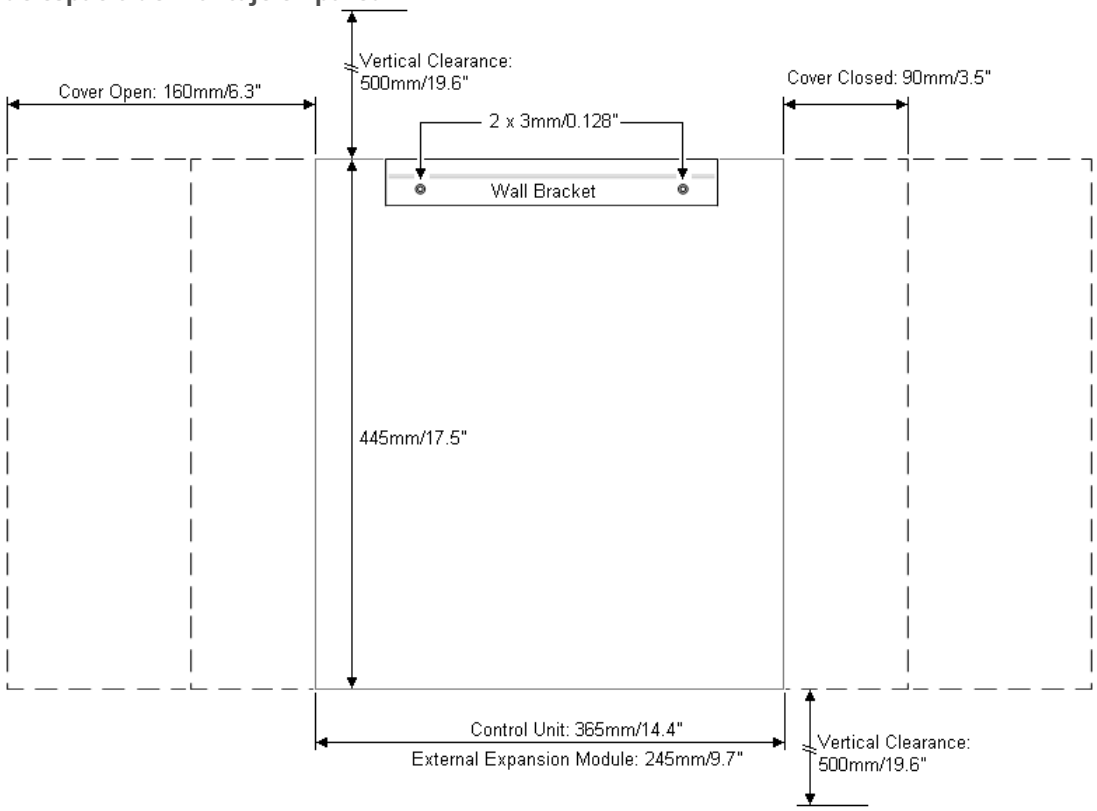
- La superficie de la pared debe ser vertical, plana y libre de vibraciones. No se admite la unión a paredes temporales.
- Solo deben usarse los tornillos proporcionados con el kit de montaje para fijar los soportes a la unidad de control oa los módulos de expansión.
- La instalación debe ser realizada por una persona de servicio.
- Asegúrese de que el sistema se haya apagado y que se haya desconectado la alimentación de todas las unidades. Apague el sistema usando un comando de apagado y luego desconecte la alimentación. No quite simplemente la energía.
- Se requiere una superficie de montaje de madera contrachapada adecuada de al menos 1 m x 1 m x 19 mm (39" x 39" x 0,75"). Si también se va a montar una caja de expansión, se requiere una superficie de montaje de madera contrachapada de al menos 1,2 mx 1,2 mx 19 mm (48" x 48" x 0,75").
- Se debe usar un mínimo de 6 tornillos de cabeza plana de 45 mm de largo y 5 mm/6 mm (1,75" n.° 10/n.° 12) para asegurar la madera contrachapada a los montantes de la pared.
- Se deben usar los tornillos para madera de 20 mm de largo y 4 mm (#8 ¾") para asegurar los soportes a la superficie de montaje de madera contrachapada

El siguiente kit está disponible actualmente:

- **KIT DE MONTAJE EN PARED IPO IP500 V3***(Código SAP 700503160)*
  Este kit se puede utilizar paramontaje en pared y en rack de unidades de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora enrutamiento de cables en la parte delantera y trasera de la unidad. Para unidades de control montadas en la pared, permite orientar las ranuras de la tarjeta base de la unidad de control hacia la izquierda o hacia la derecha.



Requisito de espacio de montaje en pared

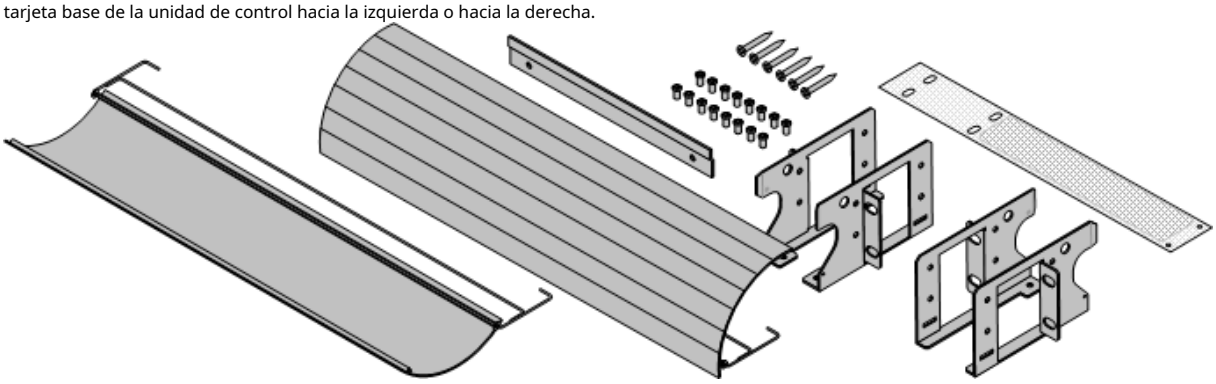


2.2.4 Requisitos de espacio en bastidor

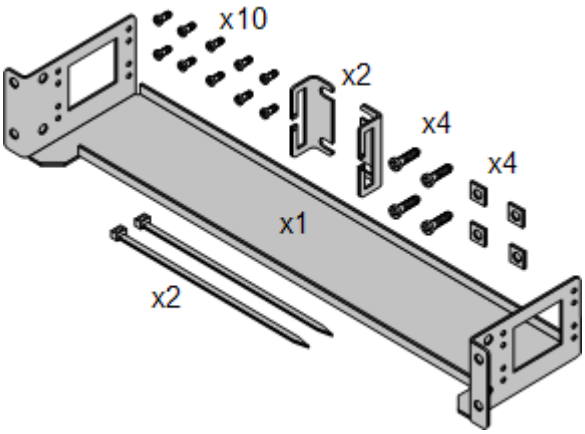
Todas las unidades de control de IP Office y los módulos de expansión externos se pueden montar en rack en sistemas de rack estándar de 19". Cada unidad requiere un espacio de ranura de 2U dentro del rack. El montaje en rack requiere un kit para cada unidad de control y módulo de expansión externo.

Cuando los sistemas se monten en rack, se debe considerar el efecto de las condiciones dentro del gabinete del rack. Por ejemplo, la temperatura del estante puede estar por encima de la temperatura ambiente y el flujo de aire dentro del estante está restringido. losRequisitos medioambientales 51 para las unidades individuales de IP Office siguen siendo aplicables dentro del gabinete del bastidor.

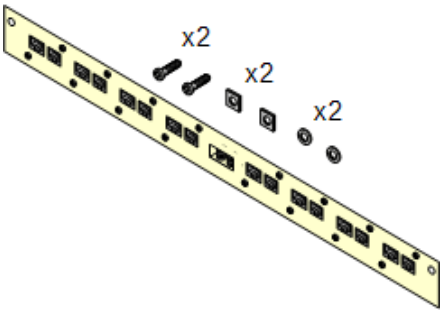
- **KIT DE MONTAJE EN PARED IPO IP500 V3***(Código SAP 700503160)*
  Este kit se puede utilizar paramontaje en pared y en rack de unidades de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora enrutamiento de cables en la parte delantera y trasera de la unidad. Para unidades de control montadas en la pared, permite orientar las ranuras de la tarjeta base de la unidad de control hacia la izquierda o hacia la derecha.



- **KIT DE MONTAJE DE RACK IPO IP500***(Código SAP 700429202)*
  Este kit contiene todos los componentes necesarios para el montaje en rack de una sola unidad de control IP500 V2 o módulo de expansión externo IP500. Esto incluye tornillos para la fijación de los soportes al módulo, pernos para asegurar el módulo en el rack y soportes pasacables.



Kit de montaje en bastidor de caja de barrera

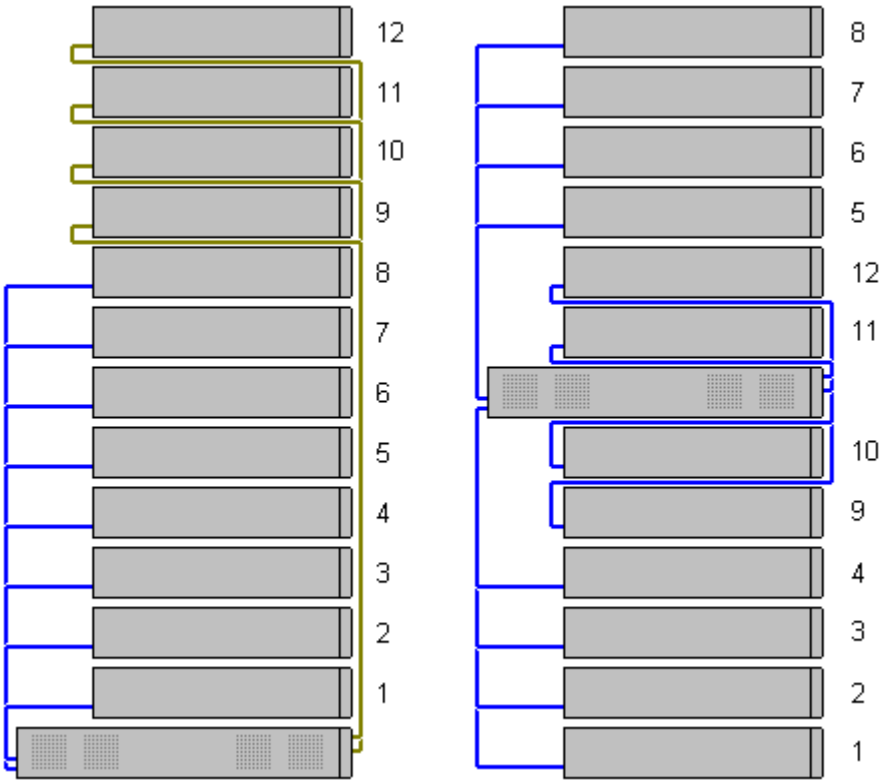


- **Kit de montaje en bastidor de caja de barrera***(SAP 700293905)* Las cajas de barrera se deben utilizar paraextensiones telefónicas analógicas fuera del edificio 36.Este soporte permite montar en rack hasta 8 cajas de barrera de IP Office y simplifica la cantidad de conexiones al punto de protección a tierra en el rack. Este kit debe usarse cuando se usan más de 3 cajas de barrera y admite un máximo de 16 cajas de barrera para un solo módulo de expansión externo.

Posicionamiento del módulo de bastidor

Los puertos de expansión integrales en una unidad de control están ubicados en la parte posterior de la unidad. Se pueden agregar 4 puertos de expansión adicionales al frente de la unidad de control instalando una tarjeta de expansión de 4 puertos IP500.

- Cada módulo de expansión externo se suministra con un cable de interconexión de expansión azul de 1 metro (3'3''). este cable deber utilizarse cuando se conecta a puertos de expansión en la parte trasera de una unidad de control.
- Cuando se conecta a puertos de expansión en una tarjeta de expansión de 4 puertos IP500, se puede usar un cable de interconexión de expansión amarillo de 2 metros (6'6") en lugar del cable azul estándar. Se suministran 4 cables amarillos con la tarjeta de expansión de 4 puertos IP500 tarjeta.



2.3 Herramientas y piezas necesarias

El siguiente es un resumen general de las herramientas requeridas. Se requerirán herramientas y equipos adicionales para el montaje en pared o en bastidor y para diseñar conexiones de cable a tierra adecuadas a los requisitos locales.

Piezas de IP Office

Las piezas mínimas requeridas son:

- oUnidad de control IP500 V2 205
- oTarjeta SD Avaya 208
- oArchivo de licencia PLDS 279
  - El ID de host PLDS utilizado para el archivo de licencia debe coincidir con el que se muestra en los 12 dígitos.**Identificación PLDS**impreso en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra con**FK**o**FK SN**. Para esas tarjetas agregue el prefijo***11***para obtener la identificación PLDS de la tarjeta.
- oEl archivo debe ser apropiado para la versión del software objeto de la licencia.
- oEl archivo debe contener un**Edición esencial**licencia adecuada para la versión de destino de IP Office.

Herramientas necesarias

- oDestornillador de punta plana de 5 mm.
- oDestornillador de estrella.
- oMuñequera antiestática y punto de tierra.
- oCable LAN Ethernet RJ45-RJ45.
- oDestornillador de cabeza cruzada M4.
- oHerramientas adecuadas para engarzar una pala de cable.
- oSi se trata de montaje en pared, taladros y herramientas para accesorios de montaje en pared.

Administracion del sistema

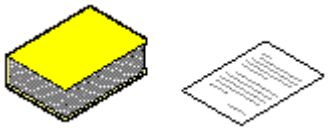
- oPC con Windows con:
  - oPaquete de administración de IP Office instalado 64.
  - oPuerto LAN Ethernet RJ45.
  - oLector de tarjetas SD.

Piezas adicionales requeridas

Además del equipo de IP Office que se puede solicitar, se requerirán los siguientes artículos.

- oCable de cobre sólido de 14 AWG para conexión a tierra de unidades de control y módulos de expansión.
- oManguito de cable que cumple con los requisitos del regulador local para cables de tierra. Típicamente verde para una tierra funcional y verde/amarillo para una tierra protectora.
- oSi se trata de un montaje en la pared, accesorios y accesorios adicionales adecuados para el tipo de pared y el kit de montaje que se está utilizando.
- oBridas y etiquetas para ordenar e identificar cables.

2.4 Documentación



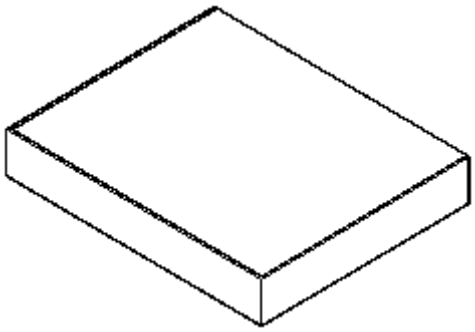
Asegúrese de haber leído este manual en su totalidad antes de comenzar la instalación. Incluya también la documentación de instalación de cualquier otro equipo y aplicación que se instale como parte del sistema IP Office.

La documentación de IP Office está disponible en los siguientes sitios web.

- **Soporte de Avaya** *(http://soporte.avaya.com)*
  Contiene documentación y otros materiales de soporte para los productos de Avaya, incluido IP Office. Las copias de las imágenes del CD de IP Office están disponibles en este sitio y los archivos .bin del software principal actualizado.
- **Base de conocimientos de IP Office de Avaya** *(https://ipofficekb.avaya.com)* Acceso a una versión en línea actualizada regularmente de las guías de usuario y manuales técnicos de IP Office.

- **!Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín técnico de IP Office relacionado con la versión del software de IP Office que pretende instalar. El boletín contiene información importante que puede no haber sido incluida en este manual. Los boletines técnicos de IP Office están disponibles en elSoporte de Avaya sitio web*(http://soporte.avaya.com)*.

2.5 Desembalaje



Utilice el siguiente procedimiento cuando desembale cualquier equipo suministrado por Avaya o un revendedor o distribuidor de Avaya.

Informacion requerida

- o**Lista de verificación del equipo**.
  Una lista de verificación de instalación de las piezas y el equipo solicitado para la instalación.

Procedimiento

1. o**Compruebe si hay daños en el embalaje**
   Antes de desembalar cualquier equipo, verifique que no haya signos de daños que puedan haber ocurrido durante el tránsito. Si existe algún daño, comuníquelo a la atención del transportista.
2. o**Compruebe que se han entregado las piezas correctas**
   Verifique todas las cajas con el albarán y asegúrese de tener los artículos correctos. Informe cualquier error u omisión al proveedor del equipo.
3. o**Conserve todo el embalaje y la documentación**
   Al desembalar el equipo, conserve todo el material de embalaje. Las devoluciones por falla solo se aceptan si se vuelven a empaquetar en el embalaje original. Si se realiza una instalación por etapas, el embalaje original también ayuda cuando se vuelve a embalar el equipo para trasladarlo al sitio de instalación final.
4. o**Asegúrese de que se observen las medidas de protección antiestática**
   Asegúrese de observar las medidas de protección antiestática en todo momento al manipular equipos con tableros de circuitos eléctricos expuestos.
5. o**Comprobar todas las piezas**
   Inspeccione visualmente cada elemento y verifique que se haya incluido toda la documentación necesaria y elementos accesorios. Informe cualquier error u omisión al distribuidor que suministró el equipo.
6. o**Consulta toda la documentación**
   Asegúrese de leer y conservar toda la documentación incluida con el equipo.

Capítulo 3.

Instalación del software del administrador

3. Instalación del software del administrador

Para instalar y mantener un sistema IP Office, debe estar familiarizado con el uso de las siguientes aplicaciones.

- **Gerente de IP Office**
  Esta es una aplicación basada en Windows. IP Office Manager se utiliza para accedertodos partes de la configuración de IP Office. Se pueden definir diferentes niveles de acceso para controlar qué partes de la configuración puede ver y modificar el usuario. IP Office Manager también se utiliza para actualizar los archivos de software utilizados por un sistema IP Office.

  - **Versión del administrador de IP Office**
    Es importante descargar e instalar la versión correcta del paquete de administración de IP Office, incluido IP Office Manager.

    - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincida con la versión de IP Office requerida en el sistema. Esto establece la versión del software cargado cuandorecreando la tarjeta SD del sistema 75.
    - Para el mantenimiento del sistema, la versión de IP Office Manager utilizada establece la versión del software cargado en un sistema cuandoactualizando el sistema 180.
    - Para la configuración del sistema, IP Office Manager es compatible con versiones anteriores. IP Office Manager versión 11.0 es compatible con versiones anteriores para configurar sistemas que ejecutan software a partir de la versión 6.0 de IP Office y en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión superior del software.

      - **Admin Lite no compatible**
        Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).

- **Administrador web de IP Office**
  Después de la instalación, también se puede acceder a la configuración de un sistema IP500 V2 a través del navegador web usando las mismas cuentas de usuario de servicio que se usan para IP Office Manager.

- **Aplicación de estado del sistema**
  System Status Application (SSA) es una herramienta de generación de informes que proporciona una amplia gama de información sobre el estado actual de un sistema IP Office. Informa los recursos y componentes disponibles dentro del sistema y los detalles de las llamadas en curso. Se muestran los detalles de las alarmas actuales e históricas. Cuando sea necesario para la escalada de diagnóstico, SSA puede tomar una imagen instantánea del estado del sistema IP Office, incluida una copia de su configuración actual.

- **Supervisar (Supervisión del sistema)**
  System Monitor es una herramienta que puede mostrar la actividad en el sistema IP Office con gran detalle. Como consecuencia, la interpretación de trazas requiere un alto nivel de conocimiento de protocolos de datos y telefonía. Sin embargo, todos los instaladores y mantenedores de IP Office deben saber cómo ejecutar Monitor para capturar un seguimiento, ya que Avaya puede solicitar esos seguimientos para investigar problemas de soporte.

3.1 Descarga del software

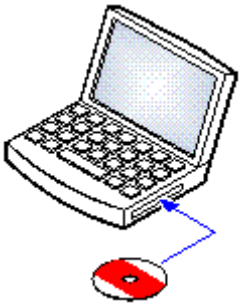
El paquete de software de administración de IP Office está disponible comoDVD disponible para pedidos 42.Sin embargo, el software también se puede descargar desde el sitio web de soporte de Avaya (http://soporte.avaya.com).

- **Versión del administrador de IP Office**
  Es importante descargar e instalar la versión correcta del paquete de administración de IP Office, incluido IP Office Manager.
  - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincida con la versión de IP Office requerida en el sistema. Esto establece la versión del software cargado cuandorecreando la tarjeta SD del sistema 75.
  - Para el mantenimiento del sistema, la versión de IP Office Manager utilizada establece la versión del software cargado en un sistema cuandoactualizando el sistema 180.
  - Para la configuración del sistema, IP Office Manager es compatible con versiones anteriores. IP Office Manager versión 11.0 es compatible con versiones anteriores para configurar sistemas que ejecutan software a partir de la versión 6.0 de IP Office y en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión superior del software.
    - **Admin Lite no compatible**
      Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).
- **!Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín técnico de IP Office relacionado con la versión del software de IP Office que pretende instalar. El boletín contiene información importante que puede no haber sido incluida en este manual. Los boletines técnicos de IP Office están disponibles en elSoporte de Avaya sitio web*(http://soporte.avaya.com)*.

Para descargar el software de Avaya:

1. Navegar a***http://soporte.avaya.com***e inicie sesión.
2. Seleccione**Soporte por producto**y haga clic**Descargas**.
3. Entrar***Oficina de PI***en el**Introduzca el nombre del producto**y seleccione la opción correspondiente de la lista que se muestra.
4. Usa el**Elija Liberar**desplegable para seleccionar la versión de IP Office necesaria.
5. Haga clic en**Descargas**. La página enumera las descargas disponibles más recientes.
6. Haga clic en**Ver descargas**para la lista completa de descargas.
7. Seleccione el paquete de software requerido para descargar.
8. La página que se muestra en una nueva pestaña o ventana detalla las opciones para descargar ese software. Para la instalación de IP500, descargue el paquete de administración completo, no los archivos binarios separados o los paquetes de descarga de Admin Lite.
9. Descargue también los documentos enumerados en el**DOCUMENTOS RELACIONADOS**encabezado si se muestra.

3.2 Instalación de las aplicaciones del administrador



El paquete de administración de IP Office consta de una serie de aplicaciones para instaladores y mantenedores de IP Office.

- o**Monitoreo del sistema**-*Instalar* ✓
- o**Gerente de IP Office**-*Instalar* ✓
- o**Aplicación de estado del sistema**-*Instalar* ✓

Requisitos

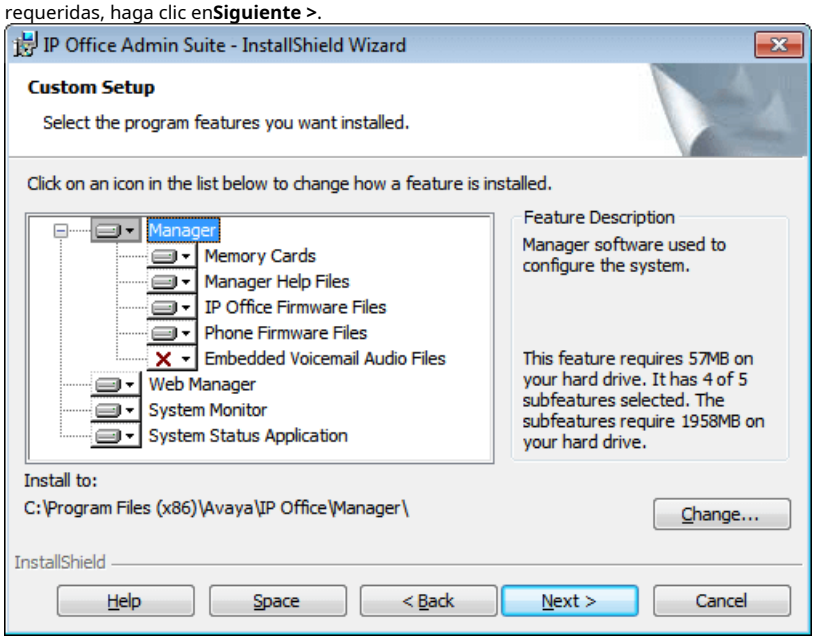
- o**Juego de DVD para usuarios/administradores de la versión 11.0 de IP Office (2) (700513659)**
  Como alternativa, el conjunto de aplicaciones de administrador de IP Office se puede descargar desdeSitio web de soporte de Avaya *(http://soporte.avaya.com).*

- o**Requisitos de PC con Windows**
  Las especificaciones a continuación son los requisitos mínimos para IP Office Manager. Si se van a instalar otras aplicaciones en la PC, también se deben cumplir sus requisitos individuales. Las versiones compatibles de Windows se enumeran en laSistemas operativos 261sección.

  - **Gerente estándar:**CPU Core i3, 4 GB de RAM, sistema operativo de 32/64 bits
  - **Administrador de la edición del servidor:**CPU Core i5, 6 GB de RAM, sistema operativo de 32/64 bits
  - **Administrador de selección de Server Edition:**CPU Core i5, 8 GB de RAM, sistema operativo de 64 bits
  - IP Office Manager solo es compatible con Windows configurado para mostrar el tamaño de fuente al 100 %.

Para instalar las aplicaciones de administrador de IP Office:

1. Usando el**Añadir o eliminar programas**opción en el Panel de control de Windows, verifique que la PC aún no tenga instalada una versión de la suite IP Office Admin.
   - Si la respuesta es 'sí' y el paquete es una versión anterior a IP Office 3.2, elimine el paquete de administración de IP Office existente a través de Agregar o quitar programas.
   - Si la suite existente es IP Office 3.2 o superior, es posible actualizar sin eliminar la instalación anterior.
2. Inserte el DVD de aplicaciones de administrador de IP Office. Seleccione la opción para el paquete de administración de IP Office. Una ventana de carpeta mostrará los archivos de instalación de la suite de administración.
3. Haga clic derecho en setup.exe y seleccione**Ejecutar como administrador**.
4. Seleccione el idioma para el proceso de instalación. Esto no afecta el idioma que utiliza IP Office Manager cuando se ejecuta. Hacer clic **Siguiente >**.
5. Haga clic en**Siguiente >**.
6. Si está de acuerdo, haga clic en**Acepto los términos del contrato de licencia**y luego haga clic**Siguiente >**.
7. Si es necesario, cambie el destino en el que se deben instalar las aplicaciones. Le recomendamos que acepte el destino predeterminado. Hacer clic**Siguiente >**.
8. La siguiente pantalla se utiliza para seleccionar qué aplicaciones deben instalarse. Al hacer clic en cada uno, se mostrará una descripción de la aplicación. Haga clic en el junto a cada aplicación para cambiar la selección de instalación. Cuando haya seleccionado las instalaciones requeridas, haga clic en**Siguiente >**.



- **Gerente**
  Instale la aplicación IP Office Manager básica necesaria para editar las configuraciones del sistema, además de cualquiera de las siguientes:
  - **Tarjetas de memoria**
    Instale los archivos necesarios para recrear una tarjeta SD de Avaya System.
  - **Archivos de ayuda del administrador**
    Instale los archivos de ayuda de la aplicación en todos los idiomas disponibles. Si no se selecciona, solo se instala el inglés.
  - **Archivos de firmware de IP Office**
    Instale los archivos de firmware utilizados por los módulos de expansión externos de IP Office. Estos archivos solo son necesarios si se va a usar IP Office Manager para actualizaciones del sistema.
  - **Archivos de firmware del teléfono**
    Instale los archivos de firmware utilizados por los diversos teléfonos IP de Avaya compatibles con IP Office. Estos archivos solo son necesarios si se va a usar IP Office Manager para actualizaciones del sistema.
  - **Archivos de audio de correo de voz integrados**
    Instale las indicaciones del correo de voz que utiliza Embedded Voicemail. Estos archivos solo son necesarios si se va a usar IP Office Manager para actualizaciones del sistema.
- **Administrador web**
  Instale una copia de los archivos que deben cargarse en un sistema para ejecutar IP Office Web Manager.
- **Monitoreo del sistema**
  Instale la aplicación Monitor del sistema.

- **Aplicación de estado del sistema**
  Instale la aplicación de aplicación de estado del sistema.

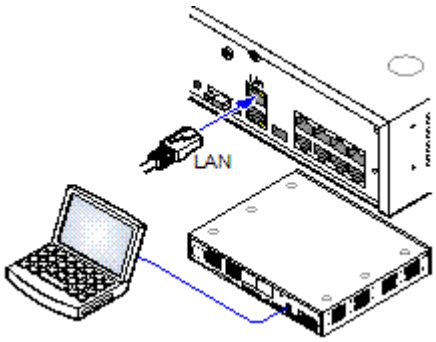
9. Asegúrese de que como mínimo**Monitoreo del sistema**y**Gerente**son seleccionados. Hacer clic**Siguiente >**.

10. Haga clic en**Instalar**. Si la instalación requiere otros componentes como Windows .Net, siga las indicaciones para instalar esos componentes.

11. Si se le solicita, reinicie la PC.

12. Haga clic en**Finalizar**.

3.3 Conexión del PC del instalador



Durante la instalación, se recomienda iniciar la unidad de control de IP Office sin que esté conectada a ninguna red. Eso garantiza que IP Office utilice de manera predeterminada un conjunto conocido de configuraciones de direcciones IP.

Si IP Office se inicia conectado a una red con un servidor DHCP, la PC de programación deberá estar conectada a la misma red como cliente DHCP o con una dirección IP válida para esa red.

Esta sección cubre la conexión de su PC de instalación directamente a la unidad de control de IP Office.

Requisitos

- o**PC de administración de IP Office**
  Una PC con Windows con elPaquete de aplicaciones de administrador de IP Office instalado 64.
- o**Cable de LAN**

Para conectarse directamente a un sistema IP Office predeterminado:

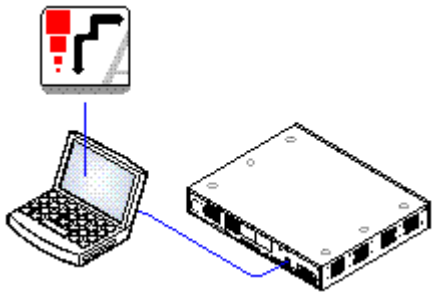
1. La dirección predeterminada para el puerto LAN de la unidad de control de IP Office es 192.168.42.1/255.255.255.0. Para conectar directamente una PC, cambie las propiedades de TCP/IP para el puerto LAN de la PC a lo siguiente:

Dirección IP fija	192.168.42.203
Máscara de subred	255.255.255.0
Puerta de enlace predeterminada	192.168.42.1.

   - Si bien se puede configurar la PC para que sea un cliente DHCP, no se recomienda para realizar funciones más avanzadas, como actualizaciones de firmware.

2. Conecte el cable LAN del puerto LAN de la PC al puerto LAN de la unidad de control de IP Office.
3. Verifique que la lámpara LED naranja en el puerto LAN de IP Office esté encendida. El LED verde también puede estar parpadeando, ya que indica tráfico a través de la conexión LAN.
4. Para probar la conexión antes de ejecutar IP Office Manager o System Status Application:
   - Seleccione**Inicio | Correr**y entrar***cmd***.
   - En la ventana de comando que aparece, ingrese ping**192.168.42.1**. Los resultados deberían mostrar una cantidad de respuestas de ping de IP Office. Esto confirma la comunicación básica entre la PC de IP Office Manager y IP Office.
   - Si no hay respuestas de ping, ingrese**ipconfig**. Los resultados deben enumerar la configuración de la dirección IP de la PC con IP Office Manager como se requiere anteriormente. Si entran**salida**y compruebe la conexión del cable.
5. Ya puedes empezarGerente de IP Office 68,Estado del sistema 69oMonitoreo del sistema 70.

3.4 Inicio de IP Office Manager



IP Office Manager se utiliza para acceder a todas las partes de la configuración de IP Office. IP Office Manager también se puede utilizar para actualizar los archivos de software utilizados por un sistema IP Office.

- **Versión del administrador de IP Office**
  Es importante descargar e instalar la versión correcta del paquete de administración de IP Office, incluido IP Office Manager.
  - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincida con la versión de IP Office requerida en el sistema. Esto establece la versión del software cargado cuandorecreando la tarjeta SD del sistema 75.
  - Para el mantenimiento del sistema, la versión de IP Office Manager utilizada establece la versión del software cargado en un sistema cuando actualizando el sistema 180.
  - Para la configuración del sistema, IP Office Manager es compatible con versiones anteriores. IP Office Manager versión 11.0 es compatible con versiones anteriores para configurar sistemas que ejecutan software a partir de la versión 6.0 de IP Office y en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión superior del software.

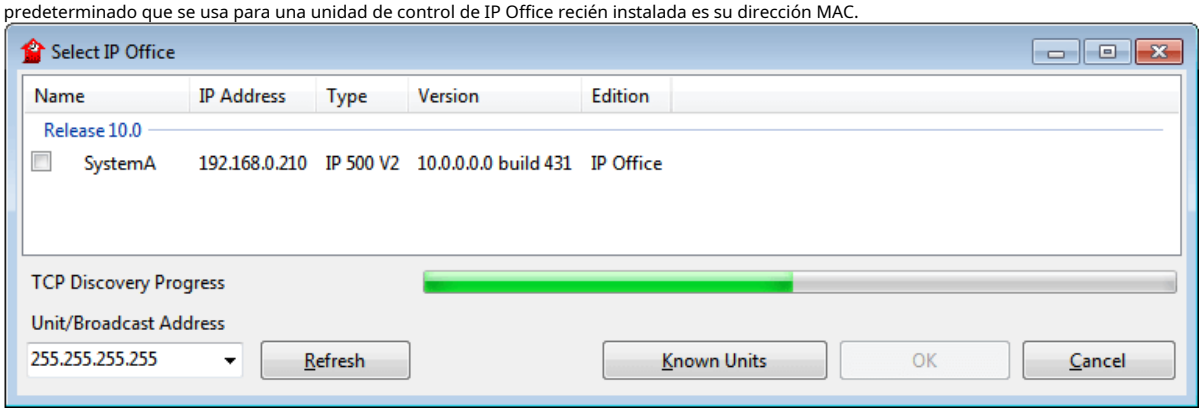
- **Admin Lite no compatible**
  Tenga en cuenta que IP Office Manager instalado desde el**AdminLite** El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).

Requisitos

- o**PC de administración de IP Office**
  Una PC con Windows con elPaquete de aplicaciones de administrador de IP Office instalado 64
- o**Cable de LAN**

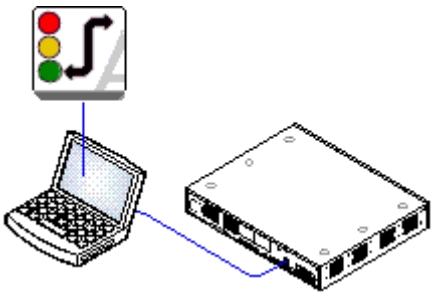
Para iniciar sesión en un sistema mediante IP Office Manager:

1. Seleccione**Inicio | Todos los programas | Oficina de PI | Gerente**.
2. Si la PC tiene instalado un software de firewall, es posible que se le pregunte si desea permitir que este programa acceda a la red. Seleccione**Sí**o**OK**.
3. Seleccione**Archivo | Configuración abierta**desde la barra de menú.
4. El**Seleccione IP Office**aparece la ventana. Después de unos segundos, debería mostrar la unidad de control de IP Office. El nombre para mostrar predeterminado que se usa para una unidad de control de IP Office recién instalada es su dirección MAC.



   - Si no se encuentra el sistema requerido, se puede cambiar la dirección utilizada para la búsqueda. Ingrese o seleccione la dirección requerida en el**Unidad/Dirección de transmisión**campo y luego haga clic en**Actualizar**para realizar una nueva búsqueda.
5. Haga clic en la casilla de verificación junto al sistema y luego haga clic en**OK**.
6. Se muestra la solicitud de nombre y contraseña. El nombre y la contraseña deben coincidir con uno de los configurados a través de la configuración de seguridad del sistema.

3.5 Inicio de la aplicación de estado del sistema

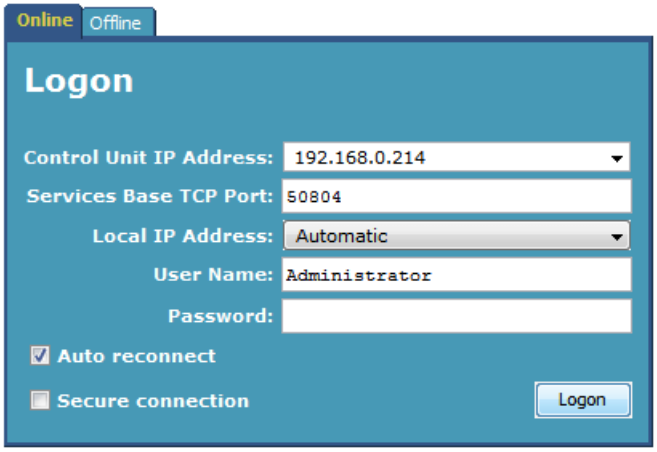


System Status Application (SSA) es una herramienta de generación de informes que proporciona una amplia variedad de información sobre el estado actual de un sistema IP Office. Puede informar los recursos y componentes disponibles dentro del sistema y los detalles de las llamadas en curso. Se registran los detalles del número de alarmas y la fecha y hora de las alarmas más recientes.

Cuando se requiere para la escalada de diagnóstico, SSA puede tomar una imagen instantánea del estado del sistema IP Office, incluida una copia de su configuración actual. El uso de SSA requiere un nombre de usuario y una contraseña de servicio de IP Office que se haya configurado para acceder al estado del sistema en la configuración de seguridad de IP Office.

Para iniciar Estado del sistema:

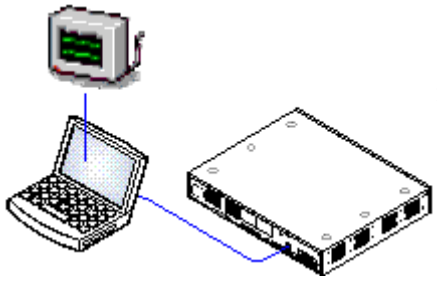
1. Hay varios métodos que se pueden utilizar para iniciar la aplicación de estado del sistema.
   - En una PC dondeEl estado del sistema ha sido instalado 64,Seleccione**Inicio | Programas | Oficina de PI | Estado del sistema**.
   - Si IP Office Manager también está instalado en la PC y se está ejecutando, seleccione**Archivo | Avanzado | Estado del sistema**.
   - Para las unidades de control IP500 V2, inicie un navegador web e ingrese la dirección IP de la unidad de control. Seleccione el enlace para el**Estado del sistema**.
   - Si ya ejecuta IP Office Web Manager, seleccione**Vigilancia**y haga clic**Estado del sistema**.
2. Una vez que System Status se haya iniciado, solicitará los detalles del sistema IP Office al que desea conectarse.



- **Dirección IP de la unidad de control**
  Ingrese la dirección IP de la interfaz LAN de las unidades de control de IP Office o utilice el menú desplegable para seleccionar una dirección utilizada anteriormente.
- **Puerto TCP base de servicios**
  Esto debe coincidir con la configuración del puerto TCP base de servicios del sistema IP Office, establecida en la configuración de seguridad de ese sistema. El valor predeterminado es 50804.
- **Dirección IP local**
  Si la PC tiene más de una dirección IP asignada a su tarjeta de red o varias tarjetas de red, se puede seleccionar la dirección a usar si es necesario.
- **Usuario Contraseña**
  Introduzca un nombre de usuario y una contraseña que se hayan proporcionado para el uso de System Status. De forma predeterminada, es el mismo nombre de usuario y contraseña que se usa con IP Office Manager. Este debe ser el nombre de un usuario del servicio de IP Office que se haya configurado para acceder al estado del sistema en la configuración de seguridad de IP Office.
- **Reconexión automática**
  Si se selecciona, System Status intentará volver a conectarse usando la misma configuración si se pierde la conexión con IP Office.
- **Conexión segura**
  Utilice una conexión TLS cifrada al sistema. Si se selecciona y el sistema no está configurado para acceso seguro, System Status Application ofrece volver a intentar la conexión utilizando un acceso no seguro.

3. Ingrese los detalles requeridos para IP Office y haga clic en**Iniciar sesión**.

3.6 Inicio del Monitor del sistema



System Monitor es una herramienta que puede mostrar toda la actividad en el sistema IP Office con gran detalle. Como consecuencia, la interpretación de las trazas de Monitor requiere un alto nivel de conocimiento del protocolo de datos y telefonía. Sin embargo, todos los instaladores y mantenedores de IP Office deben comprender cómo ejecutar Monitor cuando sea necesario, ya que Avaya puede solicitar copias de los seguimientos de Monitor para resolver problemas de soporte.

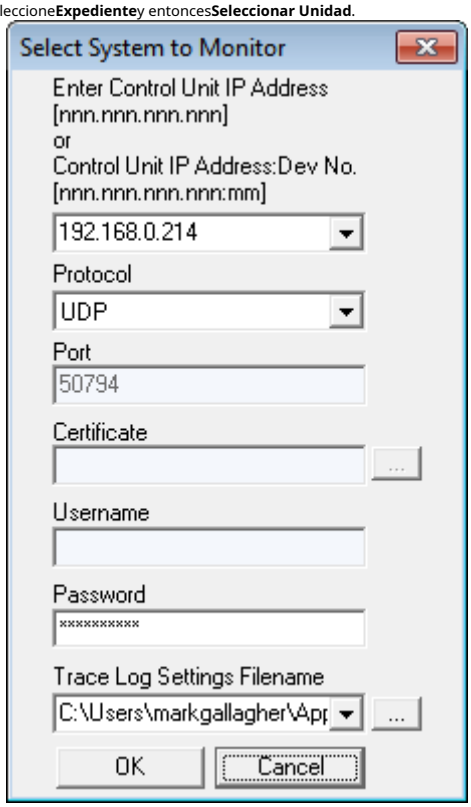
Requisitos

- o**PC de administración de IP Office**
  Una PC con Windows con el[Paquete de aplicaciones de administrador de IP Office instalado](#) 64.
- o**Cable de LAN**

1. Para iniciar el Monitor del sistema:

1. Seleccione**Inicio | Programas | Oficina de PI | Monitoreo del sistema**.

2. Seleccione**Expediente**y entonces**Seleccionar Unidad**.



3. Introduzca el**Dirección IP**y**Clave**del sistema que desea monitorear.

   - **Protocolo**
     El valor por defecto**Protocolo**,es***UDP***. La aplicación también admite conexiones TCP, HTTP y HTTPS. Para obtener detalles completos, consulte el manual "Uso de IP Office System Monitor".
   - **¿Qué contraseña?**
     Usando IP Office Manager, es posible configurar un**Supervisar contraseña**. Si el sistema no tiene un **Supervisar contraseña** configurado, System Monitor usa el sistema**Contraseña del sistema**. los**Supervisar contraseña**y **Contraseña del sistema**se establecen dentro de los parámetros de configuración de seguridad de un sistema.

4. Si desea que System Monitor comience con un conjunto de opciones de seguimiento previamente guardado, use el**Nombre de archivo de configuración de registro de seguimiento**botón Examinar para seleccionar el archivo de configuración de opciones de seguimiento.

5. Haga clic en**OK**.

3.7 Inicio de IP Office Web Manager

El acceso del navegador web al sistema se puede usar para ejecutar IP Office Web Manager. Ingrese la dirección IP del sistema y luego seleccione el **Administrador web de IP Office**Enlace. Para obtener detalles completos, consulte el Manual de IP Office Web Manager.

Para usar IP Office Web Manager, los archivos de la aplicación deben estar presentes en la tarjeta SD del sistema. Esto se hace seleccionando la opción para incluir los archivos del administrador web cuandorecreando la tarjeta SD 75.

Avaya es compatible con los siguientes navegadores para IP Office Web Manager:

- **Microsoft Internet Explorer 10**y**11**.
- **Borde de Microsoft**
- **Mozilla Firefox**
- **Google Chrome**
- **Safari**

Para iniciar sesión en un sistema mediante IP Office Web Manager:

1. Ingrese la dirección IP del sistema IP Office. En el menú que aparece, haga clic en**Administrador web de IP Office**.
   Alternativamente, ingrese*https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
2. Aparece el menú de inicio de sesión de IP Office Web Manager.

3. Introduzca el nombre y la contraseña para la administración del sistema. El nombre y la contraseña predeterminados son ambos ***Administrador***.

   - **Modo offline**
     Algunos cambios de configuración solo se pueden aplicar a un sistema mediante un reinicio, por ejemplo, cambiar la configuración de línea. Para editar esos ajustes, debe seleccionar**Modo offline**. En ese modo, la parte superior de la ventana del navegador muestra una**Guardar en IP Office**enlace que, al hacer clic, muestra un menú para reiniciar el sistema.

     - También puede cambiar al modo fuera de línea después de haber iniciado sesión haciendo clic en y seleccionando**Modo offline**.

4. Haga clic en**Acceso**.

   una. Se le solicitará que cambie cualquier contraseña predeterminada.

   b. Para un nuevo sistema, elmenú de configuración inicial 1034aparece

Capítulo 4.

Preparación de la tarjeta SD del sistema

4. Preparación de la tarjeta SD del sistema

Las nuevas unidades de control IP500 V2 se suministran sin firmware ni configuración instalada. Cuando se enciende por primera vez, la unidad de control carga e instala el firmware necesario desde Avaya**SD del sistema** 208tarjeta instalada en la unidad de control. Luego crea una configuración predeterminada que coincide con las tarjetas físicas ya instaladas en la unidad de control y cualquier módulo de expansión externo que ya esté conectado a ella.

Puede realizar una serie de acciones adicionales antes de instalar la tarjeta SD del sistema para preconfigurar el sistema. Estos pueden acelerar en gran medida la instalación física en el sitio del cliente, ya que todos se pueden hacer con anticipación.

- **Actualice el firmware de la tarjeta** 75
- **Agregar un archivo de configuración** 78
- **Agregar un archivo de licencia** 78
- **Adición de certificados de seguridad** 78
- **Agregar un archivo de imagen de protector de pantalla 9600** 79
- **Agregar archivos de música en espera** 79

Las acciones adicionales que se pueden realizar en las tarjetas SD se detallan en elGestión de tarjetas SD 142sección.

4.1 Actualice el firmware de la tarjeta

Puede usar IP Office Manager para actualizar el conjunto de archivos en una tarjeta SD del sistema para que coincidan con los esperados para la versión particular de IP Office. Esto se puede usar para actualizar la tarjeta de un sistema existente o para preparar la tarjeta para un nuevo sistema.

IP Office Manager actualiza la tarjeta con los archivos de firmware binarios para la unidad de control, los módulos de expansión externos y los teléfonos. También incluye los archivos de aviso para la operación del correo de voz incorporado y una opción para los archivos de la aplicación del administrador web.

Los archivos existentes, como la configuración del sistema, el archivo de licencia PLDS y los mensajes y saludos de correo de voz integrados, se conservan.

- Para que la tarjeta se utilice en una unidad de control**SD del sistema**ranura para tarjetadebe ser una tarjeta SD del sistema Avaya . La tarjeta debe formatearse correctamente (eso se puede hacer con IP Office Manager); sin embargo, no es necesario volver a formatear una tarjeta en funcionamiento antes de usar recrear para actualizar el contenido de la tarjeta.
- El origen de los archivos copiados a la tarjeta SD son las subcarpetas del***Tarjetas de memoria**carpeta debajo de las aplicaciones del administrador**Directorio de trabajo**(normalmente***C:\Archivos de programa (x86)\Avaya\IP Office\Manager***). Sin embargo, si el**Directorio de trabajo**se cambia a una ubicación sin un conjunto apropiado de***Tarjetas de memoria**subcarpetas, el conjunto de archivos necesario no se copiará en la tarjeta SD.

    - **!ADVERTENCIA: Instalación de unidades de control PCS14 y anteriores**
      PC 296 o unidades inferiores deben instalar primero la versión 8.1(65) (o superior 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1. Se debe tener cuidado para asegurarse de que no se realicen llamadas antes de la actualización a la Versión 10.0, de lo contrario, el sistema requerirá una licencia de actualización 10.0 a pesar de ser "nuevo". El PCS de la unidad de control está impreso en la etiqueta en la parte posterior de la unidad de control.

Configuración del nivel de software del sistema inicial

Cuando la unidad de control hace su primera llamada, la versión del software que está ejecutando se escribe en un registro permanente en la unidad de control. Este se convierte en el nivel básico de la unidad de control al considerar los requisitos futuros para licencias de actualización, etc. Por lo tanto, para un sistema nuevo es importante que actualice la tarjeta SD del sistema a la versión de software requerida antes de iniciar el sistema.

Determinación del nivel de software de la tarjeta SD del sistema

En la tarjeta SD, en el***sistema/primario***carpeta, localice y abra la carpeta***listaarchivos.txt***expediente. La sección de encabezado al comienzo del archivo termina con la versión del conjunto de archivos previamente copiados en la tarjeta. El resto del archivo enumera los archivos reales.

Para actualizar/recrear una tarjeta SD del sistema

1. Una vez iniciado, no interrumpa este proceso, por ejemplo, retirando la tarjeta SD. Este proceso dura aproximadamente 20 minutos.
2. Inserte la tarjeta SD en un lector de tarjetas en la PC IP Office Manager.
3. Usando IP Office Manager, seleccione**Archivo | Avanzado | Recrear la tarjeta SD de IP Office**.
4. Seleccione**Ley A de IP Office**o**Ley U de IP Office**. Esta selección afecta la forma en que los sistemas IP Office funcionan cuando están predeterminados con esta tarjeta presente en su**SD del sistema**ranura para tarjetas.
5. Busque la ubicación de la tarjeta y haga clic en**OK**.
6. IP Office Manager le preguntará si desea incluir archivos de Avaya IP Office Web Manager como parte del proceso de recreación. Esos archivos son necesarios si desea ejecutarAdministrador web de IP Office 71para administrar el sistema IP Office en el que está cargada la tarjeta o si desea utilizarinducción 138.
7. IP Office Manager comenzará a crear carpetas en la tarjeta SD y copiará los archivos necesarios en esas carpetas. Este proceso tomará aproximadamente 20 minutos.
8. No extraiga la tarjeta SD durante el proceso. Espere hasta que IP Office Manager muestre un mensaje.

4.2 Creación de un archivo de configuración fuera de línea

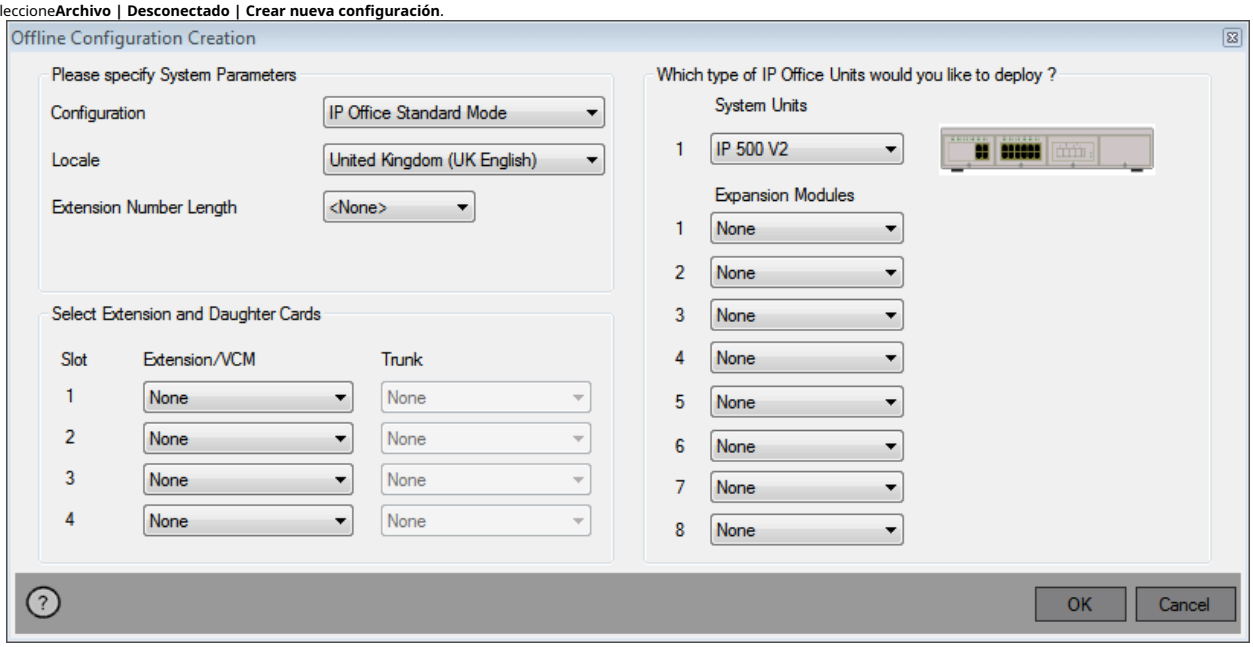
IP Office Manager se puede usar para crear una nueva configuración sin conectarse a un sistema IP Office. Durante el proceso, puede especificar la configuración regional del sistema, qué tipo de tarjetas troncales utiliza y qué tipo de unidad de control y módulos de expansión incluir.

Esto permite la creación de una configuración antes de la instalación del sistema. El archivo de configuración se puede colocar en la tarjeta SD del sistema antes de instalarlo en el sistema. De lo contrario, la configuración se puede cargar en el sistema después de la instalación inicial del sistema.

- La configuración creada debe coincidir con el equipo físico en el sistema IP Office en el que se carga. De lo contrario, es posible que el sistema IP Office se reinicie y experimente otros problemas.

Para crear un archivo de configuración sin conexión

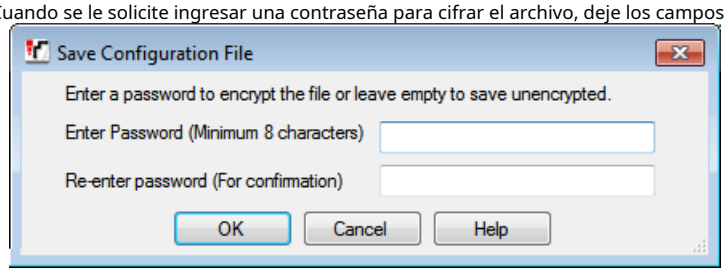
1. Inicie IP Office Manager sin configuración cargada en IP Office Manager
2. Seleccione**Archivo | Desconectado | Crear nueva configuración**.



3. Seleccione el tipo de configuración que desea crear. El equipo y la configuración están restringidos a los admitidos en el modo seleccionado.
4. Cuando haya terminado, haga clic en**OK**.
5. IP Office Manager crea y carga la configuración.
6. Edite la configuración para que coincida con los requisitos del cliente. Esto puede incluir[importar información de archivos CSV preparados previamente](#) 77

   - Tenga en cuenta que, dado que esta configuración se realiza sin conexión y sin licencia, puede configurar funciones que pueden dejar de ser compatibles una vez que la configuración se cargue en el sistema en vivo.

7. Cuando termine, seleccione**Archivo | Guardar configuración como**.
8. Cuando se le solicite ingresar una contraseña para cifrar el archivo, deje los campos en blanco y haga clic en**OK**.



4.3 Configuración de importación y exportación

IP Office Manager puede importar ajustes de configuración creados en otro lugar. Esto puede ser útil al configurar un nuevo sistema o compartir configuraciones comunes, como un directorio entre sistemas. Los ajustes se importan y exportan en dos formatos:

- **Archivos de texto de variables separadas por comas (.csv)**
  Estos son archivos de texto sin formato. Estos archivos se pueden crear y editar utilizando programas como WordPad o Excel. El formato es CSV usando comas como separador de campo, sin delimitadores de texto y sin fila de encabezado. La forma más sencilla de verificar el formato requerido para un archivo CSV antes de importarlo es exportar y estudiar la configuración de un sistema existente.

Nombre del archivo	Campos en Orden	notas
Directorio	*Nombre, Número.*	
Grupo de caza	*Nombre, Extensión, Grupo, Búsqueda, Giratorio, Inactivo, Cola activada, Correo de voz activado, Difusión, Correo electrónico de correo de voz.*	Además de Nombre, Extensión y Correo electrónico de correo de voz, los campos usan un valor de 1 o 0 para activar o desactivar.
Licencia	*Licencia, clave de licencia*	El campo Licencia es solo para información y se ignora durante la importación.
Código corto	*Código, Número de teléfono, Característica.*	
Usuario	*Nombre, Extensión, Restricciones/Derechos de usuario, Correo electrónico de correo de voz.*	
Configuración	El formato de este CSV es demasiado complejo para ser descrito. Es una exportación completa de todos los ajustes de configuración del sistema IP Office. Este formato de archivo solo debe usarse para exportar e importar entre sistemas y no para ninguna edición fuera de línea.	

- **Codificación de caracteres UTF-8**
  IP Office Manager importa y exporta archivos CSV mediante la codificación de caracteres UTF-8, que utiliza un byte doble para admitir caracteres con marcas diacríticas como ä. Otras aplicaciones, como Excel, pueden, dependiendo de la configuración de la PC del usuario, usar una codificación diferente que hará que dichos caracteres se eliminen o dañen. Se debe tener cuidado para asegurarse de que cualquier herramienta utilizada para crear o editar el CSV admita todos los caracteres esperados y utilice el formato UTF-8.

  - **Importar a Manager desde Excel**
    Desde Excel guarde el archivo como .csv. Este archivo utilizará la codificación de caracteres ANSI. Abra el archivo en el Bloc de notas y use el **Guardar como**opción para cambiar el nombre del archivo y seleccionar la codificación UTF-8. Importe la versión UTF-8 del archivo a IP Office Manager.
  - **Exportación desde IP Office Manager a Excel**
    No haga doble clic en el archivo exportado desde IP Office Manager. Inicie Excel y use**Archivo | Abierto**para seleccionar el archivo. Excel reconocerá que el archivo utiliza la codificación UTF-8 e iniciará su asistente de importación de archivos de texto. Siga las instrucciones del asistente y seleccione la coma como delimitador de campo.

Configuración de exportación

1. Dentro de IP Office Manager, cargue la configuración de IP Office. Seleccione**Archivo | Importación y exportación...**desde la barra de menú.
2. Seleccione**Exportar**.
3. Seleccione el tipo de archivo. La lista de tipos de entradas exportables cambiará para coincidir con el tipo de archivo.
4. Seleccione los tipos de elementos que deben exportarse.
5. Usa el**Guardar en**ruta para seleccionar la ubicación de los archivos exportados. La ubicación predeterminada utilizada es el subdirectorio del directorio de la aplicación IP Office Manager según el nombre del sistema IP Office cargado actualmente.
6. Haga clic en**OK**.

Configuración de importación

La importación de configuraciones sobrescribirá cualquier entrada existente que coincida con una entrada que se está importando.

1. Dentro de IP Office Manager seleccione**Archivo | Importación y exportación...**desde la barra de menú.
2. Seleccione**Importar**.
3. Seleccione el tipo de archivo. La lista de elementos cambiará para coincidir con el tipo de archivo seleccionado y si se encuentra un archivo o archivos coincidentes en la ruta del archivo actual.
4. Uso**Pase a ver**para ajustar la ruta del archivo. La ubicación predeterminada utilizada es el subdirectorio del directorio de la aplicación IP Office Manager según el nombre del sistema IP Office cargado actualmente.
5. Seleccione los tipos de elementos que deben importarse.
6. Haga clic en**OK**.

4.4 Adición de un archivo de configuración prediseñado

IP Office Manager se puede utilizar paracrear un archivo de configuración fuera de línea 76.El archivo de configuración creado previamente se puede colocar en la tarjeta SD del sistema del sistema antes de la instalación. Luego, ese archivo se carga cuando se inicia el nuevo sistema IP Office.

- La configuración creada debe coincidir con el equipo físico en el sistema IP Office en el que se carga. De lo contrario, es posible que el sistema IP Office se reinicie y experimente otros problemas.

Para cargar una configuración fuera de línea prediseñada en una tarjeta SD del sistema

1. Con IP Office, cree una configuración fuera de línea que coincida con los requisitos del cliente y el equipo que se instalará en IP Office.
2. Cambiar el nombre del archivo de configuración***config.cfg***.
3. Con un lector de tarjetas, copie el archivo en el***/sistema/primario***carpeta en la tarjeta de memoria SD del sistema.

4.5 Adición de un archivo de licencia

El archivo XML que contiene las licencias PLDS de los sistemas se almacena en la tarjeta SD del sistema. Este archivo se puede agregar a la tarjeta SD del sistema antes de la instalación. Luego, la licencia se importa automáticamente a la configuración del sistema cuando se inicia el sistema.

- El ID de host PLDS utilizado para el archivo de licencia debe coincidir con el que se muestra en los 12 dígitos.**Identificación PLDS**impreso en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra con**FK**o**FK SN**. Para esas tarjetas agregue el prefijo***11***para obtener la identificación PLDS de la tarjeta.

Requisitos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una**Edición esencial**licencia del sistema para la versión específica de IP Office que desea ejecutar.

Para cargar un archivo de licencia en una tarjeta SD del sistema

1. Cambie el nombre del archivo de licencia .XML suministrado a***PLDSkeys.xml***.
2. Con un lector de tarjetas, copie el archivo en el***/sistema/primario***carpeta en la tarjeta de memoria SD del sistema.

4.6 Adición de certificados de seguridad

El sistema IP Office puede usar certificados de seguridad para validar las conexiones entre sí mismo, las aplicaciones y otros sistemas IP Office. Los certificados también se pueden utilizar para comunicaciones de telefonía IP.

Los certificados se pueden colocar en la tarjeta SD del sistema. Esos certificados luego se cargan en el almacén de certificados del sistema cuando se inicia el sistema. La extensión del nombre del archivo del certificado debe indicar el tipo de codificación; Los archivos codificados con PEM deben terminar con***.pem***, los archivos codificados DER deben terminar con***.der***.

Para cargar un certificado para agregar:

1. Con un lector de tarjetas, copie el archivo en el***/sistema/primario/certificados/tcs/añadir***carpeta en la tarjeta de memoria SD del sistema.

Para cargar un certificado para eliminar:

El mecanismo anterior puede adaptarse para eliminar también un certificado existente.

1. Con un lector de tarjetas, copie el archivo en el***/sistema/primario/certificados/tcs/eliminar***carpeta en la tarjeta de memoria SD del sistema. Si el certificado coincidente ya existe en el almacén de certificados del sistema, ese certificado se elimina.

4.7 Adición de un archivo de protector de pantalla de la serie 9600

Cuando están inactivos, los teléfonos de la serie 9600 pueden agotar el tiempo de espera para mostrar una imagen de protector de pantalla. Varios***.jpg***los archivos están presentes en las tarjetas***/sistema/primario***carpeta por defecto.

Puede reemplazar estos archivos con sus propios archivos de marca. Los archivos deben ser más pequeños que el tamaño de la pantalla en los teléfonos de la serie 9600 para poder moverlos por la pantalla.

Teléfono	Talla máxima	Teléfono	Talla máxima	Teléfono	Talla máxima
9611	160x160	**9621G**	320x160	**9650**	320x240
9620	320x160	**9630**	320x240	**9650C**	320x240
9620L	320x160	**9640**	320x240		
9620C	320x160	**9641G**	320x240		

- Pantallas a color: la profundidad de color es de 16 bits. Una imagen en color separada se verá mejor.
- Pantallas sin color: los mejores resultados se logran con una sola imagen de logotipo en escala de grises. También se admiten 2 niveles de escala de grises.
- Para invocar fondos transparentes con logotipos, utilice un color de fondo de 0,255,0 (el verde más brillante posible).

4.8 Adición de archivos de música en espera

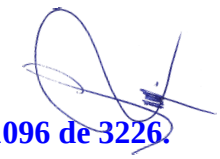
De forma predeterminada, IP Office utilizará la música interna en espera cargando un archivo de música desde la PC IP Office Manager. Para los sistemas IP500 V2, puede cargar un archivo en la tarjeta SD del sistema antes de instalarlo en IP Office.

El archivo debe tener el siguiente formato y debe llamarse***holdmusic.wav***.

Propiedad	Valor	Propiedad	Valor
Tipo de archivo	WAV	**Frecuencia de muestreo de audio**	8kHz
Tasa de bits	128kbps	**Formato de audio**	PCM
Tamaño de muestra de audio	16 bits	**Longitud**	Hasta 90 segundos.
Canales	1 (mono)		

Para cargar un archivo de música en espera en una tarjeta SD del sistema

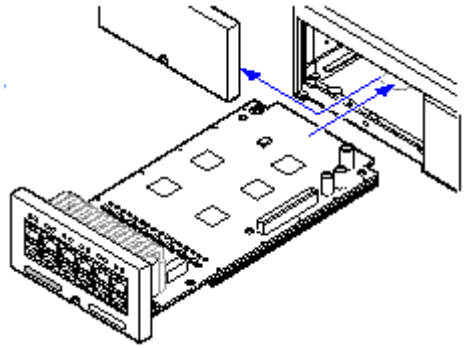
1. Cambiar el nombre del archivo de música***holdmusic.wav***.
2. Con un lector de tarjetas, copie el archivo en el***/sistema/primario***carpeta en la tarjeta de memoria SD del sistema.
3. Si IP Office está o estará configurado para archivos de música en espera adicionales (hasta 3 archivos adicionales), copie esos archivos en la misma ubicación. El nombre de los archivos adicionales debe coincidir con los especificados en la configuración del sistema IP Office.



Capítulo 5.

Instalación de las tarjetas de la unidad de control

5. Instalación de las tarjetas de la unidad de control



Las tarjetas base IP500 y las tarjetas secundarias de troncales deben instalarse antes de aplicar energía a la unidad de control. Asegúrese de que las tarjetas se inserten en el orden que coincida con la configuración planificada o prediseñada.

Este proceso tiene 2 etapas:

1. Coloque las tarjetas secundarias de troncales IP500 en las tarjetas base IP500. 83
2. Inserte las tarjetas base IP500 en la unidad de control. 84

Advertencias

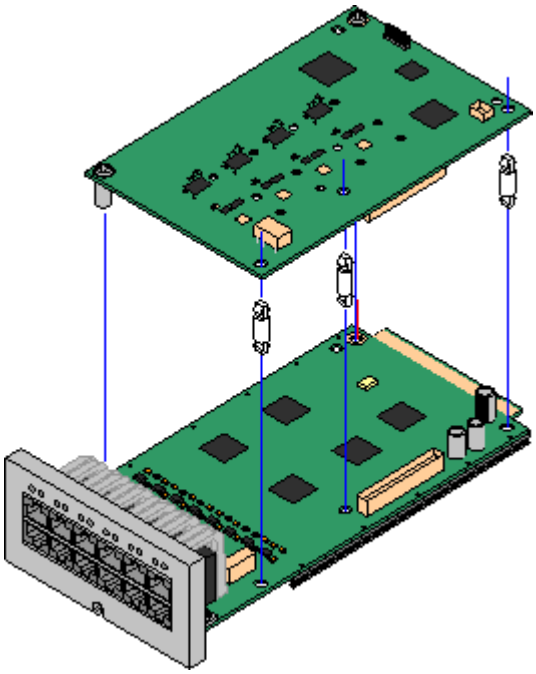
- Deben tomarse las medidas correctas de protección antiestática antes de manipular las placas de circuitos.
- **!IMPORTANTE:**
  Debe apagar la unidad de control antes de agregar, quitar o cambiar componentes Las tarjetas base, las tarjetas de troncales y los módulos de expansión externos solo se deben quitar y agregar a un sistema IP Office cuando ese sistema está apagado 163.Si no lo hace, el nuevo componente no cargará el firmware correcto y no funcionará o no funcionará correctamente. Esto se aplica incluso cuando se intercambian componentes similares.

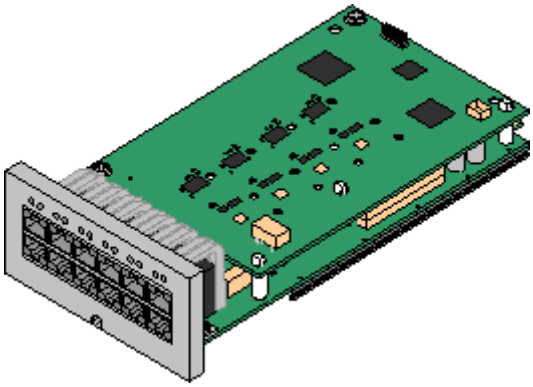
Notas generales

- Las tarjetas se pueden colocar en cualquier orden en cualquier ranura disponible. La única excepción es la tarjeta de expansión de 4 puertos IP500 que solo se puede instalar en la ranura 4 del lado derecho.
- Se recomienda colocar las tarjetas de izquierda a derecha.
- Existen restricciones en la cantidad de tarjetas admitidas de algunos tipos. Cuando se excede dicho límite, la tarjeta más a la derecha de ese tipo no funcionará.
- Asegúrese de utilizar las etiquetas suministradas para identificar la tarjeta instalada en la unidad de control.

5.1 Instalación de tarjetas secundarias IP500

Las tarjetas secundarias de troncales IP500 se pueden instalar en cualquier tarjeta base IP500, excepto en el Módulo de comunicaciones unificadas y la tarjeta de expansión de 4 puertos. Para las tarjetas combinadas IP500, la tarjeta secundaria de troncales está preinstalada y no se puede cambiar.





Advertencias

- Deben tomarse las medidas de protección antiestática correctas al manipular las placas de circuitos.

Piezas y equipos necesarios

1.o**Tarjeta base IP500**

2.o**Tarjeta auxiliar de troncales IP500**

3.o**3 pilares de separación**
Se suministran con la tarjeta auxiliar de troncales.

Herramientas necesarias

1.oDestornillador de punta plana de 5 mm.

2.oMuñequera antiestática y punto de tierra.

Procedimiento: Instalación de una tarjeta auxiliar de troncales

1. Compruebe que se han suministrado las tarjetas correctas.
2. Asegúrese de llevar una muñequera antiestática conectada a un punto de tierra adecuado.
3. En la tarjeta base, identifique la posición de los 3 orificios para los pilares de plástico de la tarjeta IP500. Estos están a lo largo del mismo borde que el conector de la tarjeta.
4. Instale los pilares de separación en la tarjeta base IP500.
5. Si hay un protector de metal con clip sobre el bloque conector en la tarjeta base, retírelo.
6. Usando una fuerza mínima y verificando que las clavijas estén ubicadas correctamente, empuje la tarjeta de troncales IP500 en su bloque de conectores y los pilares de separación.
7. Verifique que el conector de la tarjeta haya encajado en su lugar.
8. Con las arandelas y los tornillos provistos, asegure los pilares metálicos de separación a la tarjeta base.
9. Se suministra un juego de etiquetas con la tarjeta auxiliar de troncales. Coloque la etiqueta adecuada en la parte delantera de la tarjeta base.

5.2 Inserción de tarjetas base IP500

Habiendo preparado cada tarjeta base IP500 agregando cualquiertarjeta hija troncal unidad 83,la tarjeta base se puede insertar en el de control.

Advertencias

- Deben tomarse las medidas de protección antiestática correctas al manipular las placas de circuitos.
- **!IMPORTANTE:**
  Debe apagar la unidad de control antes de agregar, quitar o cambiar componentes Las tarjetas base, las tarjetas de troncales y los módulos de expansión externos solo se deben quitar y agregar a un sistema IP Office cuando ese sistema está apagado 163.Si no lo hace, el nuevo componente no cargará el firmware correcto y no funcionará o no funcionará correctamente. Esto se aplica incluso cuando se intercambian componentes similares.

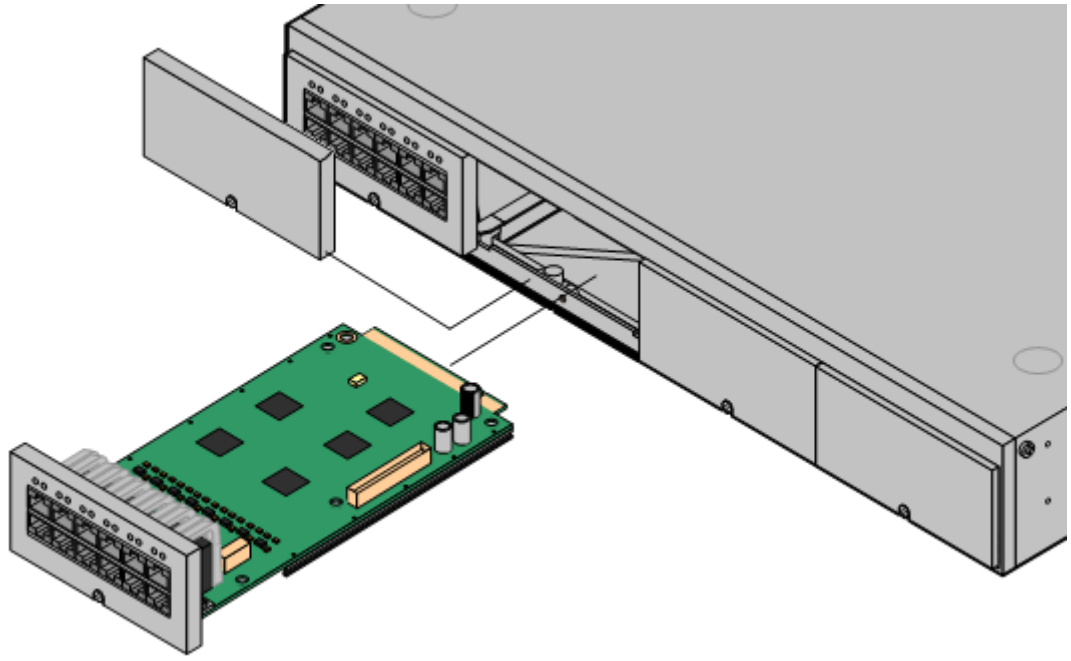
Herramientas necesarias

· oDestornillador de punta plana de 5 mm.

· oMuñequera antiestática y punto de tierra.

Instalación de una tarjeta IP500

1. Verifique que no haya energía en la unidad de control.
2. Con un destornillador de punta plana, retire la cubierta de la ranura en la parte frontal de la unidad de control que se utilizará para cada tarjeta que se instale. Esta cubierta ya no es necesaria, pero debe conservarse hasta que se haya completado la instalación.



3. Permitiendo que la tarjeta descanse contra la parte inferior de la ranura, comience a deslizarla dentro de la unidad de control. Cuando esté medio insertada, verifique que los rieles de la tarjeta se hayan enganchado con los bordes de la ranura tratando de girarla suavemente. Si la tarjeta gira, retírela y vuelva a insertarla.
4. La tarjeta debe deslizarse libremente hasta que esté casi completamente insertada. En este punto, aplique presión en la base del frente de la tarjeta para completar la inserción.
5. Con un destornillador de punta plana, asegure la tarjeta.

Capítulo 6.

Instalación del sistema físico

6. Instalación del sistema físico

Habiendo preparado para la instalación, esta sección cubre la instalación básica en el sitio.

Resumen

1. **Prepárese para la instalación** 50

   una. **Requisitos medioambientales** 51
   Verifique que el área de instalación cumpla con los requisitos ambientales del sistema.

   b. **Requisitos de espacio** 53
   Verifique que el área de instalación cumpla con los requisitos de espacio del sistema.

   C. **Herramientas y piezas necesarias** 59
   Compruebe que dispone de las herramientas y piezas adicionales necesarias.

   d. **Documentación** 60
   Asegúrese de haber obtenido y leído toda la documentación pertinente.

   mi. **Desembalaje** 60
   Verifique que se haya entregado todo el equipo requerido y que no haya daños.

2. **Instalación del software de administración** 62
   Para la instalación del sistema, necesita una PC con el software de administrador de IP Office instalado. Esto debe incluir una copia de IP Office Manager que coincida con el nivel de software de IP Office requerido.

   una. **Descarga del software** 63

   b. **Instalación de las aplicaciones del administrador** 64

3. **Preparación de la tarjeta SD del sistema** 74
   Actualice la tarjeta SD del sistema a la versión requerida del software IP Office. Además, agregue cualquier otro archivo disponible, como el archivo de licencia, la configuración preconstruida, el archivo de música en espera.

   - **!ADVERTENCIA: Instalación de unidades de control PCS14 y anteriores**
     PC 296 14 o unidades inferiores deben instalar primero la versión 8.1(65) (o superior 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1. Se debe tener cuidado para asegurarse de que no se realicen llamadas antes de la actualización a la Versión 10.0, de lo contrario, el sistema requerirá una licencia de actualización 10.0 a pesar de ser "nuevo". El PCS de la unidad de control está impreso en la etiqueta en la parte posterior de la unidad de control.

4. **Instale las tarjetas de la unidad de control** 82
   Conecte las tarjetas secundarias de troncales a sus tarjetas base IP500 e inserte las tarjetas base en la unidad de control.

5. **Instalar el sistema** 86

   una. **Montaje en pared** 87
   Si se monta en la pared, fije los soportes y coloque la unidad en la pared.

   b. **Montaje en bastidor** 89
   Si se monta en un bastidor, fije los soportes y coloque la unidad de control en el bastidor.

   C. **Conectar los módulos de expansión externos** 91
   Conecte los módulos de expansión externos a la unidad de control.

   d. **Poner a tierra el sistema** 93
   Conecte los cables de tierra necesarios a la unidad de control y a los módulos de expansión externos.

   mi. **Iniciar el sistema** 94
   Inserte la tarjeta SD del sistema y encienda el sistema.

   F. **Conexión de teléfonos** 97
   Conecte los teléfonos digitales de Avaya.

6. **Configuracion inicial**
   Una vez que se inicia el sistema físico, se puede configurar. Esto se puede hacer usando cualquiera Administrador de IP Office Administrador 100 O web de IP Office 114.

6.1 Montaje en pared

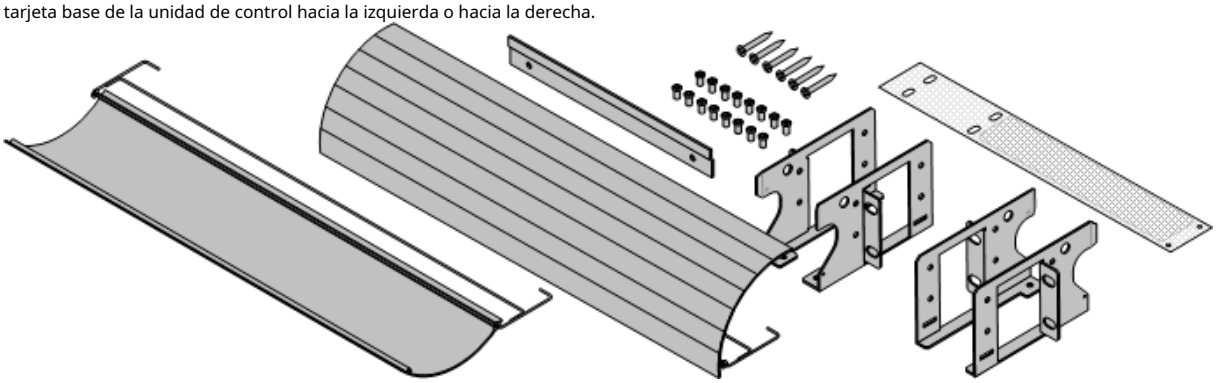
Las unidades de control IP500 V2 y los módulos de expansión externos IP500 pueden montarse en la pared o en un bastidor. Para hacer esto, se requiere un kit de montaje en pared además de las fijaciones de pared adecuadas.

Además de los existentesRequisitos medioambientales 51para un sistema IP Office, se aplican los siguientes requisitos adicionales al montar una unidad en la pared:

- La superficie de la pared debe ser vertical, plana y libre de vibraciones. No se admite la unión a paredes temporales.
- Solo deben usarse los tornillos proporcionados con el kit de montaje para fijar los soportes a la unidad de control oa los módulos de expansión.
- La instalación debe ser realizada por una persona de servicio.
- Asegúrese de que el sistema se haya apagado y que se haya desconectado la alimentación de todas las unidades. Apague el sistema usando un comando de apagado y luego desconecte la alimentación. No quite simplemente la energía.
- Se requiere una superficie de montaje de madera contrachapada adecuada de al menos 1 m x 1 m x 19 mm (39" x 39" x 0,75"). Si también se va a montar una caja de expansión, se requiere una superficie de montaje de madera contrachapada de al menos 1,2 mx 1,2 mx 19 mm (48" x 48" x 0,75").
- Se debe usar un mínimo de 6 tornillos de cabeza plana de 45 mm de largo y 5 mm/6 mm (1,75" n.° 10/n.° 12) para asegurar la madera contrachapada a los montantes de la pared.
- Se deben usar los tornillos para madera de 20 mm de largo y 4 mm (#8 ¾") para asegurar los soportes a la superficie de montaje de madera contrachapada

El siguiente kit está disponible actualmente:

- **KIT DE MONTAJE EN PARED IPO IP500 V3***(Código SAP 700503160)*
  Este kit se puede utilizar paramontaje en pared y en rack de unidades de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora enrutamiento de cables en la parte delantera y trasera de la unidad. Para unidades de control montadas en la pared, permite orientar las ranuras de la tarjeta base de la unidad de control hacia la izquierda o hacia la derecha.



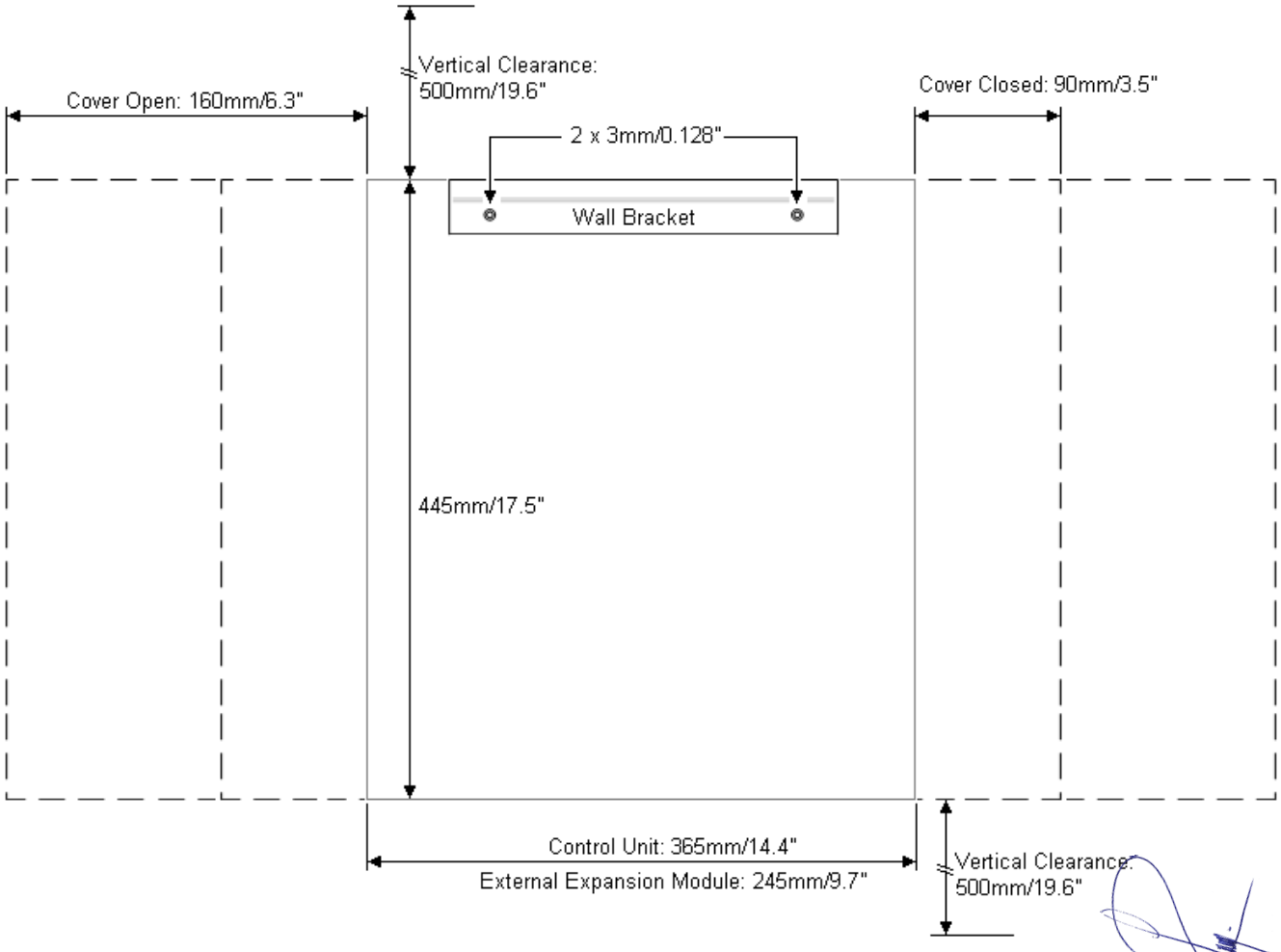
6.1.1 Kit de montaje en pared V3

Estas notas se refieren a la**KIT DE MONTAJE EN PARED IPO IP500 V3***(SAP 700503160)*. Este kit se puede utilizar para montar en pared o en rack unidades de control IP500 V2 y módulos de expansión externos IP500.

Los kits incluyen todos los componentes necesarios para el montaje en pared sobre una superficie de madera contrachapada. El uso de cubrecables es opcional.

Además de los existentesRequisitos medioambientales[51]para un sistema IP Office, se aplican los siguientes requisitos adicionales al montar una unidad en la pared:

- La superficie de la pared debe ser vertical, plana y libre de vibraciones. No se admite la unión a paredes temporales.
- Solo deben usarse los tornillos proporcionados con el kit de montaje para fijar los soportes a la unidad de control oa los módulos de expansión.
- La instalación debe ser realizada por una persona de servicio.
- Asegúrese de que el sistema se haya apagado y que se haya desconectado la alimentación de todas las unidades. Apague el sistema usando un comando de apagado y luego desconecte la alimentación. No quite simplemente la energía.
- Se requiere una superficie de montaje de madera contrachapada adecuada de al menos 1 m x 1 m x 19 mm (39" x 39" x 0,75"). Si también se va a montar una caja de expansión, se requiere una superficie de montaje de madera contrachapada de al menos 1,2 mx 1,2 mx 19 mm (48" x 48" x 0,75").
- Se debe usar un mínimo de 6 tornillos de cabeza plana de 45 mm de largo y 5 mm/6 mm (1,75" n.° 10/n.° 12) para asegurar la madera contrachapada a los montantes de la pared.
- Se deben usar los tornillos para madera de 20 mm de largo y 4 mm (#8 ¾") para asegurar los soportes a la superficie de montaje de madera contrachapada
- La instalacióndeber ser realizado por una persona de servicio solamente.
- Para las unidades de control, la pantalla de llama de malladeber instalarse en el borde inferior de la unidad de control antes del montaje. La pantalla de llama se conecta al exterior de la unidad de control.
- Asegúrese de que el sistema se haya apagado y que se haya desconectado la alimentación de todas las unidades. Apague el sistema usando un comando de apagado y luego desconecte la energía. No quite simplemente la alimentación.
- Las instrucciones completas de instalación se incluyen con el kit.

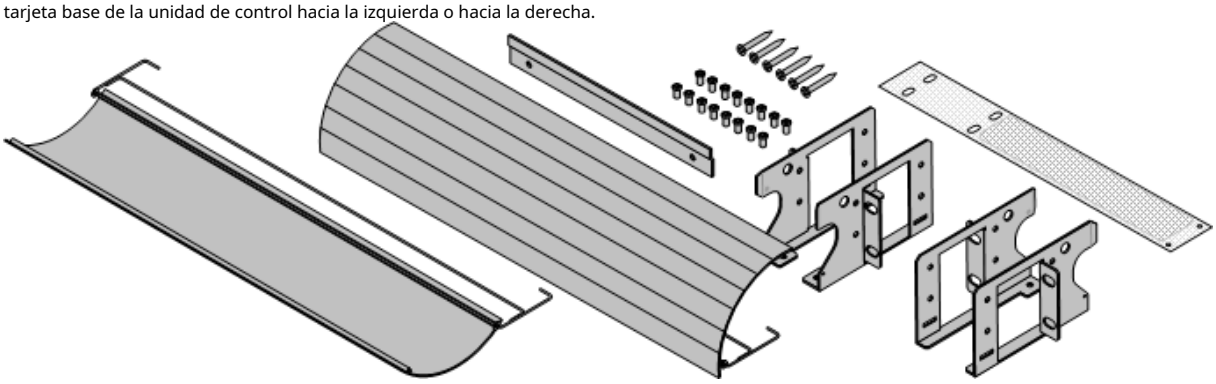


6.2 Montaje en bastidor

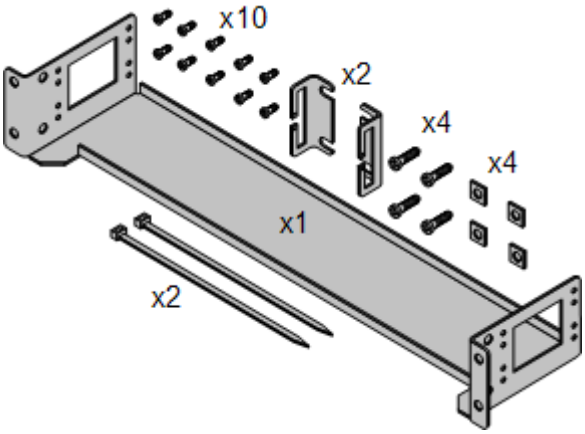
Todas las unidades de control de IP Office y los módulos de expansión externos se pueden montar en rack en sistemas de rack estándar de 19". Cada unidad requiere un espacio de ranura de 2U dentro del rack. El montaje en rack requiere un kit para cada unidad de control y módulo de expansión externo.

Cuando los sistemas se monten en rack, se debe considerar el efecto de las condiciones dentro del gabinete del rack. Por ejemplo, la temperatura del estante puede estar por encima de la temperatura ambiente y el flujo de aire dentro del estante está restringido. losRequisitos medioambientales 51 para las unidades individuales de IP Office siguen siendo aplicables dentro del gabinete del bastidor.

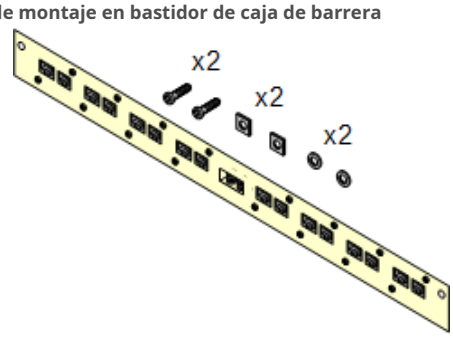
- **KIT DE MONTAJE EN PARED IPO IP500 V3***(Código SAP 700503160)*
  Este kit se puede utilizar paramontaje en pared y en rack de unidades de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora enrutamiento de cables en la parte delantera y trasera de la unidad. Para unidades de control montadas en la pared, permite orientar las ranuras de la tarjeta base de la unidad de control hacia la izquierda o hacia la derecha.



- **KIT DE MONTAJE DE RACK IPO IP500***(Código SAP 700429202)*
  Este kit contiene todos los componentes necesarios para el montaje en rack de una sola unidad de control IP500 V2 o módulo de expansión externo IP500. Esto incluye tornillos para la fijación de los soportes al módulo, pernos para asegurar el módulo en el rack y soportes pasacables.



Kit de montaje en bastidor de caja de barrera



- **Kit de montaje en bastidor de caja de barrera***(SAP 700293905)* Las cajas de barrera se deben utilizar paraextensiones telefónicas analógicas fuera del edificio 36.Este soporte permite montar en rack hasta 8 cajas de barrera de IP Office y simplifica la cantidad de conexiones al punto de protección a tierra en el rack. Este kit debe usarse cuando se usan más de 3 cajas de barrera y admite un máximo de 16 cajas de barrera para un solo módulo de expansión externo.

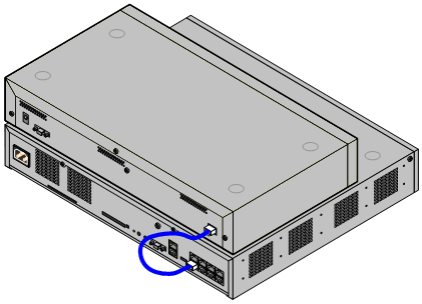
¿Comentarios sobre este documento? infodev@avaya.com

Requisitos medioambientales

Además de los existentesRequisitos medioambientales tener 51para un sistema IP Office, los siguientes factores adicionales deben en cuenta al montar una unidad en bastidor:

1. Posicionamiento del estante: asegúrese de cumplir con las instrucciones de seguridad del fabricante del estante. Por ejemplo, verifique que las patas del estante se hayan bajado y que se hayan utilizado los soportes de fijación para evitar que se vuelque.
2. Ambiente de funcionamiento elevado: si se instala en un conjunto de bastidor cerrado o de varias unidades, la temperatura ambiente de funcionamiento del entorno del bastidor puede ser superior a la temperatura ambiente de la habitación. Por lo tanto, se debe considerar la instalación del equipo en un entorno compatible con la temperatura ambiente máxima (Tma) especificada por el fabricante.
   - oTemperatura de funcionamiento: 5 °C (40 °F) a 40 °C (104 °F).
   - oHumedad de funcionamiento: 10 % a 95 % sin condensación.
3. Flujo de aire reducido: la instalación del equipo en un bastidor debe ser tal que la cantidad de flujo de aire necesaria para el funcionamiento seguro del equipo no se vea comprometida. Se debe mantener una ventilación adecuada. Las ranuras de ventilación laterales de la unidad de control IP500 no deben cubrirse ni bloquearse.
4. Carga mecánica: el montaje del equipo en el bastidor debe ser tal que no se logre una condición peligrosa debido a una carga mecánica desigual.
5. Sobrecarga del circuito: se debe considerar la conexión del equipo al circuito de suministro y el efecto que la sobrecarga de los circuitos podría tener en la protección contra sobrecorriente y el cableado de suministro. Se deben tener en cuenta las clasificaciones de la placa de identificación del equipo al abordar esta inquietud.
6. Conexión a tierra confiable: se debe mantener una conexión a tierra confiable de los equipos montados en rack. Debe prestarse especial atención a las conexiones de suministro distintas de las conexiones directas al circuito derivado (p. ej., uso de regletas).
7. ⚠ Solo se deben usar los tornillos proporcionados con el kit de montaje para fijar los soportes a la unidad de control.

6.3 Conexión de módulos de expansión externos



Todos los módulos de expansión externos deben conectarse a la unidad de control antes de aplicar energía a la unidad de control. Asegúrese de que los módulos estén conectados en el orden que coincida con la configuración planificada o prefabricada.

Los módulos de expansión externos se conectan a la unidad de control de IP Office mediante un cable de interconexión de expansión. Cada módulo se suministra con un cable de conexión de expansión y un[unidad de fuente de alimentación](#) 30.Un apropiado[cable de alimentación específico del lugar](#) 31para la fuente de alimentación debe pedirse por separado.

- Cada módulo de expansión externo se suministra con un cable de interconexión de expansión azul de 1 metro (3'3"). este cable deber utilizarse cuando se conecta a puertos de expansión en la parte trasera de una unidad de control.
- Cuando se conecta a puertos de expansión en una tarjeta de expansión de 4 puertos IP500, se puede usar un cable de interconexión de expansión amarillo de 2 metros (6'6") en lugar del cable azul estándar. Se suministran 4 cables amarillos con la tarjeta de expansión de 4 puertos IP500 tarjeta.
- **!IMPORTANTE:**
  Debe apagar la unidad de control antes de agregar, quitar o cambiar componentes Las tarjetas base, las tarjetas de troncales y los módulos de expansión externos solo se deben quitar y agregar a un sistema IP Office cuando ese sistema está [apagado](#) 163.Si no lo hace, el nuevo componente no cargará el firmware correcto y no funcionará o no funcionará correctamente. Esto se aplica incluso cuando se intercambian componentes similares.

requerimientos de instalación

· oEspacio de instalación sobre o debajo de la unidad de control de IP Office existente. Ver[Requisitos de espacio en bastidor](#) 57Para el posicionamiento de múltiples módulos apilados.

· oToma de corriente conmutada.
La toma de corriente utilizada debe incluir un interruptor y en los casos en que la[cable de alimentación](#) 31incluye un cable de tierra, que tomacorriente debe tener una conexión a tierra de protección.

- **!Importante: alimentación del módulo de expansión externo**
  Para ser detectados y operados correctamente, los módulos de expansión externos deben iniciarse antes que la unidad de control de IP Office. Normalmente esto se logra conectando todos los módulos de expansión a la misma regleta que la unidad de control. La unidad de control aplica un breve retraso a su propio proceso de inicio para garantizar que los módulos de expansión se encienden al mismo tiempo que se detectan.

· oPuerto de EXPANSIÓN disponible en la centralita.

· oRequisitos de puesta a tierra

· o**Puesta a Tierra Funcional** Conexión de un[tierra funcional](#) 35 es:

· oRecomendado para todos los módulos.

· oLa conexión de una tierra funcional es obligatoria para los módulos de troncales analógicas.

· o**Puesta a tierra de protección**
Conexiones de una tierra de protección a través de[equipo de protección contra sobretensiones](#) 365:

· oObligatorio para módulos troncales analógicos en la República de Sudáfrica.

· oObligatorio para módulos de Teléfono y Estación Digital conectados a extensiones fuera del edificio.

· oObligatorio para los módulos Digital Station V2 y Phone V2.

Herramientas necesarias

· oPC administrador de IP Office.

· o[Herramientas para montaje en bastidor](#) 89(opcional).

Piezas y equipos necesarios

· o**Módulo de expansión externo**.
Cada módulo se suministra con una fuente de alimentación externa adecuada y un cable de interconexión azul de 1 m. Los cables de interconexión amarillos de 2 m se suministran con la tarjeta de expansión de 4 puertos IP500 y solo deben usarse con esa tarjeta.

· o[Cable de alimentación para la fuente de alimentación](#) 31.

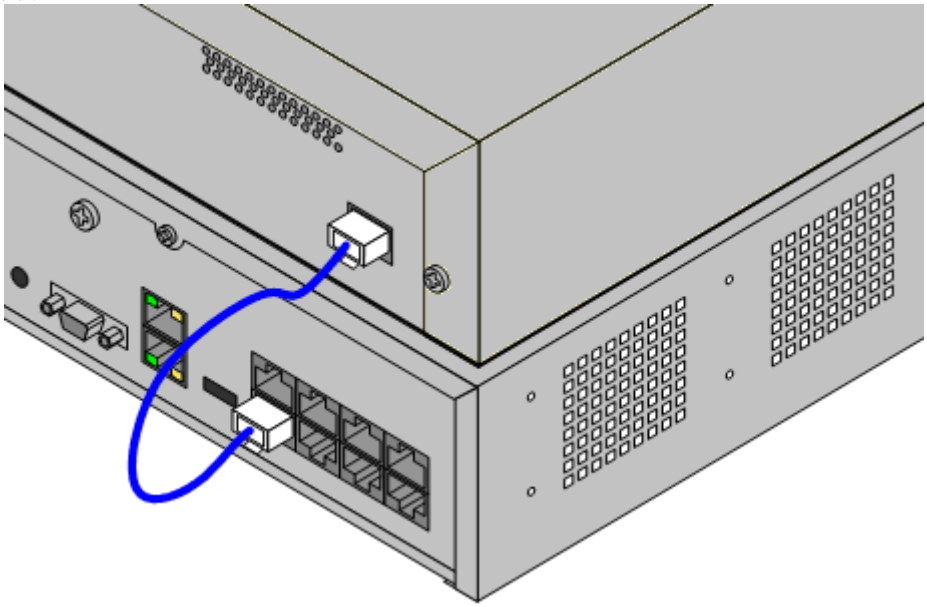
· o[Kit de montaje en bastidor](#) 37*(opcional)*.

· o[Juego de montaje en pared](#) 87*(opcional - módulos de expansión externos IP500 solamente)*.

· oEtiquetas de etiquetado de cables.

Procedimiento

1. Los módulos de expansión externos no deben conectarse a una unidad de control que tenga alimentación. Si agrega un nuevo módulo a un sistema existente,apagar el sistema 163.
2. Si el sistema IP Office se va a instalar en un bastidor, conecte elkit de montaje en bastidor 89al módulo de expansión.
3. Conecte la fuente de alimentación del módulo de expansión externo pero no lo encienda.
4. Conecte el cable de interconexión de expansión del puerto EXPANSION del módulo al puerto EXPANSION de la unidad de control.



- **Nota**
  Se recomienda conectar los módulos desde el puerto 1 hacia arriba, usando cada puerto en secuencia.

5. Tome nota cuidadosa del puerto utilizado e incluya este detalle en la etiqueta del cable y cualquier otro registro del sistema.
6. Conecte cualquier otro módulo de expansión externo que se agregue.
7. Ahora puedesconectar el cableado de puesta a tierra 93para los módulos de expansión externos.

una. Una vez que los módulos de expansión están conectados y conectados a tierra, puedeiniciar el sistema 94.Asegúrese de que los módulos de expansión externos se inicien antes que la unidad de control.

6.4 Puesta a tierra

El uso de conexiones a tierra reduce la probabilidad de problemas en la mayoría de los sistemas de telefonía y datos. Esto es especialmente importante en edificios en los que se interconectan varios elementos de equipo mediante cables largos, por ejemplo, redes telefónicas y de datos.

Todas las unidades de control de IP Office y los módulos de expansión externos deben estar conectados a una tierra funcional. Cuando la unidad esté conectada a una toma de corriente mediante un cable de alimentación con conductor de tierra, la toma de corriente debe estar conectada a una toma de tierra de protección.

En algunos casos, como las troncales de puesta en tierra, además de ser una medida de protección es un requisito funcional para el funcionamiento del equipo. En otros casos, puede ser un requisito normativo local o un paso de protección necesario, por ejemplo, áreas de alto riesgo de rayos.

- **ADVERTENCIA**
  Durante la instalación, no asuma que los puntos de tierra están correctamente conectados a tierra. Pruebe los puntos de tierra antes de confiar en ellos para conectar a tierra el equipo.
- **Equipo de protección adicional**
  Además de la conexión a tierra, se requerirá equipo de protección adicional en las siguientes situaciones.
  - En cualquier módulo de expansión externo Digital Station o Phones conectado a una extensión ubicada en otro edificio. Referirse a "Instalaciones Telefónicas Fuera de Edificio 36".
  - En la República de Sudáfrica, en todos los módulos de expansión externos de troncales analógicas (ATM16) y en cualquier unidad de control que contenga tarjetas de troncales analógicas (ATM4/ATM4U).

Herramientas necesarias

- oDestornillador de cabeza cruzada M4.
- oHerramientas adecuadas para engarzar una pala de cable.

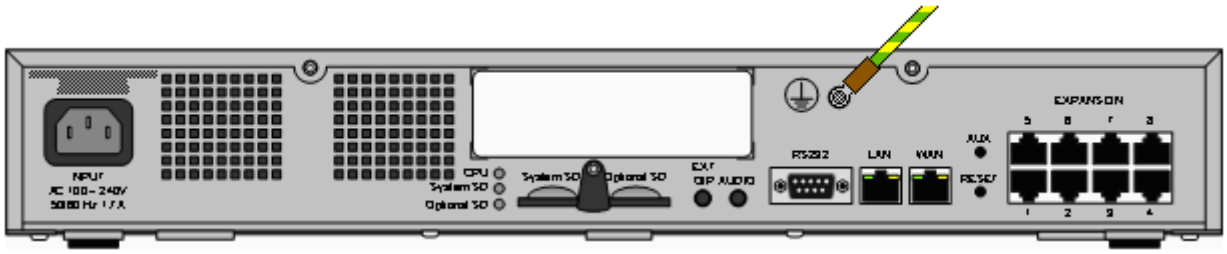
Piezas y equipos necesarios

- oCable de cobre sólido de 14 AWG para conexión a tierra.
- oManguito de cable que cumple con los requisitos del regulador local. Típicamente verde para una tierra funcional y verde/amarillo para una tierra protectora.

El punto de conexión a tierra de las unidades de control y los módulos de expansión de IP Office están marcados con un o símbolo. Terrestre las conexiones a estos puntos deben usar un cable sólido de 14 AWG con un manguito verde para una conexión a tierra funcional o un manguito verde y amarillo para una conexión a tierra protectora.

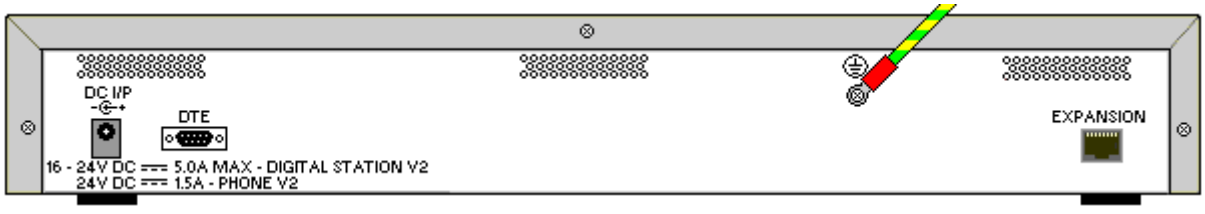
Unidad de control IP500 V2

En las unidades de control IP500 V2, el punto de tierra está ubicado sobre el puerto RS232 DTE.



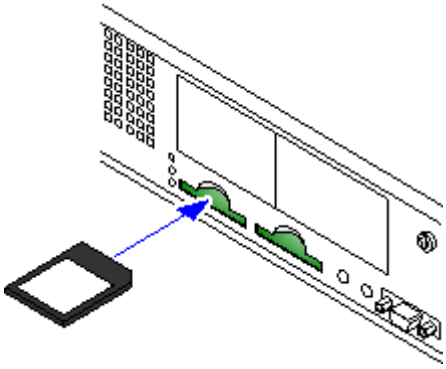
Módulos de expansión externos

En los módulos de expansión, el punto de conexión a tierra es un tornillo de 4 mm ubicado hacia la derecha en la parte posterior del módulo.



- En algunos módulos más antiguos, el tornillo de conexión a tierra dedicado no está presente. En esos casos, el tornillo de fijación de la cubierta superior central (3 mm) se puede utilizar como punto de conexión a tierra alternativo. Se debe agregar una arandela dentada para asegurar un buen contacto.

6.5 Inicio del sistema



1. Antes de insertar la tarjeta SD del sistema:

   una. Asegúrese de tener el tipo correcto de[Tarjeta SD del sistema Avaya](#) 208.

   b. Asegúrese de que la tarjeta tenga el nivel de software necesario. Si necesario, [actualizar la tarjeta usando IP Office Manager](#) 75.

2. Con la centralita apagada o sin tensión:

   una. Las ranuras para tarjetas SD están cubiertas por una pestaña de plástico. Suelte parcialmente el tornillo que sujeta la lengüeta para que pueda moverse fuera de la ranura de la tarjeta requerida.

   b. Inserte la tarjeta en el**SD del sistema**ranura en la parte trasera de la unidad de control.

3. Encienda los módulos de expansión externos.

   - **!Importante: alimentación del módulo de expansión externo**
     Para ser detectados y operados correctamente, los módulos de expansión externos deben iniciarse antes que la unidad de control de IP Office. Normalmente esto se logra conectando todos los módulos de expansión a la misma regleta que la unidad de control. La unidad de control aplica un breve retraso a su propio proceso de inicio para garantizar que los módulos de expansión se encienden al mismo tiempo que se detectan.

4. Aplique energía a la unidad de control. La toma de corriente utilizada debe incluir un interruptor y la toma de corriente debe tener una conexión a tierra de protección.

5. La unidad de control carga el firmware de la tarjeta SD del sistema con el que se actualiza a sí misma y a sus componentes internos. Esto toma aproximadamente un minuto. El final de este proceso se indica mediante el parpadeo del LED1 en cada tarjeta base cada 5 segundos. El LED9 en cada tarjeta base equipada con una tarjeta auxiliar de troncales también parpadea.

6. La unidad de control comienza a actualizar los módulos de expansión externos si es necesario. Esto se indica mediante el parpadeo rojo del LED central del módulo. Este proceso se completa cuando el LED cambia a verde fijo.

7. Si ya hay un archivo de configuración[presente en la SD del sistema](#) 78la tarjeta es cargada por IP Office. De lo contrario, los nuevos sistemas crean una configuración predeterminada y copian esa configuración en la tarjeta SD del sistema.

8. Ahora debería ser posible utilizar IP Office Manager para acceder a la configuración de IP Office.

LED de inicio de la unidad de control

Trasero

Los LED en la parte trasera de la unidad de control pasan por la siguiente secuencia durante un arranque normal. Tenga en cuenta que los tiempos son aproximadamente solo:

DIRIGIÓ	4s	4s	12s	5s	2s	5s	5s	10s	10s	Acabado
UPC	Naranja	Verde	Verde	Verde Rojo	Verde	Verde	Verde	Verde	Verde	Verde
SD del sistema	Naranja	Apagado	Verde	Verde	Verde	Apagado	Verde	Verde	Verde Destello	Verde
SD opcional Si está presente.	Naranja	Apagado	Verde	Verde	Verde	Apagado	Apagado	Verde	Verde	Verde

Frente

En el frente de la unidad de control, el LED1 en cualquier tarjeta base IP500 instalada se usa de la siguiente manera. LED9 también se utiliza para cualquier tarjeta auxiliar de troncales instalada.

DIRIGIÓ	30s	30s	Acabado
LED1/LED9	Rojo	Rojo	Rojo
		Parpadeo rápido	Parpadeo cada 5 segundos

6.6 Comprobación de los LED

LED de la unidad de control

DIRIGIÓ	Descripción
SD opcional **SD del sistema**	· **Apagado**=Apagado de tarjeta. · **Verde encendido**=Tarjeta presente. · **Verde intermitente**=Tarjeta en uso. · **Naranja fijo**=Reinicio inminente. · **rojo intermitente**=Tarjeta inicializándose o apagándose. · **Parpadeo rápido rojo**=tarjeta llena · **rojo fijo**=Fallo de tarjeta/tipo incorrecto.
UPC	· **Rojo/verde alternativo**=Empezando. · **Verde encendido**=Bueno. · **rojo encendido**=Sin software · **Rojo parpadeante**=Error/Apagado.

LED de la tarjeta base

Nota: Las tarjetas que no son compatibles con el modo IP Office Basic Edition (Expansión de 4 puertos, VCM32 y VCM64) mostrarán un LED rojo fijo hasta que el sistema tenga licencia y esté configurado para Preferred Edition o superior.

Tarjeta básica	LED 1 a 8 Uso
Todas las tarjetas	· LED1 también se utiliza para el estado de la tarjeta base: · **rojo encendido**=Error/No compatible. · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo rápido rojo**=Apagado del sistema.
Teléfono analógico IP500	· No se utilizan LED de estado para extensiones telefónicas analógicas.
Estación digital IP500	· **Verde intermitente**=Teléfono detectado. · **Verde encendido**=Teléfono activo.
IP500 TCM8	· **Verde encendido**=Teléfono detectado.
Combinación IP500	· LED 1 a 6 · **Verde intermitente**=Teléfono detectado. · **Verde encendido**=Teléfono activo.
VCM IP500	· Los LED 1 a 8 no están etiquetados. Se utilizan para indicar el uso del canal de compresión de voz. Cada LED encendido representa el 12,5 % de la capacidad del canal de compresión de voz disponible en uso (capacidad total de la tarjeta en lugar de capacidad con licencia).
Expansión de 4 puertos IP500	· Los LED 1 a 8 se utilizan para los puertos de expansión en la parte posterior de la unidad de control. Los LED 9 a 12 se utilizan para los puertos de expansión propios de la tarjeta.

Verde	**En**	Módulo de expansión presente.
Rojo	**Brillante**	Inicializando.
Rojo	**En**	Error.
Naranja	**Destello normal**	Tarjeta base bien.

LED de la tarjeta auxiliar de troncales

Tarjeta Hija Tronco	LED 9 a 12 Uso
Todas las cartas	• El LED 9 también se utiliza para el estado de la tarjeta secundaria. • **rojo encendido**=Error • **Parpadeo rojo cada 5 segundos**=Tarjeta bien. • **Parpadeo lento rojo**=Inicializando. • **Parpadeo rápido rojo**=Apagado del sistema.
Troncal analógico	• **Verde encendido**=V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde intermitente**=Línea ocupada.
Troncal PRI	• **Apagado**=No hay baúl presente. • **Verde encendido**=Tronco presente. • **Verde intermitente**=Tronco en uso. • **Parpadeo rápido rojo/verde**(puerto 9) o**Parpadeo rápido verde**(puerto 10) = Señal de indicación de alarma (AIS) desde el extremo remoto troncal. • **Rojo con parpadeo verde**(puerto 9) o**Parpadeo verde**(puerto 10) = Puerto en modo de bucle invertido (establecido a través de IP Office System Monitor).
Troncal BRI	• **Apagado**=No hay baúl presente. • **Verde encendido**=Tronco presente. • **Verde intermitente**=Tronco en uso.

LED del módulo de expansión externo

Módulo	LED
Todos	El LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **rojo intermitente**=Módulo iniciando/Cargando firmware. • **rojo encendido**=Error. • **Verde encendido**=Módulo bien. • **Verde intermitente**=Módulo iniciando/Cargando firmware (solo módulo IP500 DS16A/30A).
Troncal analógico 16	• Ninguna.
BRI So8	• **Verde encendido**=Conectado. • **Verde intermitente**=Actividad.
Emisora Digital 16/30	• **Verde intermitente**=Teléfono detectado. • **Verde encendido**=Teléfono activo.
Estación Digital 16A/30A	• **Verde encendido**=Teléfono detectado.
Teléfono	• Ninguna.

6.7 Conexión de teléfonos

Durante el encendido inicial, IP Office crea automáticamente entradas de extensión y usuario para todos los puertos de extensión analógicos y digitales (DS y BST) en el sistema. Esto permite que esos dispositivos se conecten sin ninguna programación adicional.

- **!Advertencia**
  Si el sistema se actualizó desde una versión anterior del software IP Office, todos los teléfonos no podrán realizar llamadas hasta que se ingrese una licencia de actualización. Para la versión 10.0 y posteriores significa la versión específica adecuada**Edición esencial** 279licencia. La restricción de marcación incluye no poder realizar llamadas de emergencia.

- Esta sección no cubre la instalación de teléfonos DECT, H323 y SIP. Para la instalación de estos dispositivos, consulte los manuales de instalación complementarios correspondientes.

6.7.1 Teléfonos analógicos

Conecte cualquier teléfono analógico a su correspondienteTeléfono están 276puertos Asegúrese de que aquellos conectados apuertos de falla de energía 47 claramente etiquetados como tales.

6.7.2 Teléfonos ETR

Conecte cualquier teléfono ETR a su correspondienteETR 272puertos Estos teléfonos no necesitan cargar firmware adicional.

6.7.3 Teléfonos de estación digital DS

Conecte cualquier teléfono digital a su correspondienteSD 271puertos Es posible que estos teléfonos necesiten actualizar su firmware para que coincida compatible con el software principal de IP Office. El firmware adecuado se suministra con el software IP Office Manager y se copia en la tarjeta SD del sistema para los sistemas IP500 V2.

Los teléfonos cargarán automáticamente el firmware del sistema IP Office si es necesario.

- El proceso de actualización tarda aproximadamente 10 minutos, tiempo durante el cual el teléfono mostrará una advertencia. El teléfono no debe desconectarse durante este proceso.
- Una vez que se actualizó el teléfono conectado a un puerto, IP Office no verificará si el teléfono en ese puerto debe actualizarse nuevamente, excepto después de reiniciar el sistema, es decir, no se pueden actualizar varios teléfonos intercambiando los teléfonos conectados en el mismo puerto.

6.7.4 Teléfonos IP/SIP

La instalación y configuración de teléfonos IP H323 y SIP no está cubierta por este documento. Consulte el manual de instalación de IP Office correspondiente al tipo de teléfono que se está instalando.

6.7.5 Teléfonos TCM/BST

Conecte cualquier teléfono BST a sus puertos BST apropiados. Estos teléfonos no necesitan cargar firmware adicional.

Módulo DS30B

Los módulos de expansión externos IP500 DS16B y DS30B admiten puertos BST o DS. El tipo de puerto para un módulo completo se configura mediante IP Office Manager. VerSelección del modo de puerto DS16B/30B 110.

Botones predeterminados

Para sistemas con puertos telefónicos BST, cuando un teléfono se conecta por primera vez al puerto, la programación de botones del usuario asociado se sobrescribe con la programación de botones predeterminada apropiada para el modelo de teléfono.

Si el nuevo sistema se está instalando con una configuración preestablecida que incluye la programación de botones del usuario, la configuración predeterminada automática de los botones para que coincidan con el tipo de teléfono sobrescribirá la configuración de los botones del usuario. Este comportamiento se puede evitar agregando el siguiente código corto a la configuración del usuario en la configuración preprogramada:

- **Código:***DCP
- **Rasgo:**Marcar
- **Número de teléfono:**84000004,1,1,0
  La parte 4000004 de la cadena anterior también se puede usar para ajustar los valores predeterminados para las siguientes configuraciones del teléfono:
  - El primer dígito establece el contraste del teléfono = 1 (bajo) a 9 (alto).
  - El último dígito establece el volumen del timbre = 0 (alto) a 7 (bajo).

Tenga en cuenta que la eliminación posterior de este código abreviado hará que los botones vuelvan a sus valores predeterminados según el tipo de teléfono.

Configuración del tipo de teléfono

Para algunos teléfonos, el teléfono solo puede informar su tipo general al sistema en lugar de su modelo específico. Se recomienda que después de conectar todos los teléfonos, los tipos de teléfono se establezcan correctamente en la configuración de IP Office.

- **!Importante**
  Los tipos predeterminados no se pueden cambiar después de la instalación sin establecer la configuración predeterminada. Por lo tanto, debe asegurarse de conectar el tipo correcto de teléfono a cada puerto. Si necesita intercambiar teléfonos, utilice el proceso para intercambiar números de extensión 186en lugar de cambiar el cableado.

1. Usando IP Office Manager, reciba la configuración del sistema.
2. Seleccione**Extensión**.
3. Seleccionando cada extensión a su vez, en el**Ext.**pestaña, compruebe que la**Tipo de dispositivo**el campo está configurado para el modelo de teléfono correcto.

Tipo predeterminado	Posibles modelos de teléfono
T7100	T7100, M7100, M7100N, Unidad de audioconferencia.
T7208	T7208, M7208, M7208N.
M7310	T7406E, T7406, M7310, M7310N
M7310BLF	T7316, M7310BLF
M7324	M7324, M7324N

4. Vuelva a guardar la configuración en el sistema IP Office.

Capítulo 7.

Configuración inicial usando Manager

7. Configuración inicial usando Manager

Esta sección cubre los cambios de configuración básicos necesarios para los sistemas IP Office que utilizan la aplicación IP Office Manager. Esto cubre solo la configuración básica, el rango completo de configuración posible a través de IP Office Manager se cubre en elManual del administrador de IP Office 11.

Resumen

1. **Conexión de red** 101
   Utilice IP Office Manager para conectarse al nuevo sistema.
2. **Configuracion inicial** 103
   los**Configuracion inicial**El menú se muestra la primera vez que IP Office Manager o IP Office Web Manager se conecta a un nuevo sistema.
3. **Establecer la numeración de la extensión** 104
   Vuelva a numerar todas las extensiones de usuario si es necesario.
4. **Deshabilite cualquier troncal no utilizado** 105
   Deshabilitar el uso de troncales y canales de troncales que no están disponibles.
5. **Seleccione la fuente de reloj para troncales digitales** 107
   Alterar qué troncal digital se utiliza para proporcionar a IP Office su señal de reloj para la sincronización de llamadas.
6. **Introducir prefijos de troncales** 109
   En los sistemas donde se utiliza un prefijo para la marcación externa, asegúrese de agregar el mismo prefijo a los números entrantes para permitir la devolución de llamadas.
7. **Selección del modo de puerto DS16B/30B** 110
   Estos módulos pueden admitir teléfonos Avaya T-Series y M-Series al proporcionar puertos BST u otros teléfonos digitales Avaya al proporcionar puertos DS. La selección del tipo de puerto para todo el módulo se realiza mediante IP Office Manager.
8. **Carga del archivo de licencia** 111
   Cargue el archivo de licencia provisto para el sistema y verifique el estado de la licencia para las licencias.

Configuración de seguridad básica

Después de completar la configuración básica, debe seguir los procesos en elSistema de seguridad 132capítulo.

Traducido del inglés al español - www.onlinedoctranslator.com

7.1 Conexión de red

La siguiente sección detalla cómo unnuevo El sistema IP Office determina qué dirección IP debe usar.

Resolución de dirección IP y modo DHCP

Cuando se enciende una unidad de control de IP Office predeterminada o nueva, solicita información de la dirección IP de un servidor DHCP. Esto ocurre independientemente de si un cable LAN está conectado o no. El proceso a continuación se realiza por separado para el puerto LAN (LAN1 en la configuración) y el puerto WAN (LAN2 en la configuración) en la parte posterior de la unidad de control de IP Office.

- El sistema hace una solicitud de DHCP para saber qué información de dirección IP debe usar.
- Si un servidor DHCP responde dentro de aproximadamente 10 segundos, la unidad de control se convierte en un cliente DHCP de forma predeterminada y utiliza la información de la dirección IP proporcionada por el servidor DHCP.
- Si no responde ningún servidor DHCP, la unidad de control sigue siendo el cliente DHCP por defecto, pero asume las siguientes direcciones por defecto:
  - Puerto LAN (LAN1): 192.168.42.1/255.255.255.0.
  - Puerto WAN (LAN2): 192.168.43.1/255.255.255.0.
  - Tenga en cuenta que IP Office no verifica que estas direcciones sean válidas o estén disponibles en la red.
- Los sistemas que se ejecutan en los modos estándar de IP Office se pueden configurar como un servidor DHCP. También se pueden configurar para que solo proporcionen DHCP para teléfonos IP de Avaya o para conexiones de marcado de acceso remoto. Las opciones del servidor DHCP no son compatibles con los sistemas que se ejecutan en los modos IP Office Basic Edition.
- **!**Una vez que una unidad de control IP500 V2 haya obtenido la dirección IP y la configuración del modo DHCP, conservará esa configuración incluso si se reinicia sin un archivo de configuración presente en la tarjeta SD del sistema. Para eliminar por completo la dirección IP existente y la configuración del modo DHCP, debepor defecto la configuración del sistema 170.

Conexión a la computadora

Según las condiciones que se aplicaron cuando se inició por primera vez la unidad de control de IP Office, se puede conectar una PC de la siguiente manera:

- **Si IP Office no está conectado a una red:**
  Conecte la PC directamente a IP Office. La PC debe configurarse en una dirección válida en la misma red que los valores predeterminados de IP Office anteriores.
- **Si IP Office está conectado a una red sin servidor DHCP:**
  Conecte la PC directamente a IP Office. La PC debe configurarse en una dirección válida en la misma red que los valores predeterminados de IP Office anteriores.
- **Si IP Office está conectado a una red con un servidor DHCP:**
  Conecte la PC a la red. La PC debe configurarse para ser un cliente DHCP o una dirección que sea válida para la red. La dirección que utiliza el sistema IP Office deberá determinarse a partir del servidor DHCP. La mayoría de los servidores enumeran las direcciones IP de los clientes registrados en ellos.
- **Si IP Office usó una configuración prediseñada:**
  Utilice las direcciones IP establecidas en esa configuración. Asegúrese de que la PC esté en la misma subred o en una red capaz de enrutar a esa subred.

¿Comentarios sobre este documento? infodev@avaya.com

Para iniciar sesión en un sistema mediante IP Office Manager:

1. Seleccione**Inicio | Todos los programas | Oficina de PI | Gerente**.

   - Si la PC tiene un software de firewall instalado, es posible que se le pregunte si desea permitir que este programa acceda a la red. Seleccione**Sí**o**OK**.

2. Compruebe la configuración predeterminada de la aplicación:

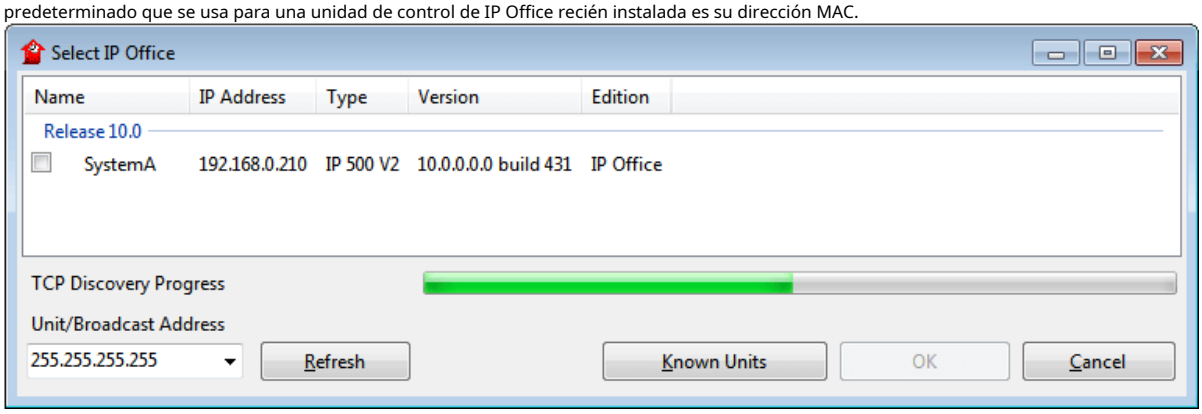
   una. Hacer clic**Archivo | preferencias**.

   b. Si no espera administrar nunca ningún sistema IP Office Basic Edition, seleccione**Predeterminado al modo estándar**. y deseleccionar**Establecer la vista simplificada como predeterminada**.

   una. Hacer clic**OK**.

3. Seleccione**Archivo | Configuración abierta**desde la barra de menú.

4. El**Seleccione IP Office**aparece la ventana. Después de unos segundos, debería mostrar la unidad de control de IP Office. El nombre para mostrar predeterminado que se usa para una unidad de control de IP Office recién instalada es su dirección MAC.



   - Si no se encuentra el sistema requerido, se puede cambiar la dirección utilizada para la búsqueda. Ingrese o seleccione la dirección requerida en el**Unidad/Dirección de transmisión**campo y luego haga clic en**Actualizar**para realizar una nueva búsqueda.

5. Haga clic en la casilla de verificación junto al sistema y luego haga clic en**OK**.

6. Se muestra la solicitud de nombre y contraseña. El nombre y la contraseña predeterminados son***Administrador***.

7. Ahora se le pedirá que pase por el menú de configuración inicial. VerConfiguracion inicial 103.

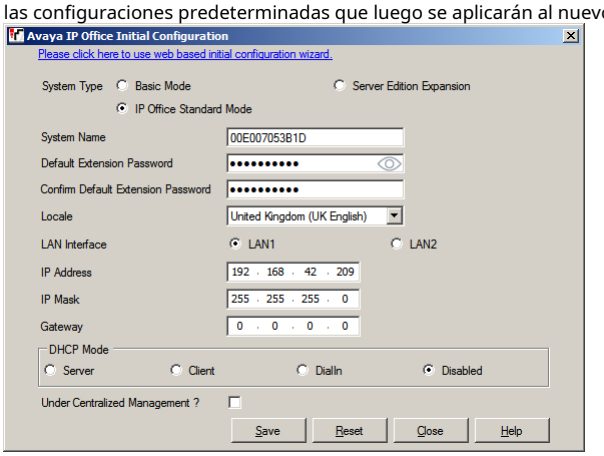
7.2 Configuración inicial

El menú de configuración inicial aparece la primera vez que IP Office Manager se conecta a un sistema nuevo o predeterminado.

- El menú de configuración inicial se puede volver a ejecutar en cualquier momento seleccionando**Archivo | Avanzado | Configuracion inicial**en IP Office Manager o**Acciones | Comandos de servicio | Configuración inicial en**Administrador web de IP Office. Sin embargo, tenga en cuenta que esto borra la mayor parte de la configuración del sistema existente.

Para iniciar la configuración inicial mediante IP Office Manager:

1. Usando IP Office Manager,conectarse al sistema 101.
2. Se le solicitará que cambie las contraseñas predeterminadas.
   - **Contraseña de administrador**
     Esta contraseña se utiliza para acceder a la configuración de telefonía del sistema.
   - **Contraseña del administrador de seguridad**
     Esta contraseña se utiliza para acceder a la configuración de seguridad del sistema. Tenga en cuenta que, de forma predeterminada, la contraseña de administrador anterior también se puede utilizar para la configuración de seguridad.
   - **Contraseña del sistema**
     Esta contraseña se usa para actualizaciones del sistema mediante IP Office Manager y también se puede usar para conectar System Monitor.
3. Introduzca las nuevas contraseñas y haga clic en**OK**.
4. El**Configuracion inicial**El menú le solicita que confirme el modo de operación requerido para el sistema. Para el **Tipo de sistema** Seleccione***Modo estándar de IP Office***y haga clic**Ahorrar**. Este modo cubre los sistemas IP Office Essential Edition y IP Office Preferred Edition.
5. El menú también le solicita configuraciones adicionales. Es importante que los verifique y configure correctamente, ya que afectan muchas de las configuraciones predeterminadas que luego se aplicarán al nuevo sistema:



   - **Nombre del sistema:**Se utiliza para ayudar a identificar y acceder al sistema.
   - **Contraseña de extensión predeterminada:**Esta contraseña se aplica al registro inicial de extensiones IP.
   - **Lugar:**Establezca un rango de configuraciones predeterminadas para cumplir con los requisitos de telefonía de ese país. También establece el idioma predeterminado para el sistema y todos los usuarios.
   - **Configuración de la dirección IP:**Compruebe que estos ajustes, especialmente el**Modo DHCP**, coincida con los requisitos de la red del cliente. Cambiar entre**LAN1**y**LAN2**para verificar la configuración de los puertos LAN y WAN respectivamente.
   - **En Gestión centralizada:**Esta configuración se usa para sistemas de sucursales en una red Avaya Aura. Consulte el separado documentación de instalación de sucursales 11
6. Haga clic en**Ahorrar**. La nueva configuración se abre en IP Office Manager. La nueva configuración no se ha guardado actualmente en el sistema. O:
   - **Continuar configuración básica:**
     Continúe con la configuración básica usando las siguientes secciones de este capítulo y luego guarde la configuración cuando termine.
   - **Guarde y luego continúe con la configuración básica:**
     Guardar la configuración 112como es actualmente. Esto puede hacer que el sistema se reinicie para usar la nueva configuración, el menú Guardar indicará si es necesario. Después de guardar la configuración, y una vez que el sistema se haya reiniciado si es necesario, vuelva a cargar la configuración y continúe con la configuración básica.
7. Continúe con la configuración básica o haga clic en continuar. icono de guardar enguardar la configuración actualizada 112y entonces

Página1119 de 3226.

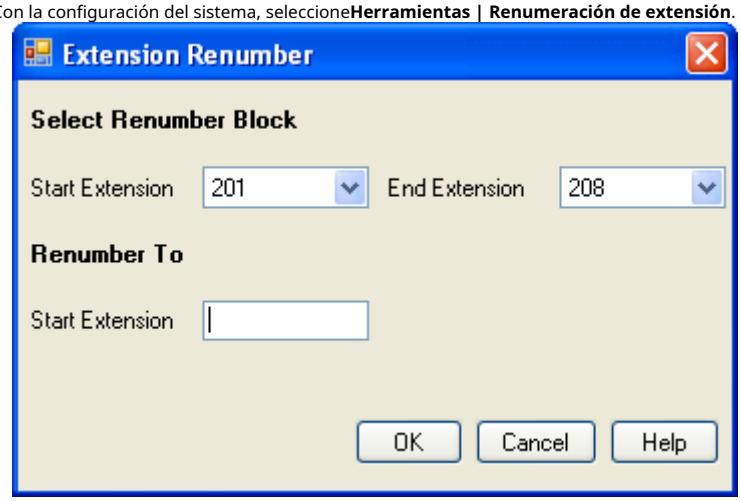
7.3 Numeración de extensiones

Los sistemas de modo estándar de IP Office pueden usar una combinación de números de extensión de hasta 15 dígitos de longitud. De forma predeterminada, los grupos de búsqueda y las extensiones reciben números de extensión de 3 dígitos a partir del 200 en adelante.

Para volver a numerar todas las extensiones de usuario mediante IP Office Manager:

Se puede usar IP Office Manager para cambiar la numeración de todas las extensiones del sistema. Esto también actualizará cualquier referencia al número de extensión en otros campos de configuración.

1. Con la configuración del sistema, seleccione**Herramientas** | **Renumeración de extensión**.



2. Seleccione el rango de extensiones de usuario existentes que desea volver a numerar e ingrese el nuevo número de extensión inicial para ese rango.

3. Haga clic en**OK**.

4. O bien:

- **Continuar configuración básica:**
  Continúe con la configuración básica usando las siguientes secciones de este capítulo y luego guarde la configuración cuando termine.
- **Guarde y luego continúe con la configuración básica:**
  Guardar la configuración [112] como es actualmente. Esto puede hacer que el sistema se reinicie para usar la nueva configuración, el menú Guardar indicará si es necesario. Después de guardar la configuración, y una vez que el sistema se haya reiniciado si es necesario, vuelva a cargar la configuración y continúe con la configuración básica.

5. Continúe con elConfiguracion basica [105] o haga clic en y luego icono de guardar enguardar la configuración actualizada [112] y continuar.

7.4 Deshabilitar troncales no utilizadas

Cada tarjeta de troncales de IP Office proporciona una cantidad fija de puertos de troncales con puertos de troncales digitales que admiten una cantidad fija de canales digitales. De manera predeterminada, la configuración de IP Office tiene entradas de configuración para todos los troncales y canales posibles.

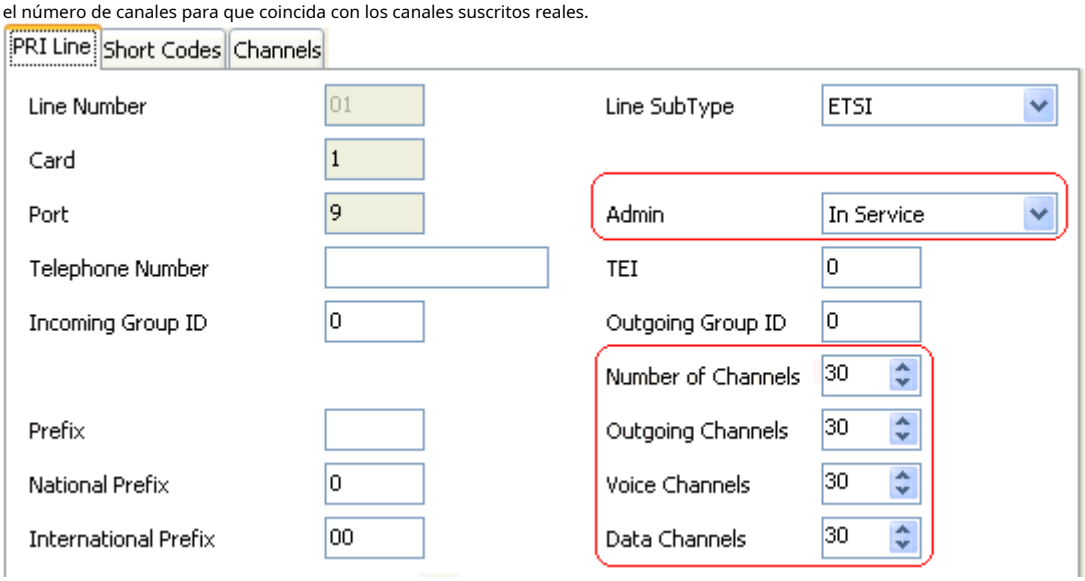
En los casos en que la cantidad de troncales o canales de troncales en uso o con licencia sea menor que la cantidad admitida por la tarjeta de troncales, las troncales y canales no utilizados deben deshabilitarse.

- ⚠ De lo contrario, se producirán problemas con las llamadas salientes. Por ejemplo, en un sistema con una tarjeta de troncales ATM4 instalada pero solo dos troncales analógicas realmente conectadas, si no se deshabilitan las otras dos troncales dentro de la configuración de IP Office, el 50 % de los intentos de llamadas salientes fallarán. Esto se debe a que el sistema no puede detectar automáticamente el estado del servicio de troncales analógicas individuales.
  - Para IP Office versión 8.1 Feature Pack 1 y superior con tarjetas IP500 Analog Trunk 4 V2 y tarjetas ATM4 Combination V2, el sistema puede detectar si las troncales analógicas están conectadas y, por lo tanto, puede tratar automáticamente los puertos de troncales no conectados como fuera de servicio.

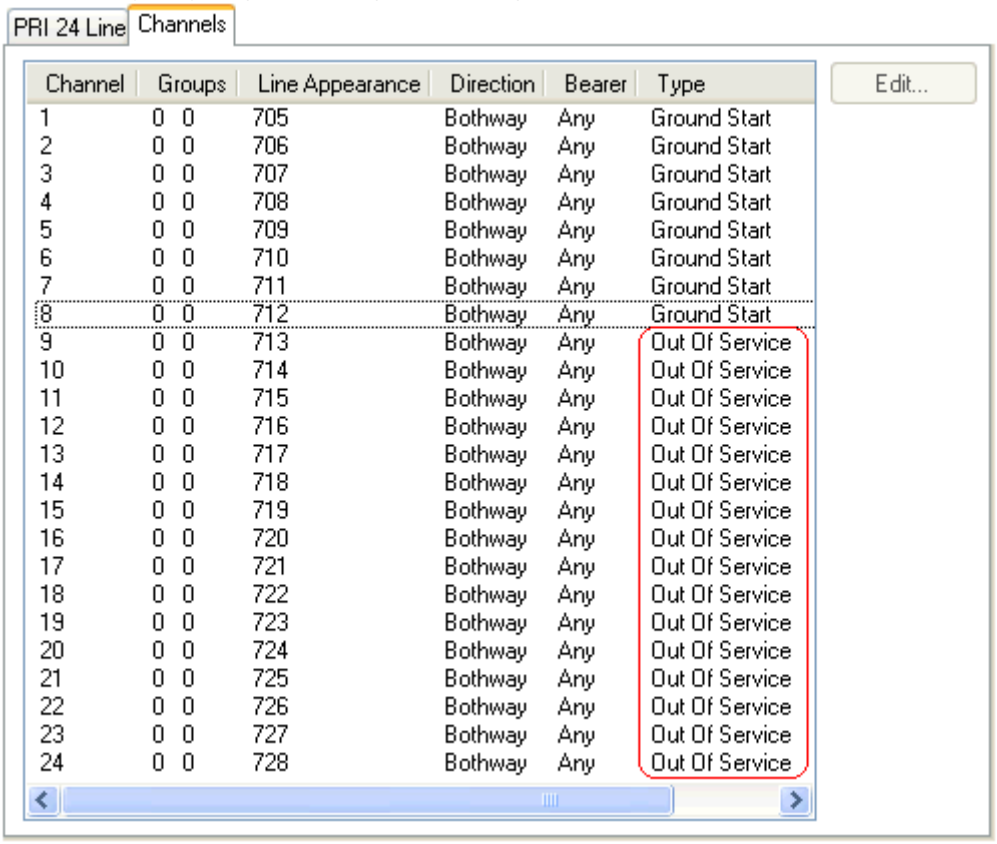
- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

Para deshabilitar las troncales no utilizadas mediante IP Office Manager:

1. Dentro de la configuración de IP Office, seleccione Línea.
2. Para cada línea, configure como fuera de servicio aquellas líneas o canales que no estén conectados o en uso. La ubicación de la configuración relevante varía para cada tipo de troncal.
   - **Troncales analógicos**
     Para deshabilitar todo el tronco, en el formulario principal configure el**Administración**opción a***Fuera de servicio***.
   - **Troncales BRI, E1 PRI, S0 y QSIG**
     Para deshabilitar todo el tronco, en el formulario principal configure el**Administración**opción a***Fuera de servicio***. De lo contrario, configure el número de canales para que coincida con los canales suscritos reales.



- **Troncales T1, T1 PRI y E1R2**
  Para deshabilitar todo el tronco, en el formulario principal configure el**Administración**opción a***Fuera de servicio***. De lo contrario, seleccione la pestaña Canales y configure aquellos canales que no se utilizan para**Fuera de servicio**.



Channel	Groups	Line Appearance	Direction	Bearer	Type
1	0 0	705	Bothway	Any	Ground Start
2	0 0	706	Bothway	Any	Ground Start
3	0 0	707	Bothway	Any	Ground Start
4	0 0	708	Bothway	Any	Ground Start
5	0 0	709	Bothway	Any	Ground Start
6	0 0	710	Bothway	Any	Ground Start
7	0 0	711	Bothway	Any	Ground Start
8	0 0	712	Bothway	Any	Ground Start
9	0 0	713	Bothway	Any	Out Of Service
10	0 0	714	Bothway	Any	Out Of Service
11	0 0	715	Bothway	Any	Out Of Service
12	0 0	716	Bothway	Any	Out Of Service
13	0 0	717	Bothway	Any	Out Of Service
14	0 0	718	Bothway	Any	Out Of Service
15	0 0	719	Bothway	Any	Out Of Service
16	0 0	720	Bothway	Any	Out Of Service
17	0 0	721	Bothway	Any	Out Of Service
18	0 0	722	Bothway	Any	Out Of Service
19	0 0	723	Bothway	Any	Out Of Service
20	0 0	724	Bothway	Any	Out Of Service
21	0 0	725	Bothway	Any	Out Of Service
22	0 0	726	Bothway	Any	Out Of Service
23	0 0	727	Bothway	Any	Out Of Service
24	0 0	728	Bothway	Any	Out Of Service

  - Para T1 establecer el**Escribe**a***Fuera de servicio***.
  - Para T1 PRI configure el**Administración**campo a***Fuera de servicio***.
  - Para troncales E1R2 configure el**Tipo de señalización de línea**a***Fuera de servicio***.

3. O bien:
   - **Continuar configuración básica:**
     Continúe con la configuración básica usando las siguientes secciones de este capítulo y luego guarde la configuración cuando termine.
   - **Guarde y luego continúe con la configuración básica:**
     Guardar la configuración [112] como es actualmente. Esto puede hacer que el sistema se reinicie para usar la nueva configuración, el menú Guardar indicará si es necesario. Después de guardar la configuración, y una vez que el sistema se haya reiniciado si es necesario, vuelva a cargar la configuración y continúe con la configuración básica.
4. Continúe con elConfiguracion basica [107] o haga clic en luego icono de guardar enguardar la configuración actualizada [112] y continuar y luego continuar.

7.5 Configuración de la fuente del reloj de la troncal digital

Las troncales digitales requieren que el sistema telefónico en cada extremo de la troncal comparta una señal de reloj para garantizar la sincronización de la señalización de llamadas. IP Office puede obtener y utilizar la señal del reloj de cualquiera de sus troncales digitales. Por lo general, se usa la señal de reloj proporcionada por un troncal digital desde la central telefónica, ya que suele ser la fuente de reloj más precisa y confiable.

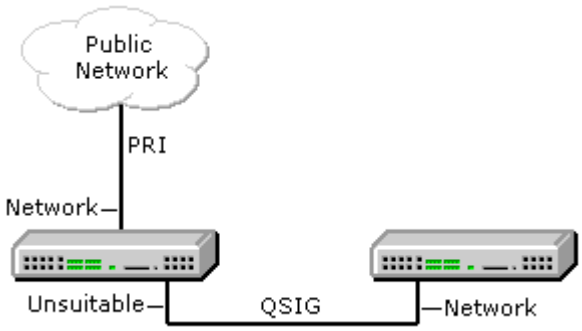
Si no hay una fuente de reloj troncal disponible, el sistema puede usar su propio reloj interno si es necesario. Sin embargo, se prefiere una fuente troncal externa. Para hacer esto, el**Calidad del reloj**la configuración en cada línea en la configuración de IP Office se establece en uno de los siguientes:

- ***La red***
  Si está disponible, la señal de reloj de esta troncal debe usarse como fuente de reloj para la sincronización de llamadas. Si se configuran varias troncales con esta configuración, la troncal utilizada se determina en el orden de las ranuras 1 a 4 y luego por puerto en cada ranura.

- ***Retroceder***
  Si está disponible, la señal de reloj de esta troncal se puede usar como fuente de reloj si ninguna de las troncales está configurada como***La red*** están proporcionando una fuente de reloj. Si se configuran varias troncales con esta configuración, la troncal utilizada se determina en el orden de las ranuras 1 a 4 y luego por puerto en cada ranura.

- ***Inadecuado***
  La fuente de reloj de este troncal no se utilizará como fuente de reloj.

En el siguiente ejemplo, la primera IP Office está configurada para usar el enlace troncal de la red pública como su fuente de reloj e ignorar la posible fuente de reloj del enlace troncal QSIG. El otro sistema IP Office utiliza la señal de reloj recibida del primer IP Office en su troncal QSIG como fuente de reloj. Por lo tanto, ambas IP Offices utilizan la misma fuente de reloj y esa fuente de reloj es el intercambio de la red pública.



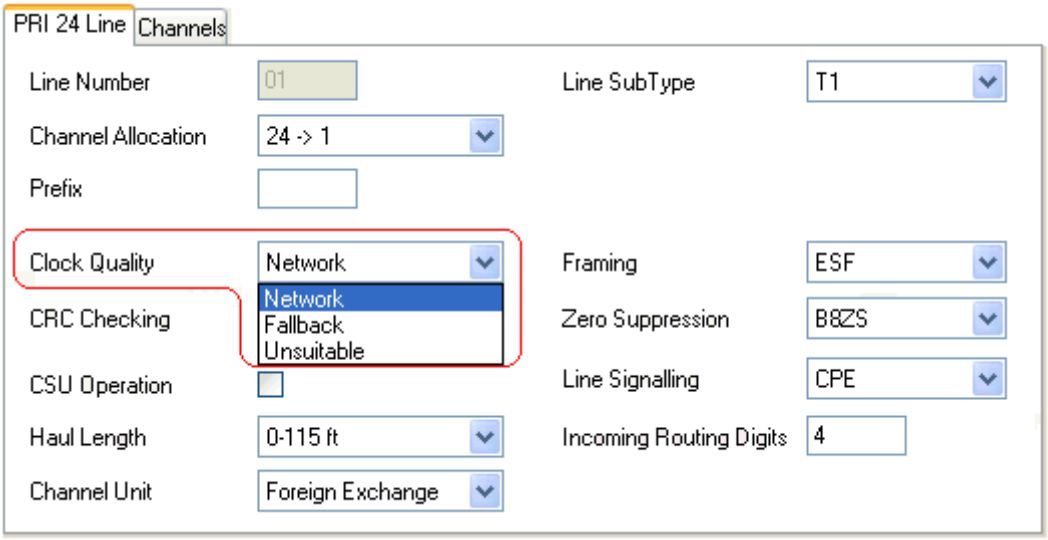
Visualización de la fuente de reloj actual

La fuente de reloj actual que utiliza un sistema IP Office se muestra en la**Recursos**dentro de la aplicación de estado del sistema.

Para configurar la fuente de calidad del reloj de una troncal mediante IP Office Manager:

1. Dentro de la configuración de IP Office, seleccione **Línea**.

2. Para cada línea digital, seleccione la línea y, en la pestaña Línea, seleccione si esa troncal debe proporcionar la fuente de reloj para la red o si la troncal no es adecuada. Para troncales E1R2 el**Calidad del reloj**el ajuste está en el **Avanzado**pestaña.



3. Asegúrese de que solo una troncal esté configurada para***La red***. Preferiblemente, debería ser una troncal digital directa a la central telefónica.

4. Otro baúl se puede configurar como***Retroceder***en caso de que se pierda la conexión troncal de red seleccionada. Si es posible, debe ser un enlace troncal de un proveedor diferente, ya que eso reduce las posibilidades de que ambas fuentes fallen al mismo tiempo.

5. Asegúrese de que todas las demás troncales digitales estén configuradas como***Inadecuado***.

6. O bien:

- **Continuar configuración básica:**
  Continúe con la configuración básica usando las siguientes secciones de este capítulo y luego guarde la configuración cuando termine.
- **Guarde y luego continúe con la configuración básica:**
  Guardar la configuración 112como es actualmente. Esto puede hacer que el sistema se reinicie para usar la nueva configuración, el menú Guardar indicará si es necesario. Después de guardar la configuración, y una vez que el sistema se haya reiniciado si es necesario, vuelva a cargar la configuración y continúe con la configuración básica.

7. Continúe con elConfiguracion basica 109o haga clic en y luego icono de guardar enguardar la configuración actualizada 112y continuar.

7.6 Configuración de los prefijos de troncales

De manera predeterminada, los sistemas con una tarjeta SD del sistema U-Law usan un prefijo 9 para llamadas externas. Los sistemas comenzaron con una tarjeta SD del sistema A-Law predeterminada sin prefijo (cualquier marcación que no coincida con un número interno se supone que es un número externo).

Cuando se usa un prefijo para las llamadas salientes, ese mismo prefijo debe agregarse a la configuración de troncales. Ese prefijo troncal se usa de la siguiente manera:

- **Llamadas entrantes**
  En las llamadas entrantes, el prefijo establecido de la troncal se agrega a cualquier identificador de llamadas entrantes recibido con la llamada y se almacena en el registro de llamadas en los teléfonos, etc. devolver llamadas. Por ejemplo, si el sistema está configurado para requerir un 9 para indicar una llamada saliente, la troncal debe agregar un 9 a la identificación de llamadas entrantes para que esa identificación pueda usarse para devolver llamadas.
- **Llamadas salientes**
  En las llamadas salientes, los códigos cortos utilizados para enrutar la llamada a una troncal deben eliminar cualquier prefijo de marcado externo (por ejemplo, 9) para que el número marcado desde el sistema a la troncal sea adecuado para el enrutamiento por parte del proveedor de la troncal.

Para establecer prefijos de líneas troncales mediante IP Office Manager:

1. Dentro de la configuración de IP Office, seleccione Línea.
2. Para cada línea ingrese el prefijo. La ubicación de la configuración del prefijo varía para cada tipo de troncal. Algunos tipos de troncales tienen un solo campo de prefijo. Otros tipos de troncales pueden tener campos de prefijo separados para llamadas nacionales, internacionales y de otro tipo.
3. O bien:
   - **Continuar configuración básica:**
     Continúe con la configuración básica usando las siguientes secciones de este capítulo y luego guarde la configuración cuando termine.
   - **Guarde y luego continúe con la configuración básica:**
     Guardar la configuración 112 como es actualmente. Esto puede hacer que el sistema se reinicie para usar la nueva configuración, el menú Guardar indicará si es necesario. Después de guardar la configuración, y una vez que el sistema se haya reiniciado si es necesario, vuelva a cargar la configuración y continúe con la configuración básica.
4. Continúe con elConfiguracion basica 110 o haga clic en y luego icono de guardar enguardar la configuración actualizada 112 y continuar.

7.7 Selección del modo de puerto DS16B/30B

Cada módulo de expansión externo IP500 DS16B/DS30B y DS16B2/DS30B2 en un sistema puede admitirPuertos de teléfono DS 271oPuertos telefónicos BST 270.Los módulos funcionan por defecto con el puerto de teléfono DS. El modo de cualquier módulo en particular se puede cambiar a través de la configuración del sistema.

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.
- **Comportamiento de actualización de DS16B/DS30B:**
  Para los módulos DS16B/DS30B, el proceso de carga del firmware apropiado para el modo seleccionado o la actualización demora hasta 10 minutos, tiempo durante el cual el módulo no está disponible.
- **Comportamiento de actualización de DS16B2/DS30B2:**
  El comportamiento de DS16/30B2 durante la actualización del firmware o el cambio de modos difiere de otras unidades de expansión externas:
  - Durante la actualización del firmware, la unidad permanece operativa y puede realizar y recibir llamadas.
  - Una vez que se completa la actualización (aproximadamente 9 minutos), la unidad se reinicia y tarda unos 45 segundos en volver al funcionamiento normal.

Para cambiar el modo de puerto del módulo IP500 DS16B/30B:

1. Dentro de la configuración de IP Office, seleccione **Unidad de control**. La unidad de control y los módulos de expansión externos están la lista.
2. Los módulos IP500 DS16B e IP500 DS30B se enumeran como***DIG ADPx16 RJ45***y***CAVAR ADPx30 RJ45***.
3. Seleccione uno de los módulos de expansión externos. En los detalles de la unidad, el**Modo operativo**La lista desplegable se utiliza para seleccionar qué tipo de teléfonos admite el módulo. Seleccione el modo requerido.
   - Para puertos DS, seleccione***Teléfonos de las series DS - 1400, 9500, 5400, 2400, T3, 4400***.
   - Para puertos BST, seleccione***BST - Teléfonos de la serie T7000, M7000***.
4. Haga clic en**OK**.
5. Continúe con elConfiguracion basica 111o haga clic en y luego icono de guardar enguardar la configuración actualizada 112y continuar.

7.8 Carga del archivo de licencia

El sistema IP Office requiere licencia para algunas funciones, consulteLicencias 279.El archivo de licencia se puede cargar manualmente oprecargado en la tarjeta SD del sistema 78.

¿Cómo se licencia el sistema?

- Se carga en el sistema un archivo XML que contiene el conjunto completo de licencias PLDS. El archivo de licencia es único para el número de serie de la clave de función de la tarjeta SD del sistema instalada en el sistema.
    - El ID de host PLDS utilizado para el archivo de licencia debe coincidir con el que se muestra en los 12 dígitos.**Identificación PLDS**impreso en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra con**FK**o**FK SN**. Para esas tarjetas agregue el prefijo***11***para obtener la identificación PLDS de la tarjeta.

Requisitos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una**Edición esencial**licencia del sistema para la versión específica de IP Office que desea ejecutar.

Para cargar el archivo de licencia mediante IP Office Manager:

1. Dentro de la configuración del sistema haga clic en **Licencia**.
2. El campo**Id. de host PLDS**muestra el número de serie de la tarjeta SD del sistema instalada en el sistema. Compruebe que este número coincida con el que se han emitido las licencias.
    - El ID de host PLDS utilizado para el archivo de licencia debe coincidir con el que se muestra en los 12 dígitos.**Identificación PLDS**impreso en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra con**FK**o**FK SN**. Para esas tarjetas agregue el prefijo***11***para obtener la identificación PLDS de la tarjeta.
3. Haga clic en**Agregar...**.
4. Para el tipo de licencia seleccione**plds**y haga clic**OK**.
5. Busque la ubicación del archivo XML proporcionado que contiene las licencias. Seleccione el archivo y haga clic en**Abierto**.
6. Continúe con elConfiguracion basica 112o haga clic en y luego icono de guardar enguardar la configuración actualizada 112y continuar.

7.9 Guardar la configuración

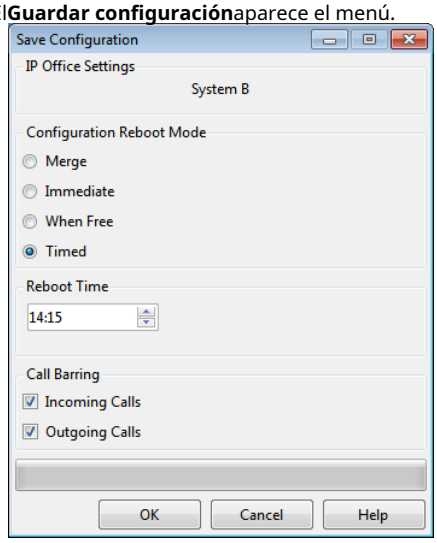
Una vez completada la configuración básica, la nueva configuración debe volver a guardarse en el sistema. Es muy probable que esto requiera que el sistema se reinicie.

Después de guardar la configuración, vuelva a cargarla en IP Office Manager;

- Si se cambió la configuración de la dirección IP, es posible que deba cambiar la configuración de su PC para volver a cargar la configuración.
- Después de volver a cargar la configuración, todas las licencias deberían aparecer ahora como ***Válido***.

Para guardar los cambios de configuración mediante IP Office Manager:

1. Haga clic en **OK** para guardar cualquier cambio en el menú actual.
2. Haga clic en el icono.
3. El **Guardar configuración** aparece el menú.



- **Unir**
  Este método se selecciona automáticamente si ninguno de los cambios de configuración realizados requiere un reinicio del sistema. Si este método se usa para una configuración que incluye cambios que requieren un reinicio, esos cambios no se aplican hasta que el sistema se reinicia manualmente.
- **Inmediato**
  Este método guarda los nuevos cambios de configuración y luego reinicia el sistema. Se finalizan todas las llamadas y servicios en curso. Este método se selecciona automáticamente si alguno de los cambios realizados hasta el momento requiere un reinicio antes de que se apliquen al sistema.
- **Libre**
  Este método permite la **Restricción de llamadas entrantes** y **Restricción de llamadas salientes** opciones a utilizar. El sistema se reinicia cuando se cumplen los criterios de las opciones seleccionadas.
- **Temporizado (HH:MM)**
  Este método reinicia el sistema a la hora seleccionada. También se puede usar con las opciones de restricción de llamadas para reiniciar solo después del tiempo establecido cuando las opciones seleccionadas coinciden.
- **Restricción de llamadas entrantes**
  Esta opción se puede utilizar con el **Libre** y **cronometrado** métodos de reinicio. Cuando se selecciona, el sistema bloquea cualquier otra llamada entrante. Sin embargo, permite que las llamadas existentes continúen hasta que finalicen.
- **Restricción de llamadas salientes**
  Esta opción se puede utilizar con el **Libre** y **cronometrado** métodos de reinicio. Cuando se selecciona, el sistema bloquea cualquier otra llamada saliente. Sin embargo, permite que las llamadas existentes continúen hasta que finalicen.
  - **!ADVERTENCIA**
    Esta opción también prohíbe la realización de llamadas de emergencia. . Por lo tanto, solo debe usarse con precaución.

4. Seleccione las opciones requeridas y haga clic en **OK**.

Configuración de seguridad básica

Después de completar la configuración básica, debe seguir los procesos en el Sistema de seguridad 132 capítulo.

Capítulo 8.

Configuración inicial con IP Office Web Manager

8. Configuración inicial mediante IP Office Web Manager

Puede usar su navegador web para configurar un sistema IP500 V2 a través de sus menús de IP Office Web Manager. Para los nuevos sistemas IP500 V2, eso incluye ejecutar una serie de menús de configuración del asistente inicial para cubrir las configuraciones clave para un nuevo sistema.

8.1 La dirección IP inicial del sistema

Para conectarse a un nuevo sistema utilizando un navegador, primero debe determinar qué dirección IP ha adoptado el sistema.

La siguiente sección detalla cómo unnuevo El sistema IP Office determina qué dirección IP debe usar.

Resolución de dirección IP y modo DHCP

Cuando se enciende una unidad de control de IP Office predeterminada o nueva, solicita información de la dirección IP de un servidor DHCP. Esto ocurre independientemente de si un cable LAN está conectado o no. El proceso a continuación se realiza por separado para el puerto LAN (LAN1 en la configuración) y el puerto WAN (LAN2 en la configuración) en la parte posterior de la unidad de control de IP Office.

- El sistema hace una solicitud de DHCP para saber qué información de dirección IP debe usar.
- Si un servidor DHCP responde dentro de aproximadamente 10 segundos, la unidad de control se convierte en un cliente DHCP de forma predeterminada y utiliza la información de la dirección IP proporcionada por el servidor DHCP.
- Si no responde ningún servidor DHCP, la unidad de control sigue siendo el cliente DHCP por defecto, pero asume las siguientes direcciones por defecto:
  - Puerto LAN (LAN1): 192.168.42.1/255.255.255.0.
  - Puerto WAN (LAN2): 192.168.43.1/255.255.255.0.
  - Tenga en cuenta que IP Office no verifica que estas direcciones sean válidas o estén disponibles en la red.
- Los sistemas que se ejecutan en los modos estándar de IP Office se pueden configurar como un servidor DHCP. También se pueden configurar para que solo proporcionen DHCP para teléfonos IP de Avaya o para conexiones de marcado de acceso remoto. Las opciones del servidor DHCP no son compatibles con los sistemas que se ejecutan en los modos IP Office Basic Edition.
- **!**Una vez que una unidad de control IP500 V2 haya obtenido la dirección IP y la configuración del modo DHCP, conservará esa configuración incluso si se reinicia sin un archivo de configuración presente en la tarjeta SD del sistema. Para eliminar por completo la dirección IP existente y la configuración del modo DHCP, debepor defecto la configuración del sistema 170.

Conexión a la computadora

Según las condiciones que se aplicaron cuando se inició por primera vez la unidad de control de IP Office, se puede conectar una PC de la siguiente manera:

- **Si IP Office no está conectado a una red:**
  Conecte la PC directamente a IP Office. La PC debe configurarse en una dirección válida en la misma red que los valores predeterminados de IP Office anteriores.
- **Si IP Office está conectado a una red sin servidor DHCP:**
  Conecte la PC directamente a IP Office. La PC debe configurarse en una dirección válida en la misma red que los valores predeterminados de IP Office anteriores.
- **Si IP Office está conectado a una red con un servidor DHCP:**
  Conecte la PC a la red. La PC debe configurarse para ser un cliente DHCP o una dirección que sea válida para la red. La dirección que utiliza el sistema IP Office deberá determinarse a partir del servidor DHCP. La mayoría de los servidores enumeran las direcciones IP de los clientes registrados en ellos.
- **Si IP Office usó una configuración prediseñada:**
  Utilice las direcciones IP establecidas en esa configuración. Asegúrese de que la PC esté en la misma subred o en una red capaz de enrutar a esa subred.

8.2 Instalación del nuevo sistema

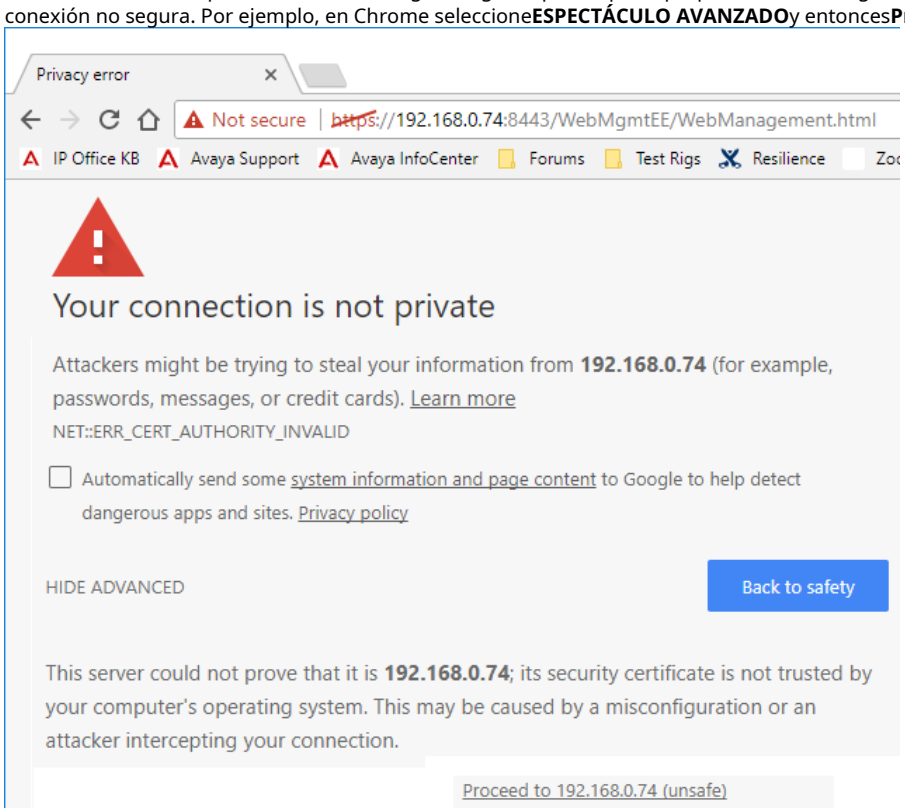
Habiendo determinado la nueva dirección IP del sistema y configurado su PC para poder conectarse a direcciones en ese rango:

1. Introduzca la dirección IP actual del sistema en la barra de direcciones de su navegador.

2. Haga clic en**Administrador web de IP Office**.

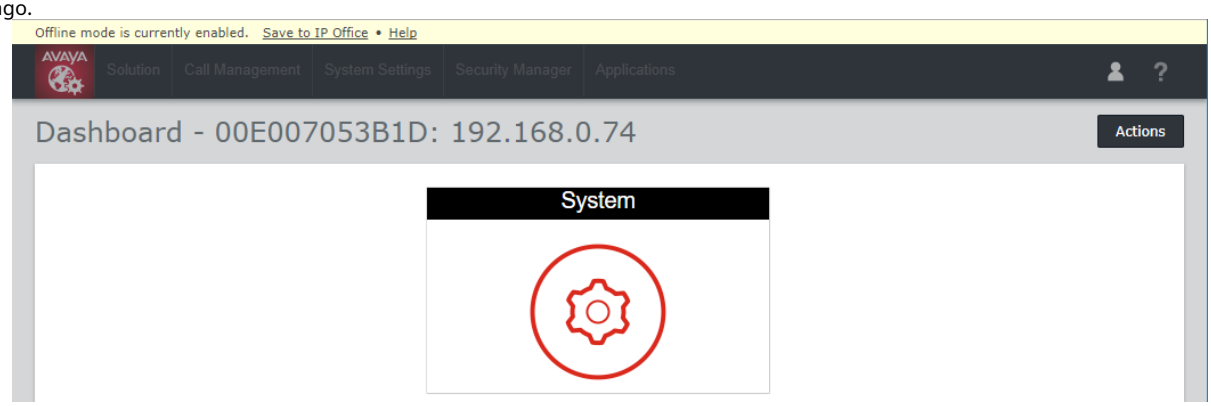
   - La dirección que se muestra ahora es similar a*https://192.168.0.42:8443/WebMgmtEE/WebManagement.html*. Esta es la dirección del administrador web para los sistemas en modo que no son de IP Office Basic Edition.

3. La conexión en esta etapa no se considera segura. Siga los pasos que le proporcione su navegador para continuar con una conexión no segura. Por ejemplo, en Chrome seleccione**ESPECTÁCULO AVANZADO**y entonces**Proceder**.

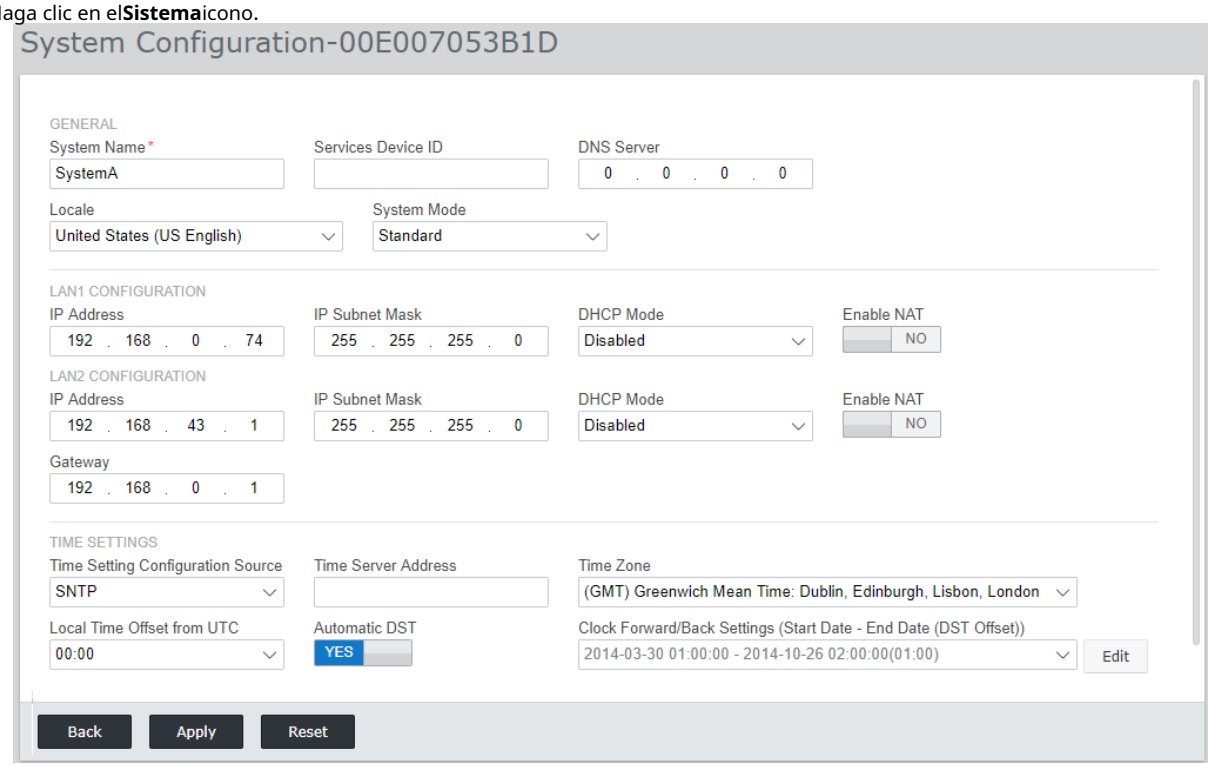


4. En el menú de inicio de sesión, inicie sesión con el nombre y la contraseña predeterminados***Administrador***.

5. IP Office Web Manager se inicia y muestra el tablero del sistema. Para un sistema nuevo, esto solo contiene el ícono para el**Sistema** mago.



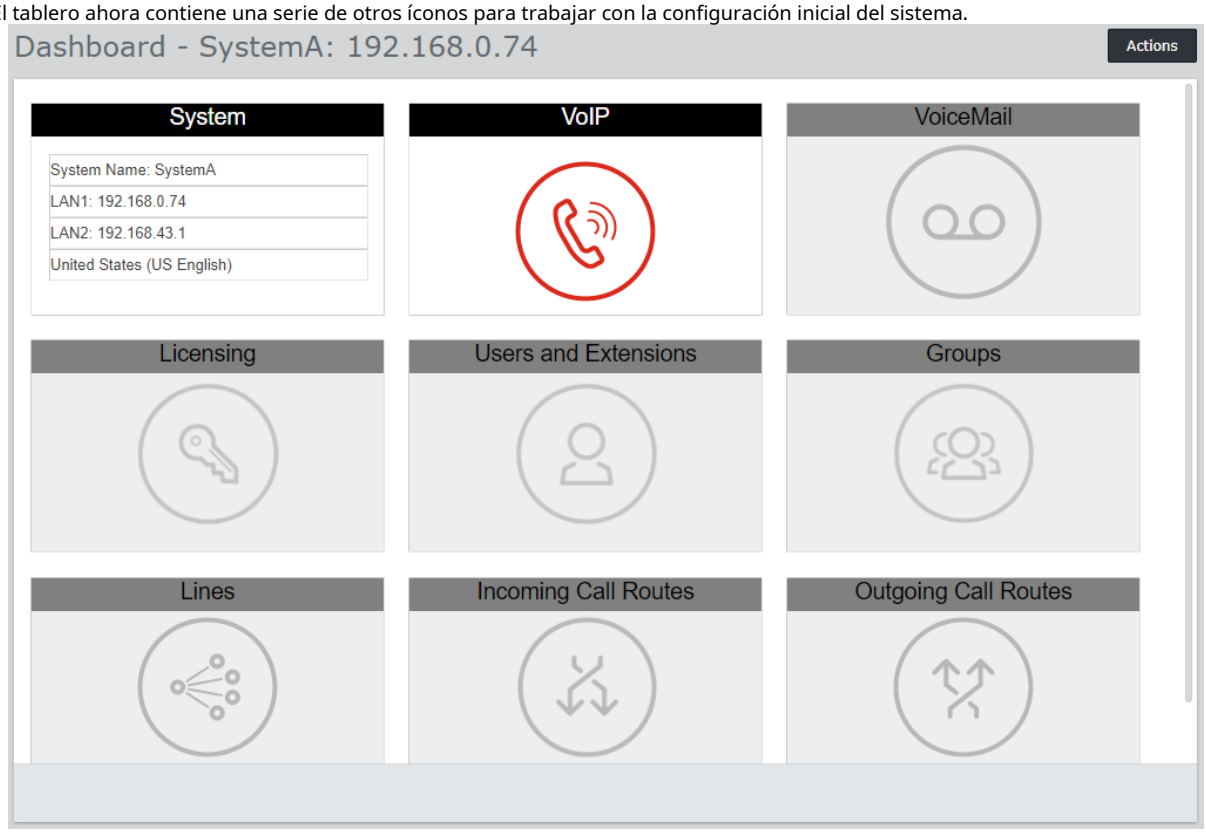
6. Haga clic en el**Sistema**icono.



7. Ingrese los detalles que desea que use el sistema. En esta etapa, los valores clave son un nombre del sistema, la configuración regional, el modo del sistema (establezca esto en Estándar) y la dirección IP. Para detalles completos de la**Sistema**opciones verAjustes del sistema [120].

8. Haga clic en**Aplicar**.

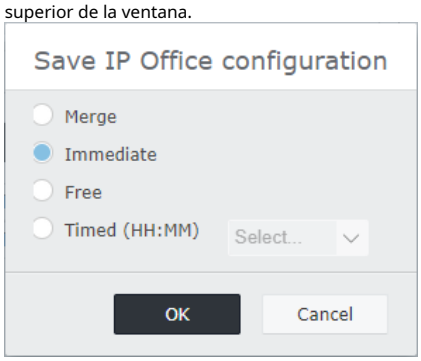
9. El tablero ahora contiene una serie de otros íconos para trabajar con la configuración inicial del sistema.



10. El siguiente icono en el que debe hacer clic se resalta en rojo. Después de completar cada conjunto de configuraciones, el ícono en el panel se reemplaza con un resumen de las configuraciones clave y se resalta el siguiente ícono. Puede volver a los paneles anteriores si desea realizar más cambios en su configuración. Para obtener detalles de los paneles individuales, utilice los siguientes enlaces:

- Sistema 120
- Licencia 124
- Líneas 127
- VoIP 122
- Usuarios y Extensiones 125
- Rutas de llamadas entrantes 128
- Mensaje de voz 123
- Grupos 126
- Rutas de llamadas salientes 129 *(Estados Unidos/Canadá solamente)*

11. Una vez que haya completado todos los pasos del asistente, haga clic en el**Guardar en IP Office**enlace que se muestra en la barra amarilla en la parte superior de la ventana.



12. El menú de configuración de guardado se muestra con una configuración de guardado recomendada basada en los cambios que ha realizado. Para una nueva instalación, es probable que se guarde usando un reinicio inmediato del nuevo sistema. Acepte la configuración recomendada y haga clic en**OK**.

13. Después del reinicio, continúe con la configuración del sistema utilizando la nueva dirección IP del sistema.

8.3 Sistema existente

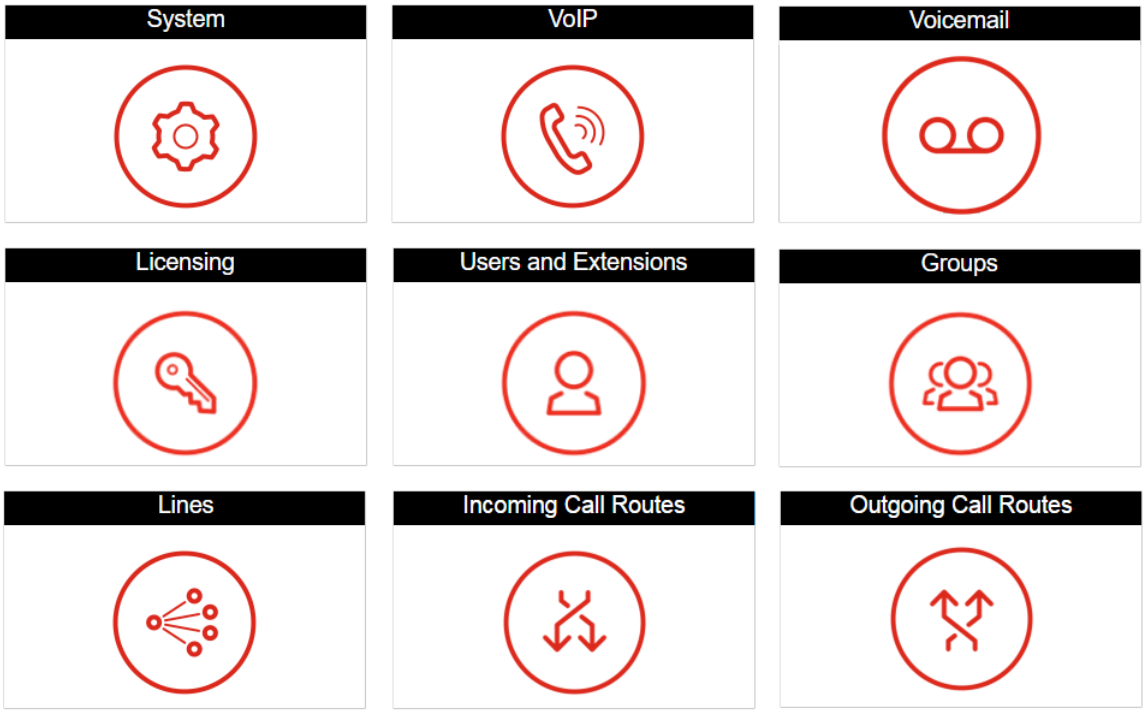
Puede volver a los menús del Tablero en cualquier momento después de haber instalado un sistema. Simplemente haga clic en**Solución**. Sin embargo, la mayoría de los paneles del tablero solo se pueden usar para cambiar la configuración del sistema si se accede mientras IP Office Web Manager está en modo fuera de línea.

Para acceder al tablero activo en un sistema configurado:

1. Haga clic en**Solución**. Se muestra el tablero.
2. Pase el cursor sobre el icono y haga clic**Modo offline**.
3. Haga clic en**OK**.
   - Si el tablero se usó anteriormente pero sin guardar todos los datos, puede mostrar una opción para **Reanudar**o**Desechar**la configuración de la sesión anterior.
4. Ahora puede utilizar elmenús del tablero 119para cambiar los ajustes de configuración clave.

8.4 Menús del asistente del tablero

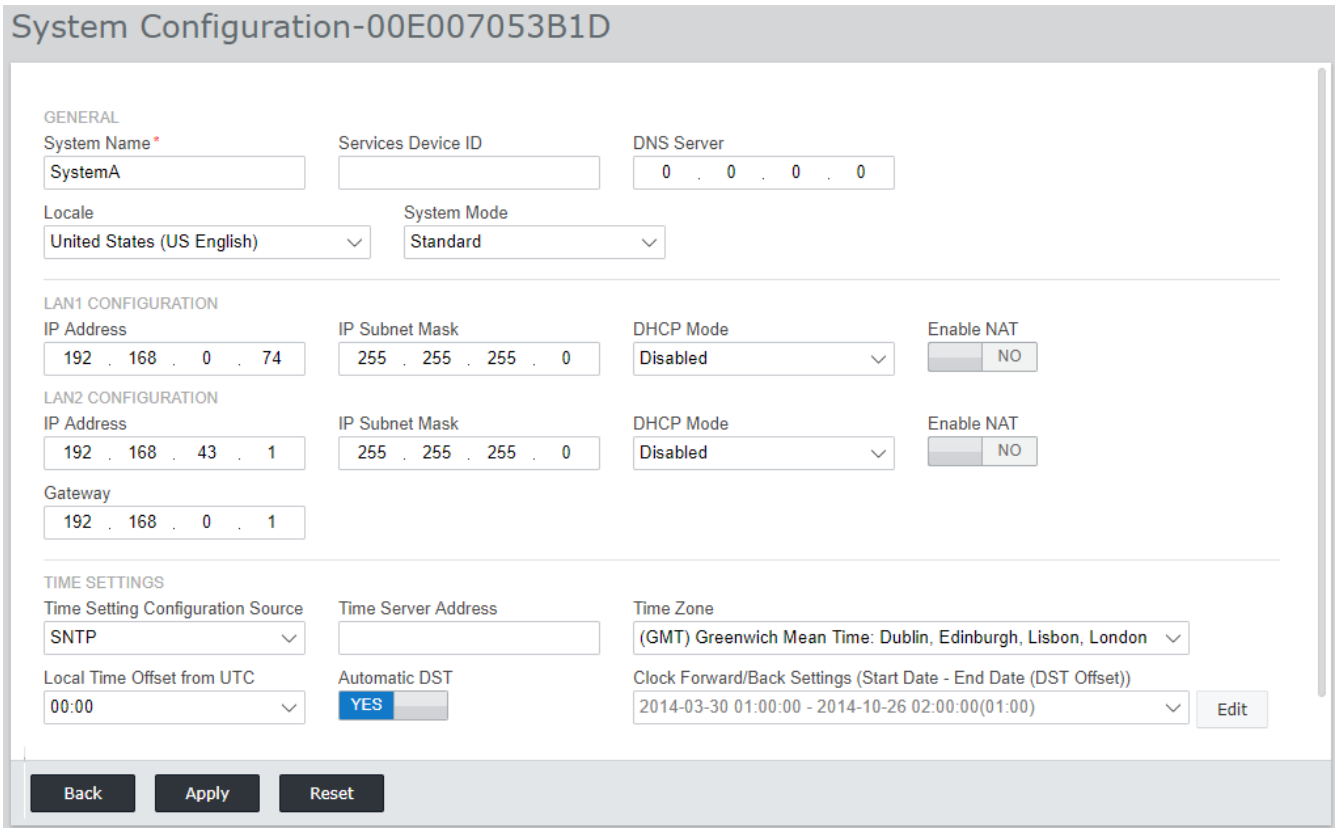
Esta sección proporciona un resumen de los menús del asistente del tablero únicamente. Para obtener detalles completos, consulte el *"Administración del sistema IP Office mediante Web Manager"* ayuda y manual.



- Sistema 120
- VoIP 122
- Mensaje de voz 125
- Licencia 124
- Usuarios y Extensiones 125
- Grupos 126
- Líneas 127
- Rutas de llamadas entrantes 128
- Rutas de llamadas salientes 129
  (Estados Unidos/Canadá solamente)

8.4.1 Configuración del sistema

Este panel permite la configuración de una serie de configuraciones clave (ubicación, modo, dirección IP y configuración de hora/fecha).



- **Nombre del sistema**
  Este nombre se utiliza para identificar el sistema en otras herramientas y menús.

- **Conservar configuración**
  Esta opción solo se muestra cuando el tablero se usa para reconfigurar un sistema existente en lugar de un sistema nuevo o predeterminado. Si se selecciona, esta opción conservará la mayor parte posible de la configuración existente, excepto las configuraciones modificadas a través del tablero. Si está deshabilitado, todos los demás ajustes de configuración que no sean los establecidos a través del tablero vuelven a sus valores predeterminados.

- **Identificación del dispositivo de servicios**
  Establezca este campo si se ha proporcionado un valor. Normalmente, un valor se establece automáticamente cuando el sistema se registra a través del Proceso de integración [138] después de la instalación.

- **Servidor DNS**
  Ingrese la dirección del servidor de nombres de dominio (DNS) que el sistema debe usar para convertir los nombres de los servidores en direcciones IP.

- **Lugar**
  Este valor establece una gran cantidad de valores predeterminados del sistema que son específicos de la ubicación, especialmente configuraciones relacionadas con la telefonía. Por lo tanto, es importante establecer este valor correctamente para que coincida con la ubicación real del sistema.

- **Modo de sistema**
  El IP500 V2 se puede utilizar en varios modos:

  - ***Básico***
    Esta opción debe seleccionarse para un sistema que se ejecutará en uno de los modos de IP Office Basic Edition. Esta opción solo está disponible cuando se configura un nuevo IP500 V2. Si se selecciona, el tablero solo mostrará la configuración del sistema. Para obtener más información, consulte la documentación de Server Edition.

  - ***Estándar***
    Esta opción debe seleccionarse para un sistema que debe ejecutarse en el modo IP Office Essential Edition o IP Office Preferred Edition.

  - ***Expansión***
    Esta opción se usa para los sistemas que se instalan como una unidad de expansión en una red Server Edition o IP Office Select. Para obtener más información, consulte la documentación de Server Edition.

- **Configuración LAN**
  Estos campos se utilizan para establecer la configuración de la dirección IP de los puertos LAN1 (LAN) y LAN2 (WAN) del sistema.

- **Ajustes de hora**
  Esta sección establece la fuente de tiempo para el sistema. Los campos disponibles dependen de la fuente de tiempo seleccionada.

- **Fuente de configuración de ajuste de hora**
  Este campo se usa para establecer la fuente de tiempo que debe usar el sistema.

  - ***SNTP***
    Si se selecciona, el sistema obtendrá su información de fecha y hora de la dirección del servidor horario configurado, por ejemplo***0.pool.ntp.org***. Las configuraciones adicionales disponibles son para luego aplicar opciones de zona horaria, compensación horaria y horario de verano (DST) si es necesario.

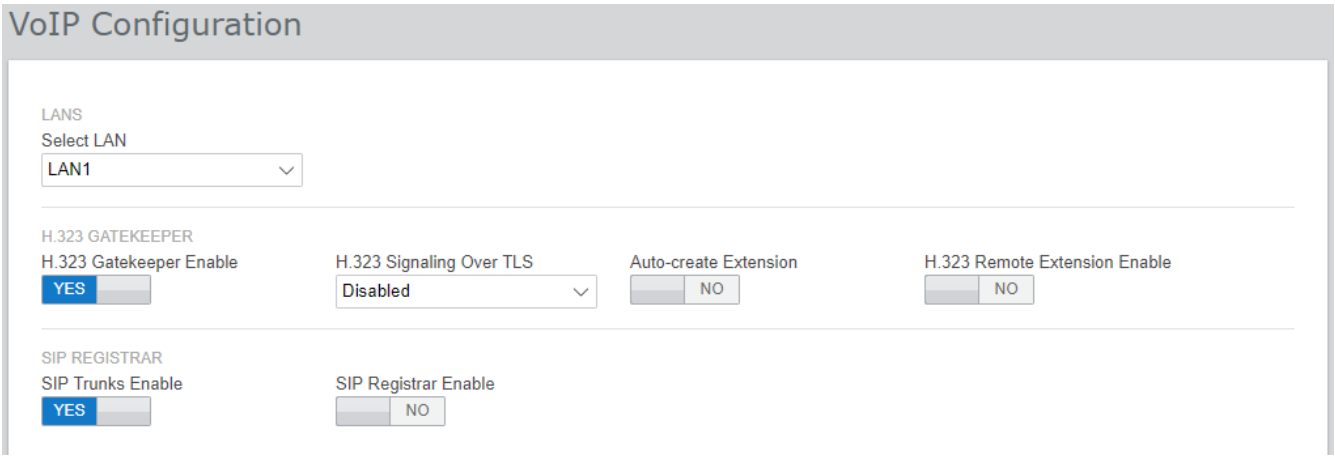
  - ***Correo de voz Pro/Administrador***
    Si se selecciona, el sistema solicitará información de fecha y hora del servidor que ejecuta la aplicación Voicemail Pro o IP Office Manager.

  - ***Ninguna***
    Si se selecciona, la fecha y la hora del sistema deberán configurarse manualmente. Eso se puede hacer desde un teléfono Avaya donde el usuario está configurado como usuario del teléfono del sistema. Consulte la ayuda de IP Office Manager.

8.4.2 Configuración VoIP

Esta pestaña se utiliza para habilitar el soporte básico para telefonía IP, troncales y extensiones, a través de conexiones H323 y/o SIP.

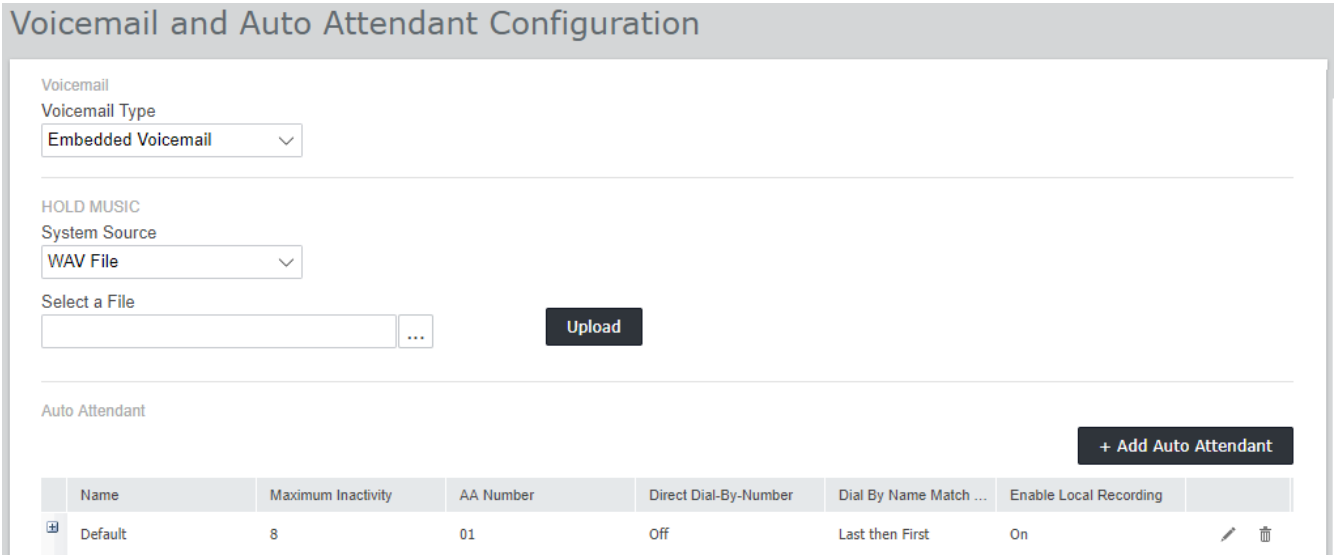
- **!Advertencia:**
  No habilite ninguna configuración a menos que esté seguro de que el sistema utilizará conexiones H323 o SIP. Habilitar conexiones innecesarias introduce requisitos de seguridad adicionales que, si no se cumplen, pueden poner en riesgo el sistema.



- **Seleccionar LAN**
  Seleccione la LAN que se está configurando.
- **H.323 Gatekeeper Habilitar**
  Solo seleccione esta opción si el sistema se instalará con troncales y extensiones H.323.
  - **Señalización H.323 sobre TLS**
    Admite señalización H.323 mediante TLS. Tenga en cuenta que habilitar esto requiere una configuración adicional y reduce la capacidad total del teléfono IP del sistema.
  - **Extensión de creación automática**
    Si se selecciona, el sistema crea automáticamente entradas de extensión SIP y de usuario en su configuración según el registro de la extensión SIP. Esta configuración se deshabilita automáticamente la configuración 24 horas después de que se habilite.
  - **H.323. Habilitar extensión remota**
    Habilite para admitir teléfonos Avaya H.323 ubicados en ubicaciones remotas.
- **Activación de troncales SIP**
  Solo seleccione esta opción si el sistema se instalará con troncales SIP.
- **Habilitar registrador SIP**
  Solo seleccione esta opción si el sistema se instalará con extensiones SIP. Cuando se selecciona, se muestran las siguientes opciones adicionales:
  - **Auto-crear Extn/Usuario:***Predeterminado = Desactivado*
    Si se selecciona, el sistema crea automáticamente entradas de extensión SIP y de usuario en su configuración según el registro de la extensión SIP. Esta configuración se deshabilita automáticamente la configuración 24 horas después de que se habilite.
  - **Habilitar extensión remota SIP:***Predeterminado = Desactivado*
    Actualmente, las opciones de extensión SIP remota solo son compatibles con las aplicaciones de cliente SIP de Avaya. La conexión remota no es compatible con dispositivos SIP de terceros.
  - **Nombre de dominio SIP:***Predeterminado = En blanco*
    Los extremos SIP utilizan este valor para registrarse en el sistema. Si se deja en blanco, el registro utiliza la dirección IP de LAN. La entrada debe coincidir con la parte del sufijo de dominio del**Registrador SIP FQDN**abajo, por ejemplo *acme.com*.
    - Nota: Para los teléfonos SIP de Avaya compatibles con resistencia, el**Nombre de dominio SIP**debe ser común a todos los sistemas de la red.
    - Este es el nombre de dominio del registrador SIP local que necesitan los dispositivos SIP para registrarse en IP Office. Si utiliza TLS, este valor debe incluirse en los certificados de seguridad aplicados a IP Office y, si se utiliza, en un servidor de archivos HTTP independiente.
  - **FQDN del registrador SIP:***Predeterminado = En blanco*
    Este es el nombre de dominio completo, por ejemplo*ejemplo.acme.com*, al que el extremo SIP debe enviar sus solicitudes de registro. Esta dirección debe poder resolverse mediante DNS a la dirección IP del sistema IP Office.

8.4.3 Configuración del correo de voz

Este panel muestra la configuración predeterminada de correo de voz y música en espera del sistema. Si usa correo de voz incorporado, el formulario también se puede usar para configurar la operadora automática para responder llamadas (hasta 40).



- **Tipo de correo de voz**
  Las principales opciones de selección se enumeran a continuación. Para obtener detalles sobre las otras opciones, consulte la ayuda de IP Office Web Manager. Se muestran campos adicionales dependiendo de la selección.

  - ***Correo de voz integrado***
    Esta opción utiliza la propia tarjeta SD del sistema como fuente de correo de voz y almacenamiento de mensajes. Esta es una solución simple de correo de voz con solo funciones básicas. Sin embargo, proporciona soporte para hasta 40 operadores automáticos.

  - ***Correo de voz Pro/Lite***
    Seleccione esta opción si el correo de voz será proporcionado por un servidor que ejecute IP Office Voicemail Pro. Introduzca la dirección IP del servidor.

- Música en espera
  Esta opción le permite seleccionar la fuente predeterminada del sistema para la música en espera. Las opciones son:

  - ***Archivo WAV***
    Utilice un archivo WAV cargado en el sistema. El archivo debe llamarse ***holdmusic.wav*** y haga coincidir la lista de formatos a continuación. Utilice la opción Seleccionar un archivo para seleccionar y cargar el archivo.

Propiedad	Valor	Propiedad	Valor
Tipo de archivo	WAV	**Frecuencia de muestreo de audio**	8kHz
Tasa de bits	128kbps	**Formato de audio**	PCM
Tamaño de muestra de audio	16 bits	**Longitud**	Hasta 90 segundos.
Canales	1 (mono)		

  - ***Externo***
    Utilice la entrada de audio del puerto de audio del sistema en la parte posterior de la unidad de control.

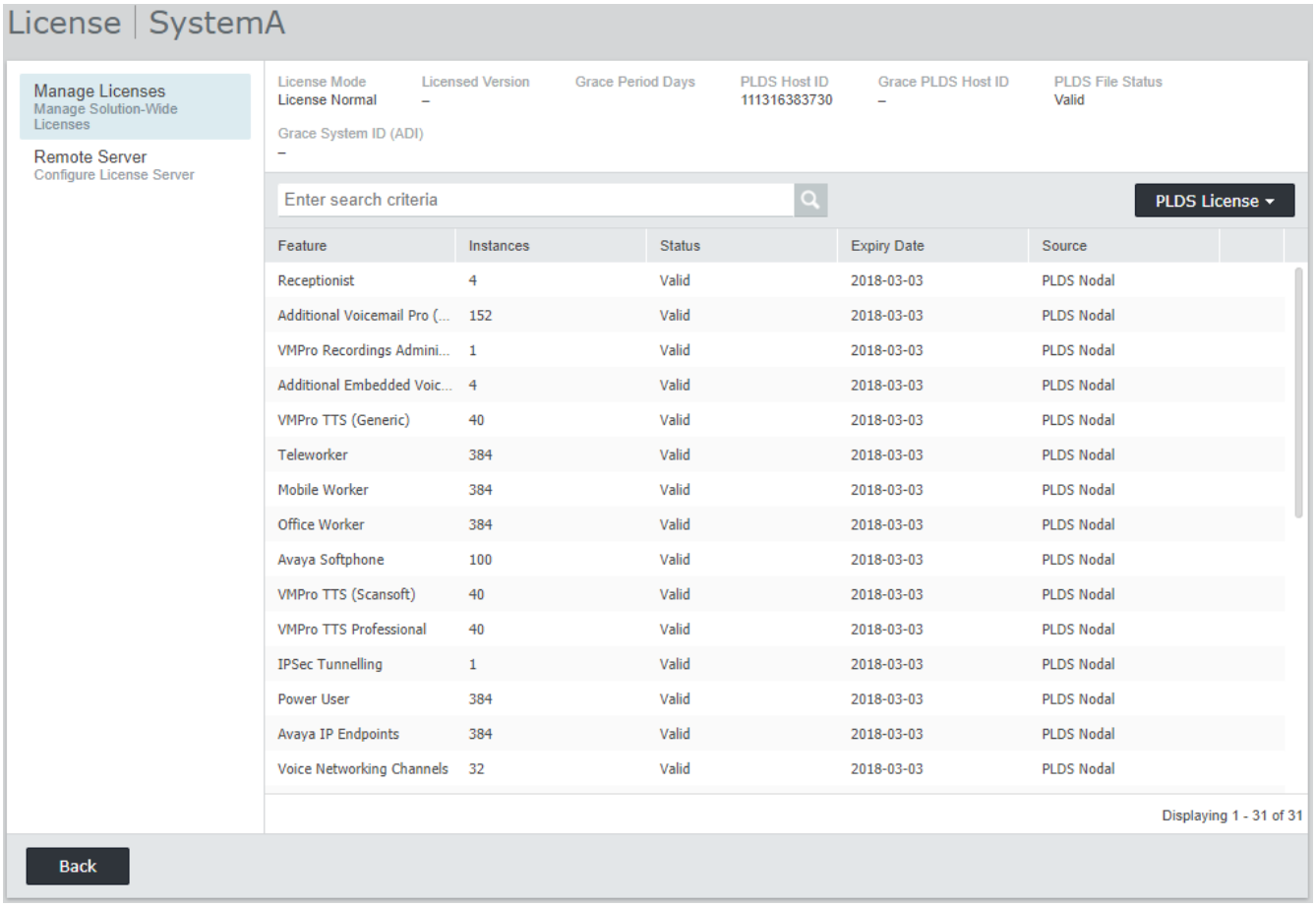
  - ***Tono***
    Utilice un tono repetido regular generado por el sistema.

- **Operador automático**
  Si el Tipo de correo de voz está configurado como Correo de voz incorporado, el tablero le permite configurar asistentes automáticos. Estos se pueden utilizar como destinos para el menú Enrutamiento de llamadas entrantes. El asistente crea automáticamente 3 perfiles de tiempo de llamada ***Mañana***, ***Tarde*** y ***Tardecita*** para uso de los asistentes automáticos. Están configurados de 08:00 a 11:59, de 12:00 a 16:59 y de 00:00 a 07:59, los 7 días de la semana, respectivamente.

8.4.4 Configuración de licencias

Esta sección del tablero le permite agregar un archivo de licencia para el sistema y ver qué licencias se incluyeron en el archivo. Un sistema sin licencia no permitirá ninguna función telefónica hasta que se agreguen licencias (como mínimo para un IP500 V2 y ***Edición esencial*** se requiere licencia). El archivo de licencia debe coincidir con el PLDS

Si el archivo de licencia se colocó en el tarjeta SD del sistema antes de iniciar el sistema, las licencias del archivo se agregan automáticamente.



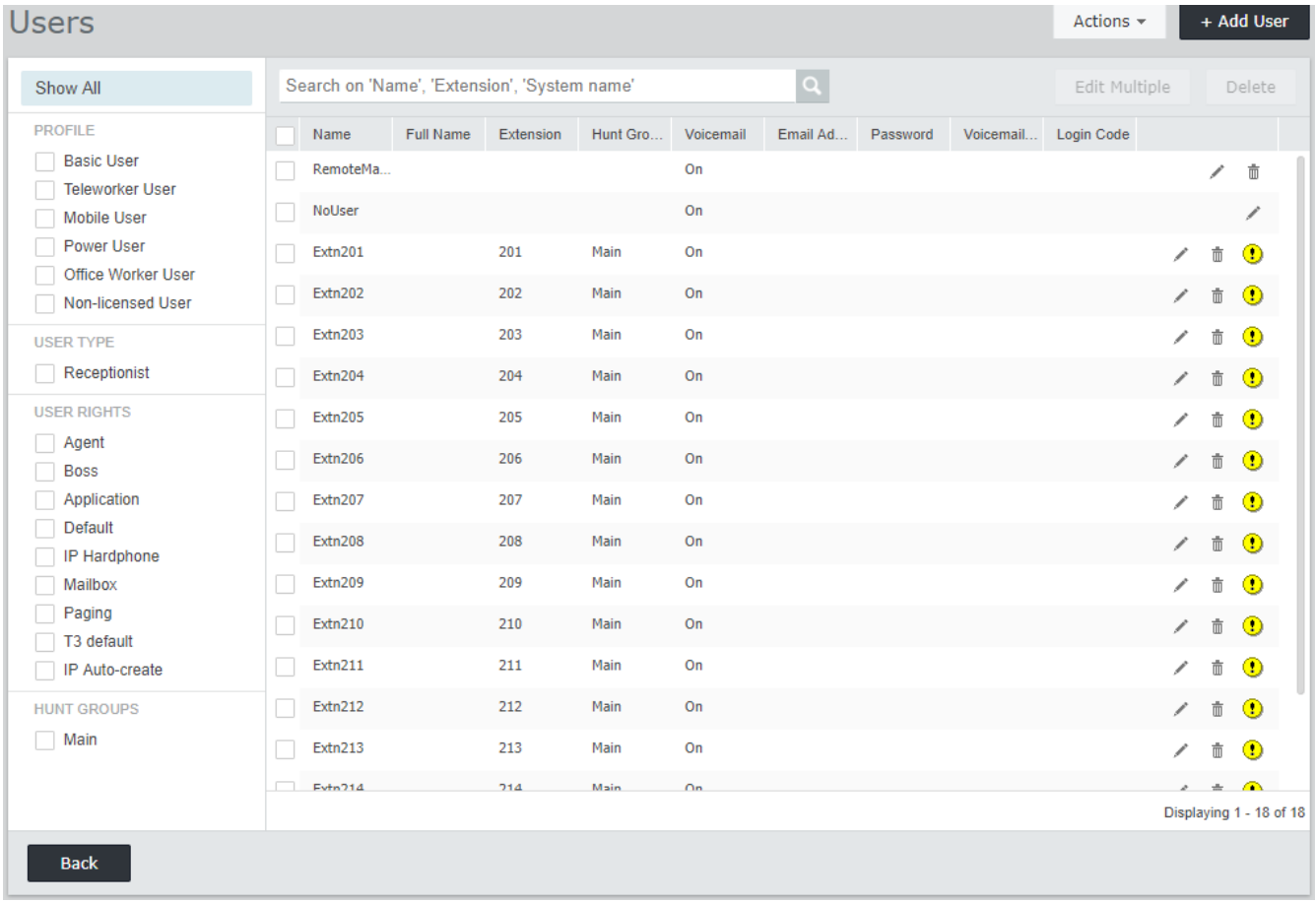
Para agregar un archivo de licencia:

1. Haga clic en **Licencia PLDS** y seleccione **Enviar a IP Office**.
2. Seleccione el archivo XML PLDS proporcionado para el sistema. El archivo debe coincidir con el ***Id. de host PLDS*** que se muestra en el menú (ese ID de host está vinculado al número de serie de la tarjeta SD del sistema instalada en el sistema).
3. Haga clic en **OK**. El archivo se carga en el sistema y reemplaza cualquier archivo de licencia anterior y las licencias que pueda contener.

8.4.5 Usuarios y Extensiones

Este formulario muestra una lista de usuarios en la configuración. Para un nuevo sistema IP500 V2, se crea automáticamente un usuario para cada puerto de teléfono físico detectado cuando se inició el sistema.

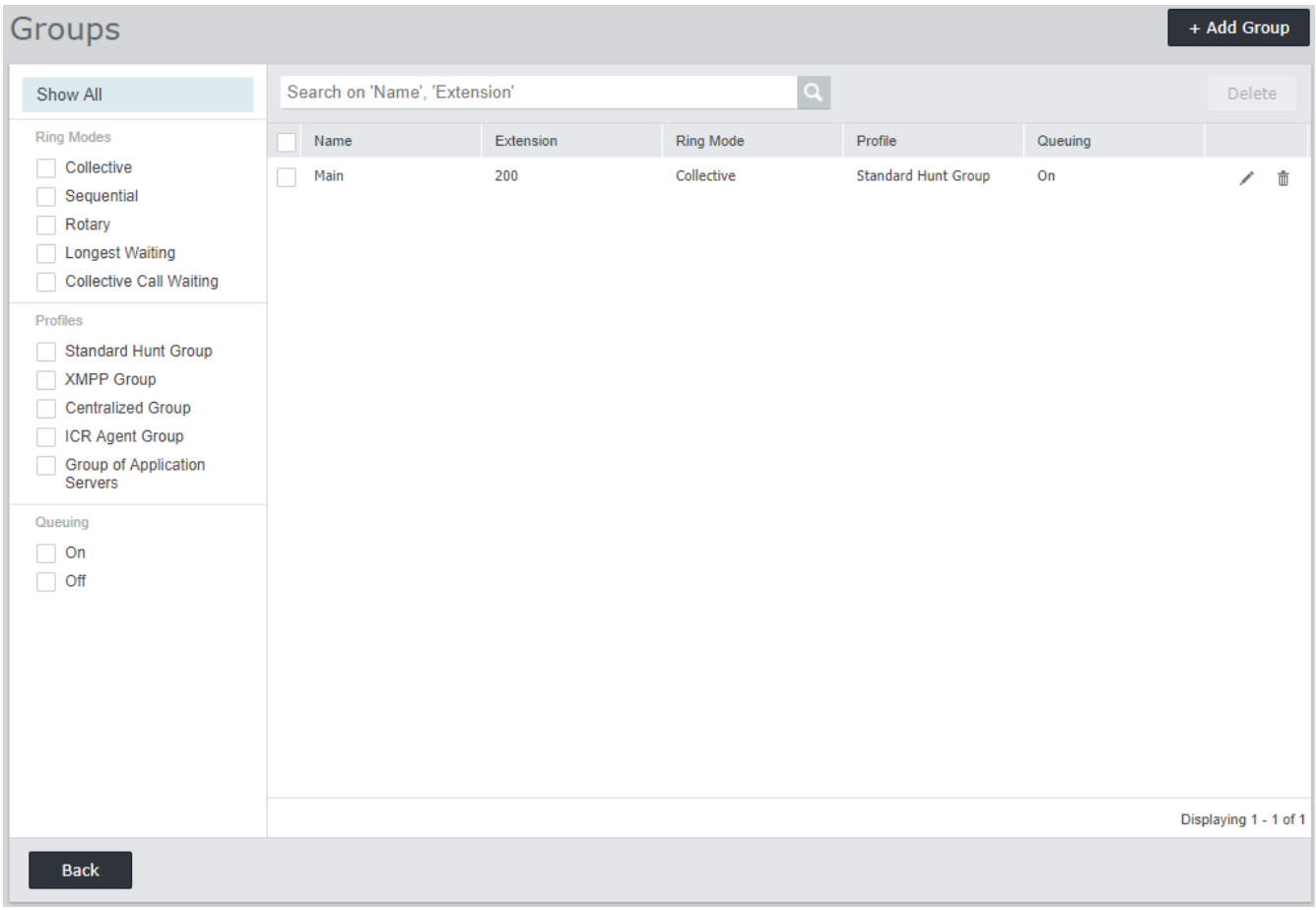
Para editar un usuario en particular, haga clic en el icono de lápiz Para agregar un nuevo usuario, haga clic en**+Agregar usuario**. Para detalles completos del usuario y la configuración de la extensión se refiere a la ayuda de IP Office Web Manager. A medida que agrega usuarios, puede usar el panel de la izquierda para filtrar qué usuarios se muestran en la lista.



8.4.6 Grupos

Este formulario muestra una lista de grupos en la configuración. Para un nuevo sistema IP500 V2, un grupo, denominado***Principal***y con el número de extensión 200, se agrega automáticamente. Este grupo contendrá todas las extensiones de teléfono que se crearon automáticamente (una para cada puerto de teléfono físico) cuando se inició el sistema.

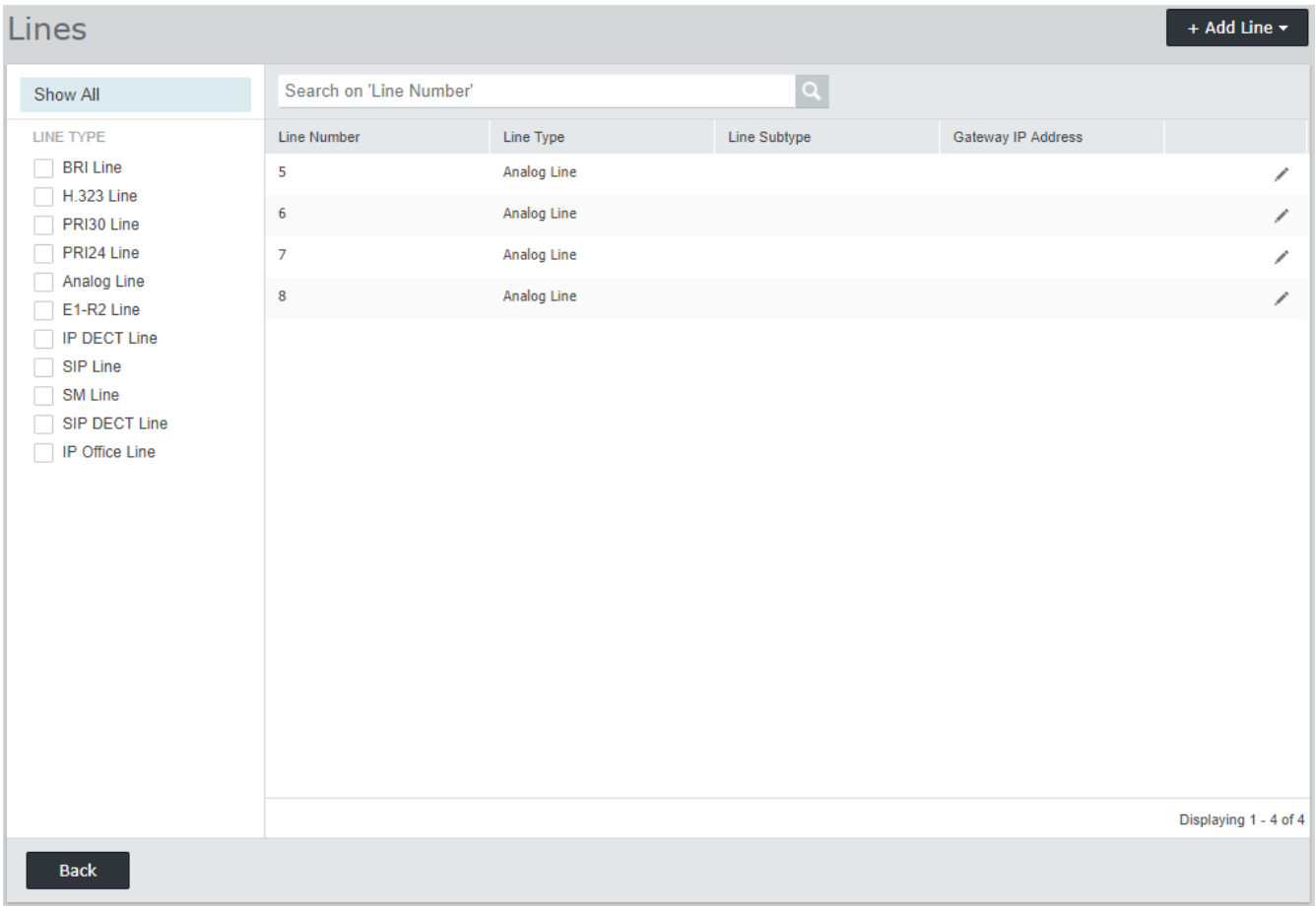
Para editar un grupo en particular, haga clic en el icono de lápiz Para agregar un nuevo grupo, haga clic en**+Añadir grupo**. Para detalles completos del grupo. los ajustes y la configuración se refieren a la ayuda de IP Office Web Manager. A medida que agrega grupos, puede usar el panel de la izquierda para filtrar qué grupos se muestran en la lista.



8.4.7 Líneas

Este formulario muestra una lista de todas las líneas externas. Para un nuevo sistema IP500 V2, las líneas analógicas, PRI y BRI se agregan automáticamente con configuraciones predeterminadas para que coincidan con las interfaces de línea física encontradas en el sistema cuando se inició. Otros tipos de línea deben agregarse manualmente.

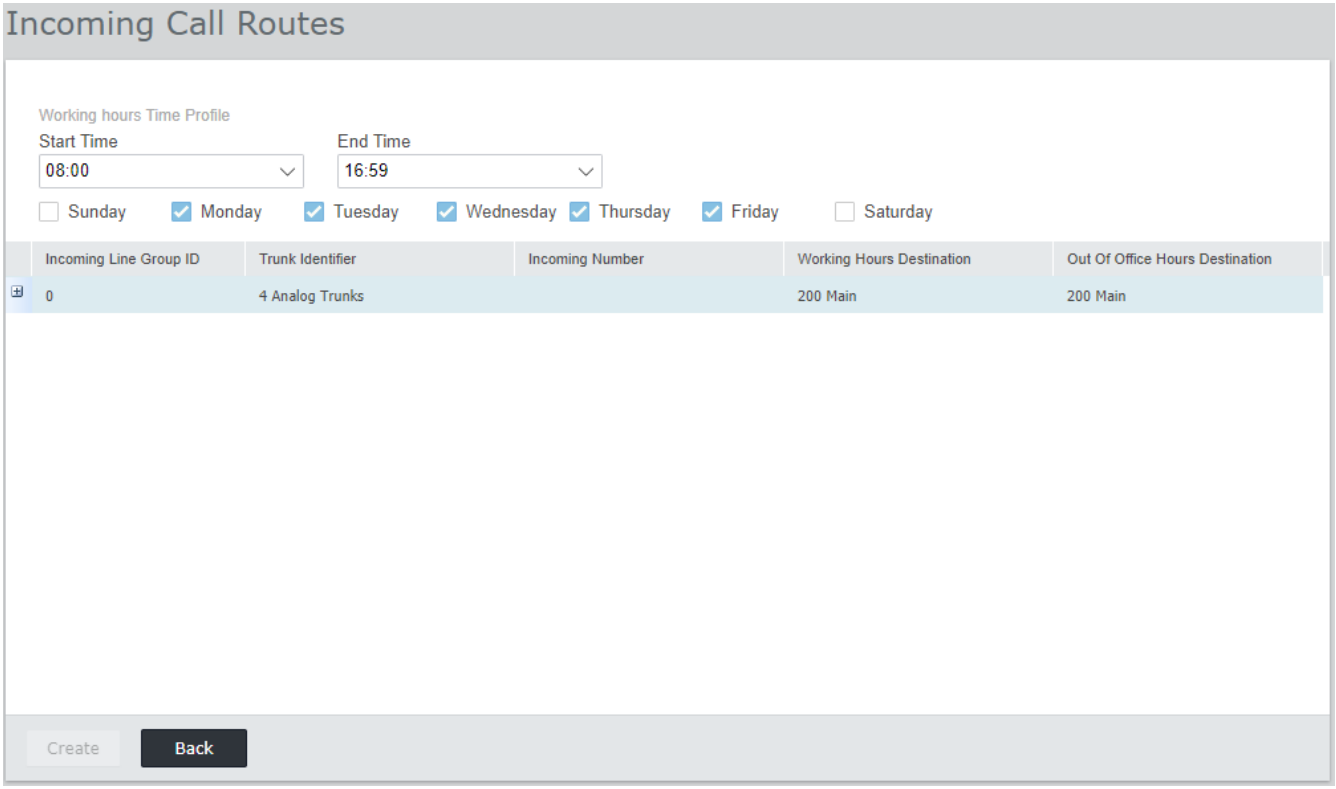
Para editar una línea en particular, haga clic en el icono de lápiz Para agregar una nueva línea, por ejemplo, una línea SIP, haga clic en**+Añadir línea**y seleccione el tipo de línea requerido. Para obtener detalles completos sobre la configuración y la configuración de la línea, consulte la ayuda de IP Office Web Manager.



8.4.8 Rutas de llamadas entrantes

Esta parte del asistente del tablero realiza dos acciones:

- Defina los días y horas para un perfil de tiempo llamado**Horas Laborales**. El valor predeterminado es de 08:00 a 16:69 de lunes a viernes.
- Seleccione los destinos para los diferentes ID de grupos de líneas entrantes, creados a través de[configuración de línea](#) 127,durante y fuera de las horas definidas por el perfil horario. Se muestra una entrada para cada grupo de líneas entrantes diferente. El destino de cada uno puede establecerse en cualquier número de extensión de usuario o grupo o en un nombre de operador automático si se han configurado operadores automáticos de correo de voz integrado.

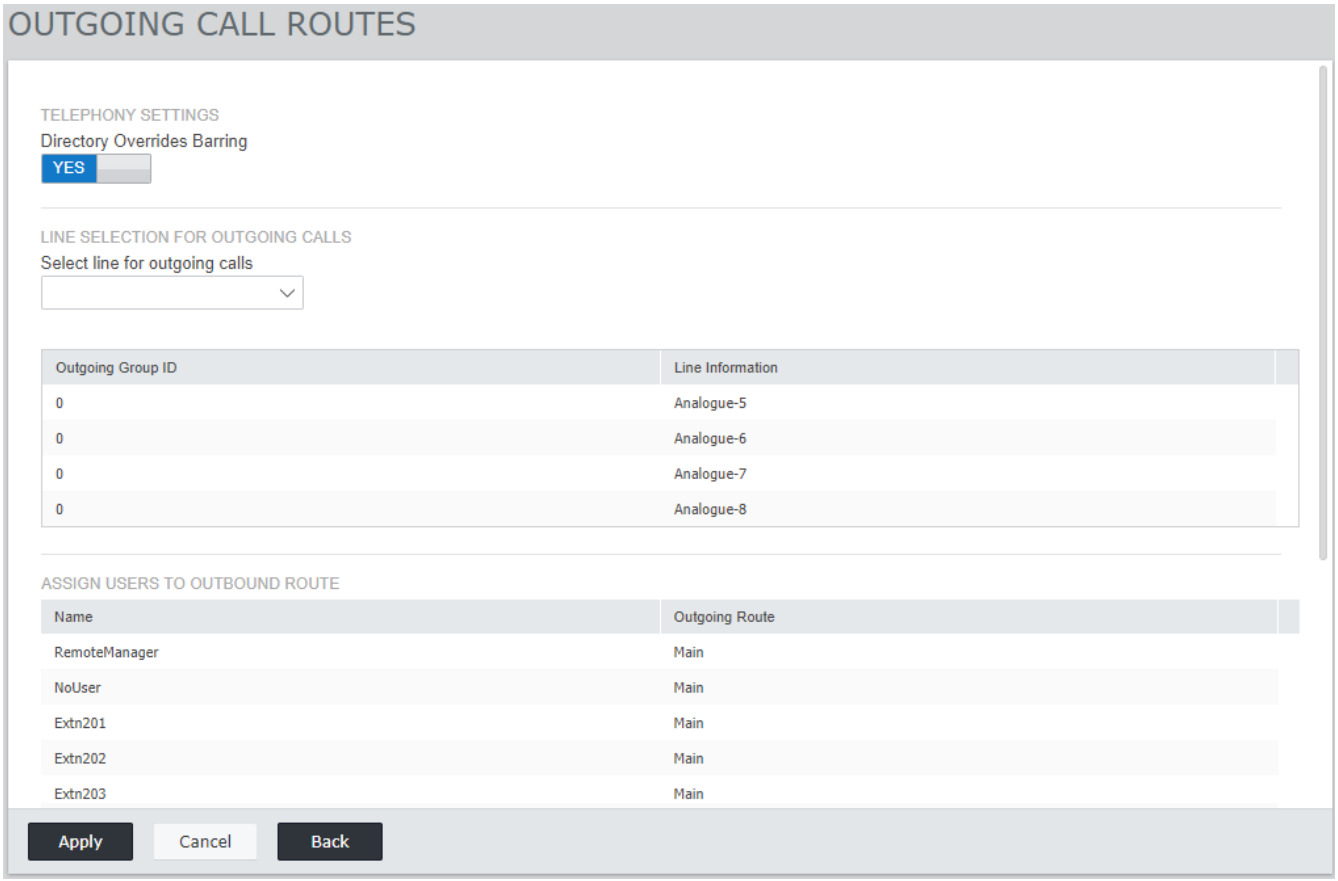


8.4.9 Rutas de llamadas salientes

Este menú del tablero solo está disponible en sistemas donde la configuración regional se ha establecido en Estados Unidos o Canadá.

De manera predeterminada, la configuración contiene una llamada de entrada de Selección automática de ruta (ARS)***Principal***. Todo el marcado de números externos por parte del usuario se dirige a esa entrada ARS para determinar qué líneas deben transmitir las llamadas salientes (con todas las líneas en forma predeterminada en el grupo de líneas 0 y ese grupo de líneas se usa para todas las llamadas).

El asistente del tablero agrega 3 entradas ARS adicionales, llamadas***Local***,***Nacional***y***Internacional***respectivamente.



- **Restricción de anulaciones de directorio**
  Si está habilitada, la marcación (incluidas las marcaciones rápidas y la selección de una lista de directorio) anula la restricción de llamadas salientes aplicada al usuario cuando el número marcado coincide con un número en el directorio del sistema.

- **Seleccionar línea para llamadas salientes**
  Al hacer clic en el menú desplegable, aparecen las ID de grupo de líneas salientes disponibles creadas duranteconfiguración de línea El ID127.La línea de grupo seleccionado se aplica a todos los códigos cortos en las nuevas entradas ARS predeterminadas (***Local***,***Nacional***y ***Internacional***) en la configuración.

- **Asignar usuarios a la ruta de salida**
  De manera predeterminada, las llamadas salientes de cada usuario se enrutan a través de la entrada principal de ARS (esto se realiza mediante el código corto del sistema 9N). Esta lista le permite seleccionar para cada usuario si sus llamadas deben enrutarse usando una de las otras entradas ARS predeterminadas (***Local***,***Nacional***o***Internacional***). Cuando se realiza una selección, se agrega un código corto 9N con el destino ARS apropiado a la configuración del usuario.

Capítulo 9.

Sistema de seguridad

9. Seguridad del sistema

El sistema IP Office y sus aplicaciones admiten una variedad de funciones para hacer que los vínculos entre ellos y los usuarios sean más seguros. Los detalles completos de las opciones disponibles se describen en la**Directrices de seguridad de la plataforma IP Office de Avaya** 11 manual.

Esta sección cubre solo algunos cambios básicos recomendados para ayudar a que un nuevo sistema sea más seguro.

1. **Cambiar la configuración de seguridad predeterminada** 133
2. **Cambiar la contraseña de usuario remoto** 135
3. **Deshabilitar la compatibilidad con troncales SIP** 136
4. **Deshabilitar el soporte telefónico H.323** 135

Recomendaciones adicionales:

- Si la red a la que está conectado IP Office tiene acceso público externo a Internet, ese acceso debe estar controlado por algunos dispositivos de seguridad adicionales, como un firewall y, para VoIP, un controlador de borde de sesión (SBC).
- Si no se utiliza LAN2 (el puerto WAN), asegúrese de que no esté conectado a la red.

9.1 Cambio de la configuración de seguridad predeterminada

Este proceso cubre los cambios de seguridad mínimos necesarios para el servicio de IP Office ejecutado por el servidor. Para obtener detalles completos de todas las configuraciones de seguridad de IP Office, consulte la ayuda de IP Office Manager.

Para establecer la configuración de seguridad inicial:

1. Inicie IP Office Manager.
2. Seleccione**Archivo | Avanzado | Configuraciones de seguridad**.
   - Si el**Seleccione el menú de IP Office**no aparece, haga clic .
3. Seleccione el servidor y haga clic en**OK**.
4. Introduzca el nombre de usuario y la contraseña del administrador.
5. Para un sistema con configuración de seguridad predeterminada, se muestran varias advertencias. Tenga en cuenta cada advertencia y haga clic en**OK**.
6. Seleccione y cambie las siguientes contraseñas:

   una.**Contraseña del sistema**
   IP Office Manager utiliza esta contraseña para las actualizaciones del software del sistema. Haga clic en el**Cambio**e ingrese una nueva contraseña. Hacer clic**OK**.

   b.**Contraseña del correo de voz**
   El servidor de Voicemail Pro utiliza esta contraseña para conectarse al sistema IP Office. Cuando se configura, también se debe configurar la misma contraseña en las preferencias del servidor de correo de voz mediante el cliente Voicemail Pro.

   C.**Supervisar contraseña**
   La aplicación System Monitor usa esta contraseña para conectarse al sistema IP Office mediante UDP o TCP. Si no se establece, el **Contraseña del sistema**En su lugar, se utiliza el conjunto anterior.

7. Seleccione **General**.

   una. Habilitar**Bloquear contraseñas de teléfonos IP**. Esto evita que los teléfonos IP H.323 y SIP se registren con códigos de acceso como 0000 o el mismo que el número de extensión.

   b. Comprobar el**Detalles del usuario de IP Office**sección. Esta sección define qué reglas de seguridad se aplican a la configuración y el uso de contraseñas de usuario (aparte de la contraseña del correo de voz).

8. El**Controles de aplicaciones**La sección indica una serie de interfaces no seguras utilizadas por el sistema. Anule la selección de aquellas que no sean requeridas por las aplicaciones planificadas del cliente. A medida que selecciona o anula la selección de los controles, el **Soporte de aplicaciones**la siguiente sección cambia para mostrar el efecto del cambio.

Control de aplicaciones	Usado por	notas
Servidor TFTP	Monitoreo del sistema	Si está deshabilitado, además de deshabilitar las otras opciones de TFTP a continuación, el sistema no puede admitir el componente de visor de red en la aplicación System Monitor.
Lectura de directorio TFTP	IP DECT	Si está deshabilitado, DECT funciona sin la función de directorio del sistema.
Correo de voz TFTP	Buzón de voz profesional	Habilite solo cuando el sistema esté utilizando un servidor de correo de voz anterior a la versión 9.1 de IP Office.
Código de programa	Gerente de IP Office	Se utiliza para actualizaciones desde IP Office Manager, se recomienda desactivar cuando no se requiera.
DevLink	DevLink	
TAPI	TAPI/DevLink	Desactive a menos que el sitio del cliente utilice aplicaciones TAPI con IP Office.
Lectura de directorio HTTP	Portal one-X para IP Office	Habilite solo cuando se usa one-X Portal for IP Office. Si está deshabilitado, one-X Portal for IP Office funciona sin la función de directorio personal.
Escritura de directorio HTTP	Portal one-X para IP Office	Habilite solo cuando se usa one-X Portal for IP Office. Si está deshabilitado, one-X Portal for IP Office funciona sin la función de actualización del directorio personal.

9. Haga clic en**OK**.
10. Haga clic en **Usuarios del servicio**. Por defecto solo el***Administrador***y***EnhTcpaServer***los usuarios están habilitados.

    una. Seleccione***EnhTcpaService***. Este servicio es utilizado por one-X Portal para IP Office. Si se está instalando one-X Portal for IP Office, recomendamos cambiar la contraseña solo después de completar la instalación. Si one-X Portal for IP Office no está instalado:

    - Haga clic en el**Cambio**e ingrese una nueva contraseña para el servicio.
    - Haga clic en**estado de la cuenta**y seleccionado***Desactivado***.

- Hacer clic**OK**.

11. Haga clic en el icono para guardar los cambios de seguridad.

9.2 Cambio de la contraseña de usuario remoto

La configuración de IP Office contiene un usuario cuya contraseña se usa como predeterminada para el acceso telefónico remoto a la red de IP Office. Se debe cambiar la contraseña de este usuario.

Para cambiar la contraseña de usuario remoto:

1. Inicie IP Office Manager 68y conéctese al sistema IP Office.
2. Haga clic en **Usuarios**y en la lista de usuarios haga clic en**Administrador remoto**.
3. En el**Usuario**pestaña, introduzca una nueva contraseña para el usuario y haga clic en**OK**.
4. Haga clic en el y guarde la configuración actualizada en el sistema IP Office.

9.3 Desactivación de la compatibilidad con troncales SIP

El sistema IP Office admite troncales SIP. Si no se requieren para la instalación del cliente, recomendamos que se deshabilite la compatibilidad con troncales SIP del sistema.

Para deshabilitar la compatibilidad con troncales SIP:

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

1. Inicie IP Office Manager 68y recibir la configuración del sistema IP Office.
2. Seleccione**Sistema**.
3. Seleccione**LAN1**y seleccione el**VoIP**pestaña.
4. Comprueba que**Activación de troncales SIP**no está seleccionado.
5. Repita el proceso para**LAN2**.
6. Haga clic en el guardar y guardar la configuración actualizada en el sistema IP Office.

9.4 Desactivación del soporte telefónico H.323

IP Office admite teléfonos IP H.323 de manera predeterminada. Si estos no son necesarios para la instalación del cliente, recomendamos que el soporte telefónico H.323 del sistema esté desactivado.

Para deshabilitar la compatibilidad telefónica con H.323:

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

1. Inicie IP Office Manager 68y recibir la configuración del sistema IP Office.
2. Seleccione**Sistema**.
3. Seleccione**LAN1**y seleccione el**VoIP**pestaña.
4. Comprueba que**H323 Gatekeeper Habilitar**no está seleccionado.
5. Comprueba que**Habilitar extensión remota H323**no está seleccionado.
6. Repita el proceso para**LAN2**.
7. Haga clic en el guardar y guardar la configuración actualizada en el sistema IP Office.

Capítulo 10.
Inducción

10. Embarque

La incorporación es un proceso a través del cual puede registrar un sistema IP500 V2 para soporte y mantenimiento remotos de Avaya. El proceso de incorporación se realiza mediante la interfaz de IP Office Web Manager.

Esta sección es un breve resumen de la incorporación. Para obtener detalles completos sobre la configuración y administración de los servicios VPN SSL, consulte la Guía de soluciones VPN SSL de IP Office de Avaya. Puedes descargar la guía desdehttp://soporte.avaya.com .

Resumen de pasos

1. Inicie sesión en IP Office Web Manager
2. **A bordo del sistema** Este proceso tiene 3 pasos principales:
   una. **Obtener un archivo de inventario**
   Desde el sistema exporta un archivo que contiene un inventario de los equipos dentro del sistema. Este archivo es necesario para registrar el sistema para soporte.
   b. **Registrar el Sistema**
   Registre el sistema en el sitio web de la herramienta de registro global de Avaya y cargue el archivo de inventario del sistema. Una vez que el sistema está registrado, se proporciona un archivo de incorporación para el sistema. Este archivo contiene los ajustes de configuración para el enlace del servicio SSL VPN.
   C. **Subir un archivo de incorporación**
   Cargue el archivo de incorporación al sistema. La información dentro del archivo se utiliza para actualizar la configuración del sistema.

Cambios de configuración causados por la incorporación

Cuando se carga un archivo de integración en el sistema IP Office Essential Edition, se pueden realizar una serie de cambios en la configuración del sistema. Es importante ser consciente de estos posibles cambios y asegurarse de que no se sobrescriban o eliminen posteriormente.

Los cambios son los siguientes. Los marcados con * son opcionales y dependen de la configuración incluida en el archivo de incorporación por parte del proveedor de servicios.

- **Servicio VPN SSL**
  Se agrega un nuevo servicio VPN SSL a la sección Servicios de la configuración.
- **Alarmas SNMP***
  Se puede configurar SNMP y agregar dos trampas de alarma SNMP a la configuración. Tenga en cuenta que esto sobrescribirá cualquier configuración de SNMP existente si SNMP ya se ha configurado.
- **Códigos cortos***
  Los códigos cortos se pueden agregar usando el***Establecer servicio nocturno de grupo de búsqueda***y***Servicio nocturno Clear Hunt Group*** comportamiento. Estos se pueden usar para habilitar y deshabilitar el servicio SSL VPN.
- **Ruta IP***
  Se puede agregar una ruta IP estática al servicio SSL VPN a las rutas IP en la configuración.
- **Certificado de seguridad**
  Se agrega un certificado de seguridad para el servicio SSL VPN a la configuración de seguridad del sistema.

10.1 Embarque

1. Iniciar sesión enAdministrador web de IP Office 7.

   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.

   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.

2. Haga clic en**Comportamiento**y seleccione**Inducción**. Se muestra el menú Incorporación.

   - **¿Está utilizando hardware de la serie TAA?**
     Los sistemas comprados bajo las Regulaciones Federales de Adquisición (FAR) de EE. UU. deben cumplir con los requisitos de la Ley de Comercio de América (TAA). Existen variantes compatibles con TAA para diversos elementos del hardware de IP Office. Seleccione esta opción si el sistema IP Office incluyeHardware TAA 296.Esto generalmente se indica mediante TAA que aparece en la etiqueta en la parte posterior de la unidad de control del sistema.

3. Haga clic en**Obtener archivo de inventario**para descargar un archivo de inventario.xml para el sistema. Cuando registra el sistema IP Office para soporte remoto, el archivo de inventario se requiere como parte del registro y se carga en la Herramienta de registro global (GRT) de Avaya, donde los datos del inventario se completan en la base de datos de Soporte al cliente de Avaya (ACS).

4. Haga clic en**Registrar Oficina de PI**para registrar el sistema con el sitio web de Avaya Global Registration Tool (GRT).

5. Una vez que el sistema esté registrado, puede descargar un archivo integrado para el sistema desde el sitio web de la herramienta de registro global de Avaya. Este archivo contiene la configuración requerida para establecer una conexión SSL VPN entre el sistema IP Office y un servidor Avaya VPN Gateway (AVG).

6. Usa el**Carga de archivos de incorporación**sección para cargar el archivo de incorporación al sistema.

Capítulo 11.
Gestión de tarjetas SD

11. Gestión de tarjetas SD

La unidad de control IP500 V2 tiene dos ranuras para tarjetas SD, etiquetadas**SD del sistema**y**SD opcional**respectivamente. Estos se utilizan de la siguiente manera:

- **Tarjeta SD del sistema**
  Una tarjeta SD de Avaya System debe estar presente en esta ranura en todo momento. Esta tarjeta contiene copias del firmware y la configuración de IP Office y se utiliza como memoria no volátil de las unidades de control IP500 V2.
  - Cada tarjeta SD de Avaya System tiene un número de serie único que se utiliza para generar y validar licencias.
  - La tarjeta almacena las indicaciones para la operación de Embedded Voicemail y actúa como el almacén de mensajes para los mensajes de Embedded Voicemail.
  - Antes de cualquier apagado o reinicio planificado del sistema IP Office, la configuración actual que se ejecuta en la memoria RAM del sistema IP Office se copia en el**/primario**carpeta en la tarjeta SD del sistema y en la memoria no volátil del sistema.
  - Después de un reinicio, el software en el**/primario**carpeta es cargada por la unidad de control IP500 V2. Si el software requerido no está presente o no es válido, se utiliza una secuencia de opciones de respaldo, consulteArrancar desde las tarjetas SD todos los detalles por
  - Después de un reinicio, si está presente, el archivo de configuración en el**/primario**carpeta es cargada por la unidad de control IP500 V2. Si no hay ningún archivo presente, el sistema buscará un archivo en su memoria interna no volátil. Si no se encuentra ninguna copia, generará un archivo de configuración predeterminado. VerArrancar desde las tarjetas SD 144para detalles completos.
  - Una vez al día (aproximadamente entre las 00:00 y las 00:30), IP Office copiará la configuración actual que se ejecuta en su memoria RAM al**/primario**carpeta en la tarjeta.
  - Los cambios de configuración realizados con IP Office Manager primero se escriben en la copia del archivo de configuración en la tarjeta y luego se fusionan con la configuración que se ejecuta en la memoria RAM del sistema IP Office.
  - Se ignora la configuración de bloqueo de escritura en las tarjetas en la ranura para tarjetas SD del sistema.
- **Tarjeta SD opcional**
  No es necesario que haya una tarjeta presente en esta ranura para el funcionamiento normal de IP Office. La ranura se puede utilizar para diversas acciones de mantenimiento.
  - Se puede insertar una tarjeta con un software o una configuración IP Office actualizados y luego transferir esos archivos a la tarjeta SD del sistema para actualizar el sistema IP Office.
  - El contenido completo de la tarjeta SD del sistema se puede copiar a la tarjeta SD opcional mientras se ejecuta el sistema IP Office.
  - Se respeta la configuración de bloqueo de escritura en las tarjetas en la ranura para tarjeta SD opcional.

Tarjeta Eliminación	Las tarjetas de memoria siempre deben estarcerrar 157antes de ser eliminado cuando el sistema está funcionando. Aunque los LED de la ranura de la tarjeta indican cuándo se están escribiendo datos en una tarjeta, la falta de parpadeo del LED no es una protección suficiente. Apagar la tarjeta deshabilita Embedded Voicemail e IP Office Web Manager. Si el**SD del sistema**se extrae la tarjeta, las funciones licenciadas por el número de serie de la tarjeta continúan funcionando hasta por 2 horas.

Especificación de la tarjeta

Las tarjetas que no son de Avaya se pueden utilizar en el**SD opcional**ranura siempre que coincidan o excedan el estándar a continuación:

- SDHC 4GB mínimo Clase 2+. Formato FAT32 de partición única. (Las tarjetas SD de Avaya IP Office son de 8 GB, las tarjetas más antiguas eran de 4 GB).

Carpetas de tarjetas SD

los**SD del sistema**tarjeta**/sistema**La carpeta contiene las siguientes subcarpetas:

- **/primario**
  Contiene los archivos de firmware para la unidad de control de IP Office, los módulos de expansión externos y los teléfonos compatibles. La carpeta también puede contener archivos de música en espera y archivos de clave de licencia. Este es el conjunto principal de archivos que utiliza el sistema IP Office al iniciarse. También contiene la copia almacenada de la configuración de IP Office.
- **/respaldo**
  Contiene una copia de la carpeta principal en algún punto anterior. Se puede invocar una copia de seguridad del contenido principal de esta carpeta de forma manual (con IP Office Manager o SSA) o como parte de la actualización del software de IP Office con IP Office Manager.
- **/copia de seguridad_apl**
- **/lvmail**
  Contiene las indicaciones del sistema utilizadas por Embedded Voicemail. Tenga en cuenta que los mensajes y saludos del buzón se almacenan en una subcarpeta del**/dinámica**carpeta.
  - la subcarpeta**/AAG**se utiliza para almacenar los saludos de la operadora automática de Embedded Voicemail.
- **/doc**
  Contiene documentación de instalación inicial para el sistema.
- **/dinámica**
  Contiene archivos utilizados por IP Office y retenidos mediante un reinicio del sistema IP Office.
  - la subcarpeta**/lvmail**se utiliza para almacenar mensajes de buzones de correo de usuarios individuales y de grupos, grabaciones de nombres y anuncios. La capacidad de almacenamiento de Embedded Voicemail está limitada a 25 horas, independientemente de la capacidad de la tarjeta.
- **/temperatura**
  Contiene archivos temporales utilizados por IP Office y que no se retienen al reiniciar el sistema IP Office.
- **/ws**

los**SD opcional**La tarjeta puede contener un conjunto similar de carpetas. Estos se utilizan como una copia de seguridad adicional o se pueden utilizar como fuente para actualizar el contenido de la tarjeta SD del sistema.

11.1 Arrancar desde las tarjetas SD

Cuando se enciende, la unidad de control IP500 V2 busca un archivo binario ip500v2.bin válido para cargar. Lo hace utilizando la posible fuente a continuación en el orden que se muestra, saltando a la siguiente fuente si el archivo no está presente o no es válido.

1. Tarjeta SD del sistema***/primario***carpeta.
2. La propia memoria interna no volátil de la central. Una vez que se ha instalado un sistema, utiliza su memoria no volátil para guardar copias de los archivos binarios de configuración y del sistema que está utilizando. Estos pueden usarse para restaurar la operación durante un reinicio del sistema. Tenga en cuenta que, aunque un sistema puede iniciarse desde una memoria no volátil, aún debe estar presente una tarjeta SD del sistema para que el sistema funcione correctamente.
3. Tarjeta SD del sistema***/respaldo***carpeta.
4. Tarjeta SD opcional***/primario***carpeta.
5. Tarjeta SD opcional***/respaldo***carpeta.
6. Si no se encuentra ningún archivo, la unidad de control volverá a realizar solicitudes BOOTP a la red. IP Office Manager puede responder a la solicitud BOOTP. VerBorrado del firmware operativo 199.

Una vez que se encuentra un archivo ip500v2.bin válido, la unidad de control de IP Office cargará ese firmware. La fuente desde la que se cargó el archivo binario de la unidad de control se utiliza para cargar más archivos.

Carga del archivo de configuración

Habiendo instalado los archivos de firmware del sistema necesarios como se indica arriba, la unidad de control IP500 V2 requiere un archivo de configuración:

- Si el IP500 V2 arrancó usando archivos binarios desde una ubicación de tarjeta SD, busca un archivo de configuración válido en la misma ubicación.
  - Si un archivo de configuración está presente y es válido, se carga.
  - Si un archivo de configuración está presente pero no es válido, cargue la copia de configuración en su memoria no volátil si está presente, de lo contrario asume una configuración predeterminada.
  - Si no hay un archivo de configuración presente, use la copia de memoria no volátil como se indicó anteriormente, a menos que el reinicio sea como resultado de un comando predeterminado del sistema.
- Si el IP500 V2 arrancó usando archivos binarios de su memoria no volátil, también cargará la copia de configuración desde esa ubicación.
  - Indicará una alarma de arranque (ver más abajo).
  - Intentará restaurar el archivo de firmware en la tarjeta SD del sistema.**/primario**carpeta usando la copia en su memoria no volátil.
  - No se produce el proceso de arranque normal de actualización del firmware del módulo de expansión. Si el**Archivo | Avanzado | Mejora**se utiliza el comando, solo los módulos de expansión externos realmente presentes en el sistema se enumeran para la actualización.

Operación posterior al arranque

Durante el funcionamiento normal, los archivos binarios y de configuración se envían a la tarjeta SD del sistema**/primario**carpeta con IP Office Manager también se escriben en la memoria no volátil.

Si el sistema se inició desde su memoria no volátil debido a un problema con la tarjeta SD, aún es posible actualizar el archivo ip500v2.bin mediante el asistente de actualización de IP Office.

Alarmas de arranque

Lo siguiente se aplica si el IP500 V2 arranca usando un software diferente al de su tarjeta SD del sistema**/primario**carpeta:

- Se mostrará una alarma en la aplicación de estado del sistema. También generará una alarma si la tarjeta en cualquier ranura no es compatible. Estas alarmas también se emiten como alarmas SNMP, Syslog o correo electrónico.
- El administrador de IP Office**Seleccione IP Office**menú mostrará un icono que indica que el sistema IP Office está ejecutándose utilizando un software que no sea el de la carpeta principal de la tarjeta SD del sistema.
- La configuración se puede leer, pero será de solo lectura. Intentar enviar una configuración al sistema causará el mensaje de error ***Error al guardar los datos de configuración. (Error interno)***.

Omitir la carpeta principal de la tarjeta SD del sistema

Se puede obligar a la unidad de control a omitir la tarjeta SD del sistema.***/primario***carpeta y memoria no volátil al iniciar. Esto se hace presionando el botón**auxiliar**mientras aplica energía a la unidad de control.

Esta acción puede ser necesaria si, luego de una actualización del sistema IP Office, se determina que se requiere una reversión al firmware y la configuración respaldados anteriormente. Utilizando el**auxiliar**El botón debe restaurar la operación del sistema usando el***/respaldo*** archivos de la carpeta mientras el instalador restaura el contenido de la***/primario***carpeta a una versión anterior.

11.2 Creación de una tarjeta SD de IP Office

Los procesos a continuación se pueden aplicar a las tarjetas SD de Avaya IP Office. También se pueden aplicar a tarjetas SD que no sean de Avaya para usar en la ranura para tarjeta SD opcional de un sistema. Para la ranura SD del sistema, solo se deben usar tarjetas SD del sistema Avaya.

La tarjeta debe tener el siguiente formato.

- SDHC 4GB mínimo Clase 2+. Formato FAT32 de partición única. (Las tarjetas SD de Avaya IP Office son de 8 GB, las tarjetas más antiguas eran de 4 GB).

- **ADVERTENCIA**
  Las tarjetas SD proporcionadas por Avaya no deben formatearse con ningún otro método que no sean los comandos de formato dentro de IP Office Manager y System Status Application. Al formatear las tarjetas con cualquier otro método, se elimina el número de serie utilizado para la licencia de IP Office de la tarjeta.

- **!Advertencia: Versión de IP Office Manager**
  Este proceso utiliza archivos de software proporcionados por la versión instalada de IP Office Manager que se está utilizando. Debe asegurarse de que la versión de IP Office Manager utilizada coincida con la versión del software requerido.

    - **Admin Lite no compatible**
      Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).

Crear una tarjeta en una PC local

Estos procesos se pueden ejecutar en una tarjeta SD insertada en un lector de tarjetas en la PC con IP Office Manager. Esa tarjeta se puede usar en la ranura para tarjeta SD del sistema de un sistema nuevo o en la ranura para tarjeta SD opcional de un sistema existente para actualizar ese sistema.

Formateo de una tarjeta SD

Las tarjetas SD de Avaya solo deben formatearse con las opciones de formato proporcionadas en las aplicaciones de IP Office. Este proceso normalmente no es necesario con las tarjetas SD de Avaya, a menos que sospeche que la tarjeta se ha formateado incorrectamente en otro lugar.

- **ADVERTENCIA: Todos los archivos serán borrados**
  Tenga en cuenta que esta acción borrará todos los archivos y carpetas existentes en la tarjeta. Una vez que se haya formateado una tarjeta, las carpetas y los archivos necesarios para el funcionamiento de IP Office se pueden cargar en la tarjeta desde la PC de IP Office Manager mediante el comando Recrear tarjeta SD de IP Office.

1. Inserte la tarjeta SD en una ranura de lector en la computadora IP Office Manager.
2. Usando IP Office Manager, seleccione**Archivo | Avanzado | Formatear la tarjeta SD de IP Office**.
3. Seleccione**Ley A de IP Office**o**Ley U de IP Office**. Esta selección solo establece la etiqueta de la tarjeta que se muestra al ver los detalles de la tarjeta. No afecta el formato real. Seleccione la etiqueta que coincida con el conjunto de archivos que colocará en la tarjeta.
4. Busque la ubicación de la tarjeta y haga clic en**OK**.
5. La barra de estado en la parte inferior de IP Office Manager mostrará el progreso del proceso de formateo.
6. Cuando se complete el formateo, puede usar el**Recrear la tarjeta SD de IP Office**comando para cargar las carpetas y archivos de IP Office en la tarjeta desde la PC IP Office Manager.

Recreación de una tarjeta SD de IP Office

Puede usar IP Office Manager para actualizar el conjunto de archivos en una tarjeta SD del sistema para que coincidan con los esperados para la versión particular de IP Office. Esto se puede usar para actualizar la tarjeta de un sistema existente o para preparar la tarjeta para un nuevo sistema.

IP Office Manager actualiza la tarjeta con los archivos de firmware binarios para la unidad de control, los módulos de expansión externos y los teléfonos. También incluye los archivos de aviso para la operación del correo de voz incorporado y una opción para los archivos de la aplicación del administrador web.

Los archivos existentes, como la configuración del sistema, el archivo de licencia PLDS y los mensajes y saludos de correo de voz integrados, se conservan.

- Para que la tarjeta se utilice en una unidad de control**SD del sistema**ranura para tarjetadebe ser una tarjeta SD del sistema Avaya . La tarjeta debe formatearse correctamente (eso se puede hacer con IP Office Manager); sin embargo, no es necesario volver a formatear una tarjeta en funcionamiento antes de usar recrear para actualizar el contenido de la tarjeta.
- El origen de los archivos copiados a la tarjeta SD son las subcarpetas del***Tarjetas de memoria**carpeta debajo de las aplicaciones del administrador**Directorio de trabajo**(normalmente***C:\Archivos de programa (x86)\Avaya\IP Office\Manager***). Sin embargo, si el**Directorio de trabajo**se cambia a una ubicación sin un conjunto apropiado de***Tarjetas de memoria**subcarpetas, el conjunto de archivos necesario no se copiará en la tarjeta SD.
  - **!ADVERTENCIA: Instalación de unidades de control PCS14 y anteriores**
    PC 296 14 o unidades inferiores deben instalar primero la versión 8.1(65) (o superior 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1. Se debe tener cuidado para asegurarse de que no se realicen llamadas antes de la actualización a la Versión 10.0, de lo contrario, el sistema requerirá una licencia de actualización 10.0 a pesar de ser "nuevo". El PCS de la unidad de control está impreso en la etiqueta en la parte posterior de la unidad de control.

Configuración del nivel de software del sistema inicial

Cuando la unidad de control hace su primera llamada, la versión del software que está ejecutando se escribe en un registro permanente en la unidad de control. Este se convierte en el nivel básico de la unidad de control al considerar los requisitos futuros para licencias de actualización, etc. Por lo tanto, para un sistema nuevo es importante que actualice la tarjeta SD del sistema a la versión de software requerida antes de iniciar el sistema.

Determinación del nivel de software de la tarjeta SD del sistema

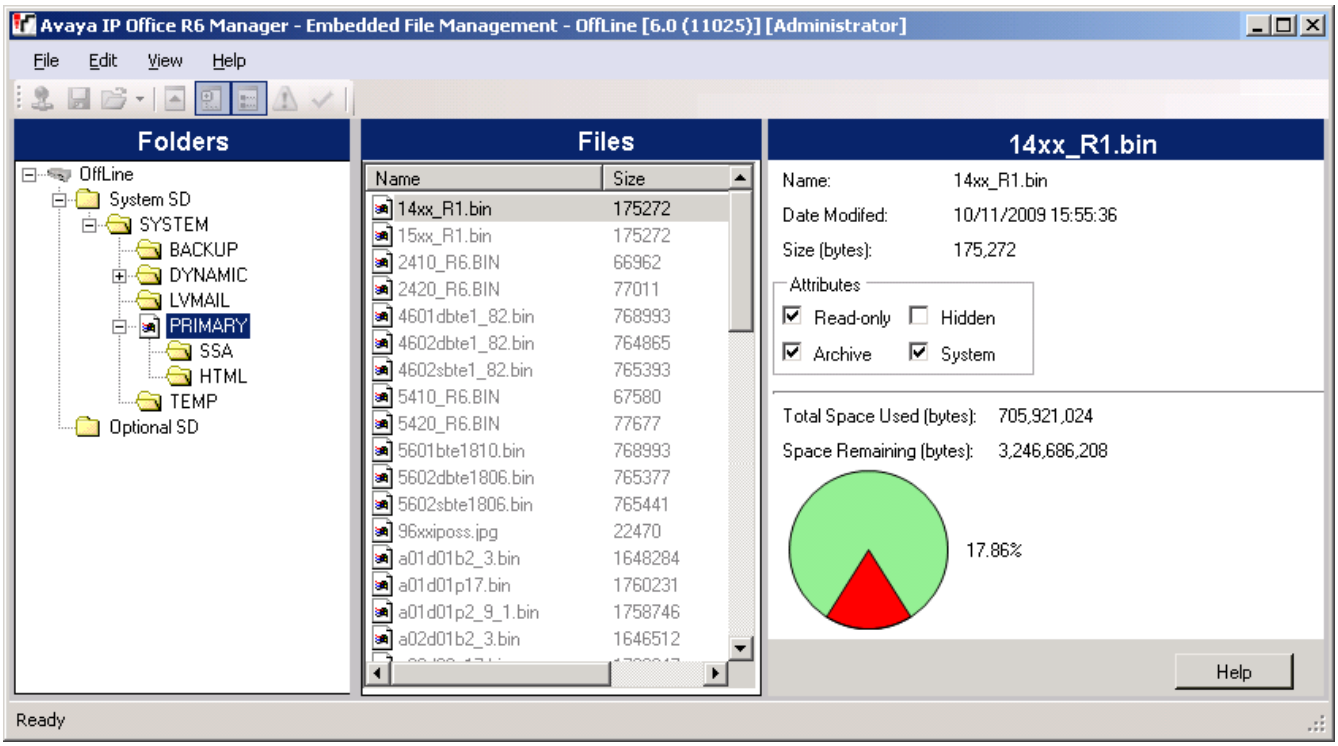
En la tarjeta SD, en el***sistema/primario***carpeta, localice y abra la carpeta***listaarchivos.txt***expediente. La sección de encabezado al comienzo del archivo termina con la versión del conjunto de archivos previamente copiados en la tarjeta. El resto del archivo enumera los archivos reales.

Para actualizar/recrear una tarjeta SD del sistema

1. Una vez iniciado, no interrumpa este proceso, por ejemplo, retirando la tarjeta SD. Este proceso dura aproximadamente 20 minutos.
2. Inserte la tarjeta SD en un lector de tarjetas en la PC IP Office Manager.
3. Usando IP Office Manager, seleccione**Archivo | Avanzado | Recrear la tarjeta SD de IP Office**.
4. Seleccione**Ley A de IP Office**o**Ley U de IP Office**. Esta selección afecta la forma en que los sistemas IP Office funcionan cuando están predeterminados con esta tarjeta presente en su**SD del sistema**ranura para tarjetas.
5. Busque la ubicación de la tarjeta y haga clic en**OK**.
6. IP Office Manager le preguntará si desea incluir archivos de Avaya IP Office Web Manager como parte del proceso de recreación. Esos archivos son necesarios si desea ejecutarAdministrador web de IP Office 71para administrar el sistema IP Office en el que está cargada la tarjeta o si desea utilizarinducción 138.
7. IP Office Manager comenzará a crear carpetas en la tarjeta SD y copiará los archivos necesarios en esas carpetas. Este proceso tomará aproximadamente 20 minutos.
8. No extraiga la tarjeta SD durante el proceso. Espere hasta que IP Office Manager muestre un mensaje.

11.3 Visualización del contenido de la tarjeta

Con IP Office Manager, puede ver las carpetas y los archivos en la tarjeta SD del sistema y la tarjeta SD opcional. Luego puede usar varios comandos para cargar y descargar archivos desde y hacia las tarjetas.



1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Gestión de archivos integrada**.
2. Usando el**Seleccione IP Office**menú, seleccione el sistema IP Office.
3. Se muestra el contenido del archivo de las tarjetas de memoria.

11.4 Copia de seguridad en la carpeta de copia de seguridad

Este proceso copia el contenido del**/primario**carpeta en la tarjeta SD del sistema sobre la**/respaldo**carpeta en la misma tarjeta. Se reemplazan todos los archivos con nombres de archivo coincidentes. Esto toma aproximadamente 6 minutos. Para conocer los métodos de restauración desde el**/respaldo**carpeta verRestaurar desde la carpeta de copia de seguridad 150.

Estos procesos no respaldan las indicaciones, los mensajes y los saludos utilizados por los buzones de correo de voz y los operadores automáticos del sistema. Se almacenan en la tarjeta**/lvmail**y**/dinámico/lvmail**carpetas

11.4.1 Copia de seguridad en la carpeta de copia de seguridad con IP Office Manager

Para hacer una copia de seguridad en la carpeta /backup usando IP Office Manager

1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Gestión de archivos integrada**.
2. Usando el**Seleccione IP Office**menú, seleccione el sistema IP Office.
3. Se muestra el contenido del archivo de las tarjetas de memoria.
4. Seleccione**Archivo | Archivos del sistema de copia de seguridad**.
   - los contenidos de la**/primario**carpeta en la tarjeta SD del sistema se copiará en la**/respaldo**carpeta. Este proceso dura aproximadamente 6 minutos.

11.4.2 Copia de seguridad en la carpeta de copia de seguridad mediante la aplicación de estado del sistema

Para hacer una copia de seguridad en la carpeta /backup usando System Status Application

1. EmpezarEstado del sistema 69y acceda a la salida de estado de IP Office.
2. En el panel de navegación, seleccione**Sistema**.
3. En la parte inferior de la pantalla, seleccione**Archivos del sistema de copia de seguridad**.
   - los contenidos de la**/primario**carpeta en la tarjeta SD del sistema se copiará en la**/respaldo**carpeta. Este proceso dura aproximadamente 6 minutos.

11.4.3 Copia de seguridad en la carpeta de copia de seguridad mediante un teléfono del sistema

Este proceso puede ser utilizado por un usuario configurado como usuario de System Phone y usando un teléfono de la serie 1400, 1600, 9500 o 9600 (excluyendo los modelos XX01, XX02 y XX03). Los usuarios**Código de inicio de sesión**se utiliza para restringir el acceso a las funciones de administración del sistema en el teléfono.

Para hacer una copia de seguridad en la carpeta /backup usando un System Phone

1. Seleccione**Características | Usuario de teléfono | Administrador del sistema**.
2. Ingrese su código de inicio de sesión de usuario de IP Office.
3. En el menú, seleccione**Tarjeta de memoria**.
4. Seleccione**Copia de seguridad del sistema**.
   - los contenidos de la**/primario**carpeta en la tarjeta SD del sistema se copiará en la**/respaldo**carpeta. Este proceso dura aproximadamente 6 minutos.

11.4.4 Copia de seguridad en la carpeta de copia de seguridad mediante IP Office Web Manager

Para hacer una copia de seguridad en la carpeta /backup usando IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7
   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.
2. Haga clic en**Comportamiento**y seleccione**Respaldo**.
2. Para seleccionar el destino***En el dispositivo***.
3. Haga clic en**Respaldo**.

11.5 Restauración desde la carpeta de copia de seguridad

los contenidos de la**/respaldo**carpeta en la tarjeta SD del sistema se puede copiar a la**/primario**carpeta en la misma tarjeta. Se reemplazan todos los archivos con nombres de archivo coincidentes. A continuación, el sistema se reinicia utilizando los archivos del**/primario**carpeta.

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

11.5.1 Restauración desde la carpeta de respaldo mediante IP Office Manager

Para restaurar desde la carpeta /backup usando IP Office Manager

1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Gestión de archivos integrada**.
2. Usando el**Seleccione IP Office**menú, seleccione el sistema IP Office.
3. Se muestra el contenido del archivo de las tarjetas de memoria.
4. Seleccione**Archivo | Restaurar archivos del sistema**.
   - los contenidos de la**/respaldo**carpeta en la tarjeta SD del sistema se copian en la**/primario**carpeta. El proceso dura aproximadamente 6 minutos.
   - Cuando se ha completado el proceso, el sistema se reinicia.

11.5.2 Restauración desde la carpeta de copia de seguridad utilizando la aplicación de estado del sistema

Para restaurar desde la carpeta /backup usando System Status Application

1. EmpezarEstado del sistema 69y acceda a la salida de estado de IP Office.
2. En el panel de navegación, seleccione**Sistema**.
3. En la parte inferior de la pantalla, seleccione**Restaurar archivos del sistema**.
   - los contenidos de la**/respaldo**carpeta en la tarjeta SD del sistema se copian en la**/primario**carpeta. El proceso dura aproximadamente 6 minutos.
   - Cuando se ha completado el proceso, el sistema se reinicia.

11.5.3 Restauración desde la carpeta de copia de seguridad utilizando un teléfono del sistema

Este proceso puede ser utilizado por un usuario configurado como usuario de System Phone y usando un teléfono de la serie 1400, 1600, 9500 o 9600 (excluyendo los modelos XX01, XX02 y XX03). Los usuarios**Código de inicio de sesión**se utiliza para restringir el acceso a las funciones de administración del sistema en el teléfono.

Para restaurar desde la carpeta /backup usando un System Phone

1. Seleccione**Características | Usuario de teléfono | Administrador del sistema**.
2. Ingrese su código de inicio de sesión de usuario de IP Office.
3. En el menú, seleccione**Tarjeta de memoria**.
4. Seleccione**Restauración del sistema**.
   - los contenidos de la**/respaldo**carpeta en la tarjeta SD del sistema se copian en la**/primario**carpeta. El proceso dura aproximadamente 6 minutos.
   - Cuando se ha completado el proceso, el sistema se reinicia.

11.5.4 Restauración desde la carpeta de respaldo mediante IP Office Web Manager

Para restaurar desde la carpeta /backup usando IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7
   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.
2. Haga clic en**Comportamiento**y seleccione**Restaurar**.
2. Para seleccionar el destino***En el dispositivo***.
3. Haga clic en**Restaurar**.

Página1166 de 3226.

11.6 Copia de seguridad en la tarjeta SD opcional

Este proceso copia todos los archivos de la tarjeta SD del sistema a la tarjeta SD opcional. Incluye el**/primario**y**/respaldo** carpetas y los archivos de Embedded Voicemail, incluidos los archivos de mensajes. Se sobrescribirán todos los archivos y carpetas que coincidan en la tarjeta SD opcional.

El proceso es una copia simple. Cualquier archivo que ya haya copiado ese cambio mientras el proceso no se vuelve a copiar. Cualquier archivo nuevo agregado mientras se ejecuta el proceso, por ejemplo, mensajes de correo de voz, no se puede copiar.

Este proceso demora al menos 90 minutos y puede demorar mucho más dependiendo de la cantidad de datos que se copiarán, por ejemplo, será más prolongado si el sistema IP Office utiliza Embedded Voicemail para tomar mensajes.

11.6.1 Copia de seguridad en la tarjeta SD opcional mediante IP Office Manager

Para hacer una copia de seguridad de la tarjeta SD del sistema en la tarjeta SD opcional mediante IP Office Manager

1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Gestión de archivos integrada**.
2. Usando el**Seleccione IP Office**menú, seleccione el sistema IP Office.
3. Se muestra el contenido del archivo de las tarjetas de memoria.
4. Seleccione**Archivo | Copiar tarjeta del sistema**.
   - El contenido de la tarjeta SD del sistema se copiará a la tarjeta SD opcional. Este proceso dura al menos 90 minutos y puede llevar mucho más tiempo.

11.6.2 Copia de seguridad en la SD opcional mediante la aplicación de estado del sistema

Para hacer una copia de seguridad de la tarjeta SD del sistema en la tarjeta SD opcional mediante System Status Application

1. EmpezarEstado del sistema 69y acceda a la salida de estado de IP Office.
2. En el panel de navegación, seleccione**Sistema**.
3. Seleccione**Tarjetas de memoria**.
4. Seleccione**Tarjeta del sistema**.
5. En la parte inferior de la pantalla, seleccione**Copiar tarjeta del sistema**.
   - El contenido de la tarjeta SD del sistema se copiará a la tarjeta SD opcional. Este proceso dura al menos 90 minutos y puede llevar mucho más tiempo.

11.6.3 Copia de seguridad en la tarjeta SD opcional mediante IP Office Web Manager

Para hacer una copia de seguridad de la tarjeta SD del sistema en la tarjeta SD opcional mediante IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 71
   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.
2. Haga clic en**Comportamiento**. Seleccione**Comandos de servicio**y seleccione**Copiar a SD opcional**.
3. Haga clic en**OK**.

11.6.4 Copia de seguridad en la tarjeta SD opcional mediante un teléfono del sistema

Este proceso puede ser utilizado por un usuario configurado como usuario de System Phone y usando un teléfono de la serie 1400, 1600, 9500 o 9600 (excluyendo los modelos XX01, XX02 y XX03). Los usuarios**Código de inicio de sesión**se utiliza para restringir el acceso a las funciones de administración del sistema en el teléfono.

Para hacer una copia de seguridad de la tarjeta SD del sistema en la tarjeta SD opcional mediante un teléfono del sistema

1. Seleccione**Características | Usuario de teléfono | Administrador del sistema**.
2. Ingrese su código de inicio de sesión de usuario de IP Office.
3. En el menú, seleccione**Tarjeta de memoria**.
4. Seleccione**Copiar**.
   - El contenido de la tarjeta SD del sistema se copiará a la tarjeta SD opcional. Este proceso dura al menos 90 minutos y puede llevar mucho más tiempo.

11.7 Restauración de una configuración desde una tarjeta opcional

Los siguientes procesos copian el archivo de configuración (***config.cfg***) y archivo de licencias (***claves.txt***). Los procesos tardan unos segundos.

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

11.7.1 Restauración desde la tarjeta SD opcional mediante IP Office Manager

Para copiar un archivo de configuración desde la tarjeta SD opcional mediante IP Office Manager

1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Gestión de archivos integrada**.
2. Usando el**Seleccione IP Office**menú, seleccione el sistema IP Office.
3. Se muestra el contenido del archivo de las tarjetas de memoria.
4. Seleccione**Archivo | Configuración de actualización**.
   - El archivo de configuración (***config.cfg***) y archivo de licencias (***claves.txt***) en el***/primario***carpeta en la tarjeta SD opcional se copian en la***/primario***carpeta en la tarjeta SD del sistema. Este proceso dura aproximadamente unos segundos.
   - Cuando se haya completado el proceso, se reiniciará el sistema IP Office.

11.7.2 Restauración desde la tarjeta SD opcional mediante un teléfono del sistema

Este proceso puede ser utilizado por un usuario configurado como usuario de System Phone y usando un teléfono de la serie 1400, 1600, 9500 o 9600 (excluyendo los modelos XX01, XX02 y XX03). Los usuarios**Código de inicio de sesión**se utiliza para restringir el acceso a las funciones de administración del sistema en el teléfono.

Para copiar un archivo de configuración desde la tarjeta SD opcional mediante un teléfono del sistema

1. Seleccione**Características | Usuario de teléfono | Administrador del sistema**.
2. Ingrese su código de inicio de sesión de usuario de IP Office.
3. En el menú, seleccione**Tarjeta de memoria**.
4. Seleccione**Actualizar configuración...**.
   - El archivo de configuración (***config.cfg***) y archivo de licencias (***claves.txt***) en el***/primario***carpeta en la tarjeta SD opcional se copian en la***/primario***carpeta en la tarjeta SD del sistema. Este proceso dura aproximadamente unos segundos.
   - Cuando se haya completado el proceso, se reiniciará el sistema IP Office.

11.8 Carga de software desde una tarjeta SD opcional

Estos procesos copian todos los archivos en la carpeta excepto el archivo de configuración (***config.cfg***) y archivo de licencias (***claves.txt***). Los procesos tardan aproximadamente 5 minutos. Estos procesos no restauran las indicaciones del correo de voz integrado (verActualización del software de la tarjeta 156).

- **!Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín técnico de IP Office relacionado con la versión del software de IP Office que pretende instalar. El boletín contiene información importante que puede no haber sido incluida en este manual. Los boletines técnicos de IP Office están disponibles en elSoporte de Avaya sitio web*(http://soporte.avaya.com)*.

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

11.8.1 Carga de software desde la tarjeta SD opcional mediante IP Office Manager

Para copiar archivos de software desde la tarjeta SD opcional mediante IP Office Manager

1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Gestión de archivos integrada**.
2. Usando el**Seleccione IP Office**menú, seleccione el sistema IP Office.
3. Se muestra el contenido del archivo de las tarjetas de memoria.
4. Seleccione**Archivo | Actualizar binarios**.
   - Los archivos de software (todos los archivos en la carpeta excepto el archivo de configuración (***config.cfg***) y archivo de licencias (***claves.txt***)) en el***/primario***carpeta en la tarjeta SD opcional se copian en la***/primario***carpeta en la tarjeta SD del sistema. Este proceso dura aproximadamente 5 minutos.
   - Cuando se haya completado el proceso, se reiniciará el sistema IP Office.

11.8.2 Carga de software desde la tarjeta SD opcional mediante un teléfono del sistema

Este proceso puede ser utilizado por un usuario configurado como usuario de System Phone y usando un teléfono de la serie 1400, 1600, 9500 o 9600 (excluyendo los modelos XX01, XX02 y XX03). Los usuarios**Código de inicio de sesión**se utiliza para restringir el acceso a las funciones de administración del sistema en el teléfono.

Para copiar archivos de software desde la tarjeta SD opcional mediante un teléfono del sistema

1. Seleccione**Características | Usuario de teléfono | Administrador del sistema**.
2. Ingrese su código de inicio de sesión de usuario de IP Office.
3. En el menú, seleccione**Tarjeta de memoria**.
4. Seleccione**Actualizar binarios...**.
   - Los archivos de software (todos los archivos en la carpeta excepto el archivo de configuración (***config.cfg***) y archivo de licencias (***claves.txt***)) en el***/primario***carpeta en la tarjeta SD opcional se copian en la***/primario***carpeta en la tarjeta SD del sistema. Este proceso dura aproximadamente 5 minutos.
   - Cuando se haya completado el proceso, se reiniciará el sistema IP Office.

Página1170 de 3226.

11.9 Copia de seguridad en una PC

Este proceso copia el**/respaldo**carpeta en la tarjeta SD del sistema a una carpeta especificada en la PC que ejecuta IP Office Web Manager. Este proceso dura aproximadamente 25 minutos.

Antes de usar este proceso, el contenido de la carpeta /Backup se puede actualizar con los archivos de la carpeta /primary en la misma tarjeta. VerCopia de seguridad en la carpeta de copia de seguridad [149].

Para hacer una copia de seguridad en una PC usando IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office [7].

   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.

   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.

2. Haga clic en**Comportamiento**y seleccione**Respaldo**.
3. Para seleccionar el destino***Máquina cliente***.
4. Haga clic en**Configurar ruta**.
5. Seleccione la ubicación para la copia de seguridad y haga clic en**Abierto**. Le recomendamos que cree una nueva carpeta y luego seleccione esa carpeta.
6. Haga clic en**Comenzar respaldo**.
7. Espere hasta que se muestre un mensaje de copia de seguridad completada. Hacer clic**Cancelar**para cerrar el menú.

11.10 Restauración desde una PC

Este proceso restaura una copia de seguridad anterior, sobrescribiendo la carpeta /principal en la tarjeta SD del sistema.

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

Para restaurar desde una copia de seguridad de la PC usando IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office [7].

   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.

   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.

2. Haga clic en**Comportamiento**y seleccione**Restaurar**.
3. Haga clic en**Restaurar desde**y seleccione***Máquina cliente***.
4. Haga clic en**OK**.
5. Haga clic en**Configurar ruta**.
6. Seleccione la carpeta que contiene la copia de seguridad anterior y haga clic en**Abierto**.
7. Haga clic en**Iniciar restauración**.
8. Espere hasta que aparezca un mensaje de restauración completada. Hacer clic**Cancelar**para cerrar el menú. El sistema se reinicia.

11.11 Actualización del software de la tarjeta

Además de utilizar la tradicionalAsistente de actualización de IP Office 181,Las unidades de control IP500 V2 se pueden actualizar cargando el conjunto requerido de archivos de firmware en la tarjeta SD del sistema y reiniciar el sistema.

- **!Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín técnico de IP Office relacionado con la versión del software de IP Office que pretende instalar. El boletín contiene información importante que puede no haber sido incluida en este manual. Los boletines técnicos de IP Office están disponibles en elSoporte de Avaya sitio web*(http://soporte.avaya.com)*.

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

Hay un número de maneras en que esto se puede hacer.

Método	Descripción	Ubicación	Software archivos	Incrustado Mensaje de voz Indicaciones
Tarjeta SD del sistema Mejora 183	En este método, la tarjeta SD del sistema se apaga y se retira de la unidad de control. El contenido de la tarjeta se actualiza mediante IP Office Manager.	**Local**	✓	✓
Actualizar desde Tarjeta SD opcional 184	Este método usa una tarjeta SD cargada con la versión requerida del software IP Office. La tarjeta se inserta en la ranura para tarjeta SD opcional de la unidad de control y su contenido se copia en la tarjeta SD del sistema.	**Local**	✓	–

11.12 Apagado/Extracción de la tarjeta de memoria

Antes de quitar una tarjeta de memoria de un sistema IP Office que se está ejecutando, la tarjeta debe apagarse. Quitar una tarjeta de memoria mientras el sistema está funcionando puede dañar el archivo. Los servicios de la tarjeta se pueden reiniciar reinsertando la tarjeta o usando un Comando de puesta en marcha 158.

11.12.1 Apagar una tarjeta mediante IP Office Manager

Para apagar una tarjeta de memoria usando IP Office Manager

1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Comandos de tarjeta de memoria | Cerrar**.
2. Usando el**Seleccione IP Office**seleccione el sistema IP Office que contiene la tarjeta de memoria.
3. Haga clic en**OK**.
   - En la parte posterior de la unidad de control, confirme que el LED de la tarjeta de memoria correspondiente esté apagado.
   - Ahora se puede retirar la tarjeta para realizar las acciones de mantenimiento necesarias.

11.12.2 Apagar una tarjeta usando la aplicación de estado del sistema

Para apagar una tarjeta de memoria mediante System Status Application

1. EmpezarEstado del sistema 69y acceda a la salida de estado de IP Office.
2. En el panel de navegación, seleccione**Sistema**.
3. Seleccione**Tarjetas de memoria**.
4. Seleccione cualquiera**Tarjeta del sistema**o**Tarjeta Opcional**.
5. En la parte inferior de la pantalla, seleccione**Cerrar**.
   - En la parte posterior de la unidad de control, confirme que el LED de la tarjeta de memoria correspondiente esté apagado.
   - Ahora se puede retirar la tarjeta para realizar las acciones de mantenimiento necesarias.

11.12.3 Apagar una tarjeta mediante IP Office Web Manager

Para apagar una tarjeta usando IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7.
   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.
2. Haga clic en**Comportamiento**. Seleccione**Comandos de servicio**y seleccione**Parada de tarjeta de memoria**.
3. Seleccione la tarjeta para detener y haga clic en**OK**.

11.12.4 Apagar una tarjeta usando un teléfono del sistema

Este proceso puede ser utilizado por un usuario configurado como usuario de System Phone y usando un teléfono de la serie 1400, 1600, 9500 o 9600 (excluyendo los modelos XX01, XX02 y XX03). Los usuarios**Código de inicio de sesión**se utiliza para restringir el acceso a las funciones de administración del sistema en el teléfono.

Para apagar una tarjeta usando un teléfono del sistema

1. Seleccione**Características | Usuario de teléfono | Administrador del sistema**.
2. Ingrese su código de inicio de sesión de usuario de IP Office.
3. En el menú, seleccione**Tarjeta de memoria**.
4. Seleccione**Sistema**para la tarjeta SD del sistema o**Opción**para la tarjeta SD opcional.
5. Seleccione**Cerrar**.
   - En la parte posterior de la unidad de control, confirme que el LED de la tarjeta de memoria correspondiente esté apagado.
   - Ahora se puede retirar la tarjeta para realizar las acciones de mantenimiento necesarias.

Página1173 de 3226.

11.13 Inicio de la tarjeta de memoria

Reinsertar una tarjeta de memoria en un sistema que ya está encendido reinicia automáticamente el funcionamiento de la tarjeta. Sin embargo, si ella tarjeta ha sido apagada [157] pero no se elimina, se puede reiniciar con IP Office Manager sin necesidad de reiniciar.

11.13.1 Iniciar una tarjeta mediante IP Office Manager

Para iniciar una tarjeta usando IP Office Manager

1. Usando IP Office Manager, seleccione **Archivo | Avanzado | Comandos de tarjeta de memoria | Puesta en marcha**.
2. Usando el **Seleccione IP Office** seleccione el sistema IP Office que contiene la tarjeta de memoria.
3. Haga clic en **OK**.

11.13.2 Iniciar una tarjeta usando la aplicación de estado del sistema

Para iniciar una tarjeta usando System Status Application

1. Empezar Estado del sistema [69] y acceda a la salida de estado de IP Office.
2. En el panel de navegación, seleccione **Sistema**.
3. Seleccione **Tarjetas de memoria**.
4. Seleccione cualquiera **Tarjeta del sistema** o **Tarjeta Opcional**.
5. En la parte inferior de la pantalla, seleccione **Puesta en marcha**.

11.13.3 Iniciar una tarjeta mediante IP Office Web Manager

Para iniciar una tarjeta usando IP Office Web Manager

1. Iniciar sesión en Administrador web de IP Office [7].
   a. Introduzca la dirección IP del sistema en el navegador. Seleccione **Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en **Acceso**.
2. Haga clic en **Comportamiento**. Seleccione **Comandos de servicio** y seleccione **Inicio de la tarjeta de memoria**.
3. Seleccione la tarjeta para comenzar y haga clic en **OK**.

11.13.4 Iniciar una tarjeta usando un teléfono del sistema

Este proceso puede ser utilizado por un usuario configurado como usuario de System Phone y usando un teléfono de la serie 1400, 1600, 9500 o 9600 (excluyendo los modelos XX01, XX02 y XX03). Los usuarios **Código de inicio de sesión** se utiliza para restringir el acceso a las funciones de administración del sistema en el teléfono.

Para iniciar una tarjeta utilizando un teléfono del sistema

1. Seleccione **Características | Usuario de teléfono | Administrador del sistema**.
2. Ingrese su código de inicio de sesión de usuario de IP Office.
3. En el menú, seleccione **Tarjeta de memoria**.
4. Seleccione **Sistema** para la tarjeta SD del sistema o **Opción** para la tarjeta SD opcional.
5. Seleccione **Puesta en marcha**.

Capítulo 12.
Procesos Adicionales

12. Procesos Adicionales

Esta sección cubre una variedad de procesos de mantenimiento.

Procesos

- Cambio de un sistema IP Office Basic Edition al modo estándar 161
- Apagar un sistema/Apagar el sistema 163
- Reinicio de un sistema 169
- Cambio de componentes 167
- Por defecto la configuración 170
- Por defecto la configuración de seguridad 173
- Cargando un nuevo archivo de configuración 177
- Intercambio de usuarios de extensión 186
- Actualización de sistemas 186
- Instalación de teléfono fuera del edificio 36
- Uso del puerto de salida externo 191
- Configuración de SNMP 192
- Botón de reinicio 197
- botón auxiliar 197
- Mantenimiento del puerto RS232 198
- Borrar el software principal 199
- Activación de IP Office Web Manager 202

Otros Procesos

Los siguientes procesos de mantenimiento adicionales se tratan en otras secciones de este documento:

- Creación de una tarjeta SD de IP Office 146
- Visualización del contenido de la tarjeta 146
- Copia de seguridad de la configuración 149
- Restauración de la configuración 150
- Copiar a la tarjeta SD opcional 152
- Restauración desde la tarjeta SD opcional 153
- Apagado/extracción de la tarjeta de memoria 157
- Inicio de la tarjeta de memoria 158
- Inducción 138
- Instalación de las aplicaciones de administración 64

¿Comentarios sobre este documento? infodev@avaya.com

12.1 Cambio de un sistema IP Office Basic Edition al modo estándar

El proceso a continuación cambiará el modo del sistema y predeterminará su configuración.

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

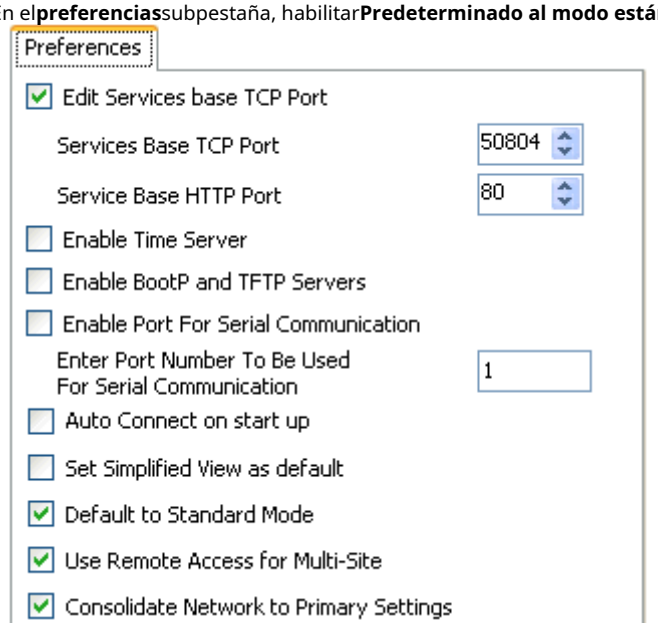
1. Usando IP Office Manager, reciba elconfiguración desde el sistema 68.
2. Cuando se le solicite, ingrese el nombre de usuario y la contraseña del servicio.
3. La aplicación IP Office Manager cambia automáticamente a su vista simplificada ya que la configuración es de un sistema que se ejecuta en el modo IP Office Basic Edition.
4. Seleccione**Archivo | Avanzado | Cambiar al modo estándar (predeterminado)**.
5. La configuración cambia a una predeterminada para un sistema IP Office Essential Edition e IP Office Manager cambia a su modo de vista avanzada.
6. Este es un momento adecuado para comenzarConfiguracion Inicial 100antes de enviar la configuración al sistema IP Office para reiniciar en IP Office Essential Edition.
   - Para que un sistema se ejecute en el modo IP Office Essential Edition o IP Office Preferred Edition, su configuración debe incluir un**Edición esencial**licencia. Un sistema sin esta licencia no permitirá ninguna función de telefonía hasta que se agregue la licencia.
7. Una vez que el sistema se haya reiniciado, use IP Office Manager para recibir nuevamente la configuración del sistema. El nombre de usuario y la contraseña para la configuración deben ser los valores predeterminados del modo IP Office Standard Version**Administrador** y **Administrador**.

12.2 Automatización del cambio a modo estándar

Si los únicos sistemas que instala son los que utilizan los modos estándar de IP Office, se puede configurar IP Office Manager para que el sistema cambie automáticamente al modo estándar de IP Office.

- **!ADVERTENCIA**
  Los procesos a continuación requieren que el sistema IP Office se reinicie para aplicar los cambios realizados. El reinicio finaliza todas las llamadas y servicios actuales.

1. En IP Office Manager, seleccione**Archivo | preferencias**.
2. En el**preferencias**subpestaña, habilitar**Predeterminado al modo estándar**.



3. Con esta opción habilitada, cuando una configuración para unnuevo o predeterminado IP Office Manager recibe un sistema que se ejecuta en IP Office Basic Edition, se convertirá automáticamente a una configuración de IP Office Essential Edition.

4. **!Importante: la configuración de la dirección IP es predeterminada para el servidor**
   La conversión establecerá el modo DHCP en***Servidor***y las direcciones LAN a sus valores predeterminados de 192.168.42.1 y 192.168.43.1. Usar IP Office Manager para cambiar esta configuración a los valores requeridos.

5. Este es un momento adecuado para comenzarConfiguracion Inicial 100antes de enviar la configuración al sistema IP Office para reiniciar en IP Office Essential Edition.

   - Para que un sistema se ejecute en el modo IP Office Essential Edition o IP Office Preferred Edition, su configuración debe incluir un**Edición esencial**licencia. Un sistema sin esta licencia no permitirá ninguna función de telefonía hasta que se agregue la licencia.

6. Al enviar la configuración al sistema, se reinicia el sistema en el modo IP Office Essential Edition.

12.3 Apagar un sistema

Los sistemas que ejecutan la versión 6.0 de IP Office deben apagarse para realizar el mantenimiento en lugar de simplemente apagarse. El apagado puede ser indefinido o por un período de tiempo determinado, después del cual IP Office se reiniciará automáticamente. Tenga en cuenta que las tarjetas de memoria de la unidad de control se pueden cerrar 157 y reiniciado 158 por separado del sistema.

Durante el proceso de apagado, la configuración actual en la memoria RAM de la unidad de control se copia en la memoria no volátil de la unidad de control. Para los sistemas IP500 V2, esa ubicación es la tarjeta SD del sistema.

- **!ADVERTENCIA**
  Siempre se debe usar un apagado para apagar el sistema. Simplemente retirar el cable de alimentación o apagar la entrada de alimentación puede causar la pérdida de datos de configuración.
  - Este no es un cierre cortés, se detendrán todas las llamadas de los usuarios y los servicios en funcionamiento. Una vez apagado, el sistema no se puede utilizar para realizar ni recibir llamadas hasta que se reinicie.
  - El proceso de apagado tarda hasta un minuto en completarse. Al apagar un sistema con Unified Communications Module instalado, el apagado puede demorar hasta 3 minutos mientras la tarjeta cierra de forma segura todos los archivos abiertos y cierra su sistema operativo.
- **Indicación LED de apagado**
  Cuando se apaga, los LED que se muestran en el sistema son los siguientes. No desconecte la alimentación del sistema ni extraiga ninguna de las tarjetas de memoria hasta que el sistema se encuentre en este estado:
  - El LED 1 de cada tarjeta base IP500 instalada también parpadeará en rojo rápidamente más el LED 9 si se instala una tarjeta secundaria de troncales en la tarjeta base.
  - El LED de la CPU en la parte posterior del sistema parpadeará en rojo rápidamente.
  - Los LED de la tarjeta de memoria SD del sistema y SD opcional en la parte posterior del sistema están apagados.
- **Reinicio de un sistema**
  Para reiniciar un sistema cuando se apaga indefinidamente, o para reiniciar un sistema antes de que expire el tiempo de reinicio, apague el sistema y vuelva a encenderlo.

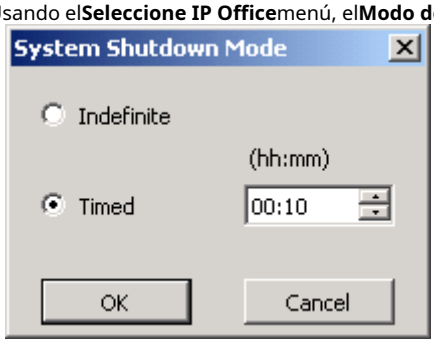
Opciones de proceso

1. Apagar un sistema usando IP Office Manager 163
2. Apagar un sistema usando la aplicación de estado del sistema 164
3. Apagar un sistema usando un System Phone 164
4. Apagar un sistema usando el botón AUX 164
5. Apagar un sistema usando IP Office Web Manager 164

12.3.1 Apagar un sistema mediante IP Office Manager

Para apagar un sistema usando IP Office Manager

1. Usando IP Office Manager, seleccione **Archivo | Avanzado | Apagado del sistema**.
2. Usando el **Seleccione IP Office** menú, el **Modo de apagado del sistema** se muestra el menú.



3. Seleccione el tipo de apagado requerido. Si **Indefinido** se utiliza, el sistema solo se puede reiniciar apagando y encendiendo de nuevo la alimentación. si un **cronometrado** se selecciona el apagado, IP Office se reiniciará después de que haya transcurrido el tiempo establecido.
4. Haga clic en **OK**.
5. Espere hasta que todos los LED en la parte frontal del sistema parpadeen rápidamente en rojo antes de realizar cualquier otra acción.

12.3.2 Apagar un sistema mediante la aplicación de estado del sistema

Para apagar un sistema mediante la aplicación de estado del sistema

1. EmpezarEstado del sistema 69y acceda a la salida de estado de IP Office.
2. En el panel de navegación, seleccione**Sistema**.
3. En la parte inferior de la pantalla, seleccione**Sistema apagado**.
4. Seleccione el tiempo de duración del apagado o indefinido.
5. Haga clic en**OK**.
6. Espere hasta que todos los LED en la parte frontal del sistema parpadeen rápidamente en rojo antes de realizar cualquier otra acción.

12.3.3 Apagar un sistema mediante un teléfono del sistema

Este proceso puede ser utilizado por un usuario configurado como usuario de System Phone y usando un teléfono de la serie 1400, 1600, 9500 o 9600 (excluyendo los modelos XX01, XX02 y XX03). Los usuarios**Código de inicio de sesión**se utiliza para restringir el acceso a las funciones de administración del sistema en el teléfono.

A diferencia de IP Office Manager, un usuario de teléfono del sistema no puede seleccionar un apagado indefinido. Pueden programar un tiempo de apagado de entre 5 minutos y 24 horas.

Para apagar un sistema mediante un teléfono del sistema

1. Seleccione**Características | Usuario de teléfono | Administrador del sistema**.
2. Ingrese su código de inicio de sesión de usuario de IP Office.
3. En el menú, seleccione**Apagado del sistema**.
4. Seleccione un período de tiempo para el apagado. Debe ser entre 5 minutos y 24 horas.
5. Presione**Hecho**y entonces**Confirmar**para comenzar el apagado.
6. Espere hasta que todos los LED en la parte frontal del sistema parpadeen rápidamente en rojo antes de realizar cualquier otra acción.

12.3.4 Apagar un sistema usando el botón AUX

Este método es compatible con las unidades de control IP500 V2.

Para apagar un sistema usando el botón IP500 V2 AUX

1. En la parte trasera de la unidad de control, mantenga presionada la**auxiliar**botón durante más de 5 segundos.
2. La unidad de control se apagará con el temporizador de reinicio establecido en 10 minutos.
3. Espere hasta que todos los LED en la parte frontal del sistema parpadeen rápidamente en rojo antes de realizar cualquier otra acción.

12.3.5 Apagar un sistema mediante IP Office Web Manager

Para apagar un sistema usando IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7
   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.
2. Haga clic en**Comportamiento**. Seleccione**Comandos de servicio**y entonces**Apagado del sistema**.
3. Haga clic en**OK**.
4. Espere hasta que todos los LED en la parte frontal del sistema parpadeen rápidamente en rojo antes de realizar cualquier otra acción.

12.4 Reinicio de un sistema

Ocasionalmente puede ser necesario reiniciar el sistema. Por ejemplo, después de reinsertar una tarjeta SD del sistema con el software del sistema actualizado. Eso se puede hacer usando cualquiera de los siguientes procesos.

- **!ADVERTENCIA**
  Siempre se debe utilizar uno de los siguientes métodos para reiniciar un sistema. Simplemente quitar y luego volver a conectar la energía al sistema puede causar la pérdida de datos y una operación inesperada del sistema.

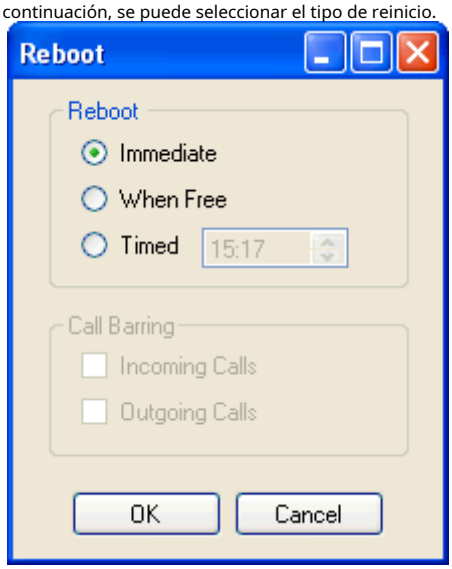
Opciones de proceso

1. Reiniciar un sistema usando IP Office Manager 165
2. Reinicie un sistema usando IP Office Web Manager 166
3. Reinicie un sistema usando el botón Restablecer 166
4. Reiniciar un sistema usando un teléfono del sistema 166

12.4.1 Reiniciar un sistema mediante IP Office Manager

Para reiniciar un sistema usando IP Office Manager

1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Reiniciar**.
2. Usa el**Seleccione IP Office**para ubicar y seleccionar el sistema IP Office. Introduzca un nombre de usuario y una contraseña válidos.
3. A continuación, se puede seleccionar el tipo de reinicio.



- **Reiniciar**
  Seleccione cuándo debe ocurrir el reinicio.
  - **Inmediato**
    Reinicie el sistema inmediatamente.
  - **Cuando libre**
    Reinicie el sistema cuando no haya llamadas en curso. Este modo se puede combinar con el**Bloqueo de llamadas** opciones
  - **cronometrado**
    Lo mismo que cuando está libre, pero espera un tiempo específico después del cual espera a que no haya llamadas en curso. El tiempo es especificado por el**Tiempo de reinicio**. Este modo se puede combinar con el**Bloqueo de llamadas** opciones
- **Tiempo de reinicio**
  Esta configuración se utiliza cuando el modo de reinicio**cronometrado**es seleccionado. Establece la hora de reinicio de IP Office. Si la hora es posterior a la medianoche, se cancela la copia de seguridad diaria normal de IP Office.
- **Bloqueo de llamadas**
  Esta configuración se puede usar cuando se selecciona el modo de reinicio Cuando está libre. Prohiben el envío o la recepción de nuevas llamadas.

4. Haga clic en**OK**.

12.4.2 Reiniciar un sistema mediante IP Office Web Manager

Para reiniciar un sistema usando IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7.

   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.

   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.

2. Haga clic en**Comportamiento**. Seleccione**Comandos de servicio**y entonces**Reiniciar**.

3. Seleccione cuándo debe ocurrir el reinicio.

   - **Inmediato**
     Reinicie el sistema inmediatamente.
   - **Libre**
     Reinicie el sistema cuando no haya llamadas en curso.
   - cronometrado
     Reinicie el sistema a la hora establecida.

4. Haga clic en**OK**.

12.4.3 Reiniciar un sistema usando el botón de reinicio

Para reiniciar un sistema usando el botón Restablecer

Utilice este proceso para reiniciar el sistema cuando esté libre. Una vez invocado, el sistema bloquea cualquier nueva llamada entrante o saliente hasta después del reinicio.

1. En la parte trasera de la unidad de control, mantenga presionada la**Reiniciar**durante 5 a 10 segundos hasta que el**UPC**lideró cambios ennaranja constante .
2. Cuando el**UPC**LED cambia anaranja constante , suelte el botón.
   - Si el**UPC**LED cambiado anaranja parpadeante orojo , mantenga presionado el botón hasta que**UPC**El LED cambia a verde intermitente. Luego suelte el botón y vuelva a intentar el proceso una vez que el LED de la CPU haya vuelto a estar en verde fijo.
3. Espere a que se complete el reinicio antes de realizar cualquier otra acción.

12.4.4 Reinicio de un sistema mediante un teléfono del sistema

Esta función no es compatible con los teléfonos del sistema en el sistema que se ejecuta en el modo estándar de IP Office.

12.5 Cambio de componentes

En las siguientes secciones, el término componente puede hacer referencia a una tarjeta instalada en IP Office o un módulo de expansión externo.

- **!IMPORTANTE:**
  Debe apagar la unidad de control antes de agregar, quitar o cambiar componentes Las tarjetas base, las tarjetas de troncales y los módulos de expansión externos solo se deben quitar y agregar a un sistema IP Office cuando ese sistema está apagado 163.Si no lo hace, el nuevo componente no cargará el firmware correcto y no funcionará o no funcionará correctamente. Esto se aplica incluso cuando se intercambian componentes similares.

Tenga en cuenta que para los puertos de extensión existentes, de manera predeterminada existirán tanto una entrada de extensión como una entrada de usuario en la configuración de IP Office. Las entradas de extensión se pueden eliminar sin eliminar la entrada de usuario correspondiente. Esto permite la retención de la configuración del usuario y la asociación del usuario con una extensión diferente al cambiar esas extensiones.**Extensión de base**número que coincida con el del usuario**ID de extensión**.

Procesos

- **Me gusta por reemplazo** 168
- **Sustitución de componentes de mayor capacidad** 168
- **Sustitución de componentes de menor capacidad** 168
- **Agregar un nuevo componente** 168
- **Eliminación permanente de un componente** 169
- **Reemplazo con un tipo diferente de componente** 169

12.5.1 Sustitución igual por igual

Si se reemplaza con un componente del mismo tipo, no se requieren cambios de configuración.

Para hacer un reemplazo de Me gusta

1. Apagar el sistema 163.
2. Desconecte la alimentación del sistema.
3. Retire la tarjeta o el módulo de expansión externo. Tenga en cuenta que la ranura para tarjetas o el puerto de expansión utilizado como reemplazo debe instalarse en la misma posición.
4. Instale el reemplazo usando el proceso apropiado para el tipo de componente (Montaje de tarjetas IP500 82, Adición de módulos de expansión externos 91).
5. Reinicie el sistema IP Office.

12.5.2 Reemplazo de mayor capacidad

Si se reemplaza con un componente del mismo tipo pero de mayor capacidad, cuando se reinicie, IP Office creará automáticamente entradas de configuración para las nuevas troncales o extensiones/usuarios.

Para reemplazar un componente con uno del mismo tipo pero de mayor capacidad

1. Apagar el sistema 163.
2. Desconecte la alimentación del sistema.
3. Retire la tarjeta o el módulo de expansión externo. Tenga en cuenta que la ranura para tarjetas o el puerto de expansión utilizado como reemplazo debe instalarse en la misma posición.
4. Instale el reemplazo usando el proceso apropiado para el tipo de componente (Montaje de tarjetas IP500 82, Adición de módulos de expansión externos 91).
5. Reinicie el sistema IP Office.
6. Use IP Office Manager para configurar las nuevas troncales o extensiones/usuarios.

12.5.3 Reemplazo de menor capacidad

Si se reemplaza con un componente del mismo tipo pero de menor capacidad, después de reiniciar IP Office, será necesario editar la configuración para eliminar las entradas redundantes.

Para reemplazar un componente con uno del mismo tipo pero de menor capacidad

1. Apagar el sistema 163.
2. Desconecte la alimentación del sistema.
3. Retire la tarjeta o el módulo de expansión externo. Tenga en cuenta que la ranura para tarjetas o el puerto de expansión utilizado como reemplazo debe instalarse en la misma posición.
4. Instale el reemplazo usando el proceso apropiado para el tipo de componente (Montaje de tarjetas IP500 82, Adición de módulos de expansión externos 91).
5. Reinicie el sistema IP Office.
6. Use IP Office Manager para eliminar las troncales o extensiones/usuarios que ya no son compatibles con el componente instalado.

12.5.4 Adición de un nuevo componente

Si agrega un nuevo componente a una ranura o puerto disponible, cuando se reinicie, IP Office creará automáticamente entradas de configuración para las nuevas troncales o extensiones/usuarios.

Para agregar un nuevo componente

1. Apagar el sistema 163.
2. Desconecte la alimentación del sistema.
3. Instale el reemplazo usando el proceso apropiado para el tipo de componente (Montaje de tarjetas IP500 82, Adición de módulos de expansión externos 91).
4. Reinicie el sistema IP Office.
5. Use IP Office Manager para configurar las nuevas troncales o extensiones/usuarios.

12.5.5 Eliminación permanente

Si elimina el componente de forma permanente, será necesario editar la configuración para eliminar las entradas redundantes de troncales o extensiones/usuarios.

Para eliminar permanentemente un componente

1. Apagar el sistema 163.
2. Desconecte la alimentación del sistema.
3. Retire la tarjeta o el módulo de expansión externo.
4. Reinicie el sistema IP Office.
5. Use IP Office Manager para eliminar las troncales o extensiones/usuarios en la configuración que se relacionan con el componente eliminado.
6. En el **Unidad de control** sección de la configuración, elimine la entrada del componente que ya no está presente en el sistema.

12.5.6 Reemplazo con un tipo diferente

En caso de sustitución de un componente por otro de otro tipo, el proceso debe dividirse en dos etapas.

1. Primero quite el componente existente usando el Eliminación permanente 169 procesar y ajustar la configuración y reiniciar.
2. Luego instale el nuevo componente usando el Agregar un nuevo componente 168 proceso.

12.6 Configuración predeterminada

Los siguientes procesos borran la configuración guardada en la memoria de la unidad de control. Eso incluye tanto la configuración actual que se usa en la memoria RAM como la configuración de respaldo almacenada en la memoria no volátil. Después de esto, el sistema se reinicia con una configuración predeterminada.

Este proceso debe realizarse desde un PC con dirección IP fija, conectado directamente a la central y con el sistema desconectado de cualquier red. Después de este proceso, la dirección IP de la unidad de control por defecto es 192.168.42.1.

- **Sistemas de modo estándar**
  Para IP Office versión 7.0 y superior, los sistemas IP500 V2 que utilizan**Ley A de IP Office**o**Ley U de IP Office**Las tarjetas SD del sistema están predeterminadas en el modo IP Office Basic Edition. Cargar la configuración cambia IP Office Manager a la vista simplificada. Para que el sistema vuelva a funcionar en el modo estándar de IP Office, consulteCambio del sistema al modo estándar 103.

Opciones de proceso

1. **Configuración predeterminada mediante IP Office Manager** 170
2. **Configuración predeterminada mediante IP Office Web Manager** 170
3. **Restablecimiento de la configuración mediante el botón Restablecer** 170
4. **Configuración predeterminada mediante un teléfono del sistema** 172
5. **Predeterminar la configuración usando Debug** 171
6. **Configuración predeterminada mediante el cargador de arranque** 172

12.6.1 Configuración predeterminada mediante IP Office Manager

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración 170antes de usar este proceso.

Para borrar la configuración mediante IP Office Manager

1. Inicie IP Office Manager.
2. Seleccione**Archivo | Avanzado | Borrar configuración (predeterminado)**.
3. Seleccione el sistema por defecto y haga clic en**OK**.
4. Introduzca un nombre de administrador y una contraseña y haga clic en**OK**.

12.6.2 Configuración predeterminada mediante IP Office Web Manager

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración 170antes de usar este proceso.

Para establecer la configuración predeterminada mediante IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7

   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.

   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.

2. Haga clic en**Comportamiento**. Seleccione**Comandos de servicio**y entonces**Borrar configuración**.
3. Haga clic en**OK**.
4. Espere hasta que el sistema se haya reiniciado antes de volver a iniciar sesión.

12.6.3 Configuración predeterminada mediante el botón Restablecer

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración 170antes de usar este proceso.

Para establecer la configuración por defecto usando el botón Restablecer

1. En la parte trasera de la unidad de control, mantenga presionada la**Reiniciar**durante 10 a 30 segundos hasta que el**UPC**lideró cambios ennaranja parpadeante .
2. Cuando el**UPC**LED cambia anaranja parpadeante , suelte el botón.
   - Si el**UPC**LED cambiado arojo , mantenga presionado el botón hasta que**UPC**El LED cambia a verde intermitente. Luego suelte el botón y vuelva a intentar el proceso una vez que el LED de la CPU haya vuelto a estar en verde fijo.
3. Espere a que se complete el reinicio antes de realizar cualquier otra acción.

12.6.4 Configuración predeterminada mediante depuración

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración 170antes de usar este proceso.

- **ADVERTENCIA**
  El uso del puerto RS232 solo debe realizarse si es absolutamente necesario y solo si las acciones no se pueden completar con IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer todo lo posible para asegurarse de tener una copia de seguridad de la configuración del sistema.

Para borrar la configuración mediante depuración:

Este proceso borra los ajustes de configuración de IP Office pero no altera sus ajustes de seguridad. Es más fácil de usar que el método del cargador de arranque.

1. Asegúrese de tener una copia de respaldo de la configuración de IP Office antes de realizar esta acción. Si no se puede descargar una copia de la configuración mediante IP Office Manager, consulte el directorio de aplicaciones de IP Office Manager para ver las configuraciones descargadas previamente.

   una. Utilice IP Office Manager para descargar una copia actualizada de la configuración. Si eso no es posible, busque en la carpeta de la aplicación IP Office Manager una copia anterior de la configuración.

   b. Usando IP Office Manager, seleccione**Archivo | Configuración abierta**.

   C. Utilizando el**Seleccione el menú de IP Office**, localice y seleccione el sistema IP Office. Hacer clic**OK**.

   d. Ingrese el nombre y la contraseña de una cuenta de usuario de servicio en esa IP Office. Hacer clic**OK**. IP Office Manager recibirá y mostrará la configuración de IP Office.

      - Si aún no lo ha hecho, esta acción crea una entrada BOOTP en IP Office Manager para el sistema IP Office.
      - Esta acción también confirma la comunicación entre la PC de IP Office Manager y IP Office antes de cualquier proceso siguiente.

   mi. Seleccione**Archivo | Guardar configuración como...**y guarde una copia del archivo de configuración en la PC.

2. Conecte el cable serial entre la PC y el puerto RS232 DTE en la unidad de control de IP Office.

   una. Inicie el programa de terminal en su PC. Asegúrese de que se ha configurado como se indica enConfiguración del puerto RS232 DTE 278 . Dentro de una sesión de HyperTerminal, la configuración actual se resume en la parte inferior de la pantalla.

   b. Ingresar**A**(nótese mayúsculas). La unidad de control debe responder***OK***.

   C. Ingresar**EN LA DEPURACIÓN**. La unidad de control debe responder con la hora y la fecha y luego***Hola>***para mostrar que está listo para aceptar comandos.

3. Para borrar la configuración actual en la memoria RAM, ingrese**borrar configuración**. los***Hola>***El símbolo del sistema vuelve a aparecer cuando se completa la acción.

4. Para borrar la configuración de respaldo almacenada en la memoria Flash no volátil, ingrese**erasenvconfig**. los***Hola>*** El símbolo del sistema vuelve a aparecer cuando se completa la acción.

5. Para reiniciar IP Office, ingrese**reiniciar**. IP Office se reiniciará y reiniciará con una configuración predeterminada.

6. Cierre la sesión del programa de terminal.

7. IP Office Manager ahora se puede usar para modificar y luego cargar un archivo de configuración anterior o recibir y editar la configuración predeterminada actual de la unidad de control.

12.6.5 Configuración predeterminada mediante un teléfono del sistema

Este proceso no es compatible con los teléfonos del sistema para un sistema que se ejecuta en el modo estándar de IP Office.

12.6.6 Configuración predeterminada mediante el cargador de arranque

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración 170antes de usar este proceso.

- **ADVERTENCIA**
  El uso del puerto RS232 solo debe realizarse si es absolutamente necesario y solo si las acciones no se pueden completar con IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer todo lo posible para asegurarse de tener una copia de seguridad de la configuración del sistema.

Para borrar los ajustes de configuración y seguridad mediante el cargador de arranque

Este proceso también establece los valores predeterminados de seguridad de IP Office.

1. Asegúrese de tener una copia de respaldo de la configuración de IP Office antes de realizar esta acción. Si no se puede descargar una copia de la configuración mediante IP Office Manager, consulte el directorio de aplicaciones de IP Office Manager para ver las configuraciones descargadas previamente.

   una. Utilice IP Office Manager para descargar una copia actualizada de la configuración. Si eso no es posible, busque en la carpeta de la aplicación IP Office Manager una copia anterior de la configuración.

   b. Usando IP Office Manager, seleccione**Archivo | Configuración abierta**.

   C. Utilizando el**Seleccione el menú de IP Office**, localice y seleccione el sistema IP Office. Hacer clic**OK**.

   d. Ingrese el nombre y la contraseña de una cuenta de usuario de servicio en esa IP Office. Hacer clic**OK**. IP Office Manager recibirá y mostrará la configuración de IP Office.

   - Si aún no lo ha hecho, esta acción crea una entrada BOOTP en IP Office Manager para el sistema IP Office.
   - Esta acción también confirma la comunicación entre la PC de IP Office Manager y IP Office antes de cualquier proceso siguiente.

   mi. Seleccione**Archivo | Guardar configuración como...**y guarde una copia del archivo de configuración en la PC.

2. Conecte el cable serial entre la PC y el puerto RS232 DTE en la unidad de control de IP Office.

   una. Inicie el programa de terminal en su PC. Asegúrese de que se ha configurado como se indica enConfiguración del puerto RS232 DTE 278
   . Dentro de una sesión de HyperTerminal, la configuración actual se resume en la parte inferior de la pantalla.

   b. Organice las ventanas del programa de modo que el programa Terminal y el registro TFTP de IP Office Manager estén visibles al mismo tiempo.

   C. Desconecte la alimentación de la unidad de control de IP Office.

   d. Encienda la unidad de control y presione la tecla de escape cada segundo hasta que reciba un mensaje de cargador. A continuación se muestra un ejemplo.

   ```
   P12  Cargador 2.4
   UPC  Revisión 0x0900
   ```

   mi. Ingresar**A**(nótese mayúsculas). La unidad de control debe responder***OK***.

   F. Si no recibe una respuesta OK, verifique la configuración de su programa de terminal y repita el proceso anterior.

3. Continúe con el proceso de borrado.

   - Para borrar el registro de alarmas ingrese***AT-X1***.
   - Para borrar la configuración actual, ingrese***AT-X2***. Una respuesta típica si***Borrado del Sector 2 (NV Config)***seguido por***OK***. Ingresar***AT-X3***. Una respuesta típica es***Borrados de sector (Config)***seguida de una serie de***OK***respuestas

4. Apague y vuelva a encender la unidad de control. Dentro del programa del terminal, debería ver varios mensajes a medida que la unidad de control realiza varias tareas de inicio.

5. Cierre la sesión del programa de terminal.

6. IP Office Manager ahora se puede usar para modificar y luego cargar un archivo de configuración anterior o recibir y editar la configuración predeterminada de la unidad de control.

12.7 Configuración de seguridad predeterminada

Si es necesario, la configuración de seguridad para el acceso al sistema puede establecerse por defecto. Esto incluye restablecer todas las cuentas de usuario del servicio de seguridad, incluidas las que utilizan las aplicaciones de IP Office. Por lo tanto, es posible que sea necesario reconfigurar esas aplicaciones para usar las nuevas cuentas de usuario del servicio o las contraseñas de las cuentas.

La configuración predeterminada de seguridad del sistema no afecta las contraseñas de los usuarios, los códigos de correo de voz y los códigos de inicio de sesión. Sin embargo, la configuración de seguridad incluye reglas para contraseñas de usuario aceptables. Por lo tanto, siguiendo un valor predeterminado de seguridad, las contraseñas de usuario existentes pueden marcarse como erróneas.

Tras el incumplimiento de seguridad, el consejo en elAsegurar el sistema 132debe seguirse el capítulo. Para detalles de la la configuración de seguridad predeterminada para un sistema consulte la documentación de IP Office Manager.

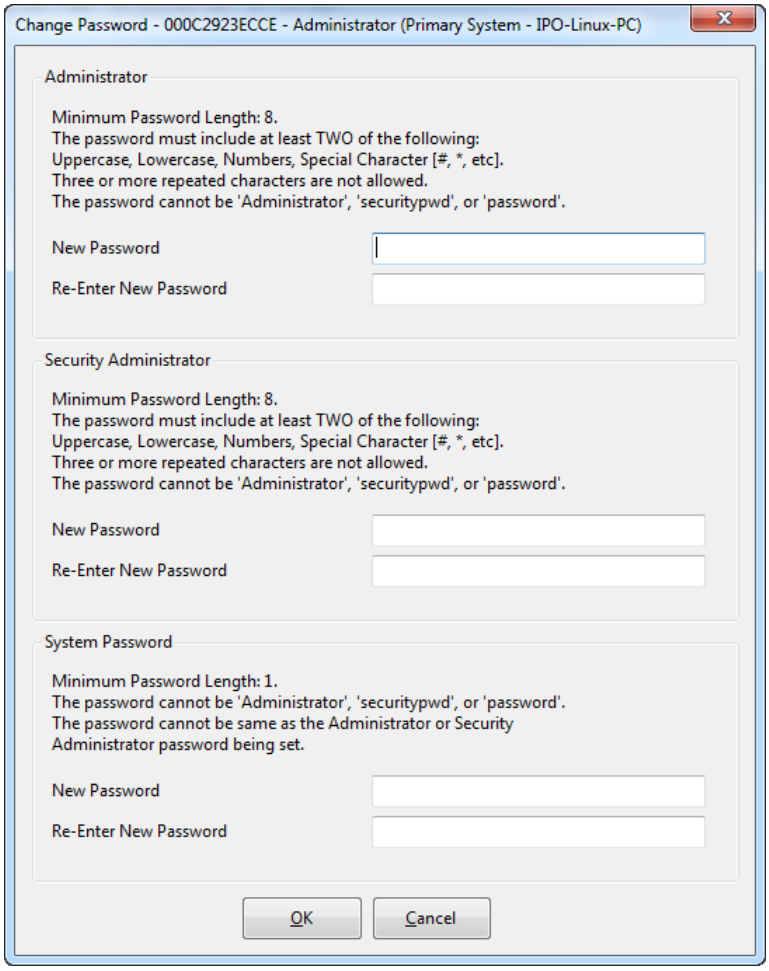
- **!Advertencia: interrupción del servicio**
  Si bien la configuración predeterminada de seguridad no requiere un reinicio del sistema, puede provocar la interrupción del servicio durante varios minutos mientras el sistema genera un nuevo certificado de seguridad predeterminado.

Opciones de proceso

1. **Configuración predeterminada de seguridad mediante IP Office Manager** 174
2. **Configuración predeterminada de seguridad mediante IP Office Web Manager** 174
3. **Configuración predeterminada de seguridad mediante el puerto RS232** 175
4. **Configuración predeterminada de seguridad mediante el cargador de arranque** 176

Iniciar sesión después de establecer la configuración de seguridad por defecto:

Cuando IP Office Manager se conecta a un sistema con configuraciones de seguridad predeterminadas, se le solicita que cambie las contraseñas predeterminadas. Esto también se aplica si cualquiera de las contraseñas se devuelve al valor predeterminado.



12.7.1 Seguridad predeterminada mediante IP Office Manager

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración de seguridad 173antes de usar este proceso.

- **!Advertencia: interrupción del servicio**
  Si bien la configuración predeterminada de seguridad no requiere un reinicio del sistema, puede provocar la interrupción del servicio durante varios minutos mientras el sistema genera un nuevo certificado de seguridad predeterminado.

Para establecer la configuración de seguridad predeterminada de un sistema mediante IP Office Manager

1. Inicie IP Office Manager.
2. Seleccione**Archivo | Avanzado | Borrar configuración de seguridad (predeterminado)**.
3. Seleccione el sistema del menú y haga clic en**OK**.
4. Introduzca un nombre y una contraseña para acceder a la configuración de seguridad.
5. IP Office Manager indica cuándo se restablecieron las configuraciones de seguridad.

12.7.2 Seguridad predeterminada mediante IP Office Web Manager

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración de seguridad 173antes de usar este proceso.

- **!Advertencia: interrupción del servicio**
  Si bien la configuración predeterminada de seguridad no requiere un reinicio del sistema, puede provocar la interrupción del servicio durante varios minutos mientras el sistema genera un nuevo certificado de seguridad predeterminado.

Para establecer la configuración de seguridad predeterminada de un sistema mediante IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7
   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.
2. Haga clic en**Comportamiento**. Seleccione**Comandos de servicio**y entonces**Borrar configuración de seguridad**.
3. Haga clic en**OK**.

12.7.3 Configuración predeterminada de la seguridad mediante el puerto RS232

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración de seguridad 173antes de usar este proceso.

- **!Advertencia: interrupción del servicio**
  Si bien la configuración predeterminada de seguridad no requiere un reinicio del sistema, puede provocar la interrupción del servicio durante varios minutos mientras el sistema genera un nuevo certificado de seguridad predeterminado.
- **ADVERTENCIA**
  El uso del puerto RS232 solo debe realizarse si es absolutamente necesario y solo si las acciones no se pueden completar con IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer todo lo posible para asegurarse de tener una copia de seguridad de la configuración del sistema.

Para establecer la configuración de seguridad predeterminada de un sistema a través de DTE

Este proceso establece los valores predeterminados de seguridad de IP Office, pero no altera sus valores de configuración.

1. Conecte el cable serial entre la PC y el puerto DTE en la unidad de control de IP Office.
2. Inicie el programa de terminal en su PC. Asegúrese de que se ha configurado como se indica enConfiguración del puerto DTE 278.Dentro de una sesión de HyperTerminal, la configuración actual se resume en la parte inferior de la pantalla.
3. Entrar**A**(nótese mayúsculas). La unidad de control debe responder***OK***.
4. Entrar**RESTABLECIMIENTO DE SEGURIDAD**.
5. Se le pedirá que confirme la dirección MAC de la unidad de control antes de continuar. Introduce la dirección.
6. Después de aproximadamente un minuto, la unidad de control responderá***OK***cuando la acción ha sido completada.
7. Cierre la sesión del programa de terminal.
8. IP Office Manager ahora se puede usar para recibir y editar la configuración de seguridad predeterminada de la unidad de control.

12.7.4 Seguridad predeterminada mediante el cargador de arranque

Lea y tenga en cuenta las advertencias sobrepor defecto la configuración de seguridad 173antes de usar este proceso.

- **!Advertencia: interrupción del servicio**
  Si bien la configuración predeterminada de seguridad no requiere un reinicio del sistema, puede provocar la interrupción del servicio durante varios minutos mientras el sistema genera un nuevo certificado de seguridad predeterminado.

- **ADVERTENCIA**
  El uso del puerto RS232 solo debe realizarse si es absolutamente necesario y solo si las acciones no se pueden completar con IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer todo lo posible para asegurarse de tener una copia de seguridad de la configuración del sistema.

Para establecer la configuración de seguridad predeterminada de un sistema a través del cargador de arranque

Este proceso establece los valores predeterminados de seguridad de IP Office y sus ajustes de configuración.

1. Asegúrese de tener una copia de respaldo de la configuración de IP Office antes de realizar esta acción. Si no se puede descargar una copia de la configuración mediante IP Office Manager, consulte el directorio de aplicaciones de IP Office Manager para ver las configuraciones descargadas previamente.

   una. Utilice IP Office Manager para descargar una copia actualizada de la configuración. Si eso no es posible, busque en la carpeta de la aplicación IP Office Manager una copia anterior de la configuración.

   b. Usando IP Office Manager, seleccione**Archivo | Configuración abierta**.

   C. Utilizando el**Seleccione el menú de IP Office**, localice y seleccione el sistema IP Office. Hacer clic**OK**.

   d. Ingrese el nombre y la contraseña de una cuenta de usuario de servicio en esa IP Office. Hacer clic**OK**. IP Office Manager recibirá y mostrará la configuración de IP Office.

      - Si aún no lo ha hecho, esta acción crea una entrada BOOTP en IP Office Manager para el sistema IP Office.
      - Esta acción también confirma la comunicación entre la PC de IP Office Manager y IP Office antes de cualquier proceso siguiente.

   mi. Seleccione**Archivo | Guardar configuración como...**y guarde una copia del archivo de configuración en la PC.

2. Conecte el cable serial entre la PC y el puerto RS232 DTE en la unidad de control de IP Office.

   una. Inicie el programa de terminal en su PC. Asegúrese de que se ha configurado como se indica enConfiguración del puerto RS232 DTE 278 . Dentro de una sesión de HyperTerminal, la configuración actual se resume en la parte inferior de la pantalla.

   b. Organice las ventanas del programa de modo que el programa Terminal y el registro TFTP de IP Office Manager estén visibles al mismo tiempo.

   C. Desconecte la alimentación de la unidad de control de IP Office.

   d. Encienda la unidad de control y presione la tecla de escape cada segundo hasta que reciba un mensaje de cargador. A continuación se muestra un ejemplo.

   ```
   P12  Cargador 2.4
   UPC  Revisión 0x0900
   ```

   mi. Ingresar**A**(nótese mayúsculas). La unidad de control debe responder***OK***.

   F. Si no recibe una respuesta OK, verifique la configuración de su programa de terminal y repita el proceso anterior.

3. Para borrar la configuración actual en la memoria RAM ingrese**AT-X3**. Una respuesta típica es***Borrados de sector (Config)*** seguida de una serie de***OK***respuestas

4. Para borrar la configuración de respaldo almacenada en la memoria no volátil, ingrese**AT-X2**. Una respuesta típica si***Borrado del Sector 2 (NV Config)***seguido por***OK***. Solo IP Office 403: si ejecuta una unidad de control IP Office 403, ingrese también**AT-X4**.

5. Apague la unidad de control y vuelva a encenderla. Dentro del programa del terminal, debería ver varios mensajes a medida que la unidad de control realiza varias tareas de inicio.

6. Cierre la sesión del programa de terminal.

7. IP Office Manager ahora se puede usar para modificar y luego cargar un archivo de configuración anterior o recibir y editar la configuración predeterminada actual de la unidad de control.

12.8 Cargando una configuración

La configuración existente de un sistema se puede reemplazar con una nueva configuración que se ha preparado por separado.

- La configuración creada debe coincidir con el equipo físico en el sistema IP Office en el que se carga. De lo contrario, es posible que el sistema IP Office se reinicie y experimente otros problemas.

Opciones de proceso

1. **Creación de un archivo de configuración fuera de línea** 178
2. **Carga de un archivo de configuración mediante IP Office Manager** 179
3. **Carga de un archivo de configuración mediante IP Office Web Manager** 179
4. **Carga de un archivo de configuración en una tarjeta SD del sistema** 179

12.8.1 Creación de un archivo de configuración fuera de línea

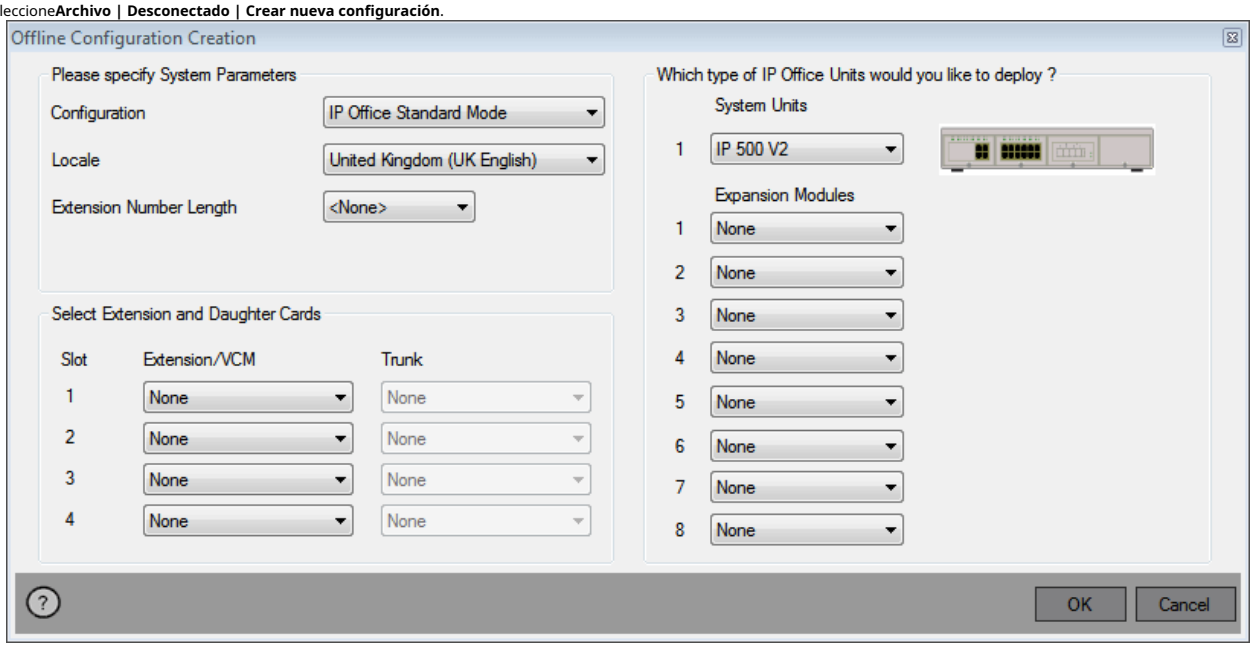
IP Office Manager se puede usar para crear una nueva configuración sin conectarse a un sistema IP Office. Durante el proceso, puede especificar la configuración regional del sistema, qué tipo de tarjetas troncales utiliza y qué tipo de unidad de control y módulos de expansión incluir.

Esto permite la creación de una configuración antes de la instalación del sistema. El archivo de configuración se puede colocar en la tarjeta SD del sistema antes de instalarlo en el sistema. De lo contrario, la configuración se puede cargar en el sistema después de la instalación inicial del sistema.

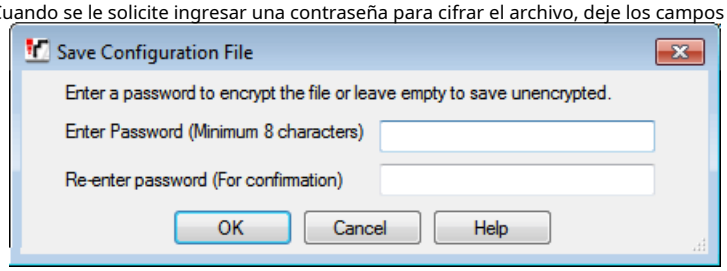
- La configuración creada debe coincidir con el equipo físico en el sistema IP Office en el que se carga. De lo contrario, es posible que el sistema IP Office se reinicie y experimente otros problemas.

Para crear un archivo de configuración sin conexión

1. Inicie IP Office Manager sin configuración cargada en IP Office Manager
2. Seleccione**Archivo | Desconectado | Crear nueva configuración**.



3. Seleccione el tipo de configuración que desea crear. El equipo y la configuración están restringidos a los admitidos en el modo seleccionado.
4. Cuando haya terminado, haga clic en**OK**.
5. IP Office Manager crea y carga la configuración.
6. Edite la configuración para que coincida con los requisitos del cliente. Esto puede incluir[importar información de archivos CSV preparados previamente](#) 77.
   - Tenga en cuenta que, dado que esta configuración se realiza sin conexión y sin licencia, puede configurar funciones que pueden dejar de ser compatibles una vez que la configuración se cargue en el sistema en vivo.
7. Cuando termine, seleccione**Archivo | Guardar configuración como**.
8. Cuando se le solicite ingresar una contraseña para cifrar el archivo, deje los campos en blanco y haga clic en**OK**.



12.8.2 Carga de una configuración mediante IP Office Manager

Este proceso reemplazará la configuración existente.

- La configuración creada debe coincidir con el equipo físico en el sistema IP Office en el que se carga. De lo contrario, es posible que el sistema IP Office se reinicie y experimente otros problemas.

Para cargar una configuración fuera de línea usando IP Office Manager

1. Inicie IP Office Manager.
2. Seleccione**Archivo | Desconectado | Abrir documento...**.
3. Seleccione el archivo de configuración y haga clic en**Abierto**.
4. Verifique que los ajustes de configuración sean los esperados y realice los ajustes necesarios.
5. Seleccione**Archivo | Desconectado | Enviar configuración...**.
6. Seleccione el sistema y haga clic en**OK**.
7. Introduzca un nombre de administrador y una contraseña y haga clic en**OK**.
8. Seleccione cuándo debe cargarse la nueva configuración. No seleccione el**Unir**opción.
9. Haga clic en**OK**.

12.8.3 Carga de una configuración mediante IP Office Web Manager

Este proceso reemplazará la configuración existente.

- La configuración creada debe coincidir con el equipo físico en el sistema IP Office en el que se carga. De lo contrario, es posible que el sistema IP Office se reinicie y experimente otros problemas.

Para cargar una configuración fuera de línea usando IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7.
   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.
   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.
2. Haga clic en**Comportamiento**. Seleccione**Comandos de servicio**y entonces**Cargar configuración**. Hacer clic**Vigilancia**y seleccione **Cargar configuración**.
3. Haga clic en**Navegar**y seleccione el archivo de configuración.
4. Haga clic en**Subir**.
5. Haga clic en**OK**.
6. Reinicie el sistema para que la nueva configuración se aplique por completo. VerReinicio de un sistema 165.

12.8.4 Cargar una configuración en una tarjeta SD del sistema

Este proceso reemplazará la configuración existente.

- La configuración creada debe coincidir con el equipo físico en el sistema IP Office en el que se carga. De lo contrario, es posible que el sistema IP Office se reinicie y experimente otros problemas.

Para cargar una configuración directamente en una tarjeta SD del sistema

1. Cambie el nombre del archivo de configuración fuera de línea como*config.cfg.*
2. Apague y extraiga la tarjeta SD del sistema. VerApagado/Extracción de la tarjeta de memoria 157.
3. Inserte la tarjeta SD en la PC y muestre el contenido de la tarjeta.
4. Abra la carpeta /system/primary y reemplace el archivo config.cfg existente con el nuevo archivo.
5. Vuelva a insertar la tarjeta SD del sistema en el sistema.
6. Reinicie el sistema. VerReinicio de un sistema 165.

12.9 Actualización de sistemas

Hay varios métodos mediante los cuales el sistema se puede actualizar a una nueva versión del software principal de IP Office.

⚠ ADVERTENCIAS

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecutan una versión anterior a la 8.1(65) primero deben actualizarse a la versión 8.1(65) de IP Office (o superior 8.1) o cualquier versión 9.0 de IP Office antes de actualizarse a la versión 9.1 o superior de IP Office. Para las versiones inferiores, no se requiere una licencia de actualización intermedia si el sistema se actualiza más.

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 10.0:**
  La versión 10 y posteriores de IP Office solo admiten licencias PLDS. Para actualizar un sistema que usa licencias ADI, esas licencias primero deben migrarse a PLDS.

  - La migración de licencias se realiza obteniendo un archivo de migración de licencias mediante IP Office Manager (**Herramientas | Migración de licencia**) y luego enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra cualquier derecho de licencia virtual que tenga el sistema a licencias PLDS equivalentes pero ahora asociadas con la clave de función. Solo actualice el sistema una vez que haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que después de la migración de la licencia, Avaya eliminará todos los registros de cualquier derecho de licencia ADI que tenga para esa clave de función.

- **!Advertencia: Requisitos de licencia de actualización**
  En un sistema nuevo, cuando se realiza la primera llamada, el nivel de software que se está ejecutando se escribe en la memoria permanente de la unidad de control. Cualquier actualización posterior a una versión superior requiere la adición de la**Edición esencial** licencia para la versión de destino. Sistemas actualizados sin esa visualización de licencia *"No hay licencia disponible"*en algunos teléfonos y no permitirá ninguna función de telefonía.

- **!Nota: Sistemas Server Edition**
  Las unidades de control IP500 V2 configuradas como sistemas de sistema de expansión IP500 V2 se licencian y actualizan a través de los menús de administración web de Server Edition. Consulte la documentación de Server Edition.

- **Consulte los boletines técnicos de IP Office**
  Consulte el Boletín técnico de IP Office más reciente para conocer la versión del software de IP Office antes de continuar. Puede contener información relacionada con los cambios que ocurrieron después de que se completó este documento. Los boletines están disponibles en http://soporte.avaya.com .

  - **!Administrador web de IP Office**
    La adición de IP Office Web Manager requiere cambios en la configuración de seguridad de los sistemas. Para los nuevos sistemas, esos cambios se realizan automáticamente. Sin embargo, para el sistema que se está actualizando, los cambios solo se pueden realizar si la configuración de seguridad del sistema está predeterminada. VerActivación de IP Office Web Manager 202para conocer los pasos adicionales que se deben realizar antes de actualizar a IP Office versión 8.0 o superior.

- **Otras aplicaciones de IP Office**
  La actualización del software central de la unidad de control de IP Office requerirá actualizaciones del software asociado. Los niveles de software de aplicación compatibles con el núcleo de IP Office se detallan en el boletín técnico de IP Office para la versión.

- **Comportamiento de actualización de DS16B/DS30B:**
  Para los módulos DS16B/DS30B, el proceso de carga del firmware apropiado para el modo seleccionado o la actualización demora hasta 10 minutos, tiempo durante el cual el módulo no está disponible.

- **Comportamiento de actualización de DS16B2/DS30B2:**
  El comportamiento de DS16/30B2 durante la actualización del firmware o el cambio de modos difiere de otras unidades de expansión externas:

  - Durante la actualización del firmware, la unidad permanece operativa y puede realizar y recibir llamadas.
  - Una vez que se completa la actualización (aproximadamente 9 minutos), la unidad se reinicia y tarda unos 45 segundos en volver al funcionamiento normal.

Opciones de proceso

1. **Actualización mediante el asistente de actualización de IP Office Manager** 181
   Este proceso actualiza el sistema o los sistemas mediante los archivos de firmware instalados con la aplicación IP Office Manager.

2. **Actualización de una tarjeta SD del sistema mediante la PC con IP Office Manager** 183
   Se puede usar una PC con IP Office Manager para actualizar directamente los archivos en una tarjeta SD. Esa tarjeta se puede insertar en el sistema y reiniciar el sistema.

3. **Actualización mediante una tarjeta SD opcional** 184
   Este proceso actualiza el sistema usando IP Office Manager para crear una tarjeta SD cargada con los archivos instalados con la aplicación IP Office Manager.

4. **Actualización mediante IP Office Web Manager** 185
   Este proceso actualiza el sistema utilizando un conjunto de archivos de firmware provistos para este propósito. No requiere IP Office Manager.

12.9.1 Actualizar mediante el asistente de actualización

El asistente de actualización es parte de IP Office Manager. Se puede utilizar para actualizar varios sistemas al mismo tiempo.

- **!Advertencia: Versión de IP Office Manager**
  Este proceso utiliza archivos de software proporcionados por la versión instalada de IP Office Manager que se está utilizando. Debe asegurarse de que la versión de IP Office Manager utilizada coincida con la versión del software requerido.

    - **Admin Lite no compatible**
      Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).

- **Múltiples Gerentes**
  Si se está ejecutando más de una copia de IP Office Manager, es posible que IP Office solicite archivos BIN de un IP Office Manager diferente al que inició el proceso de actualización. Asegúrese de que solo se esté ejecutando una copia de IP Office Manager al actualizar un sistema IP Office.

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecutan una versión anterior a la 8.1(65) primero deben actualizarse a la versión 8.1(65) de IP Office (o superior 8.1) o cualquier versión 9.0 de IP Office antes de actualizarse a la versión 9.1 o superior de IP Office. Para las versiones inferiores, no se requiere una licencia de actualización intermedia si el sistema se actualiza más.

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 10.0:**
  La versión 10 y posteriores de IP Office solo admiten licencias PLDS. Para actualizar un sistema que usa licencias ADI, esas licencias primero deben migrarse a PLDS.

    - La migración de licencias se realiza obteniendo un archivo de migración de licencias mediante IP Office Manager (**Herramientas | Migración de licencia**) y luego enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra cualquier derecho de licencia virtual que tenga el sistema a licencias PLDS equivalentes pero ahora asociadas con la clave de función. Solo actualice el sistema una vez que haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que después de la migración de la licencia, Avaya eliminará todos los registros de cualquier derecho de licencia ADI que tenga para esa clave de función.

Para actualizar sistemas usando el asistente de actualización

1. Asegúrese de tener una copia de respaldo de la configuración de IP Office antes de realizar esta acción. Si no se puede descargar una copia de la configuración mediante IP Office Manager, consulte el directorio de aplicaciones de IP Office Manager para ver las configuraciones descargadas previamente.

   una. Utilice IP Office Manager para descargar una copia actualizada de la configuración. Si eso no es posible, busque en la carpeta de la aplicación IP Office Manager una copia anterior de la configuración.

   b. Usando IP Office Manager, seleccione**Archivo | Configuración abierta**.

   C. Utilizando el**Seleccione el menú de IP Office**, localice y seleccione el sistema IP Office. Hacer clic**OK**.

   d. Ingrese el nombre y la contraseña de una cuenta de usuario de servicio en esa IP Office. Hacer clic**OK**. IP Office Manager recibirá y mostrará la configuración de IP Office.

      - Si aún no lo ha hecho, esta acción crea una entrada BOOTP en IP Office Manager para el sistema IP Office.
      - Esta acción también confirma la comunicación entre la PC de IP Office Manager y IP Office antes de cualquier proceso siguiente.

   mi. Seleccione**Archivo | Guardar configuración como...**y guarde una copia del archivo de configuración en la PC.

2. Seleccione**Archivo | Avanzado | Mejora**. UpgradeWiz se inicia y busca módulos de IP Office mediante el **Unidad/Transmisión**Dirección. Ajuste esta dirección y haga clic en**Actualizar**si no se muestran las unidades de control esperadas. Se muestra la versión actual de cada archivo BIN de IP Office guardado en la memoria de las unidades de control. Eso es independientemente de si ese archivo .bin está siendo utilizado actualmente por algún módulo en el sistema.

3. El**Versión**columna indica la versión actual del software instalado. los**Disponible**La columna indica la versión de software que IP Office Manager tiene disponible. Si la versión disponible es superior, la casilla de verificación junto a esa fila se selecciona automáticamente.

   - Si alguno de los módulos tiene instalado el software anterior a la versión 2.1, una actualización con**Validar**se requiere desmarcar. Si este es el caso, solo continúe con el proceso de actualización usando una PC con una dirección IP fija en el mismo dominio de LAN y segmento de LAN físico que la unidad de control de IP Office y solo actualice el sistema anterior a 2.1.
   - Si es necesaria una actualización de varias etapas, utilice los siguientes pasos adicionales para seleccionar el software provisional adecuado:

     - Haga clic derecho en el asistente de actualización y haga clic en**Seleccionar directorio**. Localice y seleccione el directorio que contiene el archivo bin para el nivel de software intermedio.
     - El asistente de actualización ahora debería enumerar solo la unidad de control con el software de actualización disponible.

¿Comentarios sobre este documento? infodev@avaya.com

- La actualización a niveles particulares del software IP Office 10.0 o superior requiere la licencia de Essential Edition adecuada para la versión. los**Con licencia**y**Licencia requerida**las columnas indican el derecho de licencia actual y el derecho de licencia requeridopara el software que el sistema está ejecutando actualmente .

4. Para aquellos módulos que desea actualizar, marque la casilla de verificación.

5. Las siguientes opciones adicionales están disponibles:

   - **Archivos del sistema de copia de seguridad**
     Si se selecciona, antes de actualizar al nuevo software, los archivos actuales en las tarjetas SD del sistema**/primario**carpeta se copian a su**/respaldo**carpeta. Si no hay suficiente espacio en la tarjeta SD para esta acción, IP Office Manager muestra un" *Espacio insuficiente disponible en la tarjeta SD"*advertencia.

   - **Cargar archivos del sistema**
     Si se selecciona, el conjunto completo de archivos de software que tiene IP Office Manager se copia en el**/primario**carpeta en la tarjeta SD del sistema. Además de la unidad de control y el software del módulo, esto incluye los archivos de software del teléfono y los archivos utilizados para IP Office Web Manager. Los archivos de firmware para los teléfonos IP de Avaya se cargan primero y cuando esto se completa, si**Reiniciar Teléfonos IP**a continuación también se selecciona, los teléfonos IP de Avaya se reinician. Luego, el sistema continúa cargando cualquier otro archivo. Si no hay suficiente espacio en la tarjeta SD para esta acción, IP Office Manager muestra un*"Espacio insuficiente disponible en la tarjeta SD"*advertencia.

   - **Reiniciar Teléfonos IP**
     Esta opción está disponible si**Cargar archivos del sistema**arriba también está seleccionado. Si se selecciona, una vez que el sistema se haya reiniciado y cargado los archivos de firmware del teléfono, reinicia los teléfonos IP. Esto hace que vuelvan a cargar los archivos de configuración y vuelvan a verificar si el firmware que han cargado actualmente coincide con el que ahora está disponible en su servidor de archivos configurado (de manera predeterminada, el sistema IP Office). Cuando se selecciona, después de reiniciar el sistema, los teléfonos muestran*"Actualizando desde el sistema"*hasta que el sistema lo reinicie una vez que haya cargado los archivos de firmware del teléfono.

6. Seleccione**Mejora**. Se solicitará la contraseña del sistema para cada sistema. Introdúcelo y haz clic**OK**. Los siguientes pasos dependen de las opciones de actualización seleccionadas. No cancele ni cierre el asistente de actualización mientras se ejecutan estos procesos.

   - **Espacio insuficiente disponible en la tarjeta SD**
     Este mensaje aparece si la tarjeta SD del sistema no tiene espacio suficiente. Para continuar con una actualización confiable, la tarjeta SD debeactualizado localmente [183].

   - **Actualización validada**
     Si usa el**Validado**opción, una serie de acciones se llevan a cabo de la siguiente manera;

     una. El asistente de actualización comprueba la cantidad de memoria RAM libre disponible en la unidad de control para almacenar temporalmente los nuevos archivos BIN. Si no hay suficiente memoria disponible, se le preguntará si desea continuar con una actualización fuera de línea o cancelar la actualización.

        - Si se selecciona fuera de línea, IP Office se reinicia en modo fuera de línea. Puede ser necesario utilizar el **Actualizar**dentro del asistente de actualización para volver a conectar después del reinicio. Luego se puede intentar validar la actualización para verificar nuevamente la cantidad de memoria RAM disponible para la transferencia de archivos BIN. Si la memoria sigue siendo insuficiente, se ofrece la opción de realizar una actualización no validada o cancelar.

     b. Los archivos bin necesarios se transfieren al sistema y se almacenan en la memoria temporal.

     C. Las acciones de copia de seguridad de archivos del sistema y carga de archivos del sistema se realizan si se seleccionaron.

     d. Una vez que se completen todas las transferencias de archivos, el asistente de actualización le preguntará si está bien continuar con el proceso de actualización. Seleccione**Sí**continuar. La unidad de control se reinicia y se actualiza primero. Luego continúa con la actualización de los módulos de expansión externos.

   - **Actualización no validada**
     Este método de actualización debe evitarse a menos que sea absolutamente necesario. Solo se requiere para sistemas IP Office con software anterior a 2.1 y solo debe realizarse desde una PC IP Office Manager con una dirección IP fija que se ejecuta en el mismo segmento LAN y subred que el sistema IP Office. Durante la actualización, las unidades y módulos borran su software actual y luego solicitan el nuevo archivo de software de IP Office Manager.

7. Después de la actualización, verifique que el asistente de actualización ahora muestre que las unidades y los módulos seleccionados se han actualizado. Puede ser necesario seleccionar**Actualizar**para actualizar la información en la pantalla del asistente de actualización.

8. Repita el proceso según sea necesario.

12.9.2 Actualizar localmente la tarjeta del sistema SD mediante Manager

El siguiente proceso se puede utilizar si tiene acceso físico a la unidad de control IP500 V2. Este método se puede utilizar con un reinicio programado, lo que permite que la actualización de la tarjeta se realice durante el horario normal de funcionamiento seguido de un reinicio fuera del horario normal de funcionamiento.

Si la tarjeta se usa para Embedded Voicemail, ese servicio no está disponible mientras la tarjeta está apagada. Las funciones con licencia seguirán funcionando durante un máximo de 2 horas mientras la tarjeta esté apagada.

- **!Advertencia: Versión de IP Office Manager**
  Este proceso utiliza archivos de software proporcionados por la versión instalada de IP Office Manager que se está utilizando. Debe asegurarse de que la versión de IP Office Manager utilizada coincida con la versión del software requerido.

    - **Admin Lite no compatible**
      Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecutan una versión anterior a la 8.1(65) primero deben actualizarse a la versión 8.1(65) de IP Office (o superior 8.1) o cualquier versión 9.0 de IP Office antes de actualizarse a la versión 9.1 o superior de IP Office. Para las versiones inferiores, no se requiere una licencia de actualización intermedia si el sistema se actualiza más.

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 10.0:**
  La versión 10 y posteriores de IP Office solo admiten licencias PLDS. Para actualizar un sistema que usa licencias ADI, esas licencias primero deben migrarse a PLDS.

    - La migración de licencias se realiza obteniendo un archivo de migración de licencias mediante IP Office Manager (**Herramientas | Migración de licencia**) y luego enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra cualquier derecho de licencia virtual que tenga el sistema a licencias PLDS equivalentes pero ahora asociadas con la clave de función. Solo actualice el sistema una vez que haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que después de la migración de la licencia, Avaya eliminará todos los registros de cualquier derecho de licencia ADI que tenga para esa clave de función.

Para actualizar una tarjeta SD del sistema usando una PC

1. Apague la tarjeta de memoria SD del sistema 157 y retírelo de la unidad de control.
2. Siga el proceso pararecreando la tarjeta SD 146.Este proceso sobrescribirá los archivos de software en la tarjeta con los archivos disponibles para IP Office Manager. Este proceso dura aproximadamente 20 minutos.
    - El proceso no afecta ningún archivo de configuración actual, anuncios y mensajes de Embedded Voicemail o archivos de datos SMDR temporales.
    - El proceso elimina cualquier archivo de licencia PLDS actual. El archivo debe restaurarse después de volver a crear la tarjeta SD.
3. Cuando se haya completado el proceso de recreación, vuelva a insertar la tarjeta en la unidad de control.**SD del sistema**ranura para tarjetas.
4. Utilizando IP Office Manager, seleccione**Archivo | Avanzado | Reiniciar**.
5. En el**Seleccione IP Office**seleccione el sistema IP500 V2 y haga clic en**OK**.
6. Seleccione el tipo de reinicio que desea realizar y haga clic en**OK**.
7. Cuando se reinicia el sistema, al reiniciar cargará los archivos de software en la carpeta principal de la tarjeta SD del sistema.

12.9.3 Actualización mediante una tarjeta SD opcional

La PC que ejecuta IP Office Manager se puede usar para cargar el conjunto completo de archivos de operación en una tarjeta SD. Esto incluye el firmware para el sistema central, los archivos de firmware del teléfono y los archivos para el correo de voz integrado. Si la tarjeta contiene archivos de configuración, mensajes y avisos, estos archivos no se eliminan mediante este proceso.

- **!Advertencia: Versión de IP Office Manager**
  Este proceso utiliza archivos de software proporcionados por la versión instalada de IP Office Manager que se está utilizando. Debe asegurarse de que la versión de IP Office Manager utilizada coincida con la versión del software requerido.

    - **Admin Lite no compatible**
      Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecutan una versión anterior a la 8.1(65) primero deben actualizarse a la versión 8.1(65) de IP Office (o superior 8.1) o cualquier versión 9.0 de IP Office antes de actualizarse a la versión 9.1 o superior de IP Office. Para las versiones inferiores, no se requiere una licencia de actualización intermedia si el sistema se actualiza más.

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 10.0:**
  La versión 10 y posteriores de IP Office solo admiten licencias PLDS. Para actualizar un sistema que usa licencias ADI, esas licencias primero deben migrarse a PLDS.

    - La migración de licencias se realiza obteniendo un archivo de migración de licencias mediante IP Office Manager (**Herramientas | Migración de licencia**) y luego enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra cualquier derecho de licencia virtual que tenga el sistema a licencias PLDS equivalentes pero ahora asociadas con la clave de función. Solo actualice el sistema una vez que haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que después de la migración de la licencia, Avaya eliminará todos los registros de cualquier derecho de licencia ADI que tenga para esa clave de función.

Actualizar mediante la actualización de una tarjeta SD opcional

1. Apague la tarjeta SD opcional y retírela del sistema. VerApagado/Extracción de la tarjeta de memoria 157.
2. Siga el proceso pararecreando la tarjeta SD 146.Este proceso sobrescribirá los archivos de software en la tarjeta con los archivos disponibles para IP Office Manager. Este proceso dura aproximadamente 20 minutos.
3. Vuelva a insertar la tarjeta en la ranura para tarjeta SD opcional del sistema.
4. Copie los archivos de la tarjeta SD opcional a la tarjeta SD del sistema. VerCarga de software desde una tarjeta SD opcional 154.
5. Reinicie el sistema. VerReinicio de un sistema 165.

¿Comentarios sobre este documento? infodev@avaya.com

12.9.4 Actualización mediante IP Office Web Manager

Avaya puede ofrecer paquetes de actualización para su uso con IP Office Web Manager. Una vez desempaquetado en una PC local, el proceso a continuación se puede usar para actualizar el sistema.

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecutan una versión anterior a la 8.1(65) primero deben actualizarse a la versión 8.1(65) de IP Office (o superior 8.1) o cualquier versión 9.0 de IP Office antes de actualizarse a la versión 9.1 o superior de IP Office. Para las versiones inferiores, no se requiere una licencia de actualización intermedia si el sistema se actualiza más.

- **!ADVERTENCIA: Actualización de sistemas anteriores a la versión 10.0:**
  La versión 10 y posteriores de IP Office solo admiten licencias PLDS. Para actualizar un sistema que usa licencias ADI, esas licencias primero deben migrarse a PLDS.

  - La migración de licencias se realiza obteniendo un archivo de migración de licencias mediante IP Office Manager (**Herramientas | Migración de licencia**) y luego enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra cualquier derecho de licencia virtual que tenga el sistema a licencias PLDS equivalentes pero ahora asociadas con la clave de función. Solo actualice el sistema una vez que haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que después de la migración de la licencia, Avaya eliminará todos los registros de cualquier derecho de licencia ADI que tenga para esa clave de función.

Para actualizar un sistema mediante IP Office Web Manager

1. Iniciar sesión enAdministrador web de IP Office 7

   una. Introduzca la dirección IP del sistema en el navegador. Seleccione**Administrador web de IP Office**. Alternativamente, ingrese *https://<Dirección_IP>:8443/WebMgmtEE/WebManagement.html*.

   b. Introduzca un nombre de usuario y una contraseña de administrador y haga clic en**Acceso**.

2. Descomprima los archivos de actualización en una ubicación de su PC cliente.

3. Haga clic en**Comportamiento**y seleccione**Mejora**.

4. Haga clic en**Configurar ruta**.

5. Seleccione la carpeta que contiene los archivos de actualización desempaquetados y haga clic en**Abierto**.

6. Haga clic en**Iniciar actualización**.

¿Comentarios sobre este documento? infodev@avaya.com

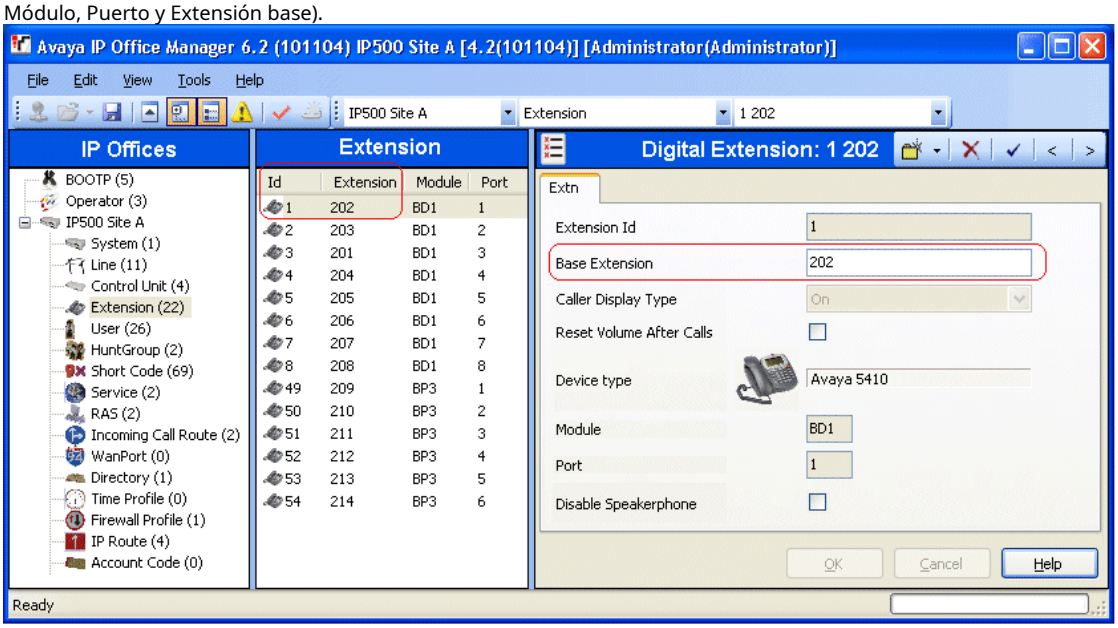
12.10 Intercambio de usuarios de extensión

Si bien el siguiente ejemplo muestra a 2 usuarios intercambiando extensiones, el método se puede usar para intercambiar varios usuarios dentro de la configuración y efectuar los intercambios después de una sola combinación de los cambios de configuración.

Intercambio de usuarios de extensión

Para este ejemplo, el Usuario A (202) y el Usuario B (203) quieren intercambiar extensiones.

1. Cargue la configuración de IP Office y seleccione **Extensión**.
2. Localice la extensión con el**Extensión de base**ajustado a***202***, es decir. coincide con el número de extensión del usuario A.
   - Si el panel de grupo está visible (**Ver | Panel de grupo**) en IP Office Manager, muestra los detalles de la extensión (ID, Módulo, Puerto y Extensión base).

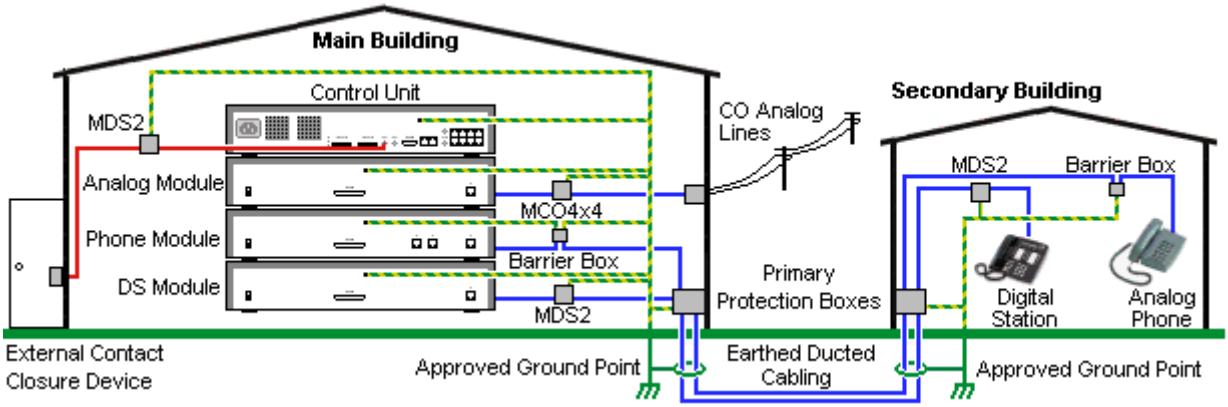


3. Seleccione esa extensión y cambie su**Extensión de base**ajuste a***203***, es decir. para ahora coincidir con el número de extensión del Usuario B. Si IP Office Manager está configurado para validar ediciones, advertirá que este cambio entra en conflicto con la configuración de Extensión base existente de otra extensión. Ignore la advertencia en esta etapa. Hacer clic**OK**.
4. Localice la otra extensión con el**Extensión de base**ajustado a***203***, es decir. coincide con el número de extensión del usuario B.
5. Seleccione esa extensión y cambie su**Extensión de base**ajuste a***202***, es decir. para que coincida ahora con el número de extensión del usuario A. Si el panel de error está visible (**Ver | Panel de errores**), las advertencias sobre conflictos de extensión ahora deberían desaparecer. Hacer clic**OK**.
6. Guarde la configuración nuevamente en el sistema IP Office.
7. En cada una de las extensiones, marque el código corto de cierre de sesión configurado en el sistema IP Office. Por defecto esto es****36***.
   - Si alguno de los usuarios está configurado para**Inicio de sesión forzado**, deberán completar el proceso de inicio de sesión en su nueva extensión utilizando su código de inicio de sesión.

12.11 Instalaciones telefónicas fuera del edificio

Los siguientes son los únicos escenarios admitidos en los que las extensiones y los dispositivos cableados fuera del edificio principal se pueden conectar al sistema IP Office. En estos escenarios, se debe instalar protección adicional, en forma de puesta a tierra protectora y protectores contra sobretensiones.

- **ADVERTENCIA**
  La instalación de protección adicional no elimina el riesgo de daños. Simplemente reduce las posibilidades de daño.



- Solo se admiten puertos en módulos de expansión externos de IP Office. No se admite la conexión fuera del edificio a puertos en tarjetas base en la unidad de control.
- Los cables de diferentes tipos, por ejemplo, líneas troncales, extensiones telefónicas, conexiones a tierra y de alimentación, deben mantenerse separados.
- Todo el cableado entre edificios debe estar encerrado en conductos conectados a tierra. Idealmente, este conducto debe estar enterrado.
- Se debe prever una Caja de Protección Primaria en el punto de entrada de los cables al edificio. Esta debe ser una protección de tres puntos (punta, anillo y tierra). Por lo general, esta sería la protección del tubo de gas proporcionada por la compañía telefónica local. El cable de tierra debe ser lo suficientemente grueso para manejar todas las líneas afectadas por un golpe indirecto al mismo tiempo.

Tipo de conección	Tipo de dispositivo de protección	Requisito
Extensiones de teléfonos analógicos Teléfonos Módulo de expansión externo (MACETA 276 O TELÉFONO puertos solamente. 276)	Caja de barrera de IP Office 189 Admite una sola conexión. Máximo de 16 en cualquier módulo de expansión.	· La conexión del módulo de expansión al teléfono debe realizarse mediante un protector contra sobretensiones en cada extremo y mediante el punto de protección principal de cada edificio. · Los módulos de expansión externos, la unidad de control y los dispositivos IROB de IP Office deben estar conectados al punto de conexión a tierra de protección en su edificio. · La conexión entre edificios debe realizarse a través de conductos puestos a tierra, preferiblemente subterráneos. El cable no debe quedar expuesto al exterior en ningún punto.
Extensiones de teléfono DS	ITW Linx MDS2 188 Admite hasta 4 conexiones. Este dispositivo se conocía anteriormente como Avaya 146E.	
Extensiones de teléfono BST	Ninguna	Actualmente no es compatible.
Troncales analógicos	ITW Linx MCO4x4 188 Admite hasta 4 líneas de dos hilos. Este dispositivo se conocía anteriormente como Avaya 146C.	Para instalaciones en la República de Sudáfrica, la instalación de protección contra sobretensiones en troncales analógicas es un requisito. Para otras ubicaciones donde se considera que el riesgo de caída de rayos es alto, se recomienda una protección adicional de las troncales analógicas entrantes.
Interruptor de salida externa	ITW Linx MDS2 188 Admite hasta 4 conexiones. Este dispositivo se conocía anteriormente como Avaya 146E.	Las conexiones desde un puerto IP Office Ext O/P a un dispositivo de retransmisión externo deben realizarse a través de un protector contra sobretensiones. Cuando use el MDS2 en el puerto Ext O/P, use solo las tomas de Línea 1 y Equipo 1, no use las tomas de Línea 2 o Equipo 2.

La gama de dispositivos towerMAX es suministrada por ITWLinx (http://www.itwlinx.com).

Página1203 de 3226.

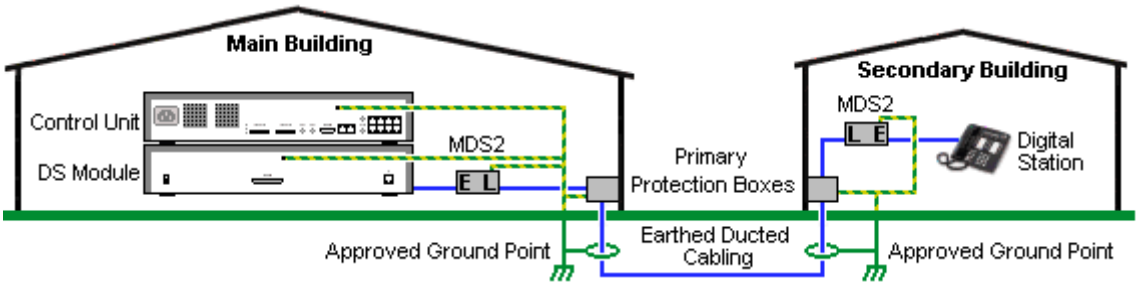
12.11.1 Teléfonos DS

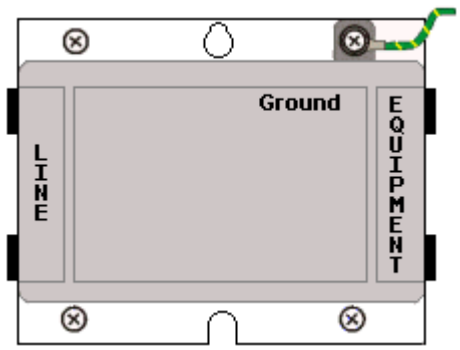
Cuando se requieren extensiones de teléfonos digitales en otro edificio, se debe usar equipo de protección adicional dentro del alcance fuera del edificio (IROB). Para teléfonos conectados a IP OfficeSD 271puertos, el dispositivo compatible suministrado por ITWLinx es un módulo towerMAX DS/2. Este dispositivo IROB fue previamente identificado por Avaya como 146E IROB.

- **!ADVERTENCIA**
  este dispositivo esNo soportado para conexiones de puerto BST, es decir. Teléfonos serie 4100, serie T, serie 7400 y serie M.

El dispositivo de protección debe instalarse según las instrucciones suministradas con el dispositivo. Los puntos de conexión a tierra de la unidad de control de IP Office y cualquier módulo de expansión externo deben conectarse a una conexión a tierra de protección mediante un cable de 18 AWG con funda verde y amarilla.

Por lo general, los 2 puertos de EQUIPO RJ45 del IROB se conectan directamente a los 2 puertos de LÍNEA RJ45. Esto permite que el cableado estructurado RJ45 existente, usando los pines 4 y 5, se use sin volver a cablear para hasta dos conexiones DS. Sin embargo, cada uno de estos puertos se puede usar para conectar una segunda extensión usando los pines 3 y 6.

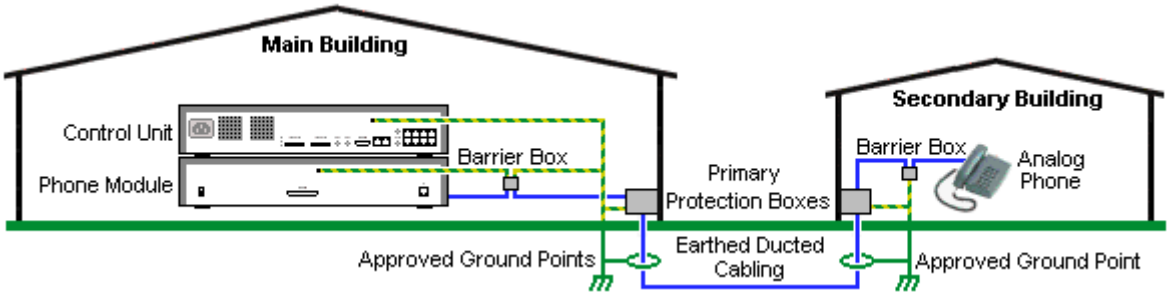


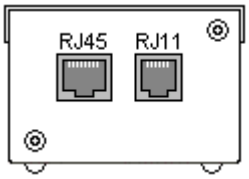
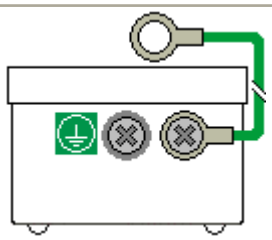
LÍNEA		Señal		EQUIPO	
RJ45	1	No utilizado.		1	RJ45
	2	No utilizado.		2	
	3	Anillo II (Opcional)		3	
	4	Anillo yo		4	
	5	Consejo I		5	
	6	Consejo II (Opcional)		6	
	7	No utilizado.		7	
	8	No utilizado.		8	

12.11.2 Caja de barrera de teléfono analógico

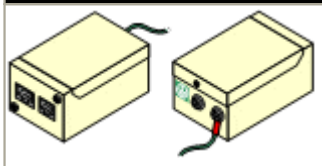
Cuando se requieran extensiones telefónicas analógicas en otro edificio, se debe usar equipo de protección adicional, en forma de cajas de protección telefónica IP Office y conexiones a tierra de protección.

- **PRECAUCIÓN**
  Los puertos de TELÉFONO (POT) en la parte frontal de las unidades de control no deben usarse para extensiones externas al edificio principal.
- Se deben usar las cajas de barrera específicas de IP Office correctas. Estos módulos han sido diseñados específicamente para los voltajes de señalización utilizados por el sistema IP Office:
  - Con los módulos Phone V1 solo se debe usar la caja de barrera de teléfono de IP Office.
  - Solo se debe usar IP Office Phone Barrier Box V2 con los módulos Phone V2.
  - No se debe utilizar ningún otro tipo de caja de barrera telefónica analógica.
- Cuando se requieran más de 3 cajas de barrera en un edificio, deben montarse en bastidor utilizando unKit de montaje en bastidor de caja de barrera 190.
- Se puede utilizar un máximo de 16 cajas de barrera con cualquier módulo telefónico.
- Phone Barrier Box no conecta el condensador de llamada en los módulos Phone V1.



Edificio principal	Caja de barrera	Edificio Secundario
• **RJ11** Conéctese al puerto TELÉFONO (POT) en el módulo de teléfono usando el cable suministrado con la caja de barrera. • **RJ45** Conectar a la caja de barrera del edificio secundario a través de la protección primaria en ambos edificios.		• **RJ11** Conéctese a un teléfono analógico. Cable no incluido. • **RJ45** Desde edificio principal vía protección primaria en ambos edificios.
• **Tornillo central** Conéctelo a la tierra de protección del edificio principal (o al terminal de tierra del kit de montaje en bastidor de la caja de barrera). Utilice un cable de 18 AWG (mínimo) con funda verde y amarilla. • **Tornillo derecho** Conéctese al punto de tierra en el módulo del teléfono usando el cable de tierra provisto con la caja de barrera.		• **Tornillo central** Conéctese a la tierra de protección del edificio principal. Utilice un cable de 18 AWG (mínimo) con funda verde y amarilla. • **Tornillo derecho** No utilizado.

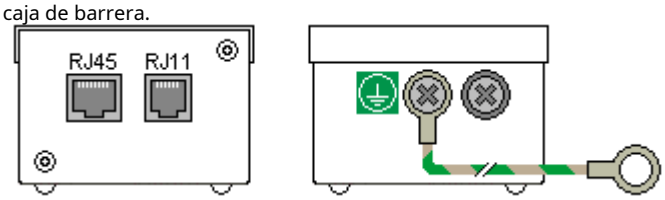
1. Los siguientes cables deben mantenerse separados, que no estén enrutados en el mismo paquete:
   - La tierra conduce desde la caja de la barrera hasta los módulos del teléfono.
   - Cables internos, por ejemplo, cables de extensión que van directamente a los módulos del teléfono.
   - Cables de teléfono externo que van directamente a las cajas de barrera.

Cajas de barrera de IP Office		Código SAP
	**Caja de barrera telefónica (81V)** Úselo con el módulo Phone V1. Incluye un cable RJ45 a RJ11 y un cable de tierra funcional.	700293897
	Caja de barrera telefónica V2 (101V) Úselo con el módulo Phone V2. Incluye un cable RJ45 a RJ11 y un cable de tierra funcional.	700385495
	Kit de montaje en bastidor de caja de barrera	700293905

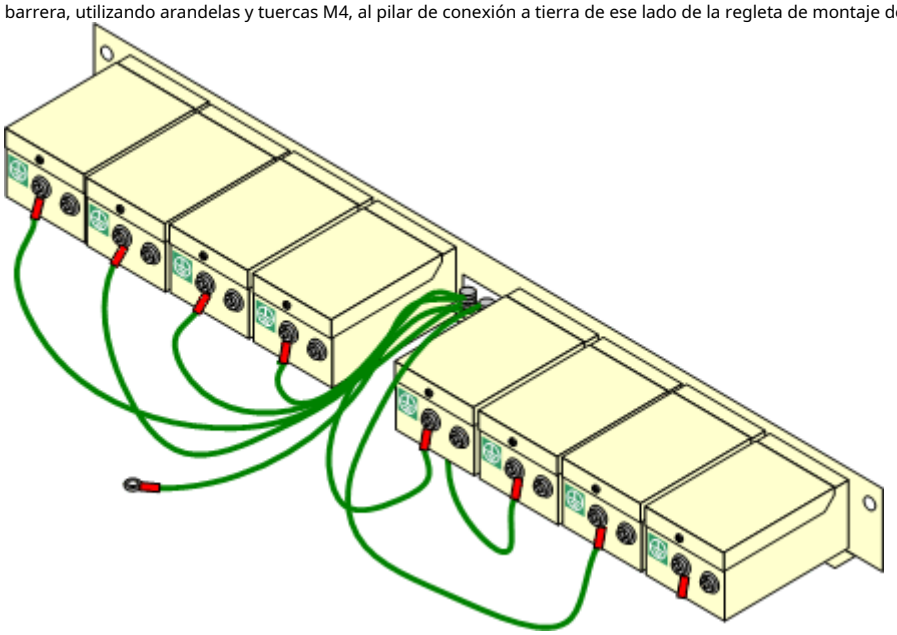
12.11.3 Cajas de barrera de montaje en rack

Cuando se utilicen más de 3 Phone Barrier Box, deben montarse en rack. El kit de montaje en bastidor de caja de barrera (código SAP 700293905) admite hasta 8 cajas de barrera telefónicas.

1. Desatornille los dos tornillos dispuestos en diagonal en la parte delantera de cada caja de barrera y use estos mismos tornillos para volver a colocar la caja de barrera en la tira de montaje del bastidor.
2. Cada caja de barrera se suministra con un cable de tierra verde sólido conectado a su tornillo de tierra funcional. Retire y deseche este cable. Conecte un cable de tierra verde/amarillo al tornillo protector de tierra en el centro del punto en la parte posterior de la caja de barrera.



3. La tira de montaje en bastidor tiene pilares de conexión a tierra M4 roscados. Conecte el otro extremo del cable de conexión a tierra de la caja de barrera, utilizando arandelas y tuercas M4, al pilar de conexión a tierra de ese lado de la regleta de montaje del bastidor.



4. Con un cable de 14 AWG con manguito verde y amarillo, conecte uno de los pilares de puesta a tierra a la tierra de protección del edificio.
5. Con un cable de 14 AWG con manguito verde y amarillo, conecte el otro pilar de conexión a tierra al módulo del teléfono.
6. Asegúrese de que los siguientes cables no estén enrutados juntos en el mismo paquete:
   - Cable de tierra desde la caja de la barrera al módulo del teléfono.
   - Cables internos, por ejemplo, cables que van directamente al módulo del teléfono.
   - Cables de teléfono externo que van directamente a las cajas de barrera.

12.12 Uso del puerto de salida externo

Todas las unidades de control de IP Office están equipadas con un puerto EXT O/P. El puerto está marcado como EXT O/P y está ubicado en la parte posterior de la unidad de control junto al enchufe de entrada de la fuente de alimentación.

El puerto se puede utilizar para controlar hasta dos dispositivos externos, como interruptores de relé de entrada de puerta. La aplicación habitual de estos interruptores es la activación de relés en porteros automáticos. Sin embargo, siempre que se cumplan los criterios de corriente y tensión máximas y, si es necesario, la protección, los interruptores se pueden utilizar para otras aplicaciones.

Los interruptores se pueden cambiar cerrados, abiertos o pulsados (cerrados durante 5 segundos y luego abiertos). Esto se puede hacer de varias maneras:

- Uso de códigos cortos de IP Office.
- A través de**Liberación de la puerta**opción en IP Office SoftConsole.
- Mediante el**Puerta abierta**acción en Voicemail Pro.

Códigos cortos predeterminados

Los siguientes son los códigos cortos predeterminados en la configuración de IP Office para la operación del interruptor de salida externa. Utilizan las funciones de código corto Relé encendido (cerrado), Relé apagado (abierto) y Relé de pulso.

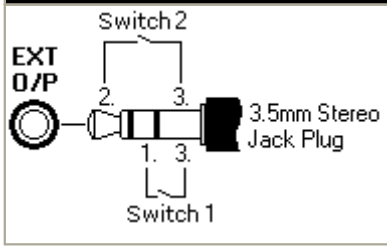
Estado	interruptor 1	interruptor 2
Cerrado	* 39	* 42
Abierto	* 40	* 43
Legumbres	* 41	* 44

12.12.1 Conexión de puerto

Estos puertos se encuentran en la parte posterior de todas las unidades de control de IP Office. Se utilizan para la conexión a relés de conmutación externos. El puerto utiliza un conector jack estéreo estándar de 3,5 mm para la conexión.

IP Office puede abrir (resistencia alta), cerrar (resistencia baja) o pulsar (cerrar durante 5 segundos y luego abrir) dos interruptores dentro del puerto. Cualquiera de los interruptores se puede operar por separado. Estos interruptores están destinados a la activación de relés externos en sistemas como los sistemas de apertura de puertas.

- **PRECAUCIÓN:**
  En las instalaciones en las que este puerto esté conectado a un dispositivo externo al edificio, la conexión debe realizarse a través de un protector contra sobretensiones MDS2 y debe proporcionarse una conexión a tierra de protección en la unidad de control de IP Office. Cuando use el MDS2 en el puerto Ext O/P, use solo las tomas de Línea 1 y Equipo 1, no use las tomas de Línea 2 o Equipo 2.

O/P EXT.	Alfiler	Descripción
	1	interruptor 1
	2	interruptor 2
	3	0 voltios (tierra/chasis)

- Capacidad de conmutación: 0.7A.
- Voltaje máximo: 55V CC
- Resistencia en estado: 0,7 ohmios.
- Corriente de cortocircuito: 1A.
- Capacidad de corriente del circuito inverso: 1.4A.
- Asegúrese de que los pines 1 y 2 estén siempre en un voltaje positivo con respecto al pin 3.

Los conectores jack de audio estéreo de 3,5 mm se venden con frecuencia como módulos sellados precableados. Puede ser necesario usar un multímetro para determinar las conexiones de cableado de un enchufe disponible. Normalmente 3 (común a ambos relés) es la pantalla del cable.

12.13 SNMP

SNMP (Protocolo simple de administración de red) es un protocolo de red estándar que permite monitorear y administrar dispositivos de datos en una red. Un agente SNMP se puede integrar en dispositivos de red como enrutadores y concentradores. Una aplicación de administrador de SNMP, por ejemplo, CastleRock o HP OpenView, puede comunicarse con esos dispositivos.

IP Office 2.0 y versiones posteriores admiten la comunicación SNMP. Esta comunicación puede ser:

- **Votación:**
  Algunas aplicaciones SNMP (llamadas "administradores") envían mensajes de sondeo a la red. Luego registran las respuestas de cualquier dispositivo habilitado para SNMP (llamados "agentes"). Esto permite que la aplicación cree un mapa de red y emita una alarma cuando los dispositivos previamente presentes no respondan.
  - La mayoría de las aplicaciones de administración de SNMP también pueden realizar un sondeo simple de direcciones IP para ubicar dispositivos no habilitados para SNMP. Sin embargo, este método de sondeo no identifica el tipo de dispositivo ni otra información.
  - Sondeo SNMP que incluye detalles sobre el dispositivo que responde. Por ejemplo, la respuesta de una unidad de control de IP Office incluye el tipo de unidad de control, el nivel de software, la información de la tabla de enrutamiento, el tiempo de actividad, etc.
- **Trampas:**
  Cuando ocurren ciertos eventos, un agente SNMP de dispositivos puede enviar detalles del evento al administrador SNMP. Esto se llama una 'trampa' SNMP. Estos aparecen en el registro de eventos del administrador SNMP. La mayoría de los administradores de SNMP se pueden configurar para dar alertas adicionales en respuesta a trampas particulares.
- **Administración:**
  Algunos agentes SNMP admiten la administración de dispositivos y los cambios de configuración a través de la interfaz del administrador SNMP. Esto no es compatible con IP Office.

El funcionamiento de IP Office SNMP se probó con Castle Rock SNMPc-EE 5.1.6c y HP OpenView Network Node Manager 6.41.

Qué información está disponible a través de SNMP

Como se describió anteriormente, la información de SNMP puede ser consultada por la aplicación SNMP o recibida como resultado de que IP Office envíe información de captura de SNMP.

Mientras que la***.mib***los archivos no se deben editar, se pueden leer con un editor de texto y contienen descripciones de todos los diversos objetos de información que se pueden sondear o enviar y la información que incluirá cada objeto. Para obtener una lista de los***.mib***archivos, verInstalación de los archivos MIB de IP Office 193.los***TIPO DE NOTIFICACIÓN***Los objetos son los que se utilizan paratrampas SNMP 195,la otro tipo de objetos son los que se pueden sondeado 195.

12.13.1 Instalación de los archivos MIB de IP Office

Para permitir una comunicación completa entre un agente SNMP y un administrador SNMP, el administrador SNMP debe cargar archivos MIB (Base de información de administración) específicos para el dispositivo del agente SNMP y las funciones que admite. Estos archivos MIB contienen detalles de la información que el agente puede proporcionar y las trampas que puede enviar. Los detalles completos de la estructura de los archivos MIB de IP Office, los grupos MIB dentro de esos archivos y las trampas de eventos se pueden encontrar en el "Manual de instalación de IP Office".

Los archivos MIB para el funcionamiento de IP Office se incluyen en el DVD de IP Office en la carpeta ***\AdminCD\snmp_mibs***. Los archivos reales necesarios y el método de carga dependen de la aplicación del administrador SNMP que se utilice. Los detalles a continuación cubren las dos aplicaciones de administrador SNMP probadas.

Administrador de nodos de red HP Open View

1. Copie los siguientes archivos MIB en la carpeta MIB de aplicaciones.

	Archivo MIB	Fuente
una.	rfc2737-entidad-mib.mib	snmp_mibs\carpeta estándar en el CD de instalación de OpenView.
b.	avayagen-mib.mib	\AdminCD\snmp_mibs\IPOffice en el DVD de administración de IP Office.
C.	ipo-prod-mib.mib	\AdminCD\snmp_mibs\IPOffice en el DVD de administración de IP Office.
d.	ipo-mib.mib	\AdminCD\snmp_mibs\IPOffice en el DVD de administración de IP Office.
mi.	inet-address-mib.mib	\AdminCD\snmp_mibs\Carpeta estándar en el DVD de administración de IP Office.
F.	rfc2213-servicios-integrados-mib.mib	\AdminCD\snmp_mibs\carpeta estándar en el CD de instalación de OpenView.
gramo.	diffserv-dscp-tc.mib	\AdminCD\snmp_mibs\Carpeta estándar en el DVD de administración de IP Office.
H.	diffserv-mib-hpov.mib	\AdminCD\snmp_mibs\Carpeta estándar en el DVD de administración de IP Office.
i.	ipo-teléfonos-mib.mib	\AdminCD\snmp_mibs\IPOffice en el DVD de administración de IP Office.

2. Inicie la consola de OpenView Network Node Manager.

3. Seleccione Opciones y luego Cargar/Descargar MIB: SNMP.

4. Seleccione Cargar y seleccione todos los archivos MIB enumerados anteriormente.

5. Seleccione Compilar.

CastleRock SNMPc 5.1.6c y anteriores

1. Copie los siguientes archivos MIB en la carpeta MIB de aplicaciones, normalmente C:\Program Files\SNMPc Network Manager\mibfiles.

	archivo MIB	Fuente
una.	ENTIDAD-MIB	\AdminCD\snmp_mibs\Standard en el DVD de administración de IP Office.
b.	AVAYAGEN-MIB.mib	\AdminCD\snmp_mibs\IPOffice en el DVD de administración de IP Office.
C.	IPO-PROD-MIB.mib	\AdminCD\snmp_mibs\IPOffice en el DVD de administración de IP Office.
d.	IPO-MIB.mib	\AdminCD\snmp_mibs\IPOffice en el DVD de administración de IP Office.
mi.	INET-ADDRESS-MIB.mib	\AdminCD\snmp_mibs\Standard en el DVD de administración de IP Office.
F.	SERVICIOS-INTEGRADOS-MIB	\AdminCD\snmp_mibs\Standard en el DVD de administración de IP Office.
gramo.	DIFFSERV-DSCP-TC.mib	\AdminCD\snmp_mibs\Standard en el DVD de administración de IP Office.
H.	DIFFSERV-MIB.mib	\AdminCD\snmp_mibs\Standard en el DVD de administración de IP Office.
i.	IPO-TELÉFONOS-MIB.mib	\AdminCD\snmp_mibs\IPOffice en el DVD de administración de IP Office.

2. En SMNPc, seleccione Configuración | Base de datos MIB.

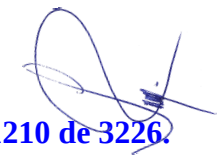
3. Seleccione Agregar y seleccione los archivos MIB enumerados anteriormente en el orden indicado.

CastleRock SNMPc V5.0.1

Las instrucciones de instalación de MIB proporcionadas anteriormente son correctas para CastleRock SNMPc V5.0.8 y posteriores. Para V5.0.1 de CastleRock SNMPc se debe realizar lo siguiente:

1. Copie todas las MIB de IP Office y las MIB estándar del DVD de aplicaciones del administrador de IP Office al directorio mibfiles de SNMPc.
2. En el directorio de archivos mib de SNMPc, abra los archivos STANDARD.mib y SNMPv2-SMI.mib en el Bloc de notas.
3. En el archivo SNMPv2-SMI.mib, busque la definición de zeroDotZero y cópiela en el portapapeles.
4. En el archivo STANDARD.MIB, busque la sección SNMPv2-SMI y pegue la definición de zeroDotZero del portapapeles antes del final de esta sección (justo antes de la instrucción END).
5. Guarde el archivo STANDARD.MIB modificado.
6. Agregue el archivo MIB SNMP-FRAMEWORK-MIB.mib a la base de datos MIB siguiendo las instrucciones proporcionadas en la guía de instalación de IP Office.
7. Agregue todos los archivos MIB enumerados en las instrucciones proporcionadas en la guía de instalación de IP Office en el orden indicado.
8. Compile las MIB listas para usar.

La razón de esto es: IPO-PHONES-MIB.mib se basa en DIFFSERV-MIB.mib para la definición de la convención textual de IndexInteger. DIFFSERV-MIB necesita la definición de la convención textual zeroDotZero que normalmente se define en SNMPv2-SMI.mib. Sin embargo, incluir SNMPv2-SMI.mib en la lista de compilación de archivos MIB genera errores debido a conflictos con lo que parecen ser definiciones internas dentro de SNMPc y la sección SNMPv2-SMI en su archivo STANDARD.mib. Por lo tanto, para resolver el problema, la definición requerida de zeroDotZero debe colocarse en la sección SNMPv2-SMI en el archivo STANDARD.mib de SNMPc.



12.13.2 Habilitación de SNMP y soporte de sondeo

Para que un administrador SNMP detecte y sondee la unidad de control de IP Office, su agente SNMP debe estar habilitado y ubicado en la misma comunidad de lectura que el administrador SNMP.

1. En IP Office Manager, reciba la configuración de la unidad de control.
2. Haga doble clic**Sistema**en el panel Árbol de configuración y seleccione la pestaña SNMP.
3. Marque**SNMP habilitado**.
4. En Puerto SNMP, ingrese el número de puerto UDP utilizado por el agente SNMP de IP Office para escuchar y responder al tráfico SNMP. El valor predeterminado normal es 161.
5. En**Comunidad (solo lectura)**, introduzca la comunidad a la que pertenece el dispositivo para el acceso de lectura. Este nombre de comunidad debe coincidir con el utilizado por la aplicación del administrador de SNMP al enviar solicitudes al dispositivo. El público de la comunidad se usa con frecuencia para establecer la comunicación y luego se cambia (tanto en el agente SNMP como en el administrador) por seguridad.
6. Haga clic en**OK**.
7. Envíe la configuración nuevamente a IP Office y seleccione reiniciar.
8. Después del reinicio de IP Office, el administrador de SNMP debería poder detectar la unidad de control.
9. La respuesta de la unidad de control incluirá detalles del tipo de unidad de control y el nivel actual del software principal.

12.13.3 Habilitación del envío de capturas SNMP

En IP Office Manager, reciba la configuración de la unidad de control.

1. Haga doble clic**Sistema**del panel del árbol de configuración y seleccione el**Eventos del sistema**pestaña.
2. Asegúrese de que**SNMP habilitado**está marcado y establezca las demás configuraciones requeridas para la sección Configuración del agente SNMP.
3. Haga clic en la pestaña Alarmas.
4. Haga clic en**Agregar...**y seleccione**Trampa**como el tipo de nueva alarma. Puede agregar hasta 2 trampas SNMP, cada una con diferentes destinos y configuraciones de alarma.
   - **Dirección del servidor**
     Ingrese la dirección IP o el nombre de dominio completo de la PC que ejecuta la aplicación del administrador SNMP.
   - **Puerto**
     Ingrese el puerto en el que se deben enviar los mensajes de trampas. Este es el puerto UDP en el que IP Office envía mensajes de captura SNMP. El valor predeterminado es 162.
   - **Comunidad**
     Establezca la comunidad que usarán el agente y el administrador de SNMP. El público de la comunidad se usa con frecuencia para establecer la comunicación y luego se cambia (tanto en el agente SNMP como en el administrador) por seguridad.
   - **Formato**
     El uso predeterminado es IP Office. SMGR solo se usa para el sistema que se administra a través de Avaya SMGR.
   - **Nivel mínimo de gravedad**
     Establezca la gravedad de la alarma o una más alta para las alarmas que deben enviarse.
5. Seleccione el**Eventos**que se debe enviar.
6. Haga clic en**OK**.
7. Envíe la configuración nuevamente a IP Office y seleccione reiniciar.

12.14 Actualización de los archivos del sistema desde el Administrador

Este proceso copiará todos los archivos del sistema que no estén presentes en la tarjeta SD del sistema y aquellos archivos que tengan una versión diferente a los que ya están presentes en la tarjeta. Este proceso se puede utilizar para actualizar el contenido de la tarjeta si se sospecha que faltan algunos archivos.

Este proceso no se admite como método de actualización. Solo debe usarse con la versión de IP Office Manager que coincida con el software que ya está ejecutando el sistema.

- **Admin Lite no compatible**
  Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).

Para actualizar un sistema utilizando el administrador de archivos integrado

1. Usando IP Office Manager, seleccione**Archivo | Avanzado | Gestión de archivos integrada**.
2. Usando el**Seleccione IP Office**menú, seleccione el sistema IP Office.
3. Se muestra el contenido del archivo de las tarjetas de memoria.
4. Seleccione**Archivo | Archivos del sistema de copia de seguridad**. los contenidos de la**/primario**carpeta en la tarjeta SD del sistema se copiará en la**/respaldo**carpeta. Este proceso dura aproximadamente 6 minutos.
5. Seleccione**Archivo | Cargar archivos del sistema**. Los archivos del sistema que tiene IP Office Manager se cargarán en el**/primario** carpeta en la tarjeta SD del sistema. Esto incluye archivos de software de IP Office y archivos de mensajes de correo de voz incorporado. No incluye el firmware del teléfono ni los archivos bin. Dependiendo de los archivos que deban actualizarse, este proceso puede demorar hasta 40 minutos.

12.15 Botón de reinicio

Las unidades de control IP500 V2 tienen un**Reiniciar**botón. Presionar el botón mientras la unidad de control se está iniciando pausará el inicio hasta que se suelte el botón. El efecto de presionar el botón durante el funcionamiento normal dependerá de cuánto tiempo se presione el botón y se indicará mediante el LED de la CPU.

Pulse Duración (segundos)	LED de CPU	Acción	Resumen
0 a 5.	Apagado	**Ninguna**	Ninguna.
5 a 10	**Naranja**	**Reiniciar cuando esté libre**	Reinicie cuando esté libre con la nueva restricción de llamadas entrantes/ salientes. Un reinicio usando el botón de reinicio se registra en el seguimiento de auditoría.
10 a 30.	**Naranja parpadeante**	**Borrar configuración**	Borre la configuración, el registro de alarmas y el registro de auditoría. Reinicio inmediato sin esperar a que finalicen las llamadas activas. Ver Borrado de la configuración 170 para detalles completos.
30 a 40	**Rojo**	**Borrar todo.**	Borre la configuración, el registro de alarmas y el software principal. Ver Borrado del software operativo 199 para detalles completos.
Mayores 40.	**Verde parpadeante**	**Ninguna**	Ninguna.

12.16 Botón AUX

Las unidades de control IP500 V2 tienen un botón AUX. Este botón se puede utilizar de la siguiente manera.

- Si se presiona durante un reinicio de la unidad de control, la unidad de controlse salta el arranque 144 desde el***/primario***carpeta en la tarjeta SD del sistema.
- Si se presiona durante más de 5 segundos cuando un sistema está funcionando, la unidad de control se apaga durante 10 minutos.

12.17 Mantenimiento del puerto RS232

El puerto RS232 en la parte posterior de la unidad de control del sistema normalmente no se usa cuando se configura un sistema IP Office. Sin embargo, el puerto se puede utilizar para varios procesos de mantenimiento.

- **ADVERTENCIA**
  El uso del puerto RS232 solo debe realizarse si es absolutamente necesario y solo si las acciones no se pueden completar con IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer todo lo posible para asegurarse de tener una copia de seguridad de la configuración del sistema.

Procesos de mantenimiento del puerto RS232

1. **Conexión y configuración del cable del puerto RS232** 278
2. **Predeterminar la configuración usando depuración** 171
3. **Configuración predeterminada mediante el cargador de arranque** 172
4. **Configuración predeterminada de la seguridad mediante el puerto RS232** 175
5. **Configuración predeterminada de la seguridad mediante el cargador de arranque** 176
6. **Borrado del software central mediante depuración** 200
7. **Borrar el software principal usando el cargador de arranque** 201

12.18 Borrado del software principal

Cuando se borra el firmware cargado por la unidad de control, la unidad de control comienza a realizar solicitudes BOOTP de archivos de firmware de reemplazo. IP Office Manager puede actuar como un servidor BOOTP y responder a la solicitud de las unidades de control con el archivo apropiado de aquellos instalados con IP Office Manager.

A diferencia de otras unidades de control, cuando se borra el firmware cargado por una unidad de control IP500 V2, la unidad de control IP500 V2 primero buscará firmware de reemplazo en sus tarjetas SD antes de recurrir a una solicitud BOOTP a IP Office Manager.

- ⚠ No realice ninguno de los siguientes procesos a menos queabsolutamente necesario. El software de IP Office normalmente se puede actualizado mediante IP Office Manager 180.
- ⚠ Este proceso borra el software operativo. Antes de intentar este proceso, debe conocer las direcciones MAC e IP del sistema, además de tener una copia de respaldo de su configuración y el archivo .bin correcto para el tipo de unidad de control y el nivel de software.
- ⚠ La presencia de cualquier firewall que bloquee TFTP o BOOTP hace que este proceso falle.

Los procesos a continuación deben realizarse desde una PC con una dirección IP fija, conectada directamente a la unidad de control de IP Office y con el sistema IP Office desconectado de cualquier red. Durante el proceso, la dirección IP de la unidad de control puede tener un valor predeterminado en el rango de 192.168.42.1 a 192.168.42.10. Si esto ocurre, es posible que sea necesario modificar la entrada BOOTP en IP Office Manager para que coincida con la dirección que usa el sistema.

Opciones de proceso

1. **Borrado del software principal con el botón Restablecer** 199
   Tenga en cuenta que este método también establece la configuración por defecto.
2. **Borrar el software principal usando Debug** 200
3. **Borrado del software principal mediante el cargador de arranque** 201

12.18.1 Borrado del software principal con el botón de reinicio

Lea la nota y las advertencias sobreborrando el software central advertencias sobre antes de usar este proceso. También lea y anote la defecto la configuración 170antes de usar este proceso.

Para borrar el software principal y la configuración con el botón Restablecer

Utilice este proceso para reiniciar el sistema cuando esté libre. Una vez invocado, el sistema bloquea cualquier nueva llamada entrante o saliente hasta después del reinicio.

1. Ejecute IP Office Manager.
   - En el**BOOTP**entradas, verifique que haya una entrada que coincida con la dirección MAC, la dirección IP y el archivo .bin utilizado por el sistema. Normalmente, una entrada se crea automáticamente cuando se carga una configuración desde esa IP Office. .
     - Si una entrada no está presente, cree una nueva entrada manualmente. Los dos primeros detalles se pueden encontrar en la configuración de la unidad de control en el archivo de configuración. Luego cierre y reinicie IP Office Manager.
   - Por debajo**Archivo | preferencias**asegúrese de que IP Office Manager esté configurado en 255.255.255.255. También comprueba que**Habilitar servidor BootP**está chequeado.
   - Seleccione**Ver | TFTPRegistro**.
   - Verifique que el archivo .bin requerido esté presente en el directorio de trabajo de Manager.
2. En la parte trasera de la unidad de control, mantenga presionada la**Reiniciar**durante 30 a 40 segundos hasta que el**UPC**lideró cambios enrojo .
3. Cuando el**UPC**LED cambia arojo , suelte el botón.
4. El sistema borra su software actual y envía una solicitud de BootP a la red para obtener software nuevo.

12.18.2 Borrado del software principal mediante depuración

Lea la nota y las advertencias sobre[borrando el software central](#) 199antes de usar este proceso.

- **ADVERTENCIA**
  El uso del puerto RS232 solo debe realizarse si es absolutamente necesario y solo si las acciones no se pueden completar con IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer todo lo posible para asegurarse de tener una copia de seguridad de la configuración del sistema.

Para borrar el software principal usando Debug

1. Ejecute IP Office Manager.
   - En el**BOOTP**entradas, verifique que haya una entrada que coincida con la dirección MAC, la dirección IP y el archivo .bin utilizado por el sistema. Normalmente, una entrada se crea automáticamente cuando se carga una configuración desde esa IP Office. .
     - Si una entrada no está presente, cree una nueva entrada manualmente. Los dos primeros detalles se pueden encontrar en la configuración de la unidad de control en el archivo de configuración. Luego cierre y reinicie IP Office Manager.
   - Por debajo**Archivo | preferencias**asegúrese de que IP Office Manager esté configurado en 255.255.255.255. También comprueba que**Habilitar servidor BootP**está chequeado.
   - Seleccione**Ver | TFTPRegistro**.
   - Verifique que el archivo .bin requerido esté presente en el directorio de trabajo de Manager.
2. Conecte el cable serial entre la PC y el puerto RS232 DTE en la unidad de control de IP Office.
   una. Inicie el programa de terminal en su PC. Asegúrese de que se ha configurado como se indica en[Configuración del puerto RS232 DTE](#) 278 . Dentro de una sesión de HyperTerminal, la configuración actual se resume en la parte inferior de la pantalla.
   b. Ingresar**A**(nótese mayúsculas). La unidad de control debe responder***OK***.
   C. Ingresar**EN LA DEPURACIÓN**. La unidad de control debe responder con la hora y la fecha y luego***Hola>***para mostrar que está listo para aceptar comandos.
3. Para borrar la configuración actual en la memoria RAM ingrese**mejora**.
4. IP Office borrará su software actual y luego enviará una solicitud de BootP a la red para obtener software nuevo. IP Office Manager responderá y comenzará a transferir el software mediante TFTP.

Traducido del inglés al español - www.onlinedoctranslator.com

12.18.3 Borrado del software principal mediante el cargador de arranque

Lea la nota y las advertencias sobreborrando el software central [199]antes de usar este proceso.

- **ADVERTENCIA**
  El uso del puerto RS232 solo debe realizarse si es absolutamente necesario y solo si las acciones no se pueden completar con IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer todo lo posible para asegurarse de tener una copia de seguridad de la configuración del sistema.

Para borrar el software principal usando el cargador de arranque

1. Ejecute IP Office Manager.
   - En el**BOOTP**entradas, verifique que haya una entrada que coincida con la dirección MAC, la dirección IP y el archivo .bin utilizado por el sistema. Normalmente, una entrada se crea automáticamente cuando se carga una configuración desde esa IP Office. .
     - Si una entrada no está presente, cree una nueva entrada manualmente. Los dos primeros detalles se pueden encontrar en la configuración de la unidad de control en el archivo de configuración. Luego cierre y reinicie IP Office Manager.
   - Por debajo**Archivo | preferencias**asegúrese de que IP Office Manager esté configurado en 255.255.255.255. También comprueba que**Habilitar servidor BootP**está chequeado.
   - Seleccione**Ver | TFTPRegistro**.
   - Verifique que el archivo .bin requerido esté presente en el directorio de trabajo de Manager.
2. Conecte el cable serial entre la PC y el puerto RS232 DTE en la unidad de control de IP Office.

   una. Inicie el programa de terminal en su PC. Asegúrese de que se ha configurado como se indica enConfiguración del puerto RS232 DTE [278] . Dentro de una sesión de HyperTerminal, la configuración actual se resume en la parte inferior de la pantalla.

   b. Organice las ventanas del programa de modo que el programa Terminal y el registro TFTP de IP Office Manager estén visibles al mismo tiempo.

   C. Desconecte la alimentación de la unidad de control de IP Office.

   d. Encienda la unidad de control y presione la tecla de escape cada segundo hasta que reciba un mensaje de cargador. A continuación se muestra un ejemplo.

   ```
   P12  Cargador 2.4
   UPC  Revisión 0x0900
   ```

   mi. Ingresar**A**(nótese mayúsculas). La unidad de control debe responder***OK***.

   F. Si no recibe una respuesta OK, verifique la configuración de su programa de terminal y repita el proceso anterior.

3. Entrar**AT-X**. La unidad de control debe responder**Borrado multisector**.
4. La unidad de control ahora solicitará el archivo .bin que requiere. Para las unidades de control IP500 V2, esto será de los archivos en la tarjeta SD del sistema. Para otras unidades de control, será de IP Office Manager y aparecerá en el Registro TFTP.
5. Si las transferencias de archivos no parecen realizarse, verifique que la dirección IP que se muestra en el registro TFTP coincida con la entrada BOOTP. Ajuste la entrada BOOTP si es necesario.
6. Cuando termine, el sistema se reiniciará.

¿Comentarios sobre este documento? infodev@avaya.com

12.19 Activación de IP Office Web Manager

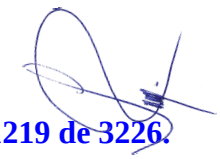
El acceso a IP Office Web Manager es a través de la dirección IP del sistema y luego seleccionando el***Administración web de IP Office***Enlace. Para utilizar IP Office Web Manager, se deben cumplir una serie de criterios que se enumeran a continuación. La mayoría de estos se aplican automáticamente a un nuevo sistema instalado con IP Office versión 8.0 o superior. Sin embargo, para los sistemas que se actualizan a IP Office versión 8.0 o superior, es posible que se requieran pasos de actualización adicionales.

Activación de IP Office Web Manager

1. Los archivos de IP Office Web Manager deben estar presentes en la tarjeta SD del sistema. Esto se puede hacer de varias maneras:
   - Al seleccionar incluir esos archivos cuando se le solicite hacerlo mientrasrecreando la tarjeta SD de IP Office 146mediante IP Office Manager.
   - Seleccionando**Cargar archivos del sistema**al actualizar el sistema mediante IP Office Manager.
2. La seguridad del sistema IP Office debe permitir la operación de IP Office Web Manager:
   - Esto se hace automáticamente para cualquier sistema nuevo instalado con el software IP Office versión 8.0 o superior.
   - Esto se hace automáticamente para cualquier sistema anterior a la versión 8.0 de IP Office durante la actualización si el sistema está configurado para usar la contraseña predeterminada anterior a la versión 8.0 de IP Office.
   - Para cualquier sistema actualizado a la versión 8.0 de IP Office sin volver a configurar primero la contraseña predeterminada, ya sea:
     - Usando IP Office Manager:
       1. Si aún no lo ha hecho, seleccione**Ver | Vista avanzada**.
       2. Seleccione**Archivo | Avanzado | Borrar configuración de seguridad (predeterminado)**.
       3. Desde el**Seleccione IP Office**diálogo, seleccione el sistema requerido y haga clic en**OK**.
       4. Introduzca el nombre de usuario**Administrador**y la contraseña de esa cuenta.
       5. IP Office Manager confirmará si la acción fue exitosa o no.
     - Por defecto elconfiguración de seguridad del sistema usando un cable RS232 DTE 173.

Capítulo 13.

Componentes del sistema



13. Componentes del sistema

Esta sección cubre los componentes individuales que pueden incluir una instalación de IP Office.

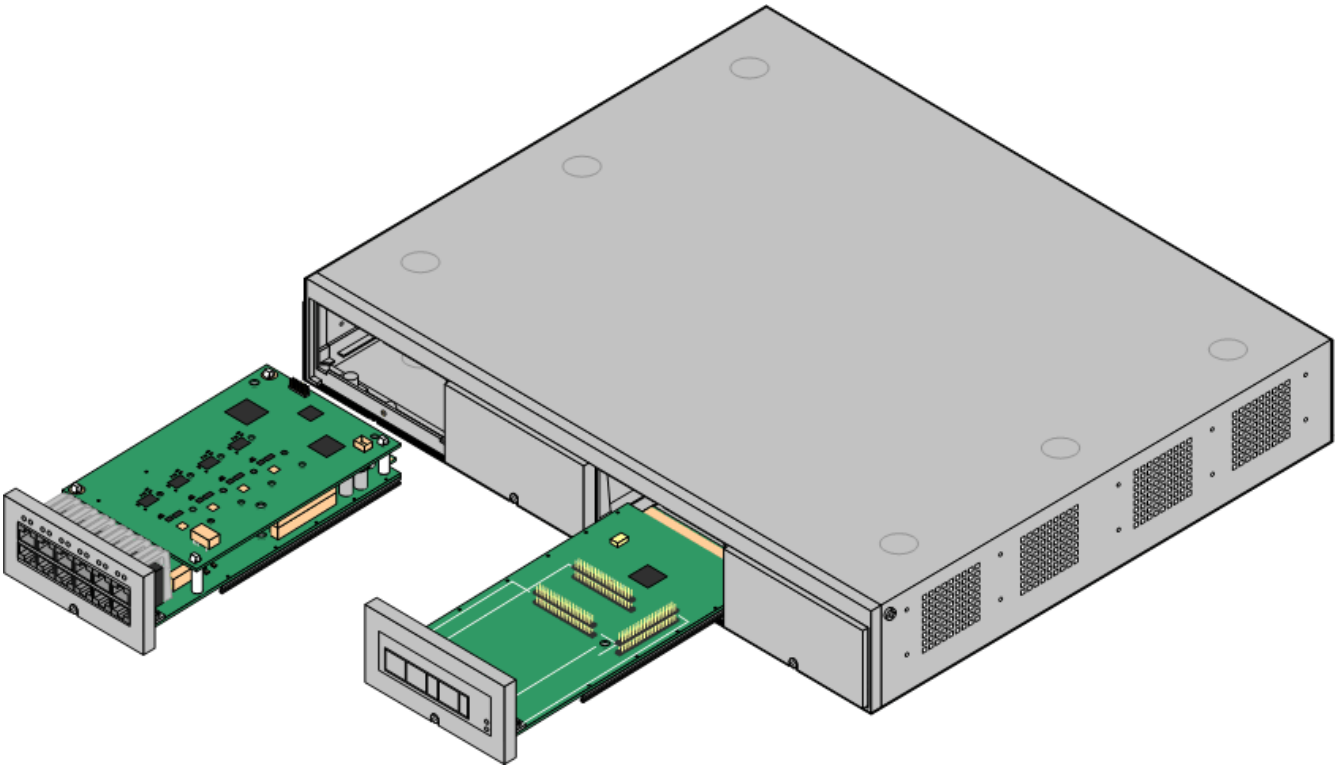
- **Unidad de control IP500 V2** 205
- **Tarjetas SD del sistema** 208
- **Tarjetas base IP500** 209
- **Tarjetas auxiliares de troncales IP500** 223
- **Módulos de expansión externos IP500** 228
- **Juegos de montaje** 247
- **Los telefonos**
- **Complementos de teléfono** 250
- **Aplicaciones** 251
- **Puertos físicos** 264
- **Licencias** 279

Se incluye información adicional para:

- **Compatibilidad de hardware y software** 286
- **Niveles de PCS de hardware** 296
- **Herrajes TAA** 296

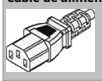
13.1 Unidad de control IP500 V2

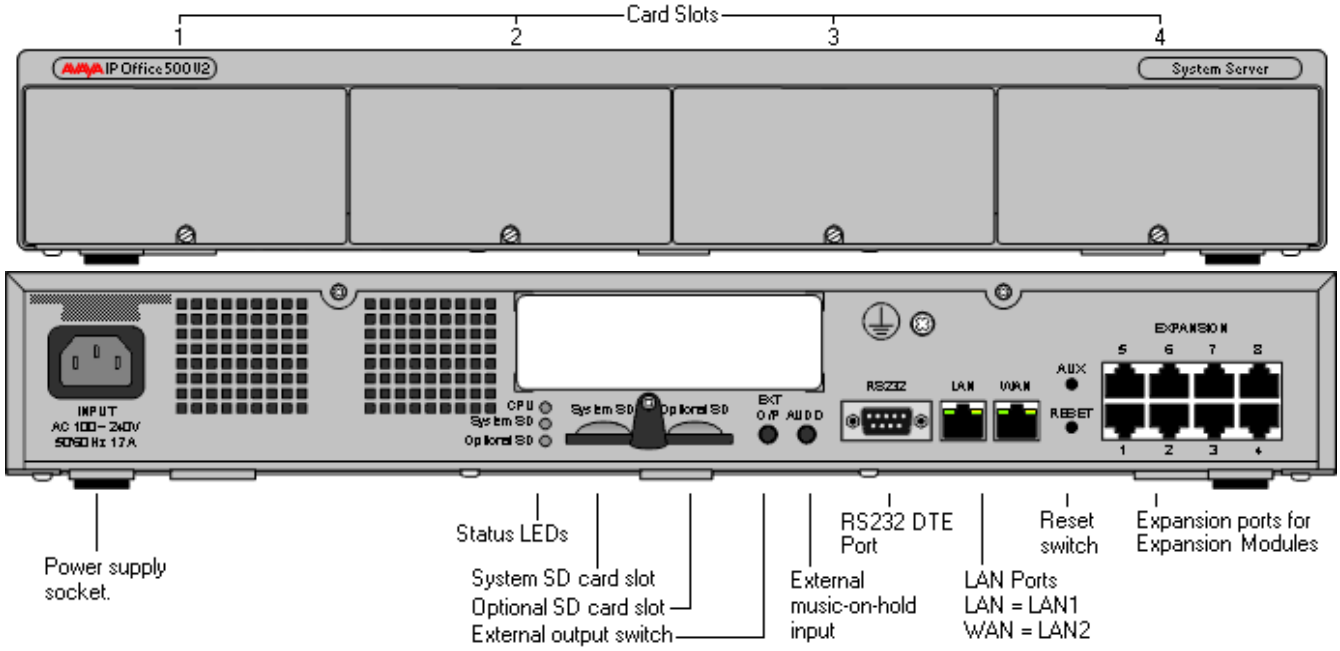
Las ranuras están numeradas del 1 al 4 de izquierda a derecha. Se pueden utilizar en cualquier orden. Sin embargo, si se excede la capacidad para un tipo particular de tarjeta, la tarjeta en la ranura más a la derecha se desactivará. La unidad no debe utilizarse con ranuras descubiertas.



- Avaya IP Office IP500 V2 también se conoce como "IPO IP500 V2 Cntrl Unit", "IP Office IP 500 v2", "IPO IP500 v2", "IP 500 V2", "IP500 V2", "IPO 500v2 System Unit Assembly" o "IP Office 500 v2". A lo largo de esta documentación se utiliza el término IP500 V2.

Rasgo	Capacidad
Máximo Extensiones	Hasta 384 extensiones en los modos estándar de IP Office.
Conferencia Fiestas	128 como estándar pero máximo 64 en cualquier conferencia individual. La supresión de silencio se aplica a conferencias con más de 10 participantes.
Tarjetas de Troncos	4 tarjetas auxiliares de troncales IP500.
Voz Compresión Canales	Hasta 148 canales con tarjetas combinadas IP500 VCM e IP500.
Mensaje de voz Canales	Máximo de 40 sesiones de conexión de Voicemail Pro/TAPI WAV sujetas a licencias disponibles. Para Embedded Voicemail, hasta 6 (2 por defecto, los canales adicionales requieren licencias).
locales	Apoyado en todoLocales de IP Office 42
Mínimo Nivel de software	IP Office Essential Edition: 6.0 mínimo. IP Office Basic Edition - Modo PARTNER®: 6.0 mínimo. IP Office Basic Edition - Modo Norstar: 6.1 mínimo. Edición básica de IP Office: 7.0 mínimo. Archivo bin = ip500v2.bin.
Fuente de alimentación	Unidad de fuente de alimentación interna.
Montaje	Independiente, montado en rack (requiere IPO IP500 RACK MNTG KIT) o montado en pared (requiere IPO IP500 WALL MNTG KIT).
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 365 mm/14,4". Altura: 73 mm/2,9"/2U. Espacio libre: 90 mm mínimo en todos los lados, 220 m en el frente.
Memoria	Tamaño máximo del archivo de configuración: 2048 KB.

Nombre		Descripción	País	Código SAP
Unidades de control IP500 V2	**Unidad de control IPO IP500 V2**	Unidad de control IP Office 500 V2		700476005
	Unidad de control IPO IP500 V2 TAA	"Ley de Acuerdos Comerciales [296] variante compatible.		700501510
Tarjeta de memoria SD de Avaya	**IPO IP500 V2 SIS TARJETA SD AL**	Tarjeta SD de ley A IP500 V2		700479702
	IPO IP500 V2 SYS TARJETA SD MUL	Tarjeta SD de ley U IP500 V2		700479710
IEC60320 C13 conectado a tierra Cable de alimentación 	**IPO - CABLE PWR (CONECTADO A TIERRA) UE CEE7/7**	CEE7/7	Europa	700289762
	IPO - CABLE PWR (CONECTADO A TIERRA) REINO UNIDO	BS1363	Reino Unido	700289747
	IPO - PWR LEAD (EARTHER) EE. UU.	NEMA5-15P	America	700289770
Juegos de montaje	**KIT DE MONTAJE EN PARED IPO IP500 V3**	KIT DE MONTAJE EN PARED IPO IP500 V3		700503160
Misceláneas	**Kit de placa ciega IP500**	Kit de placa ciega IP500		700429194



Puertos	Descripción
AUDIO 267	Conector jack estéreo de 3,5 mm. Se utiliza para entrada de fuente de música externa en espera.
auxiliar 144	• Si se presiona durante un reinicio de la unidad de control, la unidad de control se salta el arranque 144 desde el ***/primario*** carpeta en la tarjeta SD del sistema. • Si se presiona durante más de 5 segundos cuando un sistema está funcionando, la unidad de control se apaga durante 10 minutos.
UPC	Indica el estado de la unidad de control. • **Rojo/verde alternativo**=Empezando. • **rojo encendido**=Sin software • **Verde encendido**=Bueno. • **Rojo parpadeante**=Error/Apagado.
EXPANSIÓN 273	Toma RJ45. Se utiliza para la conexión directa a módulos de expansión externos mediante el cable de interconexión de expansión suministrado con el módulo de expansión.
O/P EXT. 191	Conector jack estéreo de 3,5 mm. Se utiliza para conmutar sistemas de relés externos, como controles de entrada de puerta. El puerto contiene dos conmutadores independientes controlados por IP Office.
APORTE	Puerto de entrada de alimentación de CA.
LAN 274	Toma RJ45. El puerto es un puerto cruzado MDI full-duplex de 10/100 Mbps con detección automática. Con el puerto WAN forma un conmutador Ethernet de capa 3 administrado.
Opcional 142 Dakota del Sur	Se utiliza para la tarjeta SD opcional. El LED se usa de la misma manera que para el sistema SD *(vea abajo)*.
REINICIAR 197	Este conmutador se utiliza para reiniciar IP Office y, opcionalmente, borrar la configuración o el software principal en el proceso. Ver Botón de reinicio 197.
RS232 278	Zócalo tipo D de 9 vías. Se utiliza para el mantenimiento del sistema.
Sistema 142 Dakota del Sur	Se utiliza para la tarjeta SD del sistema. El LED se utiliza de la siguiente manera. • **Apagado**=Apagado de tarjeta. • **rojo intermitente**=Tarjeta inicializándose o apagándose. • **Verde encendido**=Tarjeta presente. • **Parpadeo rápido rojo**=tarjeta llena • **Verde intermitente**=Tarjeta en uso. • **rojo fijo**=Fallo de tarjeta/tipo incorrecto. • **Naranja fijo**=Reinicio inminente.
PÁLIDO 274	Toma RJ45. El puerto es un puerto cruzado MDI full-duplex de 10/100 Mbps con detección automática. Con el puerto WAN forma un conmutador Ethernet de capa 3 administrado. Este puerto no es compatible con sistemas que se ejecutan en IP Office Basic Edition - Modo PARTNER®, IP Office Basic Edition - Modo Norstar o IP Office Basic Editions.
	Se utiliza para la conexión de un tierra funcional o de protección 93. Se recomienda el uso de una conexión a tierra para todos los sistemas y para algunos lugares puede ser un requisito reglamentario.

13.2 Tarjetas SD del sistema IP500 V2

Este tipo de tarjeta se utiliza con centrales IP500 V2 y es un elemento obligatorio. La tarjeta se utiliza para la concesión de licencias del sistema y también para Embedded Voicemail si es necesario. También contiene los archivos de firmware cargados por el sistema y los teléfonos cuando se instala el sistema.

La unidad de control debe estar equipada con una de estas teclas de funciones, incluso si no se utilizan licencias.

- El ID de host PLDS utilizado para el archivo de licencia debe coincidir con el que se muestra en los 12 dígitos.**Identificación PLDS**impreso en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra con**FK**o**FK SN**. Para esas tarjetas agregue el prefijo***11***para obtener la identificación PLDS de la tarjeta.

- De manera predeterminada, la tarjeta se puede usar para 2 puertos de Embedded Voicemail. Se pueden habilitar puertos adicionales hasta un máximo de 6 mediante la adición delicencias [279].El mensaje del buzón de correo de voz y la capacidad de aviso admiten 2 conexiones simultáneas y 15 horas de almacenamiento. Esto se puede ampliar hasta 6 canales mediante la adición de licencias, cada una de las cuales habilita dos canales adicionales y 5 horas adicionales de almacenamiento.

- **ADVERTENCIA**
  Estas tarjetas solo deben formatearse con IP Office Manager o System Status Application. Las tarjetas solo deben eliminarse de un sistema después de uncierre de tarjeta [157]o unapagado del sistema [163].

Dongle de tecla de función	Código SAP
IPO IP500 V2 SYS TARJETA SD A-LAW	700479702
IPO IP500 V2 SYS TARJETA SD MU-LAW	700479710

- **Tarjeta SD de ley U de IP Office**
  Un sistema equipado con este tipo de tarjeta utiliza de forma predeterminada telefonía U-Law e IP Office Basic Edition.***Sistema de llaves*** operación. Destinado a locales de América del Norte.

- **Tarjeta SD de ley A de IP Office**
  Un sistema equipado con este tipo de tarjeta tiene por defecto telefonía A-Law e IP Office Basic Edition***Sistema PBX*** operación. Destinado a lugares fuera de América del Norte.

Correo de voz integrado

La tarjeta SD del sistema se puede utilizar para proporcionar Embedded Voicemail para el sistema. Sin licencia, el correo de voz incorporado proporcionado por el sistema admite 2 conexiones simultáneas y 15 horas de almacenamiento. Esto se puede ampliar hasta 6 canales mediante la adición delicencias [279],cada uno de los cuales permite dos canales adicionales y 5 horas adicionales de almacenamiento.

Para obtener detalles completos sobre la instalación y configuración del correo de voz integrado, consulte el manual de instalación del correo de voz integrado.
Las tarjetas están precargadas con los siguientes idiomas:

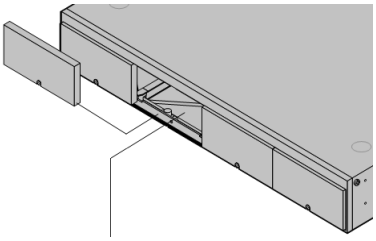
- **Arábica**,**cantonés**,**danés**,**Holandés**,**Inglés del Reino Unido)**,**Inglés (Estados Unidos)**,**finlandés**,**Francés**,**Francés (Canadá)**, **Alemán**,**hebreo**,**italiano**,**japonés**,**coreano**,**mandarín**,**noruego**,**Polaco**,**portugués**,**Portugués (Brasil)**,**ruso**,**español**,**Español (Argentina)**,**español (latín)**,**Español (México)**,**sueco**, **turco**.

Codificación PCM

- **Ley A o Ley Mu**
  PCM (modulación de código de pulso) es un método para codificar voz como datos. En telefonía, se utilizan ampliamente dos métodos de codificación PCM, A-law y Mu-law (también llamado U-law). Por lo general, la ley Mu se usa en América del Norte y en algunos otros lugares, mientras que la ley A se usa en el resto del mundo. Además de configurar la codificación PCM correcta para la región, la configuración A-Law o Mu-Law de un sistema IP Office cuando se inicia por primera vez afecta una amplia gama de valores predeterminados regionales relacionados con la configuración de línea y otros valores.

  - Para los sistemas IP500 V2, la codificación predeterminada se establece según el tipo de tarjeta SD del sistema instalada cuando se inicia el sistema por primera vez.

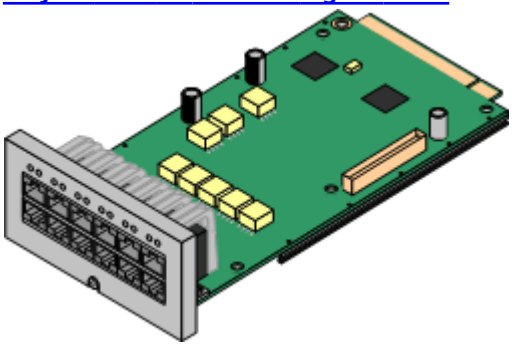
13.3 Tarjetas base IP500



La centralita IP500 V2 dispone de 4 slots para la inserción de tarjetas base IP500. Las ranuras están numeradas del 1 al 4 de izquierda a derecha. Normalmente se pueden usar en cualquier orden, sin embargo, si se excede la capacidad de un tipo de tarjeta en particular, la tarjeta en la ranura más a la derecha se desactivará.

Cada tarjeta base incluye un panel frontal integral con puertos para conexiones de cable. Por lo general, los primeros 8 puertos de la izquierda son para la conexión de dispositivos de extensión. Los 4 puertos de la izquierda se utilizan para la conexión de troncales si un[tarjeta hija troncal](#) 25se añade a la tarjeta base.

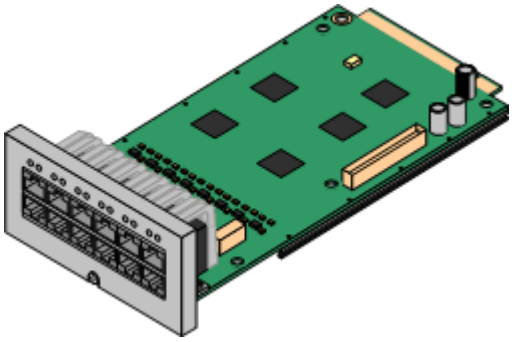
Tarjeta base de estación digital IP500 218



Esta tarjeta proporciona 8 puertos DS (estación digital) para la conexión de teléfonos digitales Avaya.

- La tarjeta se puede equipar con un[Tarjeta auxiliar de troncales IP500](#) 25que utiliza los puertos de la tarjeta base para la conexión troncal.
- **Máximo:**3 por unidad de control.
  - Las conexiones para los teléfonos 4100, 7400, M-Series y T-Series utilizan la tarjeta IP500 TCM8 Digital Station.

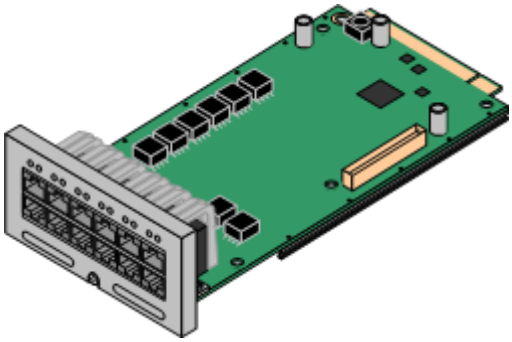
Tarjeta base de teléfono analógico IP500 213



La tarjeta está disponible en dos variantes, que admiten 2 u 8 puertos de teléfono analógico.

- La tarjeta se puede equipar con un[Tarjeta auxiliar de troncales IP500](#) 25que utiliza los puertos de la tarjeta base para la conexión troncal.
- **Máximo:**4 por unidad de control.
  - Los puertos de teléfono analógico no incluyen un condensador de llamada. Cuando este sea un requisito, la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
  - Si está equipada con una tarjeta secundaria de troncales analógicas IP500, durante un corte de energía, el puerto de teléfono 8 se conecta al puerto de troncales analógicas 12.

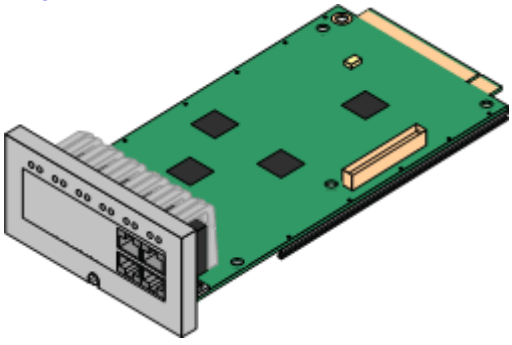
Tarjeta de estación digital IP500 TCM8 220



Esta tarjeta proporciona 8 puertos BST (estación digital) para la conexión de teléfonos Avaya 4100, 7400, M-Series y T-Series.

- La tarjeta se puede equipar con un[Tarjeta auxiliar de troncales IP500](#) 25que utiliza los puertos de la tarjeta base para la conexión troncal.
- **Máximo:**4 por unidad de control por unidad de control IP500 V2.

Tarjeta base IP500 VCM 221



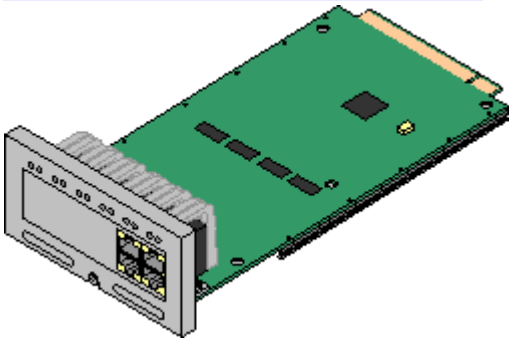
Esta tarjeta está disponible en variantes que admiten 32 o 64 canales de compresión de voz para uso con llamadas VoIP.

- La tarjeta se puede equipar con un[Tarjeta auxiliar de troncales IP500](#) 25que utiliza los puertos de la tarjeta base para la conexión troncal.
- **Máximo:**2 por unidad de control.

¿Comentarios sobre este documento? infodev@avaya.com

Tarjeta base de expansión de 4 puertos IP500

212

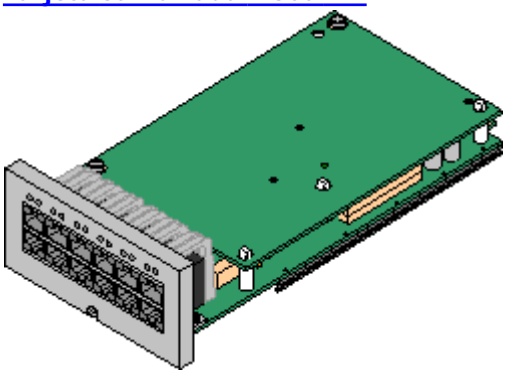


Esta tarjeta agrega 4 puertos de expansión adicionales para módulos de expansión externos. La tarjeta se suministra con cuatro cables de interconexión amarillos de 2 m.

- Esta tarjeta no acepta ninguna tarjeta auxiliar de troncales IP500.
- **Máximo:**1 por unidad de control (solo ranura derecha 4).
- **Módulos de expansión compatibles:**Se admiten los siguientes módulos de expansión externos:
  - Módulo troncal analógico IP500
  - Módulo IP500 BRI So
  - Módulo de estación digital IP500
  - Módulo de estación digital IP500
  - Módulo de estación digital IP500
  - Módulo telefónico IP500

Tarjeta combinada IP500 BRI

216

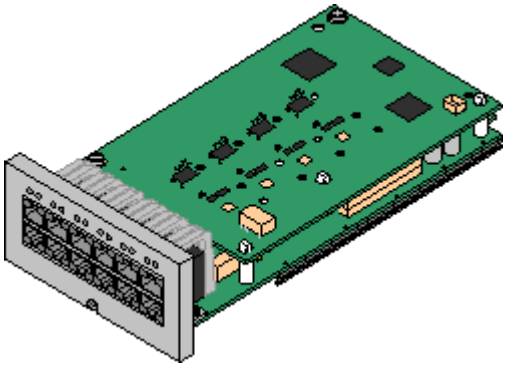


Esta tarjeta proporciona 6 puertos de estación digital (1-6), 2 puertos de extensión analógica (7-8) y 2 puertos troncales BRI (9-10, 4 canales). La tarjeta también incluye 10 canales de compresión de voz.

- **Máximo:**2 tarjetas combinadas por unidad de control IP500 V2, independientemente del tipo.
  - Las tarjetas combinadas IP500 están preinstaladas con una tarjeta secundaria de troncales que no se puede quitar ni cambiar por otra tarjeta secundaria de troncales de tipo/capacidad.
  - IP Office Basic Edition: los sistemas Norstar Mode e IP Office Basic Edition están limitados a un máximo de 12 canales BRI utilizando una combinación BRI o tarjetas auxiliares de troncales BRI.

Tarjeta combinada IP500 ATM/Tarjeta combinada IP500 ATM V2

214

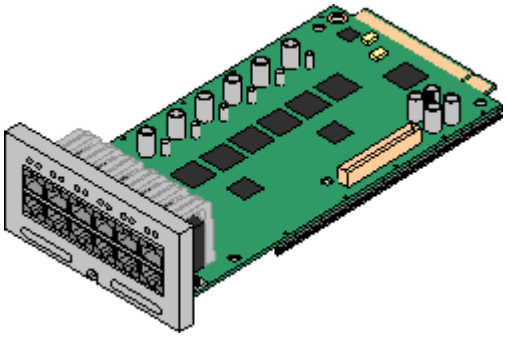


Esta tarjeta proporciona 6 puertos de estación digital (1-6), 2 puertos de extensión analógica (7-8) y 4 puertos de troncal analógica (9-12). La tarjeta también incluye 10 canales de compresión de voz.

- **Máximo:**2 tarjetas combinadas por unidad de control IP500 V2, independientemente del tipo.
  - Las tarjetas combinadas IP500 están preinstaladas con una tarjeta secundaria de troncales que no se puede quitar ni cambiar por otra tarjeta secundaria de troncales de tipo/capacidad.
  - Los puertos de teléfono analógico no incluyen un condensador de llamada. Cuando este sea un requisito, la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
  - Durante un corte de energía, el puerto telefónico 8 se conecta al puerto troncal analógico 12.

Tarjeta base IP500 ETR6

219

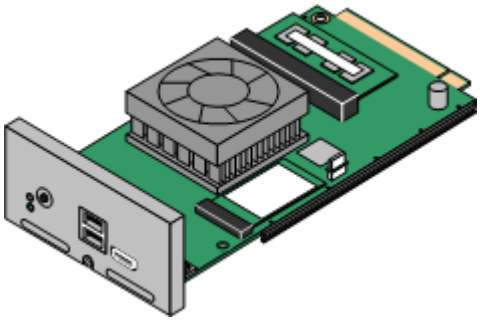


Esta tarjeta solo es compatible con una unidad de control IP500 V2 que se ejecuta en IP Office Basic Edition - Modo PARTNER® o IP Office Basic Edition. Proporciona 6 puertos ETR para la conexión de teléfonos ETR. 2 Los puertos de extensión analógica también se proporcionan para uso de emergencia solo con una tarjeta de troncal analógica.

- La tarjeta se puede equipar con una tarjeta auxiliar de troncales IP500 que utiliza los puertos de la tarjeta base para la conexión de troncales.
- **Máximo:**3 por unidad de control IP500 V2.
- Los puertos de teléfono analógico no incluyen un condensador de llamada. Cuando este sea un requisito, la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
- Si está equipado con una tarjeta secundaria de troncales analógicas IP500, durante un corte de energía, los puertos de teléfono 7 y 8 se conectan al puerto de troncales analógicas 12. Sin embargo, durante el funcionamiento normal, los puertos de teléfonos analógicos 7 y 8 no se pueden utilizar.

Módulo de comunicaciones unificadas

217

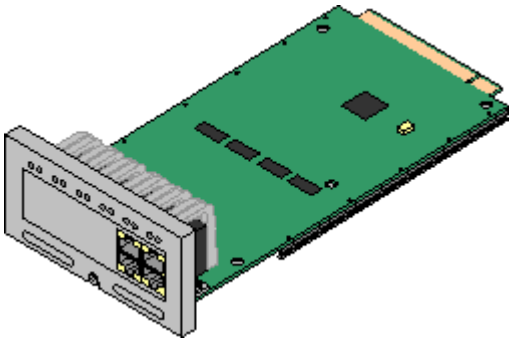


Esta tarjeta actúa como un servidor Linux integrado para las aplicaciones one-X Portal for IP Office y/o Voicemail Pro.

13.3.1 Tarjeta de expansión de 4 puertos

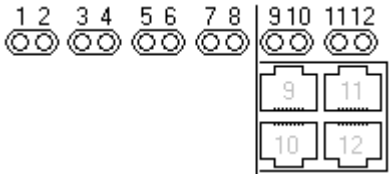
Esta tarjeta se utiliza para agregar 4 puertos de expansión adicionales a la unidad de control.

- Los sistemas que se ejecutan en los modos estándar de IP Office admiten 8 módulos de expansión externos como estándar. Si está equipado con una tarjeta base de expansión de 4 puertos IP500, se admiten hasta 12 módulos de expansión externos.



- **Soporta**
  Proporciona 4 adicionalespuertos de expansión 273para la conexión de externo módulos de expansión.
- **Módulos de expansión compatibles:**Se admiten los siguientes módulos de expansión externos:
  - Módulo troncal analógico IP500
  - Módulo IP500 BRI So
  - Módulo de estación digital IP500
  - Módulo de estación digital IP500
  - Módulo de estación digital IP500
  - Módulo telefónico IP500
- **Máximo por Unidad de Control:**1 - Ranura derecha 4 únicamente.
- **Compatibilidad con la tarjeta de troncales IP500:** ✗.
- **Modos de IP Office:**No se admite en los modos de IP Office Basic Edition.

- Cada módulo de expansión externo se suministra con un cable de interconexión de expansión azul de 1 metro (3'3"). este cable deber utilizarse cuando se conecta a puertos de expansión en la parte trasera de una unidad de control.
- Cuando se conecta a puertos de expansión en una tarjeta de expansión de 4 puertos IP500, se puede usar un cable de interconexión de expansión amarillo de 2 metros (6'6") en lugar del cable azul estándar. Se suministran 4 cables amarillos con la tarjeta de expansión de 4 puertos IP500 tarjeta.



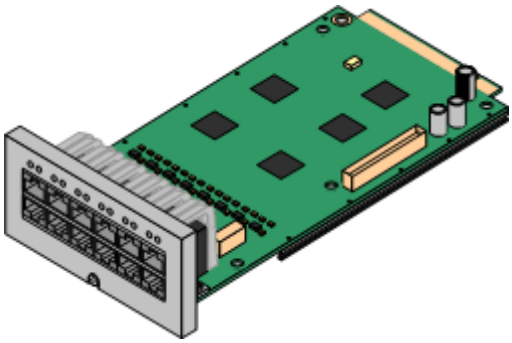
- Los LED 1 a 8 se utilizan para los puertos de expansión en la parte posterior de la unidad de control. Los LED 9 a 12 se utilizan para los puertos de expansión propios de la tarjeta.

Verde	**En**	Módulo de expansión presente.
Rojo	**Brillante**	Inicializando.
Rojo	**En**	Error.
Naranja	**Destello normal**	Tarjeta base bien.

Nombre	Descripción	Código SAP
TARJETA EXP IPO IP500 4PT	Incluye 4 cables de interconexión amarillos de 2 metros.	700472889
CABLE IPO EXP RJ45/RJ45 2M AMARILLO	Solo para usar con la tarjeta de expansión de 4 puertos.	700472871

13.3.2 Teléfono analógico

Esta tarjeta se utiliza para agregar puertos de teléfono analógico a la unidad de control. Está disponible en dos variantes, proporcionando 2 u 8 puertos de extensión analógicos.



- **Soporta**
  Proporciona 8 o 2cosa análoga 267puertos telefónicos según tarjeta variante.
- **Máximo por Unidad de Control:**4.
- **Compatibilidad con la tarjeta de troncales IP500:** ✓ 1.
- **Modos de IP Office:**Compatible en todos los modos.

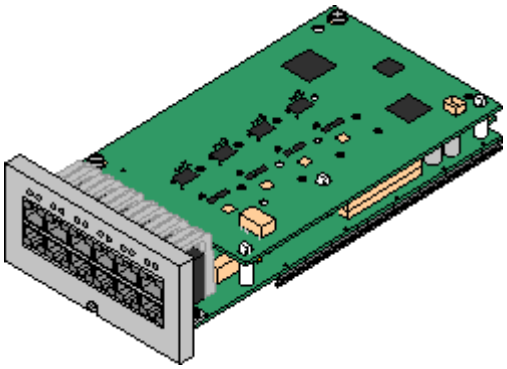
Tipo de puerto	Puertos	Características
Cosa análoga **Teléfono**	**1 a 8**	· Admite los modos ICLID DTMFA, DTMFC, DTMFD, FSK y UK20. · REN 2 (1 para dispositivo timbre externo). · Corriente descolgada: 25mA · Voltaje del timbre: 40V. · Diseñados para la conexión a teléfonos analógicos de dos hilos, los puertos no incluyen un condensador de llamada. Para la conexión a teléfonos analógicos de 4 hilos, la conexión debe realizarse a través de un enchufe maestro con condensadores de timbre. · Si está equipado con una tarjeta de troncal analógica, para el teléfono 8, durante un corte de energía, el puerto de extensión 8 se conecta al puerto de troncal analógica 12. **LED de puerto** · No se utilizan LED de estado para extensiones telefónicas analógicas. · LED1 también se utiliza para el estado de la tarjeta base: · **rojo encendido**=Error/No compatible. · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rápido rojo**=Apagado del sistema.
Opcional Tronco **Tarjeta** **Puertos**	**9 a 12**	La tarjeta se puede equipar con una tarjeta secundaria de troncales de cualquier tipo. La tarjeta secundaria de troncales luego usa los puertos 9 a 12 en la tarjeta base para sus conexiones de troncales. **LED de puerto** El uso de LED depende del tipo de tarjeta secundaria instalada en la tarjeta base: · El LED 9 también se utiliza para el estado de la tarjeta secundaria. · **rojo encendido**=Error · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rápido rojo**=Apagado del sistema. **Tarjeta Analógica** · **Verde encendido**=V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. · **Verde intermitente**=Línea ocupada. **Tarjeta PRI** · **Apagado**=No hay baúl presente. · **Verde encendido**=Tronco presente. · **Verde intermitente**=Tronco en uso. · **Parpadeo rápido rojo/verde**(puerto 9) o**Parpadeo rápido verde**(puerto 10) = Señal de indicación de alarma (AIS) desde el extremo remoto troncal. · **Rojo con parpadeo verde**(puerto 9) o**Parpadeo verde**(puerto 10) = Puerto en modo de bucle invertido (establecido a través de IP Office System Monitor). **Tarjeta BRI** · **Apagado**=No hay baúl presente. · **Verde encendido**=Tronco presente. · **Verde intermitente**=Tronco en uso.

Nombre	Descripción	Código SAP
IPO 500 Extn Tarjeta Teléfono 2	Teléfono con tarjeta de extensión IP Office 500 2	700431778
IPO 500 Tarjeta Externa Teléfono 8	Teléfono con tarjeta de extensión IP Office 500 8	700417231

¿Comentarios sobre este documento? infodev@avaya.com

13.3.3 Tarjeta combinada de cajero automático

Estas tarjetas se utilizan para agregar una combinación de puertos a una unidad de control IP500 V2. No es compatible con las unidades de control IP500. La versión más reciente de la tarjeta combinada IP500 ATM V2 es compatible con IP Office versión 8.1 Feature Pack 1 y superior únicamente.



- **Soporta**
  - 10 canales de compresión de voz. El soporte de códec es G.711, G729a y G.723 con cancelación de eco de 64 ms. G.722 es compatible con la versión 8.0 y posteriores de IP Office.
  - 6 puertos de estación digital para soporteTeléfonos digitales Avaya DS 39 (excepto Serie 3800).
  - 2 puertos de extensión analógica.
  - 4 puertos de troncales analógicas:
    Según la versión de la tarjeta combinada, V1 o V2, la tarjeta secundaria de troncales analógicas es equivalente a unaTarjeta de troncales analógicas IP500 4 224V1 o V2 respectivamente.
- Durante una falla de energía, el puerto de teléfono 8 está conectado al puerto de troncal analógico 12
- **Máximo por Unidad de Control:**2 tarjetas combinadas de cualquier tipo por unidad de control IP500 V2.
- **Compatibilidad con la tarjeta de troncales IP500:** ✓ 1.
  - Las tarjetas combinadas IP500 están preinstaladas con una tarjeta secundaria de troncales que no se puede quitar ni cambiar por otra tarjeta secundaria de troncales de tipo/capacidad.
- **Modos de IP Office:**Compatible en todos los modos.
- **Nivel mínimo de software:**6.0+.
  Esto depende de la versión de la tarjeta de la siguiente manera:
  - **V1:**6.0+. Las tarjetas PCS04 de nueva generación solo se admiten en sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) o 8.0 y posteriores. Consulte la sugerencia técnica 237 de IP Office.
  - **V2:**IP Office versión 8.1 Feature Pack 1 o superior.

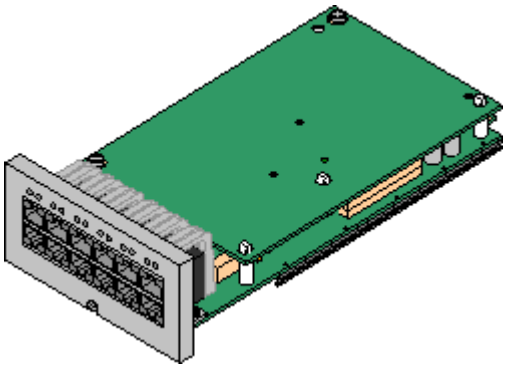
Tipo de puerto	Puertos	Características
Dígito Estación	**1 a 6**	proporcionaSD 271puertos para compatiblesTeléfonos digitales Avaya DS 39(excepto Serie 3800). **LED** • **Verde intermitente**=Teléfono detectado. • **Verde encendido**=Teléfono activo. • LED1 también se utiliza para el estado de la tarjeta base: • **rojo encendido**=Error/No compatible. • **Parpadeo lento rojo**=Inicializando. • **Parpadeo rojo cada 5 segundos**=Tarjeta bien. • **Parpadeo rápido rojo**=Apagado del sistema.
Cosa análoga **Teléfono**	**7 a 8**	• Admite los modos ICLID DTMFA, DTMFC, DTMFD, FSK y UK20. • REN 2 (1 para dispositivo timbre externo). • Corriente descolgada: 25mA • Voltaje del timbre: 40V. • Diseñados para la conexión a teléfonos analógicos de dos hilos, los puertos no incluyen un condensador de llamada. Para la conexión a teléfonos analógicos de 4 hilos, la conexión debe realizarse a través de un enchufe maestro con condensadores de timbre. • Durante un corte de energía, el puerto de extensión 8 se conecta al puerto troncal analógico 12. • No se utilizan LED de estado para extensiones telefónicas analógicas.
Cosa análoga **Tronco**	**9 a 12**	• Detección de DTMF, ICLID y tono ocupado. • Protección contra sobrevoltaje/rayos (todavía puede requirirequipo de protección adicional 36). • Marcación DTMF y LD (desconexión de bucle). • Cancelación del eco. **LED** • **Verde encendido**=V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde intermitente**=Línea ocupada. • El LED 9 también se utiliza para el estado de la tarjeta secundaria. • **rojo encendido**=Error • **Parpadeo lento rojo**=Inicializando. • **Parpadeo rojo cada 5 segundos**=Tarjeta bien. • **Parpadeo rápido rojo**=Apagado del sistema.

Página1230 de 3226.

Nombre	Descripción	Código SAP
IPO IP500 V2 TARJETA COMB ATM4	TARJETA COMBINADA IPO IP500 V2 ATM4	700476013
IPO IP500 V2 TARJETA COMB ATM4 TAA	"Ley de Acuerdos Comerciales 296variante compatible.	700501513
IPO IP500 V2 TARJETA COMB ATM4 V2	TARJETA COMBINADA IPO IP500 V2 ATM4 V2	700504556

13.3.4 Tarjeta Combinada BRI

Esta tarjeta se utiliza para agregar una combinación de puertos a una unidad de control IP500 V2.



- **Soporta**
  - 10 canales de compresión de voz. El soporte de códec es G.711, G729a y G.723 con cancelación de eco de 64 ms. G.722 es compatible con la versión 8.0 y posteriores de IP Office.
  - 6 puertos de estación digital para soporteTeléfonos digitales Avaya DS 39(excepto Serie 3800).
  - 2 puertos de extensión analógica.
  - 2 puertos troncales BRI (4 canales BRI).
- **Máximo por Unidad de Control:**2 cartas combinadas de cualquier tipo.
  - IP Office Basic Edition: los sistemas Norstar Mode e IP Office Basic Edition están limitados a un máximo de 12 canales BRI utilizando una combinación BRI o tarjetas auxiliares de troncales BRI.
- **Compatibilidad con la tarjeta de troncales IP500:** ✓ 1.
  - Las tarjetas combinadas IP500 están preinstaladas con una tarjeta secundaria de troncales que no se puede quitar ni cambiar por otra tarjeta secundaria de troncales de tipo/capacidad.
- **Modos de IP Office:**No compatible con IP Office Basic Edition - modo PARTNER® Mode.

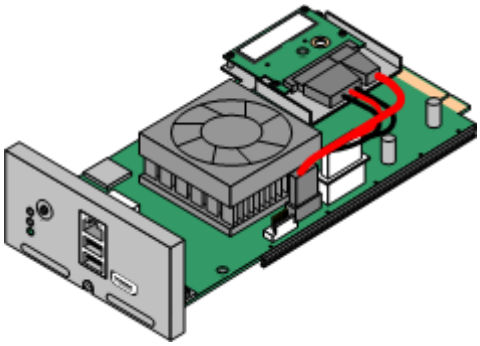
Tipo de puerto	Puertos	Características
Dígito Estación	**1 a 6**	proporcionaSD 271puertos para compatiblesTeléfonos digitales Avaya DS 39(excepto Serie 3800). **LED** · **Verde intermitente**=Teléfono detectado. · **Verde encendido**=Teléfono activo. · LED1 también se utiliza para el estado de la tarjeta base: · **rojo encendido**=Error/No compatible. · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo rápido rojo**=Apagado del sistema.
Cosa análoga Teléfono	**7 a 8**	· Admite los modos ICLID DTMFA, DTMFC, DTMFD, FSK y UK20. · REN 2 (1 para dispositivo timbre externo). · Corriente descolgada: 25mA · Voltaje del timbre: 40V. · Diseñados para la conexión a teléfonos analógicos de dos hilos, los puertos no incluyen un condensador de llamada. Para la conexión a teléfonos analógicos de 4 hilos, la conexión debe realizarse a través de un enchufe maestro con condensadores de timbre. · No se utilizan LED de estado para extensiones telefónicas analógicas.
BRI Tronco	**9 a 10**	· Cada puerto troncal admite canales 2B+D. · Protocolo de tarifa básica ETSI o AusTS013 establecido a través de la configuración de IP Office. **LED** · **Apagado**=No hay baúl presente. · **Verde encendido**=Tronco presente. · **Verde intermitente**=Tronco en uso. · El LED 9 también se utiliza para el estado de la tarjeta secundaria. · **rojo encendido**=Error · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo rápido rojo**=Apagado del sistema.
No utilizado	**11 a 12**	–

Nombre	Descripción	Código SAP
TARJETA COMB IPO IP500 V2 BRI	TARJETA COMBINADA IPO IP500 V2 BRI	700476021

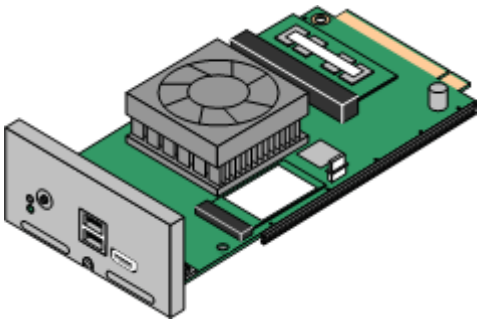
13.3.5 Módulo de comunicaciones unificadas

Esta tarjeta es un servidor integrado que permite que las aplicaciones de IP Office basadas en Linux se ejecuten dentro de la unidad de control de IP Office en lugar de requerir PC separadas. La dirección IP del servidor se establece durante su configuración inicial y luego se puede cambiar mediante el acceso del navegador web al servidor.

Hay dos tipos de tarjeta. El Unified Communications Module v2 es compatible con la versión 9.1 y posteriores de IP Office. El Unified Communications Module v1 es compatible con IP Office versión 8.0 Q1 2012 Service Pack o superior. Aunque físicamente diferentes, los dos tipos de tarjetas actuales admiten las mismas aplicaciones y capacidades de aplicación. Sin embargo, v2 no proporciona una licencia Preferred Edition implícita y no se suministra con software preinstalado.



Módulo de comunicaciones unificadas v1



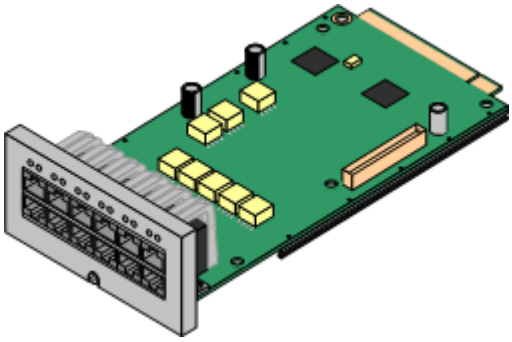
Módulo de comunicaciones unificadas v2

- **Soporta**
  Aplicaciones de Voicemail Pro y one-X Portal para IP Office.
  - **Usuarios de IP Office:**Hasta 200 usuarios cuando se ejecuta Voicemail Pro y one-X Portal for IP Office. Más de 200 usuarios cuando se ejecuta solo Voicemail Pro.
  - **Portal one-X simultáneo para usuarios de IP Office:**50
  - **Número máximo de puertos de correo de voz:**Hasta 20 puertos cuando se ejecuta Voicemail Pro y one-X Portal for IP Office. Hasta 40 puertos cuando se ejecuta solo Voicemail Pro.
  - **Red comunitaria pequeña:**Máximo 6 sistemas.
- **Licencias**
  Para ambos tipos de tarjetas, un**Edición esencial**Se requiere licencia como requisito previo. El servidor de correo de voz en la tarjeta también requiere que el sistema tenga un**Edición preferida**licencia.
  - En los sistemas anteriores a la versión 10 de IP Office, Unified Communications Module v1 otorga al sistema host la licencia virtual Preferred Edition que necesita para Voicemail Pro. Esto ya no se aplica a la versión 10 y posteriores de IP Office. Los sistemas IP Office existentes que se actualicen a la versión 10 de IP Office deben utilizar el proceso de migración de licencias de IP Office para conservar la licencia existente.
- **Máximo por Unidad de Control:**1 por unidad de control.
- **Compatibilidad con la tarjeta de troncales IP500:** ✗
- **Modos de IP Office:**No se admite en los modos de IP Office Basic Edition.
- **!ADVERTENCIA:**
  La tarjeta Unified Communications Module v1 se suministra con una cubierta de plástico extraíble que se ubica sobre los puertos externos (LAN, USB y HDMI) en la placa frontal de la tarjeta. Esta tapa siempre debe estar en su lugar durante el funcionamiento normal de la tarjeta. La cubierta solo debe retirarse temporalmente durante las acciones de mantenimiento que requieran acceso a los puertos y debe reemplazarse cuando finalice el mantenimiento.
- **!ADVERTENCIA: La tarjeta permanece caliente después del apagado del sistema**
  Al quitar un módulo de comunicaciones unificadas de un sistema, se debe tener cuidado de no tocar el disipador de calor del módulo. El disipador de calor permanece caliente durante un largo período después de apagar el sistema.

Nombre	Descripción	Código SAP
MÓDULO UC IPO	Módulo de comunicaciones unificadas de IP Office v1	700501442
MÓDULO IPO UC V2	Módulo de comunicaciones unificadas de IP Office v2	700507449

13.3.6 Estación digital

Esta tarjeta se usa para agregar puertos de extensión de estación digital (DS) a una unidad de control IP500 e IP500 V2. Proporciona 8 puertos de extensión RJ45 DS para usar con Teléfonos digitales Avaya DS 39. Se proporcionan 4 puertos RJ45 adicionales para conexiones de troncales cuando se instala una tarjeta de troncales IP500 en esta tarjeta.



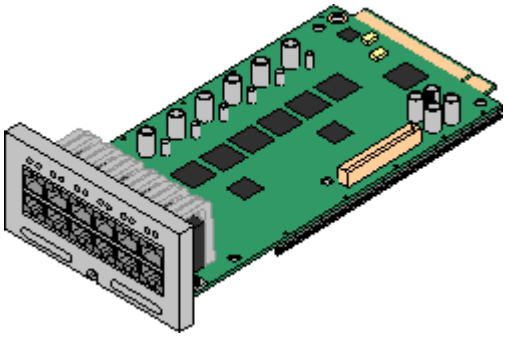
- **Soporta**
  Proporciona 8 SD 271 puertos para Teléfonos digitales Avaya DS 39.
- **Máximo por Unidad de Control:** 3 por unidad de control.
- **Compatibilidad con la tarjeta de troncales IP500:** ✔ 1.
- **Modos de IP Office:** Compatible en todos los modos.

Tipo de puerto	Puertos	Características
Dígito Estación	**1 a 8**	proporciona SD 271 puertos para compatibles Teléfonos digitales Avaya DS 39 (excepto Serie 3800). **LED** · **Verde intermitente**=Teléfono detectado. · **Verde encendido**=Teléfono activo. · LED1 también se utiliza para el estado de la tarjeta base: · **rojo encendido**=Error/No compatible. · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo rápido rojo**=Apagado del sistema.
Opcional Tronco Tarjeta Puertos	**9 a 12**	La tarjeta se puede equipar con una tarjeta secundaria de troncales de cualquier tipo. La tarjeta secundaria de troncales luego usa los puertos 9 a 12 en la tarjeta base para sus conexiones de troncales. **LED de puerto** El uso de LED depende del tipo de tarjeta secundaria instalada en la tarjeta base: · El LED 9 también se utiliza para el estado de la tarjeta secundaria. · **rojo encendido**=Error · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo rápido rojo**=Apagado del sistema. **Tarjeta Analógica** · **Verde encendido**=V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. · **Verde intermitente**=Línea ocupada. **Tarjeta PRI** · **Apagado**=No hay baúl presente. · **Verde encendido**=Tronco presente. · **Verde intermitente**=Tronco en uso. · **Parpadeo rápido rojo/verde**(puerto 9) o **Parpadeo rápido verde**(puerto 10) = Señal de indicación de alarma (AIS) desde el extremo remoto troncal. · **Rojo con parpadeo verde**(puerto 9) o **Parpadeo verde**(puerto 10) = Puerto en modo de bucle invertido (establecido a través de IP Office System Monitor). **Tarjeta BRI** · **Apagado**=No hay baúl presente. · **Verde encendido**=Tronco presente. · **Verde intermitente**=Tronco en uso.

Nombre	Descripción	Código SAP
Tarjeta IPO 500 Extn Dgtl Sta 8	Tarjeta de extensión IP Office 500 Estación digital 8	700417330
IPO IP500 Tarjeta Externa Dgtl Sta 8 TAA	"Ley de Acuerdos Comerciales 296 variante compatible.	700501512

13.3.7 Tarjeta ETR6

Esta carta se usa para sumar 6ETR 39puertos de extensión telefónica a una unidad de control IP500 V2. También incluye 2 puertos de extensión analógicos que son para uso de emergencia solo cuando la tarjeta está equipada con una tarjeta secundaria de troncales analógicas. Se proporcionan otros 4 puertos RJ45 (9 a 12) para conexiones de troncales cuando se instala una tarjeta secundaria de troncales IP500 en esta tarjeta.



- **Soporta**
  ETR 39y teléfonos analógicos. Cada teléfono ETR se puede utilizar para un teléfono ETR o analógico. La compatibilidad con el teléfono ETR 34D está limitada a un máximo de 2 por tarjeta ETR6 y 4 en total.
  - La paginación a equipos de paginación externos no es compatible a través de los puertos ETR6. Es compatible a través de puertos POT.
  - Los únicos teléfonos analógicos probados por Avaya para IP Office Essential Edition son los Avaya 6200 Series. Si se utilizan otros teléfonos analógicos, es responsabilidad del cliente asegurarse de que esos teléfonos funcionen según lo requerido.
- **Máximo por Unidad de Control:**3.
- **Compatibilidad con la tarjeta de troncales IP500:** ✓ 1. El troncal secundario IP500 BRI la tarjeta no es compatible.
- **Modos de IP Office:**Solo se admite en los modos IP Office Basic Edition - PARTNER® Mode o IP Office Basic Edition (U-Law) con una configuración regional norteamericana.

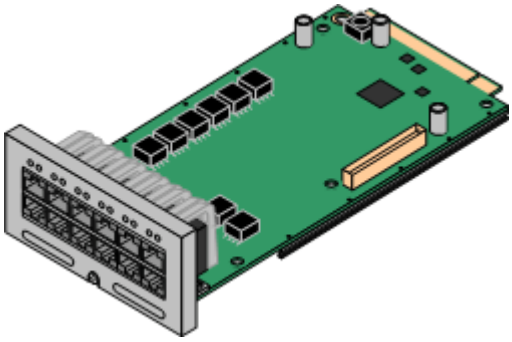
Tipo de puerto	Puertos	Características
ETR	**1 a 6**	· REN 1. · Sólo marcación DTMF. · Indicación de mensaje en espera 51V escalonada. · Modo ICLID Bellcore 202. **LED** · No se utilizan LED de estado para los puertos ETR. · LED1 también se utiliza para el estado de la tarjeta base: · **rojo encendido**=Error/No compatible. · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo rápido rojo**=Apagado del sistema.
FE	**7 a 8**	· Si está equipada con una tarjeta auxiliar de troncales IP500, durante un corte de energía, ambos puertos se conectan al puerto 12 de troncales analógicas. · Admite los modos ICLID DTMFA, DTMFC, DTMFD, FSK y UK20. · REN 2 (1 para dispositivo timbre externo). · Corriente descolgada: 25mA · Voltaje del timbre: 40V. · Diseñados para la conexión a teléfonos analógicos de dos hilos, los puertos no incluyen un condensador de llamada. Para la conexión a teléfonos analógicos de 4 hilos, la conexión debe realizarse a través de un enchufe maestro con condensadores de timbre. · No se utilizan LED de estado para extensiones telefónicas analógicas.
Opcional Tronco Puertos	**9 a 12**	Depende del tipo de tarjeta auxiliar de troncales instalada. El ETR6 se puede equipar con unTroncal analógico 224tarjeta oTroncal PRI 227tarjeta. **LED** El uso de LED depende del tipo de tarjeta secundaria instalada en la tarjeta base: · El LED 9 también se utiliza para el estado de la tarjeta secundaria. · **rojo encendido**=Error · **Parpadeo lento rojo**=Inicializando. · **Parpadeo rojo cada 5 segundos**=Tarjeta bien. · **Parpadeo rápido rojo**=Apagado del sistema. **Cosa análoga Tarjeta** · **Verde encendido**=V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. · **Verde intermitente**=Línea ocupada. **Tarjeta PRI** · **Apagado**=No hay baúl presente. · **Verde encendido**=Tronco presente. · **Verde intermitente**=Tronco en uso. · **Parpadeo rápido rojo/verde**(puerto 9) o**Parpadeo rápido verde**(puerto 10) = Señal de indicación de alarma (AIS) desde el extremo remoto troncal. · **Rojo con parpadeo verde**(puerto 9) o**Parpadeo verde**(puerto 10) = Puerto en modo de bucle invertido (establecido a través de IP Office System Monitor).

Nombre	Descripción	Código SAP
IPO IP500 V2 TARJETA EXTN ETR6	IPO IP500 V2 TARJETA EXTN ETR6	700417235

Página 1235 de 3226.

13.3.8 Estación digital TCM8

Esta tarjeta se utiliza para agregar puertos de extensión BST RJ45 a una unidad de control IP500 V2. Proporciona 8 puertos de extensión RJ45 para soporte Teléfonos digitales Avaya BST 39.Se proporcionan 4 puertos RJ45 adicionales para conexiones de troncales cuando se instala una tarjeta de troncales IP500 en esta tarjeta.



- **Soporta**
  Proporciona 8 puertos BST para estaciones digitales 4100, 7400, M y T-Series compatibles.
- **Máximo por Unidad de Control:**4.
- **Compatibilidad con la tarjeta de troncales IP500:** ✔ 1.
- **Modos de IP Office:**Compatible en todos los modos.

Tipo de puerto	Puertos	Características
BST	**1 a 8**	**LED** • **Verde encendido**=Teléfono detectado. • LED1 también se utiliza para el estado de la tarjeta base: • **rojo encendido**=Error/No compatible. • **Parpadeo lento rojo**=Inicializando. • **Parpadeo rojo cada 5 segundos**=Tarjeta bien. • **Parpadeo rápido rojo**=Apagado del sistema.
Opcional Tronco **Tarjeta Puertos**	**9 a 12**	La tarjeta se puede equipar con una tarjeta secundaria de troncales de cualquier tipo. La tarjeta secundaria de troncales luego usa los puertos 9 a 12 en la tarjeta base para sus conexiones de troncales. **LED** El uso de LED depende del tipo de tarjeta secundaria instalada en la tarjeta base: • El LED 9 también se utiliza para el estado de la tarjeta secundaria. • **rojo encendido**=Error • **Parpadeo lento rojo**=Inicializando. • **Parpadeo rojo cada 5 segundos**=Tarjeta bien. • **Parpadeo rápido rojo**=Apagado del sistema. **Tarjeta Analógica** • **Verde encendido**=V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde intermitente**=Línea ocupada. **Tarjeta PRI** • **Apagado**=No hay baúl presente. • **Verde encendido**=Tronco presente. • **Verde intermitente**=Tronco en uso. • **Parpadeo rápido rojo/verde**(puerto 9) o**Parpadeo rápido verde**(puerto 10) = Señal de indicación de alarma (AIS) desde el extremo remoto troncal. • **Rojo con parpadeo verde**(puerto 9) o**Parpadeo verde**(puerto 10) = Puerto en modo de bucle invertido (establecido a través de IP Office System Monitor). **Tarjeta BRI** • **Apagado**=No hay baúl presente. • **Verde encendido**=Tronco presente. • **Verde intermitente**=Tronco en uso.

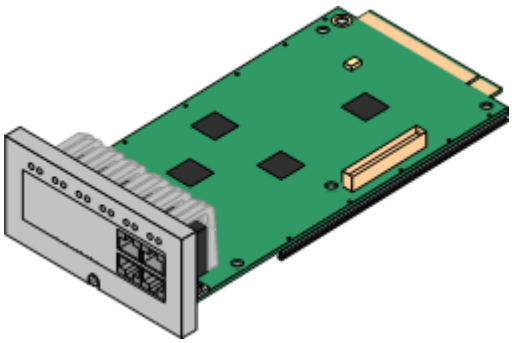
Nombre	Descripción	Código SAP
Conjunto de tarjeta de extensión IPO 500 TCM 8	IP Office 500 TCM 8	700500758

¿Comentarios sobre este documento? infodev@avaya.com

13.3.9 VCM

Este tipo de tarjeta se utiliza para añadir canales de compresión de voz a la unidad de control. Esos canales se utilizan para llamadas de VoIP, incluidas las extensiones de IP o las troncales de IP. Las unidades de control IP500 V2 admiten hasta 148 canales de compresión de voz, utilizando tarjetas IP500 VCM y Tarjetas combinadas IP500 214.

Las tarjetas están disponibles en variantes de 32 y 64 canales. Todas las variantes de tarjeta tienen 4 puertos RJ45 que se utilizan para conexiones troncales cuando Tarjeta auxiliar de troncales IP500 223 está equipado.



- **Soporta**
  Códecs G.711, G.729ab y G.723 con cancelación de eco de 64ms. La cantidad máxima de canales simultáneos que se pueden usar en una tarjeta base IP500 VCM se ve afectada por el códec que se usa. La siguiente tabla asume que todas las llamadas que usan VCM usan el mismo códec. Nota: Si bien las tarjetas IP500 VCM son compatibles con G729b, no es compatible con otros sistemas IP Office, como los sistemas basados en Linux.
  - G.722 es compatible con IP Office versión 8.0 y superior en sistemas con una tarjeta VCM IP500 o una tarjeta combinada IP500.

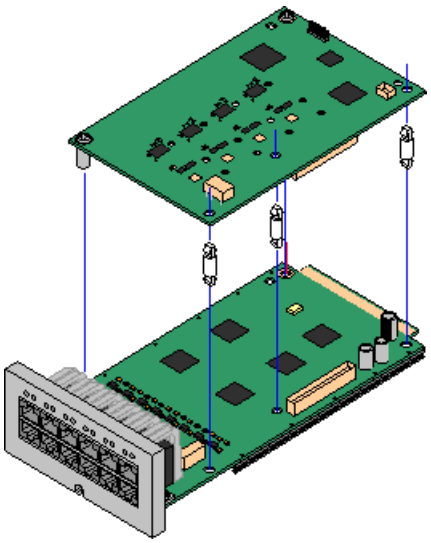
códec	IP500 VCM 32 IP500 VCM 32 V2	IP500 VCM 64 IP500 VCM 64 V2
G.711	32	64
G.729ab	30	60
G.723	22	44
G.722	30	60

- **Máximo por Unidad de Control:**2.
- **Compatibilidad con la tarjeta de troncales IP500:** ✓ 1.
- **Modos de IP Office:**No se admite en los modos de IP Office Basic Edition.

Tipo de puerto	Puertos	Características
No presente	**1 a 8**	No presente. **LED** • Los LED 1 a 8 no están etiquetados. Se utilizan para indicar el uso del canal de compresión de voz. Cada LED encendido representa el 12,5 % de la capacidad del canal de compresión de voz disponible en uso (capacidad total de la tarjeta en lugar de capacidad con licencia). • LED1 también se utiliza para el estado de la tarjeta base: • **rojo encendido**=Error/No compatible. • **Parpadeo lento rojo**=Inicializando. • **Parpadeo rojo cada 5 segundos**=Tarjeta bien. • **Parpadeo rápido rojo**=Apagado del sistema.
Opcional Tronco **Tarjeta** **Puertos**	**9 a 12**	La tarjeta se puede equipar con una tarjeta secundaria de troncales de cualquier tipo. La tarjeta secundaria de troncales luego usa los puertos 9 a 12 en la tarjeta base para sus conexiones de troncales. **LED** El uso de LED depende del tipo de tarjeta secundaria instalada en la tarjeta base: • El LED 9 también se utiliza para el estado de la tarjeta secundaria. • **rojo encendido**=Error • **Parpadeo lento rojo**=Inicializando. • **Parpadeo rojo cada 5 segundos**=Tarjeta bien. • **Parpadeo rápido rojo**=Apagado del sistema. **Tarjeta Analógica** • **Verde encendido**=V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde intermitente**=Línea ocupada. **Tarjeta PRI** • **Apagado**=No hay baúl presente. • **Verde encendido**=Tronco presente. • **Verde intermitente**=Tronco en uso. • **Parpadeo rápido rojo/verde**(puerto 9) o**Parpadeo rápido verde**(puerto 10) = Señal de indicación de alarma (AIS) desde el extremo remoto troncal. • **Rojo con parpadeo verde**(puerto 9) o**Parpadeo verde**(puerto 10) = Puerto en modo de bucle invertido (establecido a través de IP Office System Monitor). **Tarjeta BRI** • **Apagado**=No hay baúl presente. • **Verde encendido**=Tronco presente. • **Verde intermitente**=Tronco en uso.

	Nombre	Descripción	Código SAP
Voz IP500 Compresión Módulos	**IPO IP500 MC VCM 32**	Módulo de codificación de voz de tarjeta de medios IP Office 500 32	700417389
	IPO IP500 VCM 32 TAA	"Ley de Acuerdos Comerciales 296variante compatible.	700501518
	IPO IP500 MC VCM 64	Módulo de codificación de voz de la tarjeta de medios IP Office 500 64	700417397
Voz IP500 Compresión Módulos V2	**IPO IP500 MC VCM 32 V2**	Módulo de codificación de voz de tarjeta de medios IP500 32 V2	700504031
	IPO IP500 VCM 32 TAA V2	"Ley de Acuerdos Comerciales 296variante compatible.	700504033
	IPO IP500 MC VCM 64 V2	Módulo de codificación de voz de tarjeta de medios IP500 64 V2	700504032

13.4 Tarjetas auxiliares de troncales IP500

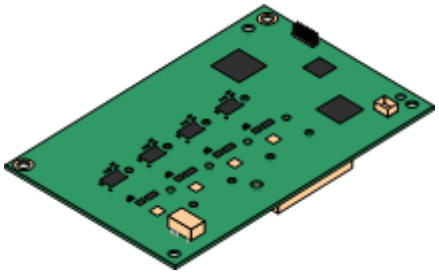


MuchosTarjetas base IP500 [223] se puede equipar con tarjetas secundarias de troncales IP500 para admitir la conexión de troncales a la tarjeta base.

Cada tarjeta secundaria se suministra con los pilares de separación necesarios para la instalación y una etiqueta para identificar la presencia de las tarjetas secundarias en el frente de la tarjeta base después de la instalación.

- Las tarjetas combinadas IP500 están preinstaladas con una tarjeta secundaria de troncales que no se puede quitar ni cambiar por otro tipo de tarjeta secundaria de troncales.

Tarjeta de troncales analógicas IP500/Tarjeta de troncales analógicas IP500 V2 [224]

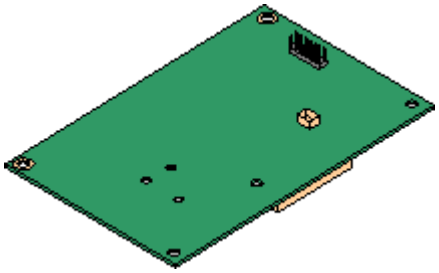


Estas tarjetas permiten que la tarjeta base admita 4 troncales analógicas de inicio en bucle.

- Los puertos de teléfono analógico no incluyen un condensador de llamada. Cuando este sea un requisito, la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
- Si la tarjeta base está equipada con puertos telefónicos analógicos, durante un corte de energía, el puerto telefónico 8 se conecta al puerto troncal analógico 12.

- **Máximo:**4 por unidad de control. La tarjeta de troncales analógicas IP500 V2 solo es compatible con IP500 V2.

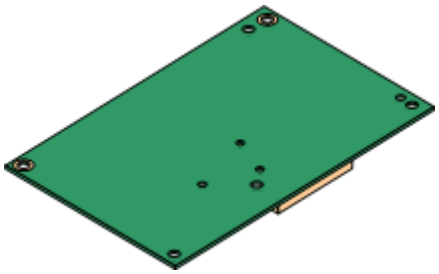
Tarjeta de troncales IP500 PRI-U [227]



Esta tarjeta permite que la tarjeta base admita hasta 2 conexiones de troncales PRI. La tarjeta está disponible en variantes de puerto único y doble. La tarjeta se puede configurar para troncales E1 PRI, T1 bit robado, T1 PRI o E1R2 PRI. También está disponible una variante T1(J) para uso en Japón.

- **Máximo:**4 por unidad de control.
- El sistema IP Office admite 8 canales B sin licencia en cada puerto IP500 PRI-U instalado. Se requieren canales B adicionales, hasta la capacidad de los puertos instalados y el modo PRI seleccionado**IP500 Universal PRI (canales adicionales)** [280]licencias añadidas a la configuración. Estos canales adicionales consumen las licencias según los canales adicionales configurados como en servicio desde el puerto 9 de la ranura 1 hacia arriba. Los canales D no se ven afectados por las licencias.

Tarjeta de troncales IP500 BRI [226]



Esta tarjeta permite que la tarjeta base admita hasta 4 conexiones de troncales BRI, cada troncal proporciona 2 canales digitales B+D. La tarjeta está disponible en variantes de 2 puertos (4 canales) y 4 puertos (8 canales).

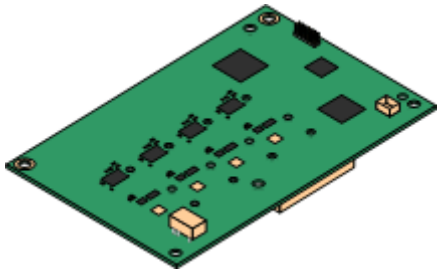
- **Máximo:**4 por unidad de control.
- **Conexión S-Bus**: La tarjeta se puede cambiar del modo A troncal al modo So. Este modo requiere resistencias de terminación adicionales y una conexión de cable cruzado ISDN, consultePuerto BRI (So) [268].
  - IP Office Basic Edition: los sistemas Norstar Mode e IP Office Basic Edition están limitados a un máximo de 12 canales BRI utilizando una combinación BRI o tarjetas auxiliares de troncales BRI.

¿Comentarios sobre este documento? infodev@avaya.com

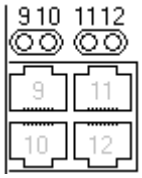
13.4.1 Tarjeta de troncales analógicas

Estas tarjetas se pueden agregar a una tarjeta base IP500 para proporcionar a esa tarjeta soporte para 4 troncales analógicas de inicio en bucle. La versión más reciente de la tarjeta de troncales analógicas IP500 V2 es compatible con los sistemas IP500 V2 que ejecutan IP Office versión 8.1 Feature Pack 1 o superior únicamente.

Esta tarjeta se puede instalar en cualquier tarjeta base IP500 que no sea combinada, excepto en la tarjeta de expansión de 4 puertos IP500 y el módulo de comunicaciones unificadas.



- **Puertos/Canales**
  4 puertos troncales analógicos de inicio de bucle. Conexiones a través de la tarjeta base host IP500.
  - Detección de DTMF, ICLID y tono ocupado.
  - Protección contra sobrevoltaje/rayos (todavía puede requerirequipo de protección adicional 36).
  - Marcación DTMF y LD (desconexión de bucle).
  - Cancelación del eco.
- **Cancelación del eco**
  La tarjeta admite la cancelación de eco que varía según el tipo de tarjeta.
  - **V1:**Cancelación de eco seleccionable manualmente para cualquiera***8***,***dieciséis***,***32***,***64***o***128***milisegundos o***Apagado***. El valor predeterminado es 16 milisegundos.
  - **V2:**Cancelación de eco seleccionable manualmente para cualquiera***En***o***Apagado***. El valor predeterminado es***En***. La tarjeta de troncales analógicas IP500 V2 también es compatible con la reducción de eco, que está configurada para***En***por defecto.
- **Indicación de estado de servicio/estado de línea**
  - **V1:**No se admite la detección del estado de línea individual para líneas inactivas. Por lo tanto, los LED de la tarjeta y la aplicación de estado del sistema simplemente indican que la tarjeta está instalada y cuando la línea está en uso.
  - **V2:**Se admite la detección automática del estado de línea para líneas inactivas. Los LED de la tarjeta y la aplicación de estado del sistema indican que la línea individual está conectada e inactiva o en uso.
- **Coincidencia de impedancia**
  - **V1:**Para esta tarjeta, solo se puede usar la coincidencia de impedancia manual y solo en lugares seleccionados.
  - **V2:**Esta tarjeta admite la coincidencia de impedancia automática al iniciar el sistema y este modo está habilitado de manera predeterminada. Si es necesario, se puede utilizar una adaptación de impedancia manual o nula. La coincidencia de impedancia se admite en todas las configuraciones regionales.
- **Detección de actividad de voz (VAD)**
  Compatibilidad con tarjetas ATM4U-V2 en IP Office versión 9.1 y superior únicamente. Cuando está habilitado, permite el soporte en troncales analógicas de funciones que requieren indicación de progreso de llamada, por ejemplo, el uso de hermanamiento móvil. Esta función no habilita la compatibilidad con el control de llamadas móviles. La función no está habilitada por defecto.
- **Puerto de falla de energía**
  Independientemente de la tarjeta IP500 que la aloje, durante un corte de energía, los pines 4 y 5 del puerto 12 se conectan a los pines 7 y 8. Además, cuando se instala en una tarjeta base IP500 Analog Phone 8, durante un corte de energía, el puerto de extensión 8 se conecta al puerto troncal analógico 12.
- **Licencia:**No se requiere licencia.
- **Máximo por Unidad de Control:**4.
- **Nivel mínimo de software:**
  Esto depende de la versión de la tarjeta de la siguiente manera:
  - **V1:**4.0+.
    Las nuevas tarjetas PCS10 y superiores solo se admiten en sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) u 8.0 y superior. Consulte la sugerencia técnica 237 de IP Office.
  - **V2:**8.1 Paquete de características 1+



Puertos de tarjeta secundaria (9-12)
Los LED de los puertos 9 a 12 de la tarjeta base IP500 se utilizan de la siguiente manera:

- **Verde encendido**=V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva.
- **Verde intermitente**=Línea ocupada.

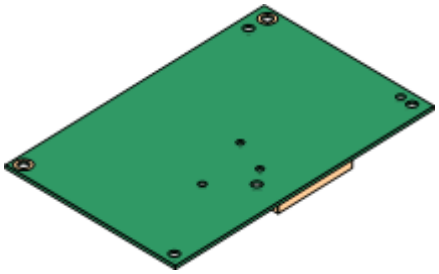
- El LED 9 también se utiliza para el estado de la tarjeta secundaria.
  - **rojo encendido**=Error
  - **Parpadeo lento rojo**=Inicializando.
  - **Parpadeo rojo cada 5 segundos**=Tarjeta bien.
  - **Parpadeo rápido rojo**=Apagado del sistema.

Nombre	Descripción	Código SAP
IPO 500 Trnk Anlg 4 Uni	Tarjeta de troncales IP Office 500 analógica 4 universal	700417405
IPO IP500 Tarjeta de troncales Anlg 4 V2	Tarjeta de troncales IP Office 500 analógica 4 universal V2	700503164

13.4.2 Tarjetas de troncales BRI

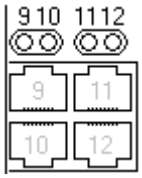
Esta tarjeta se puede agregar a una tarjeta base IP500 para proporcionar a esa tarjeta soporte paraBRI-A 269bañador. la tarjeta es disponible en variantes de 8 canales (4 troncales físicas) o 4 canales (2 troncales físicas).

Esta tarjeta se puede instalar en cualquier tarjeta base IP500 que no sea combinada, excepto en la tarjeta de expansión de 4 puertos IP500 y el módulo de comunicaciones unificadas.



- **Puertos/Canales**
  2 o 4 puertos troncales BRI. Conexiones a través de los puertos 9 a 12 de la tarjeta base host IP500.
  - Cada puerto troncal admite canales 2B+D.
  - Protocolo de tarifa básica ETSI o AusTS013 establecido a través de la configuración de IP Office.
- **Licencia:**No se requiere licencia.
- **Máximo por Unidad de Control:**4.
- **Nivel mínimo de software:**4.0+.
- **Conexión S-Bus:**En los sistemas IP Office 4.2+, la tarjeta se puede cambiar deA 269modo troncal aAsi que 268modo. Este modo requiere resistencias de terminación adicionales y una conexión de cable cruzado ISDN, consultePuerto BRI (So) 268.
- Esta tarjeta está aprobada para su uso en los siguientes países:

Brasil.	Nueva Zelanda.
Porcelana.	Rusia.
India.	Sudáfrica.
argentino	Emiratos Árabes Unidos (EAU).
Australia.	Unión Europea (UE).



Puertos de tarjeta secundaria (9-12)
Los LED de los puertos 9 a 12 de la tarjeta base IP500 se utilizan de la siguiente manera:

- **Apagado**=No hay baúl presente.
- **Verde encendido**=Tronco presente.
- **Verde intermitente**=Tronco en uso.

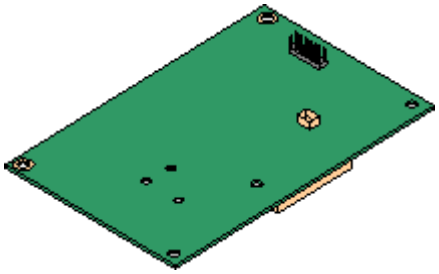
- El LED 9 también se utiliza para el estado de la tarjeta secundaria.
  - **rojo encendido**=Error
  - **Parpadeo lento rojo**=Inicializando.
  - **Parpadeo rojo cada 5 segundos**=Tarjeta bien.
  - **Parpadeo rápido rojo**=Apagado del sistema.

Nombre	Descripción	Código SAP
IPO 500 Trnk BRI 4 Uni	IP Office 500 Tarjeta de líneas troncales Tarifa básica 4 Universal	700417413
IPO IP500 TRNK BRI 4 UNI TAA	"Ley de Acuerdos Comerciales 296variante compatible.	700501515
IPO 500 Trnk BRI 8 Uni	IP Office 500 Tarjeta de líneas troncales Tarifa básica 8 Universal	700417421
IP0 IP500 BRI S0 CONVTR CBL	Cable convertidor IP500 BRI So	700458649

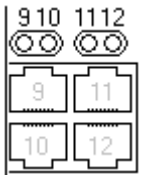
13.4.3 Tarjetas de troncales PRI

Esta tarjeta se puede agregar a una tarjeta base IP500 para proporcionar a esa tarjeta soporte para troncales PRI. La tarjeta está disponible en variantes de un solo puerto o de dos puertos.

Esta tarjeta se puede instalar en cualquier tarjeta base IP500 que no sea combinada, excepto en la tarjeta de expansión de 4 puertos IP500 y el módulo de comunicaciones unificadas.



- **Puertos/Canales**
  1 o 2Puertos troncales PRI 277.Cada puerto admite los siguientes tipos de líneas PRI.
  En las tarjetas de doble puerto, ambos puertos serán del mismo tipo de línea. La selección del tipo de línea se puede cambiar mediante IP Office Manager. Las opciones disponibles dependen del modo de funcionamiento y la configuración regional de IP Office.
  - E1 PRI (30B+D canales por puerto).
  - E1R2 PRI (30B canales por puerto).
  - Bit robado T1 (24B canales por puerto) o T1 PRI (23B+D canales por puerto).
  - También está disponible una variante T1(J) para usar en Japón (9.1 Feature Pack y superior).
  - El modo requerido se puede seleccionar dentro de IP Office Manager haciendo clic derecho en el icono de línea y seleccionando**Cambiar el tipo de línea de la tarjeta PRI Universal**y luego seleccionando el tipo de línea requerido.
  - La conexión troncal física se realiza a través de los puertos 9 y 10 de la tarjeta base host IP500.
  - Los puertos 11 y 12 se pueden usar como puntos de prueba para la conexión de equipos de prueba y monitoreo para el puerto adyacente.
- **Licencias**
  El sistema IP Office admite 8 canales B sin licencia en cada puerto IP500 PRI-U instalado. Se requieren canales B adicionales, hasta la capacidad de los puertos instalados y el modo PRI seleccionado**IP500 Universal PRI (canales adicionales)** licencias añadidas a la configuración. Estos canales adicionales consumen las licencias según los canales adicionales configurados como en servicio desde el puerto 9 de la ranura 1 hacia arriba. Los canales D no se ven afectados por las licencias.
- **Máximo por Unidad de Control:**4 por unidad de control en los modos estándar de IP Office. 1 tarjeta de un solo puerto solo en otros modos.
- **Nivel mínimo de software:**4.1+.



Puertos de tarjeta secundaria (9-12)
Los LED de los puertos 9 a 12 de la tarjeta base IP500 se utilizan de la siguiente manera:

- **Apagado**=No hay baúl presente.
- **Verde encendido**=Tronco presente.
- **Verde intermitente**=Tronco en uso.
- **Parpadeo rápido rojo/verde**(puerto 9) o**Parpadeo rápido verde**(puerto 10) = Señal de indicación de alarma (AIS) desde el extremo remoto troncal.
- **Rojo con parpadeo verde**(puerto 9) o**Parpadeo verde**(puerto 10) = Puerto en modo de bucle invertido (establecido a través de IP Office System Monitor).

- El LED 9 también se utiliza para el estado de la tarjeta secundaria.
  - **rojo encendido**=Error
  - **Parpadeo lento rojo**=Inicializando.
  - **Parpadeo rojo cada 5 segundos**=Tarjeta bien.
  - **Parpadeo rápido rojo**=Apagado del sistema.

Nombre	Descripción	Código SAP
IPO 500 TRNK PRI UNVRSL SNGL	IP Office 500 Tarjeta de líneas troncales Tasa primaria 1 Universal	700417439
IPO IP500 TRNK PRI UNVRSL SNGL TAA	"Ley de Acuerdos Comerciales 296variante compatible.	700501514
IPO 500 TRNK PRI UNIVRSL DOBLE	IP Office 500 Tarjeta de líneas troncales Tasa primaria 2 Universal	700417462
IPO IP500 TRNK PRI UNVSL DOBLE TAA	"Ley de Acuerdos Comerciales 296variante compatible.	700501517
IPO IP500 Troncal TARJETA T1(J) PRI DUAL JAPÓN	Tarjeta de interfaz doble T1(J)	700509377

¿Comentarios sobre este documento? infodev@avaya.com

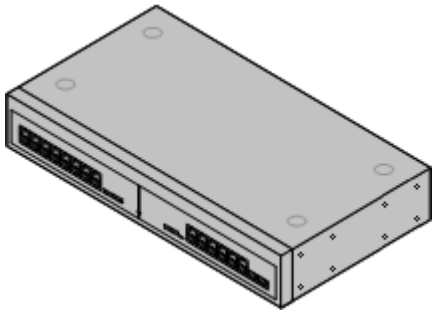
13.5 Módulos de expansión externos IP500

Los siguientes módulos de expansión externos IP500 son compatibles con la versión 11.0 de IP Office. Cada módulo utiliza un externo unidad de fuente de alimentación 30 suministrado con el módulo. Un lugar específicocable de alimentación 31para la fuente de alimentación debe pedirse por separado.

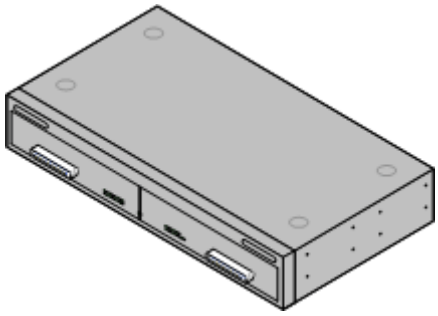
El módulo externo se puede apilar encima de la unidad de control. También se pueden montar en la pared o en un bastidor utilizando uno de losJuegos de montaje de IP Office 247.

- Los sistemas que se ejecutan en los modos estándar de IP Office admiten 8 módulos de expansión externos como estándar. Si está equipado con una tarjeta base de expansión de 4 puertos IP500, se admiten hasta 12 módulos de expansión externos.

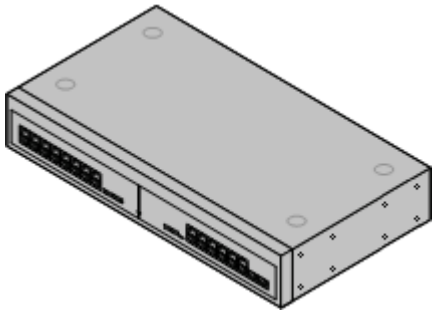
- **Módulos de estación digital IP500** 231
  Proporciona, según la variante, 16 o 30 RJ45 adicionalesSD soportado 271puertos para Teléfonos digitales Avaya DS 39.



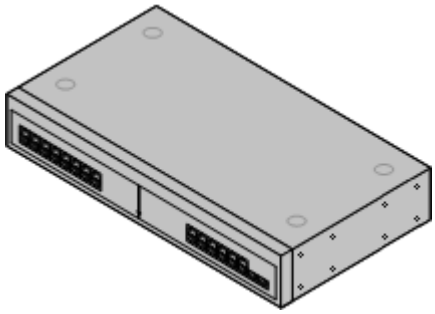
- **Módulos de estación digital A IP500** 233
  Proporciona, según variante, puertos RJ21 para la conexión de 16 o 30 adicionalesTeléfonos digitales Avaya BST 39.Solo compatible con IP500 V2.



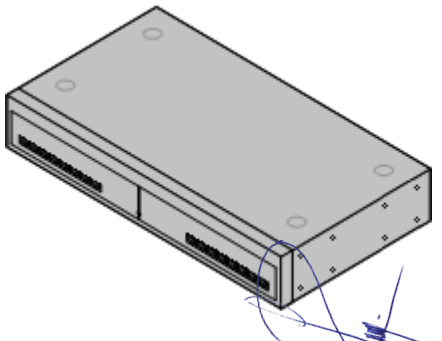
- **Módulos B/B2 de estación digital IP500** 236
  Proporciona, según la variante, 16 o 30 puertos RJ45 adicionales. Estos se pueden utilizar comoSD 271puertos para compatiblesTeléfonos digitales Avaya DS 39o BST 274puertos para compatiblesTeléfonos digitales Avaya BST 39.Sin embargo, el módulo solo puede admitir un tipo de puerto en cualquier momento. Para la versión 10.1 de IP Office, los módulos DS16B/DS30B fueron reemplazados por los modelos DS16B2/DS30B2.



- **Módulos telefónicos IP500** 238
  Proporciona, según la variante, 16 o 30 adicionalesTELÉFONO Conexión 276puertos para de teléfonos analógicos.



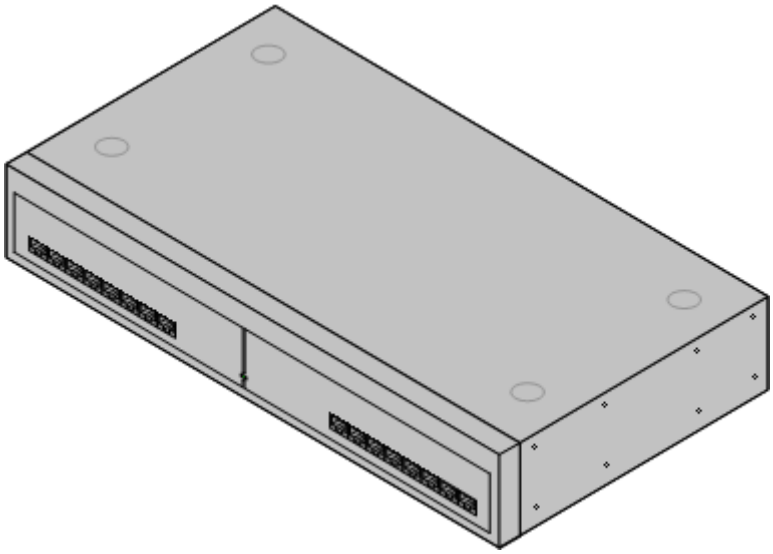
- **Módulo troncal analógico IP500** 229
  Proporciona 16 adicionalesCOSA ANÁLOGA 267Puertos para conexión de troncales analógicas. Admite troncales de inicio en bucle y de inicio en tierra.
  - El uso con troncales de inicio desde tierra requiere que el módulo de troncales y la unidad de control de IP Office estén conectados a tierra.
  - En IP Office Basic Edition - Modo PARTNER®, IP Office Basic Edition - Modo Norstar e IP Office Basic Editions, solo se admite 1 módulo de troncal analógica.



13.5.1 Troncal analógico 16

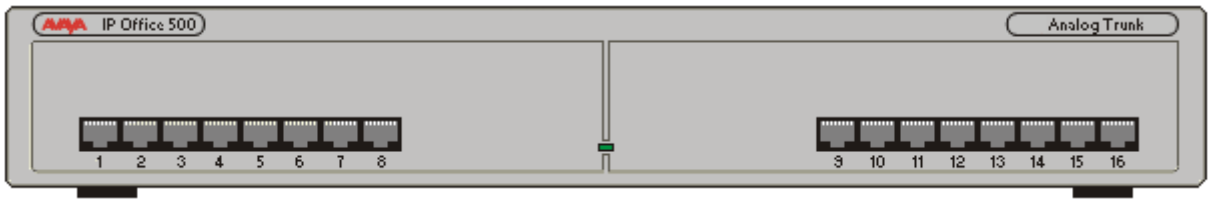
El módulo de troncales analógicas IP500 se puede usar para agregar 16 troncales analógicas adicionales a un sistema IP Office. El módulo admite tanto arranque en bucle como, con una conexión a tierra adecuada, troncales de arranque a tierra.

- En IP Office Basic Edition - Modo PARTNER®, IP Office Basic Edition - Modo Norstar e IP Office Basic Editions, solo se admite 1 módulo de troncal analógica.
  - **ADVERTENCIA**
    En todas las instalaciones de IP Office, cualquier módulo que se utilice para conexiones de troncales analógicas debe estar conectado a untierra funcional 35.
  - **ADVERTENCIA**
    Dentro de las áreas de alto riesgo de rayos, cualquier módulo que use conexiones troncales analógicas debe estar conectado a untierra protectora 35y paraequipo de protección contra sobretensiones 36.



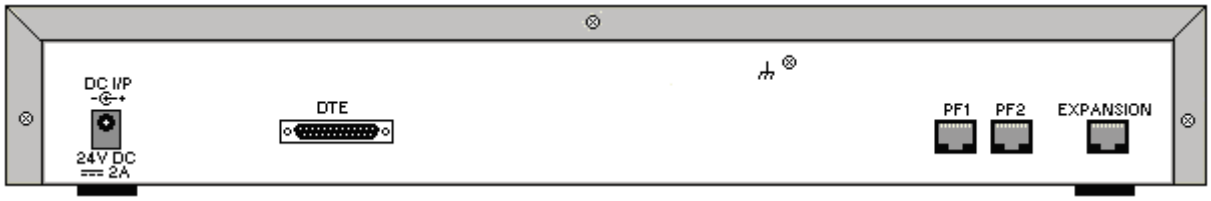
Rasgo	Detalles
locales	Actualmente, este módulo solo es compatible con las configuraciones regionales de América del Norte.
Software Mínimo Nivel	Nivel de software básico de IP Office 1.0 como mínimo. Archivo bin = naatm16.bin.
Incluido	Unidad de fuente de alimentación (consulte a continuación) y cable de interconexión de expansión.
Fuente de alimentación	El módulo se suministra con una fuente de alimentación externa de 2 pines y 40 W. La fuente de alimentación tiene un cable de alimentación integral para la conexión a la toma DC I/P del módulo. Un lugar específicoCable de alimentación IEC60320 C13 30 para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
Montaje	El módulo está diseñado como un módulo independiente que se puede apilar sobre o debajo de otros módulos de IP Office. El módulo se puede montar en la pared o en un bastidor utilizando elKIT DE MONTAJE DE RACK IPO IP500 V3 247.
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8"/2U.
Peso	Sin caja: 2,9 kg/6,6 libras. En caja: 4,2 kg/9,4 libras.

Frente del módulo



LED de puerto	Ninguna
Centro de módulos DIRIGIÓ	El LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **rojo intermitente**=Módulo iniciando/Cargando firmware. • **rojo encendido**=Error. • **Verde encendido**=Módulo bien.

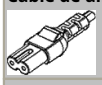
Parte trasera del módulo



Puertos	Descripción
COSA ANÁLOGA 267	Toma RJ45. Se utiliza para la conexión a troncales analógicas. Los puertos se pueden configurar como troncales de inicio por bucle o de inicio por tierra a través de la configuración de IP Office. En caso de corte de energía, los puertos analógicos 1 y 2 se conectan directamente a los puertos de extensión analógicos PF1 y PF2, respectivamente. Si se usan, los teléfonos conectados deben estar claramente etiquetados como dispositivos de corte de energía. Esto solo se admite para troncales analógicas de inicio de ciclo.
E/P CC 271	Puerto de entrada de alimentación de CC. Se utiliza para la conexión del cable de alimentación de una fuente de alimentación externa Avaya de 40 W suministrada con el módulo de expansión. Un lugar específicoCable de alimentación IEC60320 C7 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
DTE 278	Zócalo tipo D de 25 vías. Solo para uso de Avaya.
EXPANSIÓN 273	Enchufe RJ45. Se utiliza para la conexión directa a un puerto de expansión en una unidad de control de IP Office mediante el cable de interconexión de expansión suministrado con el módulo.
FP 275	Toma RJ45. Puertos de extensión analógica de falla de energía. Consulte la sección Analógica anterior.
	Punto de tierra. Se utiliza para la conexión de untierra funcional 35si es requerido. En módulos más antiguos donde este tornillo no está presente, se debe usar el tornillo de la cubierta superior central en su lugar. · IMPORTANTE En todas las instalaciones de IP Office, cualquier módulo que se utilice para conexiones de troncales analógicas debe estar conectado a untierra funcional 35. · ADVERTENCIA Dentro de las áreas de alto riesgo de rayos, cualquier módulo que use conexiones troncales analógicas debe estar conectado a un tierra protectora 35y paraequipo de protección contra sobretensiones 36.

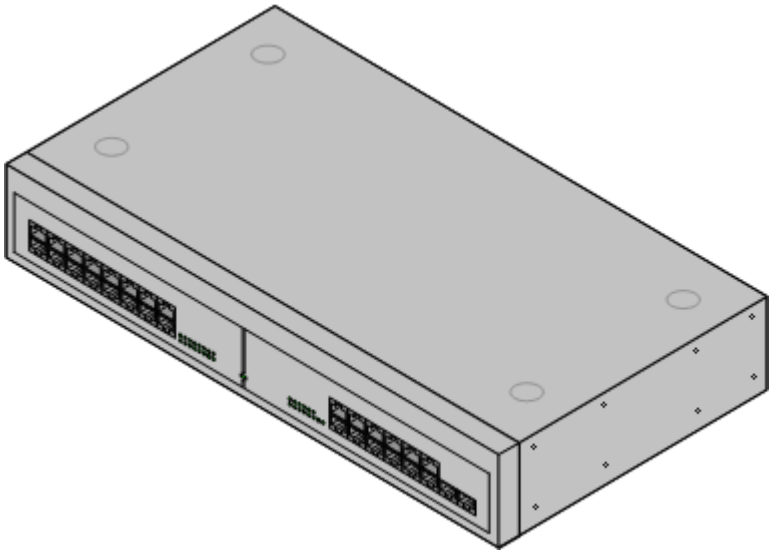
Códigos de piezas y equipos relacionados

Todos los módulos de expansión se suministran con un nivel de software base y deben actualizarse para que coincidan con el software central de la unidad de control en el sistema IP Office. Los módulos de expansión incluyen una unidad de fuente de alimentación (PSU) externa y un cable de interconexión adecuado. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

Artículo	Variante	País	Código SAP
IPO IP500 EXP MOD ANLG TRNK 16	**America**	America	700449473
IPO IP500 EXP MOD ANLG TRNK 16 TAA	"Acuerdos Comerciales Acto 396variante compatible.	America	700501511
Cable de alimentación IEC60320 C7 	**NEMA1-15**	America	700213390
Kit de montaje	**KIT DE MONTAJE EN PARED IPO IP500 V3**	Todos	700503160

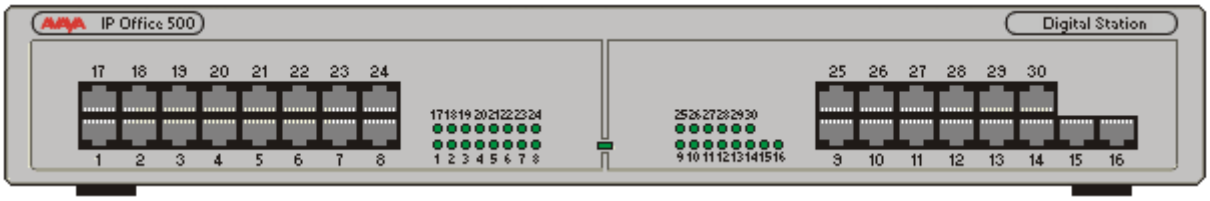
13.5.2 DS16/30

Los módulos de la estación digital IP Office 500 se pueden usar para agregarPuertos DS 271a un sistema IP Office para soporteAvaya Teléfonos digitales DS 39. El módulo está disponible en variantes de 16 y 30 puertos, denominados IP500 DS16 e IP500 DS30 respectivamente. Estos módulos también se conocen como módulos IP500 DS V2. Estos módulos han sido reemplazados por el IP500 DS16B/30B 236.



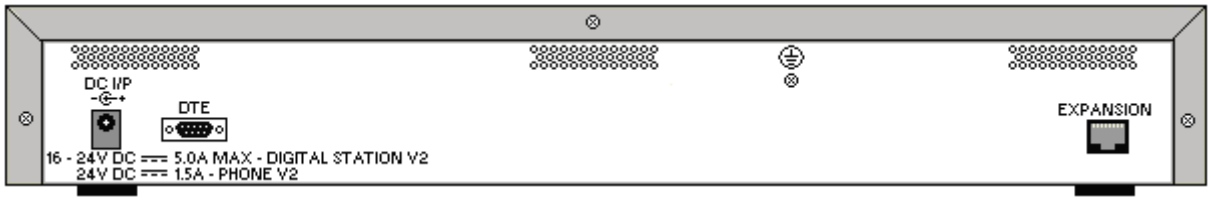
Rasgo	Detalles
locales	Apoyado en todoLocales de IP Office 42.
Mínimo Nivel de software	Nivel de software básico de IP Office 2.1(31) como mínimo. Archivo bin = nadcpV2.bin.
Incluido	Unidad de fuente de alimentación (consulte a continuación) y cable de interconexión de expansión.
Fuente de alimentación	El módulo se suministra con un módulo de fuente de alimentación externa de 60 W y 3 pines conectado a tierra. La fuente de alimentación tiene un cable de alimentación integral para la conexión a la toma DC I/P del módulo. Un lugar específicoCable de alimentación IEC60320 C13 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
Montaje	El módulo está diseñado como un módulo independiente que se puede apilar sobre o debajo de otros módulos de IP Office. El módulo se puede montar en la pared o en un bastidor utilizando elKIT DE MONTAJE DE RACK IPO IP500 V3 247.
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8".
Peso	Sin caja: 3,5 kg/7,8 libras. En caja: 4,8 kg/10,8 libras. (Basado en DS30)

Frente del módulo



LED de puerto	· **Verde intermitente**=Teléfono detectado. · **Verde encendido**=Teléfono activo.
Centro de módulos DIRIGIÓ	El LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: · **rojo intermitente**=Módulo iniciando/Cargando firmware. · **rojo encendido**=Error. · **Verde encendido**=Módulo bien.

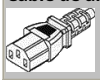
Parte trasera del módulo



Puerto	Descripción
E/P CC 271	Puerto de entrada de alimentación de CC. Se utiliza para la conexión del cable de alimentación de una fuente de alimentación externa de 60 W con conexión a tierra de Avaya suministrada con el módulo de expansión. Un lugar específicoCable de alimentación IEC60320 C13 para la fuente de alimentación externa es necesaria pero no se suministra con el módulo. 30
SD 271	Toma RJ45. Puerto de estación digital. Se utiliza para la conexión de IP Officeteléfonos DS compatibles 39.Si está conectado a unextensión fuera del edificio 36,la conexión debe realizarse mediante dispositivos de barrera IROB adicionales además de la protección primaria del edificio. El módulo también debe estar conectado a una tierra de protección.
DTE 278	Zócalo tipo D de 9 vías. Solo para uso de Avaya.
EXPANSIÓN 273	Enchufe RJ45. Se utiliza para la conexión directa a un puerto de expansión en una unidad de control de IP Office mediante el cable de interconexión de expansión suministrado con el módulo.
⏚	Punto de tierra de protección. Se requiere el uso de una tierra protectora para todas las instalaciones, consultePuesta a tierra (puesta a tierra) 93.Cuando el módulo está conectado a extensiones analógicas en otro edificio, se requiere una IP Office Phone Barrier Box V2 (101 V) en ambos extremos, consulteProtección contra rayos/Conexiones fuera del edificio 36.

Códigos de piezas y equipos relacionados

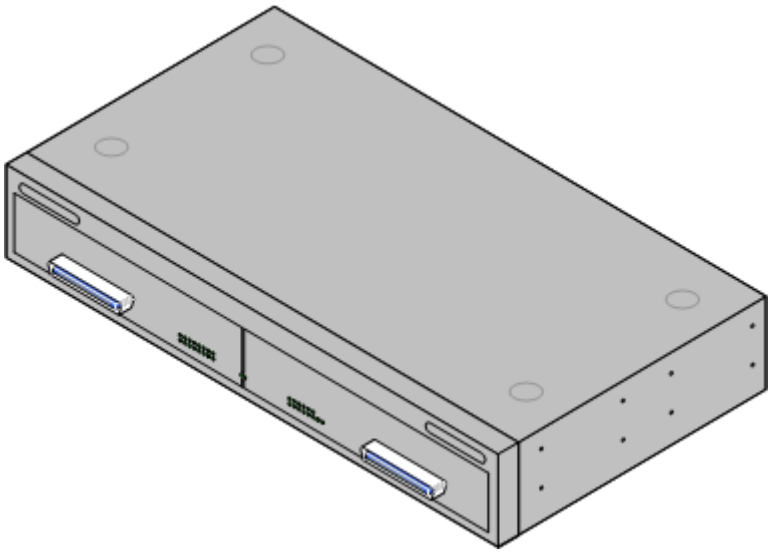
Todos los módulos de expansión se suministran con un nivel de software base y deben actualizarse para que coincidan con el software central de la unidad de control en el sistema IP Office. Los módulos de expansión incluyen una unidad de fuente de alimentación (PSU) externa y un cable de interconexión adecuado. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

Artículo	Variante	País	Código SAP
IPO IP500 EXP MOD DGTL ESTA 16	**16 puertos**	Todos	700449499
IPO IP500 EXP MOD DGTL STA 16 TAA	"Ley de Acuerdos Comerciales 296obediente variante.		–
IPO IP500 EXP MOD DGTL STA 30	**30 puertos**		700426216
Cable de alimentación IEC60320 C13 	**CEE7/7**	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	America	700289770
Kit de montaje	**KIT DE MONTAJE EN PARED IPO IP500 V3**	Todos	700503160

13.5.3 DS16A/30A

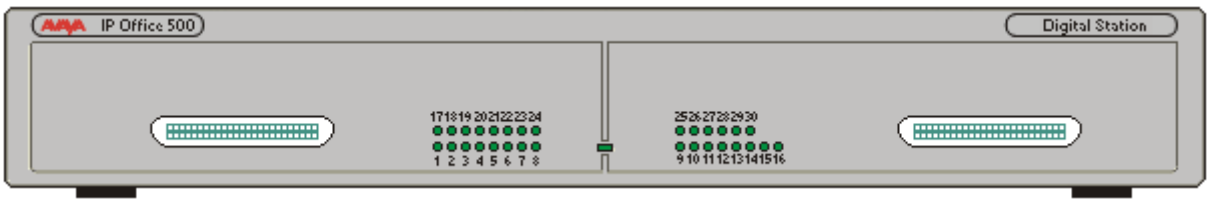
Estos módulos se pueden utilizar para agregarPuertos BST 270para apoyadoTeléfonos digitales Avaya BST 39.el módulo es disponible en variantes de 16 y 30 puertos, denominadas IP500 DS16A e IP500 DS30A respectivamente.

Los módulos utilizan conectores RJ21; 1 en la versión de 16 puertos, 2 en la versión de 30 puertos. Para conexiones BST usando el puerto RJ45, use elMódulos IP500 DS16B/30B 236.



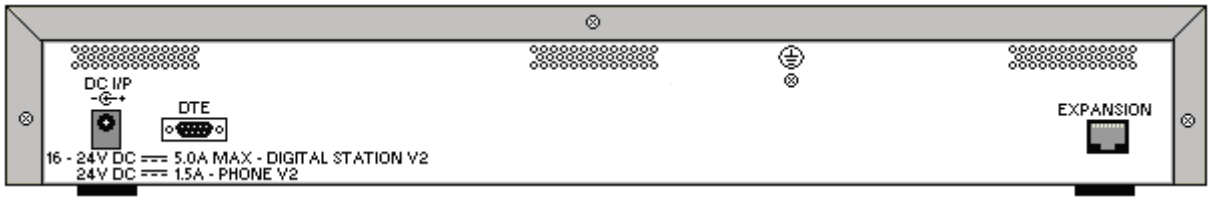
Rasgo	Detalles
locales	Apoyado en todoLocales de IP Office 42.
Mínimo Nivel de software	Versión 7.0 de IP Office como mínimo (solo BST). Archivo bin = nadcpaV1.bin.
Incluido	Unidad de fuente de alimentación (consulte a continuación) y cable de interconexión de expansión.
Fuente de alimentación	El módulo se suministra con un módulo de fuente de alimentación externa de 60 W y 3 pines conectado a tierra. La fuente de alimentación tiene un cable de alimentación integral para la conexión a la toma DC I/P del módulo. Un lugar específicoCable de alimentación IEC60320 C13 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
Montaje	El módulo está diseñado como un módulo independiente que se puede apilar sobre o debajo de otros módulos de IP Office. El módulo se puede montar en la pared o en un bastidor utilizando elKIT DE MONTAJE DE RACK IPO IP500 V3 247.
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8".
Peso	Sin caja: 3,5 kg/7,8 libras. En caja: 4,8 kg/10,8 libras. (Basado en DS30A RJ21)

Frente del módulo



LED de puerto	• **Verde encendido**=Teléfono detectado.
Centro de módulos DIRIGIÓ	El LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **rojo intermitente**=Módulo iniciando/Cargando firmware. • **rojo encendido**=Error. • **Verde encendido**=Módulo bien. • **Verde intermitente**=Módulo iniciando/Cargando firmware (solo módulo IP500 DS16A/30A).

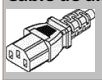
Parte trasera del módulo



Puertos	Descripción
E/P CC 271	Puerto de entrada de alimentación de CC. Se utiliza para la conexión del cable de alimentación de una fuente de alimentación externa de 60 W con conexión a tierra de Avaya suministrada con el módulo de expansión. Un lugar específicoCable de alimentación IEC60320 C13 para la fuente de alimentación externa es necesaria pero no se suministra con el módulo. 30
RJ21 270	Para la versión 7.0 de IP Office, los módulos solo admiten teléfonos que requierenPuertos BST 270.
DTE 278	Zócalo tipo D de 9 vías. Solo para uso de Avaya.
EXPANSIÓN 273	Enchufe RJ45. Se utiliza para la conexión directa a un puerto de expansión en una unidad de control de IP Office mediante el cable de interconexión de expansión suministrado con el módulo.
⏚	Punto de tierra de protección. Se requiere el uso de una tierra protectora para todas las instalaciones, consultePuesta a tierra (puesta a tierra) 93.Cuando el módulo está conectado a extensiones analógicas en otro edificio, se requiere una IP Office Phone Barrier Box V2 (101 V) en ambos extremos, consulteProtección contra rayos/Conexiones fuera del edificio 36.

Códigos de piezas y equipos relacionados

Todos los módulos de expansión se suministran con un nivel de software base y deben actualizarse para que coincidan con el software central de la unidad de control en el sistema IP Office. Los módulos de expansión incluyen una unidad de fuente de alimentación (PSU) externa y un cable de interconexión adecuado. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

Artículo	Variante	País	Código SAP
Estación digital IPO 500 16A RJ21 CONJUNTO DE UNIDAD	**RJ21**	Todos	700500699
Estación digital IPO 500 30A RJ21 CONJUNTO DE UNIDAD	**RJ21**		700500698
Cable de alimentación IEC60320 C13 	**CEE7/7**	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	América del norte	700289770
Kit de montaje	**KIT DE MONTAJE EN PARED IPO IP500 V3**	Todos	700503160

Asignación de pines del cable RJ21

El siguiente pin-out se utiliza para los puertos RJ21.

1er Conector RJ21

Puerto		Alfiler	Cable
1	Consejo	26	Blanco azul
	Anillo	1	Azul blanco
2	Consejo	27	Blanco/Naranja
	Anillo	2	Naranja/Blanco
3	Consejo	28	Blanco verde
	Anillo	3	Verde blanco
4	Consejo	29	Blanco/Marrón
	Anillo	4	Cafe Blanco
5	Consejo	30	Blanco/Pizarra
	Anillo	5	Pizarra/Blanco
6	Consejo	31	Rojo azul
	Anillo	6	Azul rojo
7	Consejo	32	Naranja roja
	Anillo	7	Rojo naranja
8	Consejo	33	Rojo verde
	Anillo	8	Verde rojo
9	Consejo	34	Rojo marrón
	Anillo	9	Rojo marrón
10	Consejo	35	Rojo/Pizarra
	Anillo	10	Pizarra/Rojo
11	Consejo	36	Azul negro
	Anillo	11	Azul negro
12	Consejo	37	Negro/Naranja
	Anillo	12	Naranja/Negro
13	Consejo	38	Verde negro
	Anillo	13	Verde/Negro
14	Consejo	39	Marrón oscuro
	Anillo	14	Marrón/Negro
15	Consejo	40	Negro/Pizarra
	Anillo	15	Pizarra/Negro
dieciséis	Consejo	41	Amarillo azul
	Anillo	dieciséis	Azul amarillo
No utilizado		42	Amarillo naranja
		17	Naranja amarillo
		43	Violeta/Pizarra
		08	Pizarra/Violeta

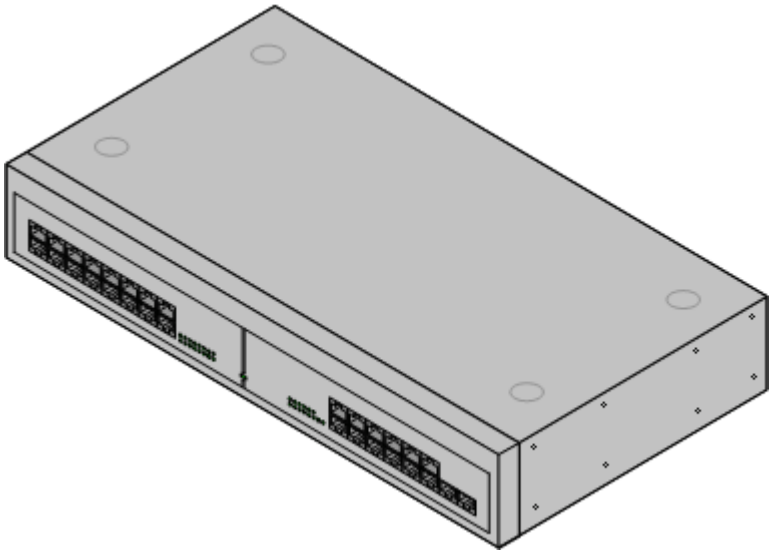
2do conector RJ21

Puerto		Alfiler	Cable
17	Consejo	26	Blanco azul
	Anillo	1	Azul blanco
18	Consejo	27	Blanco/Naranja
	Anillo	2	Naranja/Blanco
19	Consejo	28	Blanco verde
	Anillo	3	Verde blanco
20	Consejo	29	Blanco/Marrón
	Anillo	4	Cafe Blanco
21	Consejo	30	Blanco/Pizarra
	Anillo	5	Pizarra/Blanco
22	Consejo	31	Rojo azul
	Anillo	6	Azul rojo
23	Consejo	32	Naranja roja
	Anillo	7	Rojo naranja
24	Consejo	33	Rojo verde
	Anillo	8	Verde rojo
25	Consejo	34	Rojo marrón
	Anillo	9	Rojo marrón
26	Consejo	35	Rojo/Pizarra
	Anillo	10	Pizarra/Rojo
27	Consejo	36	Azul negro
	Anillo	11	Azul negro
28	Consejo	37	Negro/Naranja
	Anillo	12	Naranja/Negro
29	Consejo	38	Verde negro
	Anillo	13	Verde/Negro
30	Consejo	39	Marrón oscuro
	Anillo	14	Marrón/Negro
No utilizado		40	Negro/Pizarra
		15	Pizarra/Negro
		41	Amarillo azul
		dieciséis	Azul amarillo
		42	Amarillo naranja
		17	Naranja amarillo
		43	Violeta/Pizarra
		08	Pizarra/Violeta

13.5.4 DS16B/30B, DS16B2/30B2

Este tipo de módulo se puede utilizar para agregar puertos RJ45 adicionales para teléfonos digitales. A través de la configuración del sistema, cada módulo se establece en[SD](271)modo de apoyo[Teléfonos digitales Avaya DS](39)o[BST](274)puertos de modo para compatibles [Teléfonos digitales Avaya BST](39)(Puertos DS solo en unidades de control IP500). Ver[Selección de modo de puerto DS16B2/30B2](110).

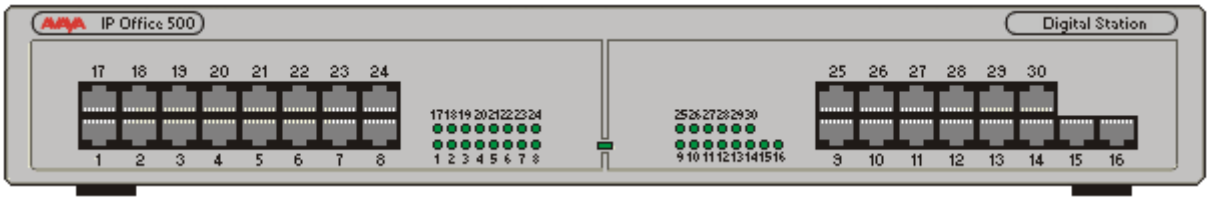
Los módulos están disponibles en variantes de 16 y 30 puertos, denominados IP500 DS16B e IP500 DS30B respectivamente. Los modelos DS16B y DS30B ahora han sido reemplazados por los modelos DS16B2 y DS30B2 que brindan la misma funcionalidad.



Rasgo	Detalles
locales	Apoyado en todo[Locales de IP Office](42)
Mínimo Nivel de software	· **DS16B/DS30B:**IP Office versión 9.0. IP500 (solo DS) e IP500 V2 (DS o TCM). Para la versión 8.1 de IP Office (Service Pack 9+), estos módulos solo admiten puertos DS. · **DS16B2/DS30B2:**Versión de IP Office 10.1. También versión de IP Office 9.1 SP12 y versión de IP Office 10.0 SP5.
Incluido	Unidad de fuente de alimentación (consulte a continuación) y cable de interconexión de expansión.
Fuente de alimentación	El módulo se suministra con un módulo de fuente de alimentación externa de 60 W y 3 pines conectado a tierra. La fuente de alimentación tiene un cable de alimentación integral para la conexión a la toma DC I/P del módulo. Un lugar específico[Cable de alimentación IEC60320 C13](30)para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
Montaje	El módulo está diseñado como un módulo independiente que se puede apilar sobre o debajo de otros módulos de IP Office. El módulo se puede montar en la pared o en un bastidor utilizando el[KIT DE MONTAJE DE RACK IPO IP500 V3](247).
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8".
Peso	Sin caja: 3,5 kg/7,8 libras. En caja: 4,8 kg/10,8 libras. (Basado en DS30)

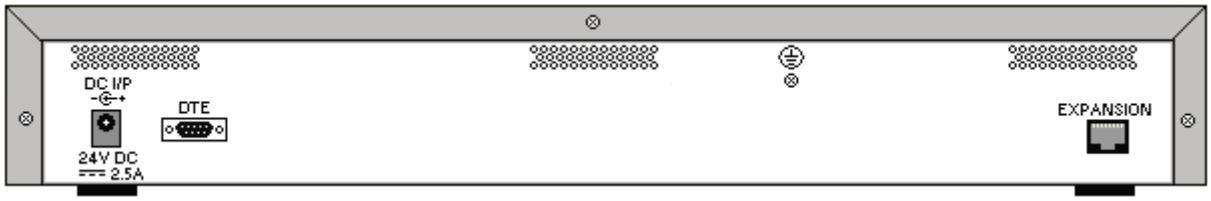
- **Comportamiento de actualización de DS16B/DS30B:**
  Para los módulos DS16B/DS30B, el proceso de carga del firmware apropiado para el modo seleccionado o la actualización demora hasta 10 minutos, tiempo durante el cual el módulo no está disponible.
- **Comportamiento de actualización de DS16B2/DS30B2:**
  El comportamiento de DS16/30B2 durante la actualización del firmware o el cambio de modos difiere de otras unidades de expansión externas:
  - Durante la actualización del firmware, la unidad permanece operativa y puede realizar y recibir llamadas.
  - Una vez que se completa la actualización (aproximadamente 9 minutos), la unidad se reinicia y tarda unos 45 segundos en volver al funcionamiento normal.

Frente del módulo



LED de puerto	· **Verde intermitente**=Teléfono detectado. · **Verde encendido**=Teléfono activo.
Centro de módulos DIRIGIÓ	El LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: · **rojo intermitente**=Módulo iniciando/Cargando firmware. · **rojo encendido**=Error. · **Verde encendido**=Módulo bien.

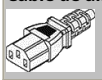
Parte trasera del módulo



Puerto	Descripción
E/P CC 271	Puerto de entrada de alimentación de CC. Se utiliza para la conexión del cable de alimentación de una fuente de alimentación externa de 60 W con conexión a tierra de Avaya suministrada con el módulo de expansión. Un lugar específicoCable de alimentación IEC60320 C13 para la fuente de alimentación externa es necesaria pero no se suministra con el módulo. 30
SD 271	Toma RJ45. Puerto de estación digital. Se utiliza para la conexión de IP Officeteléfonos DS compatibles 39.Si está conectado a unextensión fuera del edificio 36,la conexión debe realizarse mediante dispositivos de barrera IROB adicionales además de la protección primaria del edificio. El módulo también debe estar conectado a una tierra de protección.
DTE 278	Zócalo tipo D de 9 vías. Solo para uso de Avaya.
EXPANSIÓN 273	Enchufe RJ45. Se utiliza para la conexión directa a un puerto de expansión en una unidad de control de IP Office mediante el cable de interconexión de expansión suministrado con el módulo.
⏚	Punto de tierra de protección. Se requiere el uso de una tierra protectora para todas las instalaciones, consultePuesta a tierra (puesta a tierra) 93.Cuando el módulo está conectado a extensiones analógicas en otro edificio, se requiere una IP Office Phone Barrier Box V2 (101 V) en ambos extremos, consulteProtección contra rayos/Conexiones fuera del edificio 36.

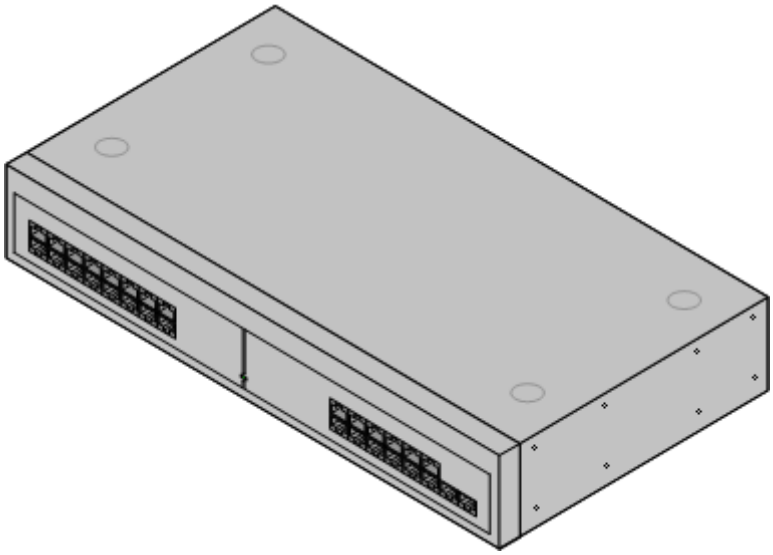
Códigos de piezas y equipos relacionados

Todos los módulos de expansión se suministran con un nivel de software base y deben actualizarse para que coincidan con el software central de la unidad de control en el sistema IP Office. Los módulos de expansión incluyen una unidad de fuente de alimentación (PSU) externa y un cable de interconexión adecuado. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

Artículo	Variante	País	Código SAP
IPO IP500 EXP MOD DS16B DGTL ST	**16 puertos**	Todos	700501585
IPO IP500 EXP MOD DS30B DGTL ST	**30 puertos**	Todos	700501586
IPO IP500 EXP MOD DS16B2 DGTL ST	**16 puertos**	Todos	700511093
IPO IP500 EXP MOD DS30B2 DGTL ST	**30 puertos**	Todos	700511094
Cable de alimentación IEC60320 C13 	**CEE7/7**	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	America	700289770
Kit de montaje	**KIT DE MONTAJE EN PARED IPO IP500 V3**	Todos	700503160

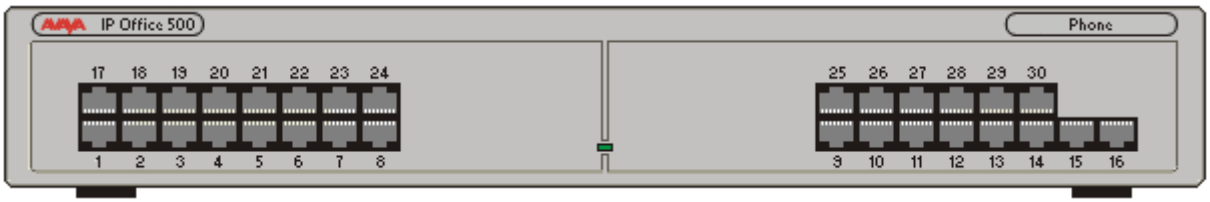
13.5.5 Teléfono 16/30

Los módulos de teléfono IP500 se pueden usar para agregar puertos de TELÉFONO adicionales a un sistema IP Office. El módulo está disponible en variantes de 16 y 30 puertos, denominados IP500 Phone 16 e IP500 Phone 30 respectivamente.



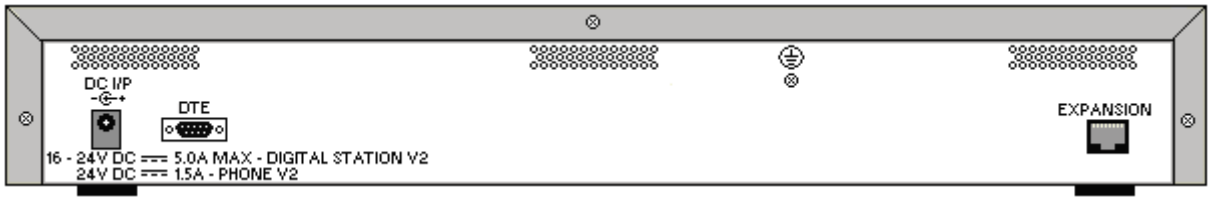
Rasgo	Detalles
locales	Apoyado en todoLocales de IP Office 42.
Software Mínimo Nivel	Nivel de software básico de IP Office 2.1(36) como mínimo. Archivo bin = dvpots.bin.
Incluido	Unidad de fuente de alimentación (consulte a continuación) y cable de interconexión de expansión.
Fuente de alimentación	El módulo se suministra con una fuente de alimentación externa de 3 pines y 60 W conectada a tierra. La fuente de alimentación tiene un cable de alimentación integral para la conexión a la toma DC I/P del módulo. Un lugar específicoCable de alimentación IEC60320 C13 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
Montaje	El módulo está diseñado como un módulo independiente que se puede apilar sobre o debajo de otros módulos de IP Office. El módulo se puede montar en la pared o en un bastidor utilizando elKIT DE MONTAJE DE RACK IPO IP500 V3 247.
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8".
Peso	Sin caja: 3,1 kg/6,94 libras. En caja: 4,4 kg/9,7 libras. (Basado en el teléfono 30 V2)

Frente del módulo



Centro de módulos DIRIGIÓ	El LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: · **rojo intermitente**=Módulo iniciando/Cargando firmware. · **rojo encendido**=Error. · **Verde encendido**=Módulo bien. · **Verde intermitente**=Módulo iniciando/Cargando firmware (solo módulo IP500 DS16A/30A).

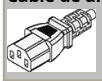
Parte trasera del módulo



Puertos	Descripción
E/P CC 271	Puerto de entrada de alimentación de CC. Se utiliza para la conexión del cable de alimentación de una fuente de alimentación externa de 60 W con conexión a tierra de Avaya suministrada con el módulo de expansión. Un lugar específicoCable de alimentación IEC60320 C13 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
DTE 278	Zócalo tipo D de 9 vías. Solo para uso de Avaya.
EXPANSIÓN 273	Enchufe RJ45. Se utiliza para la conexión directa a un puerto de expansión en una unidad de control de IP Office mediante el cable de interconexión de expansión suministrado con el módulo.
TELÉFONO 276	Toma RJ45. Se utiliza para la conexión de teléfonos analógicos. Diseñado para teléfonos analógicos de dos hilos. Para la conexión a teléfonos analógicos de 4 hilos, la conexión debe realizarse a través de un enchufe maestro con condensadores de llamada. Si está conectado a unextensión fuera del edificio 36la conexión debe realizarse a través deCajas de barrera de IP Office 189además de la protección primaria de los edificios. El módulo también debe estar conectado a una tierra de protección.
⏚	Punto de tierra de protección. Se requiere el uso de una tierra protectora para todas las instalaciones, consultePuesta a tierra (puesta a tierra) 35.Cuando el módulo está conectado a extensiones analógicas en otro edificio, se requiere una IP Office Phone Barrier Box V2 (101 V) en ambos extremos, consulteProtección contra rayos/Conexiones fuera del edificio 36.

Códigos de piezas y equipos relacionados

Todos los módulos de expansión se suministran con un nivel de software base y deben actualizarse para que coincidan con el software central de la unidad de control en el sistema IP Office. Los módulos de expansión incluyen una unidad de fuente de alimentación (PSU) externa y un cable de interconexión adecuado. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

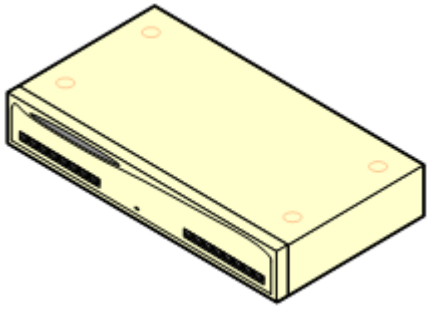
Artículo	Variante	País	Código SAP
IPO IP500 EXP MOD TELÉFONO 16	**16 puertos**	Todos	700449507
IPO IP500 EXP MOD TELÉFONO 30	**30 puertos**	Todos	700426224
Cable de alimentación IEC60320 C13 	**CEE7/7**	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	America	700289770
Kit de montaje	**KIT DE MONTAJE EN PARED IPO IP500 V3**	Todos	700503160
CAJA DE BARRERA TELÉFONO IPO (101V) RHS		Todos	700385495

13.6 Módulos de expansión IP400

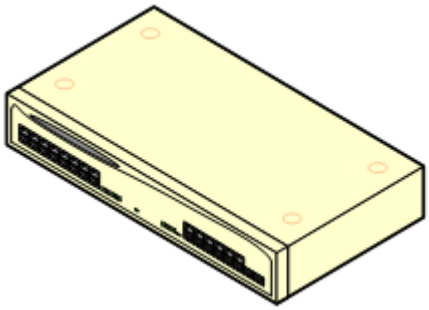
Los siguientes módulos de expansión externos IP400 son compatibles con la versión 11.0 de IP Office y se pueden usar con unidades de control IP500 V2. Cada módulo utiliza un externounidad de fuente de alimentación 30suministrado con el módulo. Un lugar específicocable de alimentación 31para la fuente de alimentación debe pedirse por separado.

Si se van a montar en bastidor, estas unidades utilizan el kit de montaje en bastidor IP400. Si se montan en rack, estas unidades utilizan el KIT DE MONTAJE EN RACK IPO IP500. No se pueden montar en la pared.

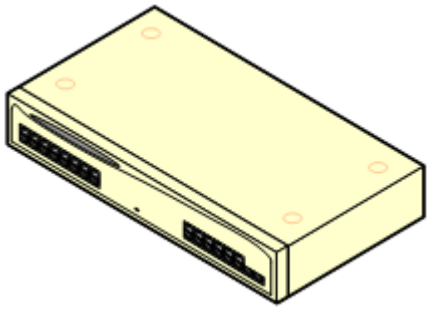
- **Módulo troncal analógico IP400 (ATM16)** 241
  Proporciona 16 adicionalesCOSA ANÁLOGA 267Puertos para conexión de troncales analógicas. Admite troncales de inicio en bucle y de inicio en tierra.
  - Disponible en una serie de variantes para diferentes lugares.
  - El uso con troncales de inicio desde tierra requiere que el módulo de troncales y la unidad de control de IP Office estén conectados a tierra.



- **Módulo de estación digital IP400 V2** 243
  Proporciona, según la variante, 16 o 30 adicionalesSD 271puertos para soportadoTeléfonos digitales Avaya 39.Reemplaza el módulo de Estación Digital anterior.



- **Módulo telefónico IP400 V2** 245
  Proporciona, según la variante, 16 o 30 adicionalesTELÉFONO 276puertos para teléfonos analógicos. Reemplaza el módulo Teléfono anterior. Con IP Office 3.1, Phone V2 admite una gama más amplia de opciones de indicación de mensaje en espera (MWI) que los módulos Phone V1.

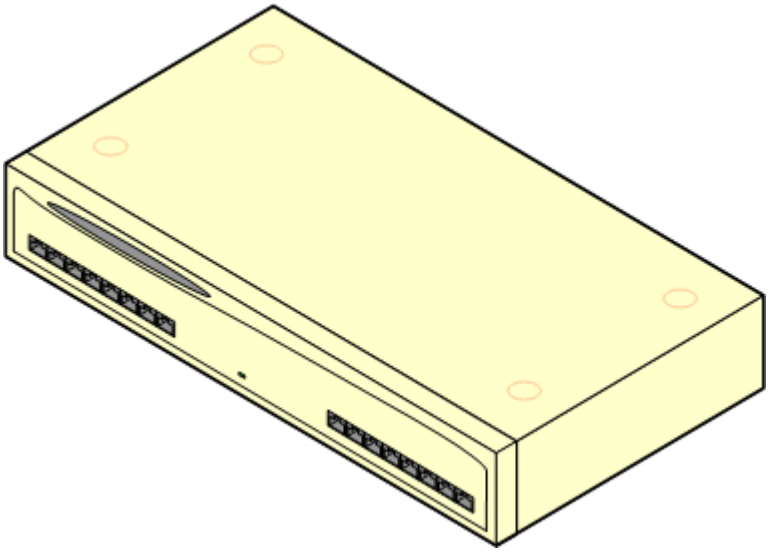


13.6.1 Troncal analógico 16

El módulo de troncales analógicas IP400 (también conocido como ATM16) se utiliza para agregar 16 troncales analógicas adicionales a un sistema IP Office.
El módulo admite tanto arranque en bucle como, con una conexión a tierra adecuada, troncales de arranque a tierra.

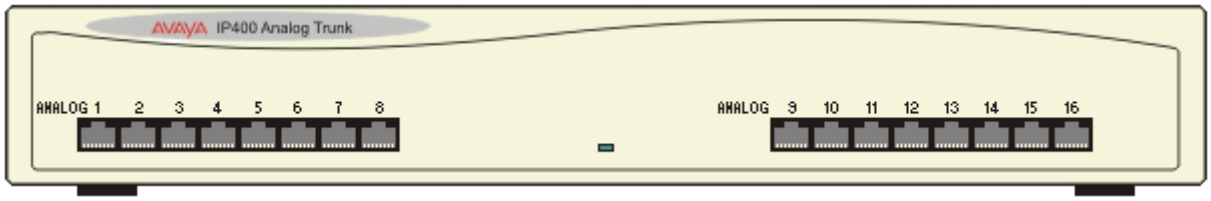
- **ADVERTENCIA**
  En todas las instalaciones de IP Office, cualquier módulo que se utilice para conexiones de troncales analógicas debe estar conectado a untierra funcional 35.

- **ADVERTENCIA**
  Dentro de la República de Sudáfrica y en áreas de alto riesgo de rayos, cualquier módulo que use conexiones troncales analógicas debe estar conectado a untierra protectora 35y paraequipo de protección contra sobretensiones 36.

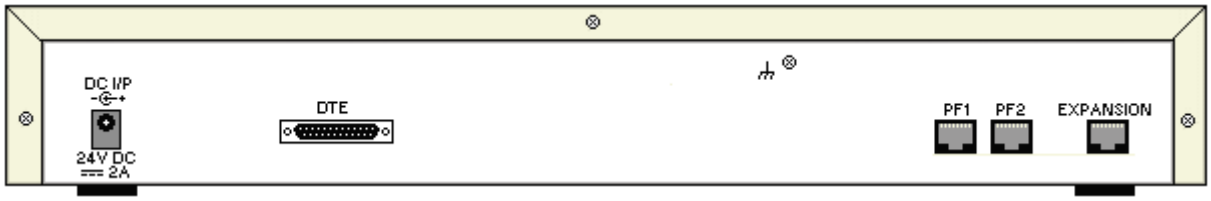


Rasgo	Detalles
locales	Se proporcionan variantes específicas para diferentes configuraciones regionales de IP Office, consulte a continuación.
Software Mínimo Nivel	Nivel de software básico de IP Office 1.0 como mínimo. Archivo bin = naatm16.bin.
Incluido	Unidad de fuente de alimentación (consulte a continuación) y cable de interconexión de expansión.
Fuente de alimentación	El módulo se suministra con una fuente de alimentación externa de 2 pines y 40 W. La fuente de alimentación tiene un cable de alimentación integral para la conexión a la toma DC I/P del módulo. Un lugar específicoCable de alimentación IEC60320 C13 30 para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
Montaje	El módulo está diseñado como un módulo independiente que se puede apilar sobre o debajo de otros módulos de IP Office. El módulo se puede montar en rack en un sistema de rack de 19" utilizando el kit de montaje en rack IP400 opcional.
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8"/2U.
Peso	Sin caja: 2,9 kg/6,6 libras. En caja: 4,2 kg/9,4 libras.

Frente del módulo



Parte trasera del módulo



Puertos	Descripción
COSA ANÁLOGA 267	Toma RJ45. Se utiliza para la conexión a troncales analógicas. Los puertos se pueden configurar como troncales de inicio por bucle o de inicio por tierra a través de la configuración de IP Office. En caso de corte de energía, los puertos analógicos 1 y 2 se conectan directamente a los puertos de extensión analógicos PF1 y PF2, respectivamente. Si se usan, los teléfonos conectados deben estar claramente etiquetados como dispositivos de corte de energía. Esto solo se admite para troncales analógicas de inicio de ciclo.
E/P CC 271	Puerto de entrada de alimentación de CC. Se utiliza para la conexión del cable de alimentación de una fuente de alimentación externa Avaya de 40 W suministrada con el módulo de expansión. Un lugar específicoCable de alimentación IEC60320 C7 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
DTE 278	Zócalo tipo D de 25 vías. Solo para uso de Avaya.
EXPANSIÓN 273	Enchufe RJ45. Se utiliza para la conexión directa a un puerto de expansión en una unidad de control de IP Office mediante el cable de interconexión de expansión suministrado con el módulo.
FP 275	Toma RJ45. Puertos de extensión analógica de falla de energía. Consulte la sección Analógica anterior.
	Punto de tierra. Se utiliza para la conexión de untierra funcional 35si es requerido. En módulos más antiguos donde este tornillo no está presente, se debe usar el tornillo de la cubierta superior central en su lugar. · IMPORTANTE En todas las instalaciones de IP Office, cualquier módulo que se utilice para conexiones de troncales analógicas debe estar conectado a untierra funcional 35. · ADVERTENCIA Dentro de la República de Sudáfrica y en áreas de alto riesgo de rayos, cualquier módulo que use conexiones troncales analógicas debe estar conectado a untierra protectora 35y paraequipo de protección contra sobretensiones 36.

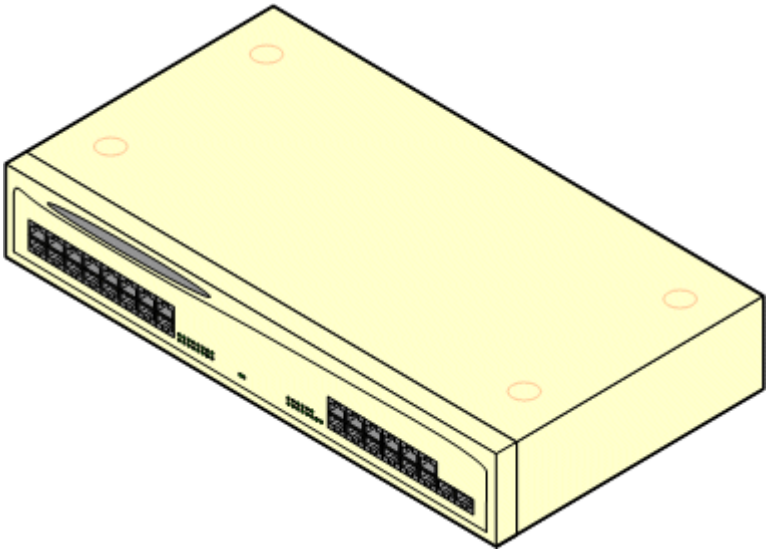
Códigos de piezas y equipos relacionados

Todos los módulos de expansión se suministran con un nivel de software base y deben actualizarse para que coincidan con el software central de la unidad de control en el sistema IP Office. Los módulos de expansión incluyen una unidad de fuente de alimentación (PSU) externa y un cable de interconexión adecuado. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

Artículo	Variante	País	Código SAP
Troncal analógico IP400 16	America	America	700211360
	Europa	Europa	700241680
	Nueva Zelanda	Nueva Zelanda	700241698
Cable de alimentación IEC60320 C7	CEE7/16	Europa	700213382
	BS1363	Reino Unido	700213374
	NEMA1-15	America	700213390
	Corea	Corea	700254519
Kit de montaje en bastidor IP400		Todos	700210800

13.6.2 Estación Digital V2

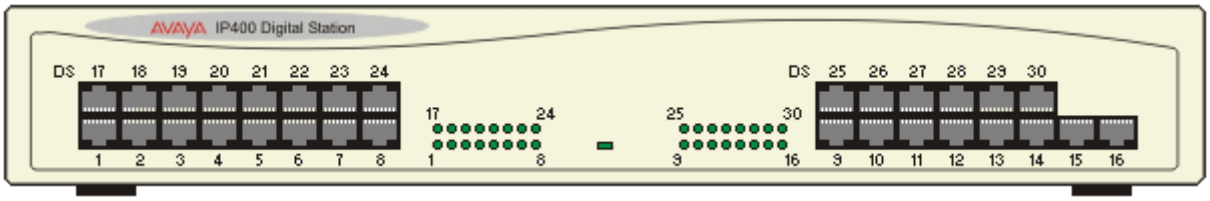
La estación digital IP400 V2 (también conocida como DS V2) se usa para agregar puertos DS adicionales a un sistema IP Office. El DS V2 está disponible en variantes de 16 y 30 puertos, denominadas DS16 V2 y DS30 V2 respectivamente.



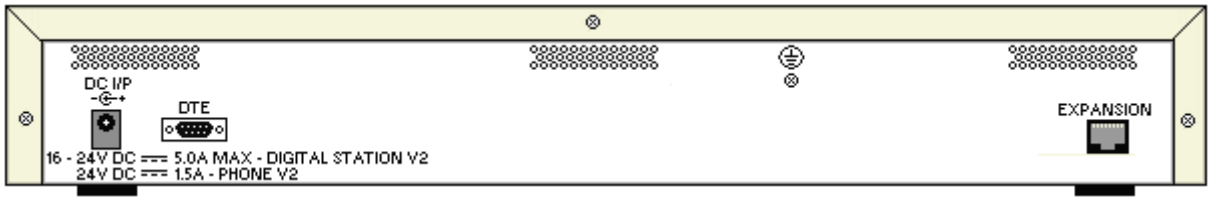
El DS V2 reemplaza a la estación digital IP400 original, ahora conocida como DS V1. La versión del módulo se indica mediante etiquetas tanto en la base como en la parte trasera del módulo.

Rasgo	Detalles
locales	Apoyado en todoLocales de IP Office 42.
Software Mínimo Nivel	Nivel de software básico de IP Office 2.1(31) como mínimo. Archivo bin = nadcpV2.bin.
Incluido	Unidad de fuente de alimentación (consulte a continuación) y cable de interconexión de expansión.
Fuente de alimentación	El módulo se suministra con un módulo de fuente de alimentación externa de 60 W y 3 pines conectado a tierra. La fuente de alimentación tiene un cable de alimentación integral para la conexión a la toma DC I/P del módulo. Un lugar específicoCable de alimentación IEC60320 C13 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
Montaje	El módulo está diseñado como un módulo independiente que se puede apilar sobre o debajo de otros módulos de IP Office. El módulo se puede montar en rack en un sistema de rack de 19" utilizando el kit de montaje en rack IP400 opcional.
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8"/2U.
Peso	Sin caja: 3,5 kg/7,8 libras. En caja: 4,8 kg/10,8 libras. (Basado en DS30 V2)

Frente del módulo



Parte trasera del módulo



Puertos	Descripción
E/P CC 271	Puerto de entrada de alimentación de CC. Se utiliza para la conexión del cable de alimentación de una fuente de alimentación externa de 60 W con conexión a tierra de Avaya suministrada con el módulo de expansión. Un lugar específicoCable de alimentación IEC60320 C13 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
SD 271	Toma RJ45. Puerto de estación digital. Se utiliza para la conexión de IP Officeteléfonos DS compatibles 39.Si está conectado a un extensión fuera del edificio 36,la conexión debe realizarse mediante dispositivos de barrera IROB adicionales además de la protección primaria del edificio. El módulo también debe estar conectado a una tierra de protección.
DTE 278	Zócalo tipo D de 9 vías. Solo para uso de Avaya.
EXPANSIÓN 273	Enchufe RJ45. Se utiliza para la conexión directa a un puerto de expansión en una unidad de control de IP Office mediante el cable de interconexión de expansión suministrado con el módulo.
⏚	Punto de tierra de protección. Se requiere el uso de una tierra protectora para todas las instalaciones, consultePuesta a tierra (puesta a tierra) 35.Cuando el módulo está conectado a extensiones analógicas en otro edificio, se requiere una IP Office Phone Barrier Box V2 (101 V) en ambos extremos, consulteProtección contra rayos/Conexiones fuera del edificio 36.

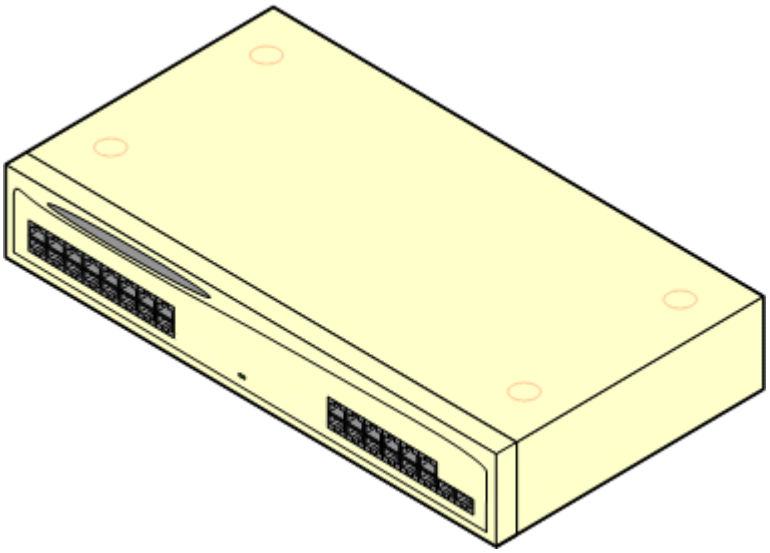
Códigos de piezas y equipos relacionados

Todos los módulos de expansión se suministran con un nivel de software base y deben actualizarse para que coincidan con el software central de la unidad de control en el sistema IP Office. Los módulos de expansión incluyen una unidad de fuente de alimentación (PSU) externa y un cable de interconexión adecuado. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

Artículo	Variante	País	Código SAP
Estación digital IP400 V2	16 puertos	Todos	700359839
	30 puertos		700359847
Cable de alimentación IEC60320 C13	CEE7/7	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	America	700289770
Kit de montaje en bastidor IP400		Todos	700210800

13.6.3 Teléfono V2

El módulo Phone V2 de IP400 (también conocido como módulo Phone V2) se usa para agregar puertos de TELÉFONO analógicos adicionales a un sistema IP Office. El módulo Phone V2 está disponible en variantes de 16 y 30 puertos, denominados Phone 16 y Phone 30 respectivamente.

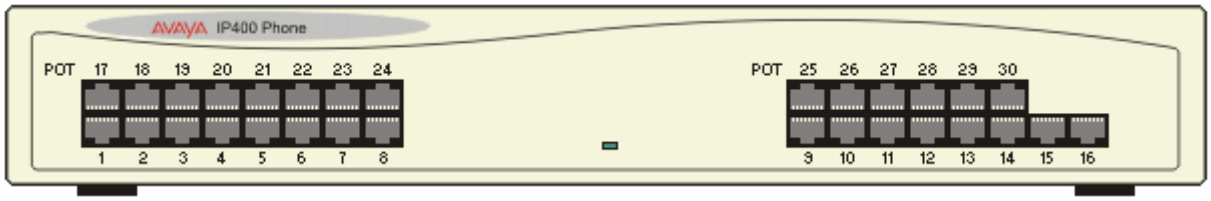


El módulo Phone V2 reemplaza al módulo Phone IP400 original, ahora denominado Phone V1. La versión del módulo se indica mediante etiquetas tanto en la base como en la parte posterior del módulo. Los cambios clave son:

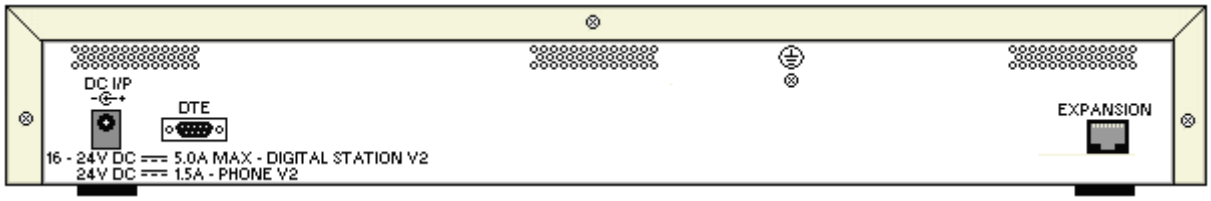
- El Phone V2 utiliza una fuente de alimentación externa de 60 W y 3 pines con conexión a tierra.
- Con IP Office 3.1, la indicación de mensaje en espera (MWI) en cada puerto se puede configurar para ***Ninguna***, ***En***, ***51V escalonado***, ***81V***, ***Inversión de línea A*** o ***Inversión de línea B***. ***En*** utiliza el valor predeterminado determinado por la configuración regional del sistema. Los puertos en un módulo Phone V2 también se pueden configurar para ***101V*** operación.
- Estos puertos no incluyen un condensador de llamada. Por lo tanto, para la conexión a teléfonos analógicos de 4 hilos, donde esto es un requisito (normalmente en el Reino Unido y Nueva Zelanda), la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.
- El puerto serie DTE en la parte posterior del módulo se ha cambiado a un enchufe tipo D de 9 pines.

Rasgo	Detalles
locales	Compatible con todas las configuraciones regionales de IP Office.
Software Mínimo Nivel	Nivel de software básico de IP Office 2.1(36) como mínimo. Archivo bin = dvpots.bin.
Incluido	Unidad de fuente de alimentación (consulte a continuación) y cable de interconexión de expansión.
Fuente de alimentación	El módulo se suministra con una fuente de alimentación externa de 3 pines y 60 W conectada a tierra. La fuente de alimentación tiene un cable de alimentación integral para la conexión a la toma DC I/P del módulo. Un lugar específicoCable de alimentación IEC60320 C13 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
Montaje	El módulo está diseñado como un módulo independiente que se puede apilar sobre o debajo de otros módulos de IP Office. El módulo se puede montar en rack en un sistema de rack de 19" utilizando el kit de montaje en rack IP400 opcional.
Dimensiones	Ancho: 445 mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8"/2U.
Peso	Sin caja: 3,1 kg/6,94 libras. En caja: 4,4 kg/9,7 libras. (Basado en el teléfono 30 V2)

Frente del módulo



Parte trasera del módulo



Puertos	Descripción
E/P CC 271	Puerto de entrada de alimentación de CC. Se utiliza para la conexión del cable de alimentación de una fuente de alimentación externa de 60 W con conexión a tierra de Avaya suministrada con el módulo de expansión. Un lugar específicoCable de alimentación IEC60320 C13 30para la fuente de alimentación externa es necesaria pero no se suministra con el módulo.
DTE 278	Zócalo tipo D de 9 vías. Solo para uso de Avaya.
EXPANSIÓN 273	Enchufe RJ45. Se utiliza para la conexión directa a un puerto de expansión en una unidad de control de IP Office mediante el cable de interconexión de expansión suministrado con el módulo.
TELÉFONO 276	Toma RJ45. Se utiliza para la conexión de teléfonos analógicos. Diseñado para teléfonos analógicos de dos hilos. Para la conexión a teléfonos analógicos de 4 hilos, la conexión debe realizarse a través de un enchufe maestro con condensadores de llamada. Si está conectado a unextensión fuera del edificio 36la conexión debe realizarse a través deCajas de barrera de IP Office 189 además de la protección primaria de los edificios. El módulo también debe estar conectado a una tierra de protección.
⏚	Punto de tierra de protección. Se requiere el uso de una tierra protectora para todas las instalaciones, consultePuesta a tierra (puesta a tierra) 93.Cuando el módulo está conectado a extensiones analógicas en otro edificio, se requiere una IP Office Phone Barrier Box V2 (101 V) en ambos extremos, consulteProtección contra rayos/Conexiones fuera del edificio 36.

Códigos de piezas y equipos relacionados

Todos los módulos de expansión se suministran con un nivel de software base y deben actualizarse para que coincidan con el software central de la unidad de control en el sistema IP Office. Los módulos de expansión incluyen una unidad de fuente de alimentación (PSU) externa y un cable de interconexión adecuado. No incluyen un cable de alimentación específico para la región para la fuente de alimentación externa ni ningún cable de extensión de teléfono.

Artículo	Variante	País	Código SAP
Teléfono IP400 V2	16 puertos	Todos	700359904
	30 puertos		700359912
Cable de alimentación IEC60320 C13	CEE7/7	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	America	700289770
Kit de montaje en bastidor IP400		Todos	700210800

13.7 Juegos de montaje

Los siguientes kits de montaje están disponibles para usar con los sistemas IP Office.

13.7.1 Kits de montaje en pared IP500

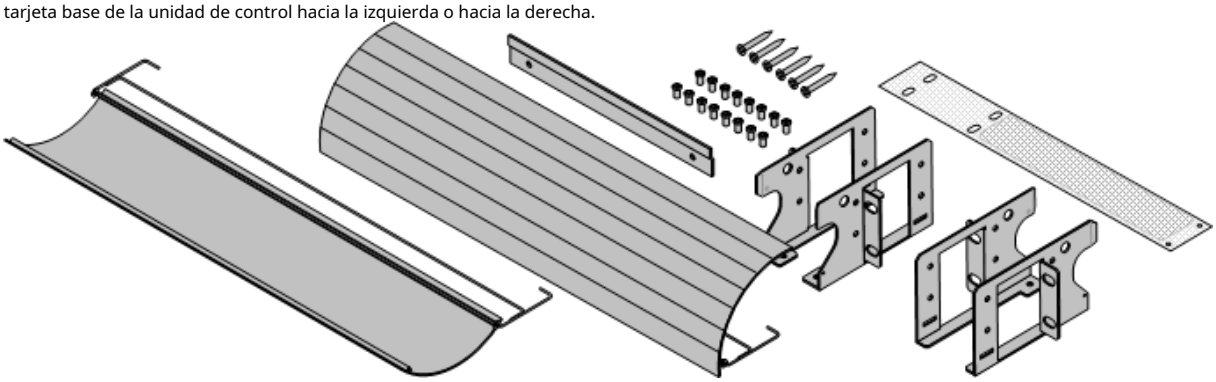
Las unidades de control IP500 V2 y los módulos de expansión externos IP500 pueden montarse en la pared o en un bastidor. Para hacer esto, se requiere un kit de montaje en pared además de las fijaciones de pared adecuadas.

Además de los existentes Requisitos medioambientales 51 para un sistema IP Office, se aplican los siguientes requisitos adicionales al montar una unidad en la pared:

- La superficie de la pared debe ser vertical, plana y libre de vibraciones. No se admite la unión a paredes temporales.
- Solo deben usarse los tornillos proporcionados con el kit de montaje para fijar los soportes a la unidad de control oa los módulos de expansión.
- La instalación debe ser realizada por una persona de servicio.
- Asegúrese de que el sistema se haya apagado y que se haya desconectado la alimentación de todas las unidades. Apague el sistema usando un comando de apagado y luego desconecte la alimentación. No quite simplemente la alimentación.
- Se requiere una superficie de montaje de madera contrachapada adecuada de al menos 1 m x 1 m x 19 mm (39" x 39" x 0,75"). Si también se va a montar una caja de expansión, se requiere una superficie de montaje de madera contrachapada de al menos 1,2 mx 1,2 mx 19 mm (48" x 48" x 0,75").
- Se debe usar un mínimo de 6 tornillos de cabeza plana de 45 mm de largo y 5 mm/6 mm (1,75" n.° 10/n.° 12) para asegurar la madera contrachapada a los montantes de la pared.
- Se deben usar los tornillos para madera de 20 mm de largo y 4 mm (#8 ¾") para asegurar los soportes a la superficie de montaje de madera contrachapada

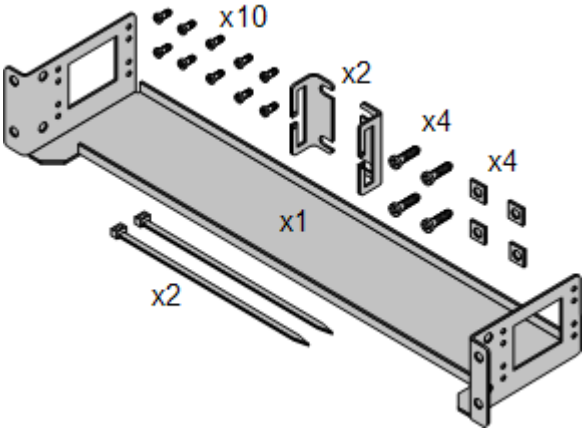
El siguiente kit está disponible actualmente:

- **KIT DE MONTAJE EN PARED IPO IP500 V3***(Código SAP 700503160)*
  Este kit se puede utilizar para montaje en pared y en rack de unidades de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora enrutamiento de cables en la parte delantera y trasera de la unidad. Para unidades de control montadas en la pared, permite orientar las ranuras de la tarjeta base de la unidad de control hacia la izquierda o hacia la derecha.

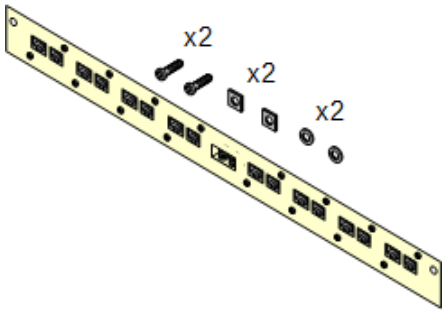


13.7.2 Kit de montaje en bastidor

- **KIT DE MONTAJE DE RACK IPO IP500***(Código SAP 700429202)*
  Este kit contiene todos los componentes necesarios para el montaje en rack de una sola unidad de control IP500 V2 o módulo de expansión externo IP500. Esto incluye tornillos para la fijación de los soportes al módulo, pernos para asegurar el módulo en el rack y soportes pasacables.



13.7.3 Kit de montaje en bastidor de caja de barrera



- **Kit de montaje en bastidor de caja de barrera***(SAP 700293905)* Las cajas de barrera se deben utilizar para[extensiones telefónicas analógicas fuera del edificio](#) 36.Este soporte permite montar en rack hasta 8 cajas de barrera de IP Office y simplifica la cantidad de conexiones al punto de protección a tierra en el rack. Este kit debe usarse cuando se usan más de 3 cajas de barrera y admite un máximo de 16 cajas de barrera para un solo módulo de expansión externo.

13.8 Teléfonos

La versión 11.0 de IP Office es compatible con los siguientes teléfonos y complementos de teléfono. La disponibilidad puede depender de la ubicación y puede estar sujeta a restricciones locales. Para soporte telefónico histórico, consulteCompatibilidad de hardware/software 290.

Punta y anillo mejorados (puertos ETR)

Estos teléfonos solo son compatibles con una tarjeta ETR6 en sistemas IP500 V2. Solo se admiten en los sistemas IP Office Basic Edition - PARTNER® Mode e IP Office Basic Edition que ejecutan una configuración regional de América del Norte y U-Law.

- **Serie ETR:**ETR6, ETR6D, ETR18, ETR18D, ETR34D*(Los teléfonos ETR 34D están limitados a un máximo de 2 por tarjeta y 4 en total)*

Teléfonos digitales Avaya DS (puertos DS)

Estas estaciones digitales se conectan a IP Office a través deSD 271puertos Son compatibles con todos los modos de IP Office.

- **Serie 1400:**1403, 1408, 1416
- **Serie 9500:**9504, 9508

Los siguientes teléfonos con puerto DS adicionales solo se admiten en los modos estándar de IP Office:

- **Serie 2400:**2402, 2410, 2420.

Teléfonos digitales BST de Avaya (puertos BST)

Estas estaciones digitales se conectan al sistema IP Office IP500 V2 a través de puertos BST.

- **Serie 4100:**4135, 4136, 4145, 4145EX, 4146, 4146EX: conexión a puertos IP Office BST a través de un sistema Digital Mobility Solution.
- **Serie 7400:**7420, 7430, 7434, 7439, 7440, 7444, 7449: conexión a los puertos BST de IP Office a través de un sistema Digital Mobility Solution.
- **UCA:**Unidad de audioconferencia
- **Serie M:**M7100, M7100N, M7208, M7208N, M7310, M7310N, M7324, M7324N.
- **Serie T:**T7000, T7100, T7208, T7316, T7316E, T7406, T7406E

Teléfonos Analógicos

Los teléfonos y dispositivos analógicos se conectan aTELÉFONO 276puertos con el sistema IP Office. Sin embargo, debido a la variedad de analógicos teléfonos y dispositivos disponibles no se da garantía de funcionamiento. Es responsabilidad del instalador y del mantenimiento de IP Office probar y verificar el funcionamiento del equipo analógico propuesto.

- **Serie 6200:**6211, 6219, 6221*(América del norte)*.
- **Serie B100:**B149, B159, B169*.
- **Intercuarzo Géminis:**9330-AV, 9335-AV, 9281-AV*(Europa, Oriente Medio, África, Asia-Pacífico)*.

Teléfonos IP

Los teléfonos IP (SIP y H323) se conectan al sistema IP Office a través de la LAN o WAN RJ45. Estos dispositivos requieren una licencia de Avaya IP Endpoint y recursos de compresión de voz.

H323:

- **Serie 1600:**1603IP/SW, 1608, 1608-I, 1616, 1616-I
- **Serie 3600:**3641, 3645
- **Serie 3700:**3701, 3711 - Conexión a través de estaciones base DECT. 3720, 3725, 3730, 3735, 3740, 3745, 3749 - Conexión a través de estaciones base DECT R4.
- **Serie 9600:**9608, 9608G, 9611G, 9620L, 9620C, 9621G, 9630G, 9640, 9640G, 9641G, 9641GS, 9650, 9650C.

SORBO:

- **Serie 1000:**1010, 1040
- **Serie 1100:**1120E, 1140E
- **Serie 1200:**1220, 1230
- **Serie B100:**B169*, B179, B199.
- **Serie D100:**Estos teléfonos DECT (hasta 8) utilizan una estación base que se conecta al sistema IP Office mediante una troncal SIP y aparecen en IP Office como extensiones SIP.
- **E129:**Un teléfono SIP simple, el E129 admite la operación de respuesta automática, manos libres y auriculares.
- **H175:**Videoteléfono SIP.
- **H200:**H229, H239, H249.
- **Serie J100:**J129, J139, J159, J169, J179.
- **Serie K100:**K155*, K165, K175.

* El B169 es un teléfono DECT que se conecta a una estación base DECT. La estación base se conecta a IP Office. Existen estaciones base analógicas y SIP.

13.9 Módulos de botones de teléfono

El número máximo combinado de botones en los módulos de botonespor sistema es 1024 .

- **1100 KEM:***+18 (máx. 3 por teléfono, 56 por sistema)*
  Complemento para teléfonos 1120E y 1140E. Cada módulo proporciona 18 botones programables adicionales.
- **1200 KEM:***+12 (máx. 7 por teléfono, 85 por sistema)*
  Complemento para teléfonos 1220 y 1230. Cada módulo proporciona 12 botones programables adicionales.
- **BM12:***+24 (máx. 3 por teléfono, 42 por sistema)*
  Complemento para teléfonos 9508, 9608, 9611 y 9641. Proporciona 12 botones físicos asignables en 2 páginas para 24 botones programables en total. Cuando se usa con un 9508, se debe suministrar energía al teléfono usando un módulo de energía en línea.
- **BM32:***+32 (Máx. 3 por teléfono, 32 por sistema)*
  Complemento para los teléfonos 1616 que proporciona dos columnas de 16 botones. Se admiten hasta 3 módulos BM32 con cualquier 1616. Sin embargo, cuando se usa con más de un módulo, el teléfono debe recibir alimentación de una fuente de alimentación en lugar de PoE.
- **JEM24:***+24 (Máx. 3 por teléfono, 14/42 por sistema*)*
  Complemento para los teléfonos J169 y J179. Cada módulo proporciona 24* botones programables de doble LED con pantalla de información adyacente a cada botón.
  - * Un solo JEM24 conectado a un teléfono admite 72 ranuras de botones programables dispuestas en 3 páginas, a las que se accede mediante el botón de desplazamiento de página del módulo. Cuando se conectan varios módulos CBM24 a un teléfono, cada uno solo admite 24 ranuras de botones programables (es decir, una sola página). Esto debe tenerse en cuenta al considerar la capacidad, un solo módulo conectado a un teléfono usa la misma capacidad de botón que 3 módulos en el mismo teléfono.
  - Para admitir más de 2 módulos de botones, el teléfono debe usar la fuente de alimentación principal J100 de 5 V en lugar de PoE.
  - Los módulos de botones JEM24 y JBM24 no se pueden combinar en el mismo teléfono.
- **DBM32:***+32 (Máx. 3 por teléfono, 32 por sistema)*
  Complemento para los teléfonos 1416 que proporciona dos columnas de 16 botones. Se admiten hasta 3 módulos BM32 con cualquier 1416. Cuando se utiliza con un módulo de botones DBM32, el teléfono debe alimentarse desde una fuente de alimentación.
- **UE24:***+24 (máximo 1 por teléfono, 8 por sistema)*
  Complemento para 2420, 4620, 4620SW, 4625, 5620, 5620SW y 5621. Proporciona 24 botones programables adicionales. Los íconos de visualización de botones están en dos páginas intercambiables con 12 íconos en cada página.
- **EU24BL:***+24 (máximo 1 por teléfono, 8 por sistema)*
  Según el EU24 anterior, pero con una función de retroiluminación para que coincida con el 4621. No compatible con el 2420.
- **JBM24:***+24 (máx. 3 por teléfono, 42 por sistema)*
  Complemento para los teléfonos J169 y J179. Cada módulo proporciona 24 botones programables de doble LED con pantalla de información adyacente a cada botón.
  - Para admitir más de 2 módulos de botones, el teléfono debe usar la fuente de alimentación principal J100 de 5 V en lugar de PoE.
  - Los módulos de botones JEM24 y JBM24 no se pueden combinar en el mismo teléfono.
- **KLM:***+48 (Máx. 2 por teléfono, 21 por sistema)*
  Usado con teléfonos M7324. Se admiten hasta 2 módulos de botones por teléfono. Cada módulo de botones proporciona 48 botones programables.
- **SMB24:***+24 (Máx. 3 por teléfono, 42 por sistema).*
  Compatible con teléfonos 9630G, 9640, 9640G, 9650 y 9650C. Para la versión 9.0 de IP Office, también compatible con 9608, 9608G, 9611G, 9641G y 9641GS.
- **T7316E KEM:***+24 (Máx. 9 por teléfono, 42 por sistema).*
  Usado con teléfonos T7316E. Cada módulo de botones proporciona 24 botones programables. Se admiten hasta 4 módulos de botones por teléfono sin fuente de alimentación adicional. Se pueden soportar de 5 a 9 módulos con alimentación adicional. Máximo 9 por teléfono (4 sin alimentación adicional).

13.10 Aplicaciones

Esta sección describe los requisitos para varias aplicaciones de IP Office. Estos son solo esquemas, para obtener detalles completos, consulte los manuales de instalación específicos para esas aplicaciones y los boletines técnicos de IP Office.

- Servidor de aplicaciones de IP Office 252
- Cliente del lugar de trabajo de Avaya IX 254
- Portal one-X para IP Office 255
- Comunicador de Avaya 256
- Cliente web de IP Office 254
- SoftConsole 257
- TAPI 258
- Buzón de voz profesional
- Colaboración web 260
- Gerente de IP Office 253
- Administrador de medios 253
- Monitoreo del sistema 255
- Solicitud de estado del sistema (SSA) 257

¿Comentarios sobre este documento? infodev@avaya.com

13.10.1 Servidor de aplicaciones de IP Office

Esta no es una sola aplicación, IP Office Application Server es un paquete de instalación de un solo servidor para las aplicaciones que se enumeran a continuación. El DVD instala un sistema operativo CentOS Linux, las aplicaciones de IP Office y un conjunto de páginas web para la administración del servidor. Tenga en cuenta que la instalación sobrescribe cualquier sistema operativo y datos existentes en la PC del servidor.

- **Portal one-X para IP Office** 255
  El acceso de usuario y configuración se realiza a través del navegador web de la misma manera que para una instalación de servidor Windows de one-X Portal for IP Office.
  - **Cliente web de IP Office** 254
    Este es un cliente WebRTC compatible con un navegador. Permite al usuario realizar, contestar y controlar llamadas de audio y video desde su PC. Lo pueden utilizar los usuarios configurados para one-X Portal for IP Office. Requiere un servidor de aplicaciones de IP Office con el servicio de puerta de enlace WebRTC configurado.
- **Buzón de voz profesional**
  El acceso a la configuración se realiza mediante una instalación de Windows del software de cliente Voicemail Pro. Se incluye un paquete de instalación para el cliente Voicemail Pro en el servidor de IP Office Application Server.

Para el servidor de Voicemail Pro que se ejecuta en una plataforma basada en Linux, las siguientes funciones no son compatibles:

- **Secuencias de comandos VB**
- **VPNM**
- **Correo de voz web de UMS**
  (Sin embargo, el acceso a través de IMAP y one-X Portal for IP Office están disponibles como alternativas).

Cuando se inicia sesión en el servidor de correo de voz mediante el cliente Voicemail Pro, las funciones no admitidas aparecen atenuadas u ocultas. Si esas funciones están presentes en un flujo de llamadas importado, no funcionarán y las llamadas que intenten usar esas funciones se desconectarán.

Las funciones de respaldo y restauración del cliente de Voicemail Pro no se pueden usar actualmente para mover datos de correo de voz entre un servidor basado en Linux y un servidor basado en Windows o viceversa. Se pueden utilizar las funciones de cliente para el módulo de importación y exportación y la base de datos de flujo de llamadas.

Para escenarios de Small Community Network donde hay varios servidores de correo de voz, por ejemplo, servidor distribuido y de respaldo, se permite una combinación de servidores basados en Linux y Windows.

- **Administrador de medios** 253
  Voicemail Pro se puede utilizar para la grabación manual y automática de llamadas. Esas grabaciones se colocan en buzones. Media Manager permite que esas grabaciones se redirijan a una tienda separada donde los detalles de cada grabación se mantienen en una base de datos de búsqueda. Esto permite que las grabaciones se archiven, busquen y reproduzcan por separado de los mensajes del buzón. Esta aplicación requiere la entrada de licencias adicionales en la configuración de IP Office. Esta aplicación requiere un servidor de aplicaciones de IP Office que incluya un disco duro adicional para el almacenamiento de grabaciones.
- **Colaboración web** 260
  Comparta documentos y mensajes en una conferencia. Web Collaboration proporciona al usuario funciones para compartir documentos, aplicaciones y su escritorio en una conferencia de colaboración web. Esto se ejecuta en paralelo con una conferencia de audio organizada por el sistema IP Office. Los usuarios internos con licencia para la colaboración web pueden usar WebRTC para transmitir audio a través de la conferencia de colaboración web en lugar de tener que realizar una llamada telefónica paralela a la conferencia de audio.

Detalles	
DVD	Juego de DVD IP Office Application Server versión 11.0 (2)
Licencia	✓ - Depende de las aplicaciones de IP Office seleccionadas durante la instalación. La Oficina de PI El servidor de Application Server en sí no requiere ninguna licencia.

Requisitos de la computadora

Referirse a *"Instalación y mantenimiento del servidor de aplicaciones IP Office de Avaya"* manual.

13.10.2 Administrador de IP Office

Esta herramienta se utiliza para acceder a todas las partes de la configuración de IP Office. Se pueden definir diferentes niveles de acceso para controlar qué partes de la configuración puede ver y modificar el usuario de IP Office Manager. IP Office Manager también se utiliza para actualizar los archivos de software utilizados por un sistema IP Office. Cuando se ejecuta, también actúa como un servidor TFTP desde el cual algunos teléfonos Avaya pueden solicitar nuevo software.

- **Versión del administrador de IP Office**
  Es importante descargar e instalar la versión correcta del paquete de administración de IP Office, incluido IP Office Manager.
  - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincida con la versión de IP Office requerida en el sistema. Esto establece la versión del software cargado cuandorecreando la tarjeta SD del sistema 75.
  - Para el mantenimiento del sistema, la versión de IP Office Manager utilizada establece la versión del software cargado en un sistema cuandoactualizando el sistema 180.
  - Para la configuración del sistema, IP Office Manager es compatible con versiones anteriores. IP Office Manager versión 11.0 es compatible con versiones anteriores para configurar sistemas que ejecutan software a partir de la versión 6.0 de IP Office y en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión superior del software.
  - **Admin Lite no compatible**
    Tenga en cuenta que IP Office Manager instalado desde el**AdminLite**El instalador no es la versión completa. Se ejecuta solo en inglés y no incluye los archivos necesarios para acciones como actualizaciones del sistema IP500 V2, compatibilidad con el firmware del teléfono, recreación de tarjetas SD, etc. Para admitir los sistemas IP500 e IP500 V2, asegúrese de descargar e instalar la administración completa de IP Office instalador de la suite (aproximadamente 1,46 GB en comparación con el instalador AdminLite de 100 MB).

Detalles	
DVD	IP Office versión 11.0 Juego de DVD para usuarios/administradores (2) (700513659) (Disco 1)
Idiomas	Inglés, brasileño, chino (simplificado), holandés, francés, alemán, italiano, ruso, español (mexicano).
Licencia	✗ No se requiere licencia.

Requisitos de la computadora

Para conocer los requisitos de la PC, consulte el manual de instalación o implementación de IP Office correspondiente a la aplicación. Para conocer la compatibilidad con el sistema operativo y el navegador, consulteResumen del sistema operativo 261.

13.10.3 Administrador de medios

Buzón de voz profesional 259se puede utilizar para la grabación de llamadas manual y automática. Normalmente esas grabaciones se colocan en el buzón especificado para el usuario o grupo de búsqueda cuya llamada se está grabando y luego se tratan como mensajes normales. Media Manager permite que esas grabaciones se redirijan a una base de datos en el servidor que ejecuta Media Manager. Esto permite que las grabaciones se archiven y busquen por separado de los mensajes de los usuarios. El acceso del usuario es a través del navegador web.

Media Manager es un servicio que se puede ejecutar en un servidor de aplicaciones de IP Office que también puede albergar Voicemail Pro y/o one-X Portal para IP Office. Sin embargo, el servidor debe configurarse con un disco o partición independiente para el almacenamiento de las grabaciones de llamadas.

Detalles	
Licencia	✓ Administrador de medios. VerLicencias de Voicemail Pro 284.

13.10.4 Cliente Avaya IX Workplace (Equinox)

Esta es una aplicación de comunicación unificada que admite llamadas, contactos de directorio, presencia, mensajería instantánea y muchas otras características. Es compatible como aplicación en una amplia gama de sistemas operativos; Windows, Android, macOS e iOS (verSoporte del sistema operativo 261t para más detalles).

Avaya IX Workplace Client en teléfonos Vantage es compatible desde 11.0.4.0 en adelante con el firmware Vantage R2.0.1.

En los sistemas IP500 V2, Avaya IX Workplace Client es compatible con los siguientes usuarios:

Perfil del usuario	Licencias del sistema	Licencias de usuario	Modo	sistema operativo
Usuario Básico	Edición esencial	Licencia de Softphone de Avaya	Ser único	mac OS, Windows
Usuario móvil	Edición Esencial + Edición preferida	Trabajador Móvil + Licencia de Softphone de Avaya	Ser único	mac OS, Windows
Usuario teletrabajador	Edición Esencial + Edición preferida	teletrabajador	Simultáneo	mac OS, Windows
Usuario trabajador de oficina	Edición Esencial + Edición preferida	Empleado de oficina	Simultáneo	mac OS, Windows
Usuario de poder	Edición Esencial + Edición preferida	Usuario de poder	Simultáneo	Android, iOS, mac OS, ventanas

- **Modo independiente**
  En este modo, Avaya IX Workplace Client es el único dispositivo de telefonía de los usuarios mientras están conectados a Avaya IX Workplace Client. Iniciar sesión en Avaya IX Workplace Client los desconectará de cualquier otra extensión. Del mismo modo, iniciar sesión en otro teléfono los desconectará de Avaya IX Workplace Client.
- **Modo simultáneo**
  En este modo, el usuario puede iniciar sesión tanto en un teléfono de escritorio físico como en un cliente de softphone como Avaya IX Workplace Client al mismo tiempo. Pueden elegir hacer y contestar llamadas en cada extensión
  - Los clientes de Softphone incluyen clientes Avaya IX Workplace Client, clientes Avaya Communicator, clientes one-X Mobile, IP Office Web Client y IPOCC Agent Web Client.
  - Anteriormente, el uso de clientes simultáneos solo se admitía si el cliente de softphone se registraba en la misma IP Office en la que estaba configurado el usuario. Para R11.0, el cliente de softphone se puede registrar en cualquier IP Office de la red.
- **Modo de control compartido**
  Modo simultáneo Los usuarios de Windows y macOS pueden poner su cliente Avaya IX Workplace Client en modo de control compartido. En ese modo, la aplicación se utiliza para realizar y contestar llamadas a través de su teléfono de escritorio.

  oActualmente solo se admite para clientes de Avaya IX Workplace Client y teléfonos de escritorio registrados en la misma IP Office servidor.

  oSolo llamadas de audio, no admite videollamadas.

Notas adicionales

- La instalación de Avaya IX Workplace Client en Windows reemplaza automáticamente cualquier instalación de Avaya Communicator en la misma PC.

13.10.5 Cliente web de IP Office

Este es un cliente WebRTC de Avaya que se puede usar con los sistemas IP Office. Para instalaciones IP500 V2, requiere que IP500 V2 sea compatible conPortal one-X para IP Office 255corriendo de unServidor de aplicaciones de IP Office 252.La Oficina de PI
El servidor del servidor de aplicaciones está configurado con un servicio de puerta de enlace WebRTC.

Cualquier usuario con licencia y configurado para one-X Portal for IP Office puede usar la aplicación y usar el navegador Chrome en una PC con Windows o macOS.

Un cliente pesado también está disponible para Windows. El instalador se puede descargar desde one-X Portal for IP Office o con una sesión de navegador de IP Office Web Client. El cliente pesado incluye una versión integrada de Chrome y, por lo tanto, no requiere que la PC del usuario tenga Chrome instalado como navegador.

Para obtener detalles sobre la instalación, consulte el *"Instalación y mantenimiento del servidor de aplicaciones de IP Office"*manual.

13.10.6 Supervisar

Monitor (también conocido como System Monitor) es una herramienta que puede mostrar toda la actividad en el sistema IP Office con gran detalle. Como consecuencia, la interpretación de las trazas de Monitor requiere un alto nivel de conocimiento del protocolo de datos y telefonía. Sin embargo, todos los instaladores y mantenedores de IP Office deben comprender cómo ejecutar Monitor cuando sea necesario, ya que Avaya puede solicitar copias de los seguimientos de Monitor para resolver problemas de soporte.

Para IP Office 4.0 y superior, la[Aplicación de estado del sistema](#) 257se ha añadido para facilitar la interpretación información que la proporcionada por Monitor.

Detalles	
DVD	IP Office versión 11.0 Juego de DVD para usuarios/administradores (2) (700513659) (Disco 1)
Idiomas	Solo inglés.
Licencia	✗ No se requiere licencia.

Requisitos de la computadora

Para conocer los requisitos de la PC, consulte el manual de instalación o implementación de IP Office correspondiente a la aplicación. Para conocer la compatibilidad con el sistema operativo y el navegador, consulte[Resumen del sistema operativo](#) 261.

13.10.7 Portal one-X para IP Office

Esta aplicación se instala en una PC servidor conectada a IP Office. Los usuarios pueden acceder al portal one-X desde su propia PC usando un navegador web.

La aplicación permite al usuario controlar sus teléfonos, acceder a mensajes de correo de voz, registros de llamadas y directorios telefónicos.

Detalles	
DVD	IP Office versión 11.0 Juego de DVD para usuarios/administradores (2) (700513659) (disco 2) o IP Office Application Server versión 11.0 Juego de DVD (2)
Licencia	✓ Ver[Licencias de usuario](#) 282.
Idiomas	Portugués brasileño, checo, holandés, inglés (Reino Unido), inglés (EE. UU.), francés, alemán, italiano, japonés, coreano, polaco, ruso, sueco, turco y español latino.

La aplicación de servidor one-X Portal for IP Office puede instalarse en un servidor de Windows o ser proporcionada por un[Servidor de aplicaciones de IP Office](#) 252o[Módulo de comunicaciones unificadas](#) 217.

Requisitos de la computadora

Para conocer los requisitos de la PC, consulte el manual de instalación o implementación de IP Office correspondiente a la aplicación. Para conocer la compatibilidad con el sistema operativo y el navegador, consulte[Resumen del sistema operativo](#) 261.

13.10.8 Comunicador de Avaya

Avaya Communicator es una aplicación de softphone de usuario que permite al usuario realizar y contestar sus llamadas desde una variedad de dispositivos telefónicos. El software de cliente Avaya Communicator está disponible en dispositivos Windows y iPad. Esta documentación no cubre una versión adicional, Avaya Communicator for Web compatible con Google Chrome.

Detalles	
Licencia	✓ Consulte la tabla a continuación.
Idiomas	Holandés, inglés (Reino Unido), inglés (EE. UU.), francés, italiano, portugués brasileño, ruso y español.

Las funciones disponibles para el usuario dependen de la licencia del usuario para Avaya Communicator y de si el sistema también incluye Portal one-X para IP Office [259] y Buzón de voz profesional [259].

		Modo comunicador de Avaya	
		El modo ligero	**Modo avanzado**
Caracteristicas basicas		· Realice llamadas, retenga llamadas, silencie y transfiera llamadas. · directorio del sistema. · Registro de llamadas de la aplicación local.	· Realice llamadas, retenga llamadas, silencie y transfiera llamadas. · directorio del sistema. · Registro de llamadas de la aplicación local.
Características avanzadas *(Requiere one-X Portal para IP Office y Voicemail Pro)*		–	· Directorios de usuarios y registros de llamadas a través de one-X Portal for IP Office · Presencia (XMPP). · Mensajería instantánea de 2 partes · Videollamadas de 2 partes. · Soporte de doble extensión.
Licencias Requerido	**Licencia del sistema**	· **Edición esencial**	· **Edición Esencial + Edición Preferida**
	Licencias de usuario	· **Softphone de Avaya**	· **Empleado de oficina**o · **teletrabajador**o · **Usuario de poder**.
Modo de sistema	**Oficina de PI Edición esencial**	✓ Sí	–
	Oficina de PI Edición preferida	✓ Sí	✓ Sí
Conexión del cliente		El sistema IP Office proporciona soporte para las funciones del modo básico directamente.	Las aplicaciones one-X Portal for IP Office y Voicemail Pro brindan soporte para funciones de modo avanzado.

- **software de cliente**
  El origen del software de cliente Avaya Communicator depende del dispositivo del usuario. Sin embargo, dado que Avaya Communicator es compatible con varias plataformas de Avaya, en todos los casos el instalador debe asegurarse de obtener un cliente de Avaya Communicator que indique específicamente la compatibilidad con IP Office.

Requisitos de PC con Windows

Para conocer los requisitos de la PC, consulte el manual de instalación o implementación de IP Office correspondiente a la aplicación. Para conocer la compatibilidad con el sistema operativo y el navegador, consulte Resumen del sistema operativo [261].

13.10.9 SoftConsole

Esta es una aplicación con licencia. Está destinado a operadores de sistemas telefónicos o recepcionistas. Muestra los detalles de las llamadas dirigidas al usuario y le permite ver rápidamente el estado del destino requerido por la persona que llama y transferir la llamada. El usuario de SoftConsole puede acceder a una variedad de detalles sobre el estado de los usuarios y grupos en el sistema IP Office.

- SoftConsole de IP Office funciona junto con un teléfono de extensión físico de IP Office para proporcionar la ruta de voz para las llamadas.
- Se pueden licenciar hasta 4 usuarios simultáneos de SoftConsole.

Detalles	
DVD	IP Office versión 11.0 Juego de DVD de usuario/administrador (2) (700513659) (Disco 1) o ficha Centro de aplicaciones del servidor Linux.
Idiomas	Brasileño, chino (simplificado), danés, holandés, inglés (Reino Unido), inglés (EE. UU.), finlandés, francés, alemán, italiano, coreano, japonés, español latino, noruego, portugués, ruso, español y sueco.
Licencia	✓ Aplicación con licencia. Vea abajo.

Licencias

Licencia	Descripción	Nombre de RFA	SAVIA
Recepcionista	Agrega un usuario adicional de SoftConsole. Se puede licenciar un máximo de cuatro usuarios de SoftConsole.	RECEPCIONISTA DE IPO LIC RFA	171987

Requisitos de la computadora

Para conocer los requisitos de la PC, consulte el manual de instalación o implementación de IP Office correspondiente a la aplicación. Para conocer la compatibilidad con el sistema operativo y el navegador, consulteResumen del sistema operativo 261.

13.10.10 Aplicación de estado del sistema

Esta herramienta proporciona una amplia gama de información sobre el estado actual de un sistema IP Office 4.0 o superior. Incluye los recursos y componentes disponibles dentro del sistema. Esto incluye detalles de la llamada actual en curso. Se registran los detalles del número de alarmas y la fecha y hora de las alarmas más recientes.

Cuando se requiere para la escalada de diagnóstico, SSA puede tomar una imagen instantánea del estado del sistema IP Office, incluida una copia de su configuración actual. El uso de SSA requiere un nombre de usuario y una contraseña de servicio de IP Office que se haya configurado para acceder al estado del sistema en la configuración de seguridad de IP Office.

- Para los sistemas IP500 V2, SSA está preinstalado en la tarjeta de memoria SD de Avaya del sistema y se puede ejecutar navegando hasta la dirección IP del sistema IP Office.

Detalles	
DVD	IP Office versión 11.0 Juego de DVD para usuarios/administradores (2) (700513659) (Disco 1)
Licencia	✗ No se requiere licencia.

Requisitos de la computadora

Para conocer los requisitos de la PC, consulte el manual de instalación o implementación de IP Office correspondiente a la aplicación. Para conocer la compatibilidad con el sistema operativo y el navegador, consulteResumen del sistema operativo 261.

13.10.11 TAPI

IP Office TAPI es una aplicación de PC cliente que permite que las aplicaciones compatibles con TAPI interactúen con IP Office. El software TAPI de IP Office se puede utilizar en uno de dos modos, dependiendo de si tiene licencia o no. El mismo software se instala en cualquier caso con las licencias, si las hay, ingresadas en la configuración del sistema IP Office.

- **Primera parte TAPI**
  En este modo sin licencia, el software TAPI admite el control de la extensión asociada de un usuario individual, lo que permite que una aplicación compatible con TAPI responda (requiere un teléfono que admita la respuesta de manos libres) y realice llamadas.
- **TAPI de terceros**
  En este modo con licencia, el software TAPI se puede utilizar para controlar la función de llamada en extensiones de múltiples usuarios. Este modo se usa con las aplicaciones CTI Developer.

Detalles	
DVD	IP Office versión 11.0 Juego de DVD para usuarios/administradores (2) (700513659) (Disco 1)
Licencia	❌ Opcional. Se requieren licencias para el funcionamiento en modo TAPI de terceros. VerLicencias CTI 285.

Requisitos de la computadora

Para conocer los requisitos de la PC, consulte el manual de instalación o implementación de IP Office correspondiente a la aplicación. Para conocer la compatibilidad con el sistema operativo y el navegador, consulteResumen del sistema operativo 261.

13.10.12 Voicemail Pro

Esta aplicación requiere varias licencias ingresadas en la configuración de IP Office para controlar las funciones que ofrece y la cantidad de conexiones simultáneas (40). El funcionamiento de Voicemail Pro se puede personalizar para proporcionar servicios especiales. .

El software Voicemail Pro se puede instalar como partes separadas de cliente y servidor de Voicemail Pro. Esto permite la administración remota del servidor Voicemail Pro desde una PC con solo el cliente Voicemail Pro instalado. Una copia del cliente se instala automáticamente de forma local con el servidor de Voicemail Pro.

Fuente	
DVD	IP Office versión 11.0 Juego de DVD para usuarios/administradores (2) (700513659) (disco 1) o IP Office Application Server versión 11.0 Juego de DVD (2)
Idiomas	Chino mandarín, chino cantonés, danés, holandés, inglés británico, inglés estadounidense, finlandés, francés, francés canadiense, alemán, griego, hebreo, húngaro, italiano, japonés, coreano, noruego, polaco, portugués, portugués brasileño , Ruso, Español, Español-Argentino, Sueco, Turco.
Licencia	✓ VerLicencias de Voicemail Pro 284.

Los detalles a continuación son para una instalación de servidor basada en Windows de Voicemail Pro. Voicemail Pro también se puede instalar como parte de una instalación de servidor basada en Linux usando elDVD del servidor de aplicaciones de IP Office 252.

La parte del servidor de Voicemail Pro del software consta de varios componentes además del software del servidor central, estos son:

- **Campañas**
  Voicemail Pro se puede configurar para ejecutar una campaña. Consiste en una serie de preguntas para las cuales Voicemail Pro registra la respuesta de la persona que llama o las pulsaciones de teclas. Los usuarios pueden reproducir las grabaciones resultantes. El aspecto web de las campañas permite al usuario realizar esta reproducción y procesamiento de las grabaciones de la campaña a través de su navegador web. Esto requiere que se ejecute un servidor web IIS en la misma PC que el software Voicemail Pro.
- **Texto a voz (TTS)**
  Al agregar licencias adicionales, Voicemail Pro puede usar las funciones TTS de Windows para hablar texto y números a las personas que llaman, además de grabar avisos. Esto está diseñado principalmente para escenarios en los que Voicemail Pro obtiene valores de texto y números de una base de datos de clientes.
- **Servicio de mensajería unificada (UMS)**
  Voicemail Pro admite una función llamada correo electrónico de correo de voz para enviar mensajes o alertas de mensajes al buzón de correo electrónico de un usuario. Sin embargo, este es un proceso unidireccional sin vínculo al buzón de correo de voz del usuario sobre si el correo electrónico ha sido leído o eliminado. UMS permite que esto se convierta en un proceso bidireccional, donde los usuarios pueden reproducir mensajes de correo de voz a través de su buzón de correo electrónico o buzón de correo de voz.

Requisitos de la computadora

Para conocer los requisitos de la PC, consulte el manual de instalación o implementación de IP Office correspondiente a la aplicación. Para conocer la compatibilidad con el sistema operativo y el navegador, consulteResumen del sistema operativo 261.

13.10.13 Colaboración web

Web Collaboration es un servicio compatible con IP Office Application Server. Funciona junto con one-X Portal para IP Office y Voicemail Pro.

Web Collaboration proporciona al usuario funciones para compartir documentos, aplicaciones y su escritorio en una conferencia de colaboración web. Esto se ejecuta en paralelo con una conferencia de audio organizada por el sistema IP Office.

- La capacidad coincide con la capacidad de audioconferencia de IP Office. Requisito de ancho de banda de 250 kbps por usuario.
- Los usuarios host deben tener licencia para one-X Portal for IP Office como**Empleado de oficina**,**teletrabajador**o**Usuario de poder** perfil más también un**Colaboración web**licencia.
- La programación de conferencias, a través de one-X Portal for IP Office, requiere un**Usuario de poder**licencia.
- Los anfitriones pueden cargar documentos en formatos PDF, JPEG y PNG.
  - 10 documentos por usuario
  - 6 MB por documento.
- El uso compartido de aplicaciones y escritorio no es compatible con usuarios de PC MAC.
- lanzamiento desdeURL del navegador 263o directamente desde Avaya Communicator, one-X Portal (incluido el complemento de Outlook y Call Assistant) e IP Office Web Client.
- Idiomas: inglés, francés, español, alemán, italiano, portugués, ruso, sueco, chino, japonés, coreano.
- El vídeo no es compatible.
- Para la versión 10.0 de IP Office, los usuarios internos con licencia para la colaboración web pueden usar WebRTC para transmitir audio a través de la conferencia de colaboración web en lugar de tener que realizar una llamada telefónica paralela a la conferencia de audio.

13.10.14 Puertos de IP Office

Los detalles del rango de puertos utilizados por IP Office y las aplicaciones de IP Office se encuentran en https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003 .

La mayoría de los cortafuegos de PC solicitan al usuario que permita varias excepciones cuando se ejecuta por primera vez una aplicación recién instalada. Sin embargo, este no es siempre el caso, especialmente si el firewall está ubicado en otro lugar que no sea la PC del usuario.

13.11 Compatibilidad con el sistema operativo

Esta sección resume la compatibilidad con las aplicaciones de IP Office de la versión 11.0 de IP Office.

Algunas características específicas de las aplicaciones pueden tener requisitos adicionales. Dichos requisitos se detallarán en el manual de instalación específico de la aplicación. A menos que se indique lo contrario, el sistema operativo es la última versión compatible del desarrollador del sistema operativo.

13.11.1 Soporte de Windows

La siguiente tabla enumera las aplicaciones de IP Office que se pueden instalar en el sistema operativo Windows compatible. no incluye aplicaciones navegables 263.

Microsoft Windows	7	8.1	10	2012/ 2012 R2	2016
	Profesional, Empresa, Último	Pro, Empresa	Pro, Empresa	Estándar	Estándar, Esenciales
Aplicaciones de servidor					
Portal one-X para IP Office	–	–	–	✓	✓
Centro de contacto de IP Office	–	–	–	✓	–
Servidor Voicemail Pro	✓	✓	✓	✓	✓
. . . más UMS	–	–	–	✓	✓
. . . más campañas	–	–	–	✓	✓
. . . Servicio MAPI para Linux Voicemail Pro	✓	–	–	✓	✓
Aplicaciones de usuario					
Complemento one-X Portal para Outlook	✓	✓	✓	–	–
Asistente de llamadas	✓	✓	✓	–	–
complemento para MS Lync 2013	✓	✓	✓	–	–
Cliente grueso de IP Office Web Client	✓	✓	✓	–	–
Comunicador de Avaya	✓	✓	✓	–	–
Cliente del lugar de trabajo de Avaya IX	✓	✓	✓	–	–
SoftConsole	✓	✓	✓	–	–
TAPI - Primera fiesta	✓	✓	✓	✓	✓
TAPI - Terceros	✓	✓	✓	✓	✓
TAPI WAV[1]	✓	✓	✓	–	–
Escritorio compartido de conferencias web	✓	✓	✓	–	–
Aplicaciones de mantenimiento					
Gerente de IP Office	✓	✓	✓	✓	✓
Monitoreo del sistema	✓	✓	✓	✓	✓
Aplicación de estado del sistema	✓	✓	✓	✓	✓
Cliente Voicemail Pro	✓	✓	✓	✓	✓

1. TAPI WAV no es compatible con sistemas operativos de 64 bits.

13.11.1.1 Compatibilidad con Exchange/Outlook

Soporte de Outlook

Aplicación\Versión de Outlook	2007	2010	2013	2016
Voicemail Pro UMS/IMAP	–	✓	✓	✓
Marcación TAPI	–	✓	✓	✓
Complemento one-X Portal for IP Office para Outlook	–	✓	✓[1]	✓[1]

1. No se admiten las pantallas emergentes de los contactos de Outlook.

Soporte de intercambio

Aplicación\Servidor Exchange	2010	2013	2016
Correo de voz Pro UMS	✓	✓	✓
one-X Portal para la presencia de IP Office	✓	✓	✓
Calendario one-X Portal para IP Office	✓	✓	–
Calendario de cliente de Avaya IX Workplace	✓	✓	✓

13.11.2 Compatibilidad con Android

La siguiente tabla enumera las aplicaciones de IP Office compatibles con los sistemas operativos Android. no incluyeaplicaciones navegables [263].

Aplicación IP Office	4.4	5.x	6.X	7.X	8.0
	Kit Kat	Chupete	Malvavisco	Turrón	Oreo
Cliente del lugar de trabajo de Avaya IX [254]	✓[1]	✓[1]	✓	✓	✓

1. Los servicios Zang no son compatibles.

13.11.3 Soporte de Apple

PC macOS

La siguiente tabla enumera las aplicaciones de IP Office compatibles con los sistemas operativos macOS. no incluyeaplicaciones navegables [263].

Solicitud	10.8	10.9	10.10	10.11	10.12	10.13
	Montaña León	Mavericks	Yosemite	El Capitán	Sierra	Alto Sierra
Escritorio compartido de conferencias web [260]	✓	✓	✓	✓	✓	✓
Cliente del lugar de trabajo de Avaya IX [254]	–	–	–	✓	✓	✓

iPad

- Comunicador de Avaya [256]es compatible con iOS 6.1 y superior.
- Cliente del lugar de trabajo de Avaya IX [254]es compatible con iOS 10 y 11.

iPhone

- one-X Mobile es compatible con iOS 7.0 y versiones posteriores.
- Avaya IX Workplace Client es compatible con iOS 10 y 11.

13.11.4 Compatibilidad con Linux

Las siguientes aplicaciones de servidor de IP Office son compatibles con los sistemas IP500 V2 cuando se ejecutan en unServidor de aplicaciones de IP Office [252].El IP Office Application Server incluye la instalación de su propio sistema operativo.

- Buzón de voz profesional
- **Portal one-X para IP Office**
- Administrador de medios

- **Colaboración web**
- **Puerta de enlace WebRTC**(para compatibilidad con el uso de IP Office Web Client)

13.11.5 Compatibilidad con navegador

La siguiente tabla enumera la compatibilidad con las aplicaciones de IP Office a las que se accede mediante un navegador web.

Aplicación\Navegador	explorador de Internet		Borde	Firefox	Google Cromo	Mac OS Safari 8 Safari 9 safari10
	10.0[5]	11.0				
Campañas Voicemail Pro	✓	✓	✓	–	–	–
Correo web Voicemail Pro UMS	✓	✓	✓	–	–	–
Portal one-X para IP Office[1]	✓	✓	✓	✓	✓	✓
Cliente web de IP Office	–	–	–	–	✓	–
Avaya Communicator para Web	–	✓	–	–	✓	–
Administrador IP DECT R4	✓	✓	✓	✓	✓	✓
Administrador DECT D100	✓	✓	✓	✓	✓	✓
Colaboración web[4]	✓	✓	✓	✓	✓	✓
Administrador web de IP Office[3]						
" en computadora	✓	✓	✓	✓	✓	✓
" en tableta iPad (iOS6+)	–	–	–	–	✓	✓
" en tableta Android (KitKat 4.4+)	–	–	–	–	✓	–
Avaya Communicator para Web	–	✓	–	–	✓	–

Notas:

1. La exploración de one-X Portal for IP Office no es compatible con los sistemas operativos de servidor de Windows.
2. La versión de IE debe coincidir con el sistema operativo. Por ejemplo, navegador de 32 bits en un sistema operativo de 32 bits.
3. Algunas funciones de IP Office Web Manager solo se admiten en los sistemas operativos de PC con Windows, por ejemplo, copia de seguridad, restauración, actualización, lanzamiento de System Status Application/Voicemail Pro/IP Office Manager, carga de archivos.
4. El audio de WebRTC solo es compatible con Chrome o Firefox.
5. IE10 solo es compatible con Windows Server 2012 (no R2).

13.12 Puertos físicos

Los siguientes tipos de puertos se encuentran en la unidad de control de IP Office y en los módulos de expansión externos:

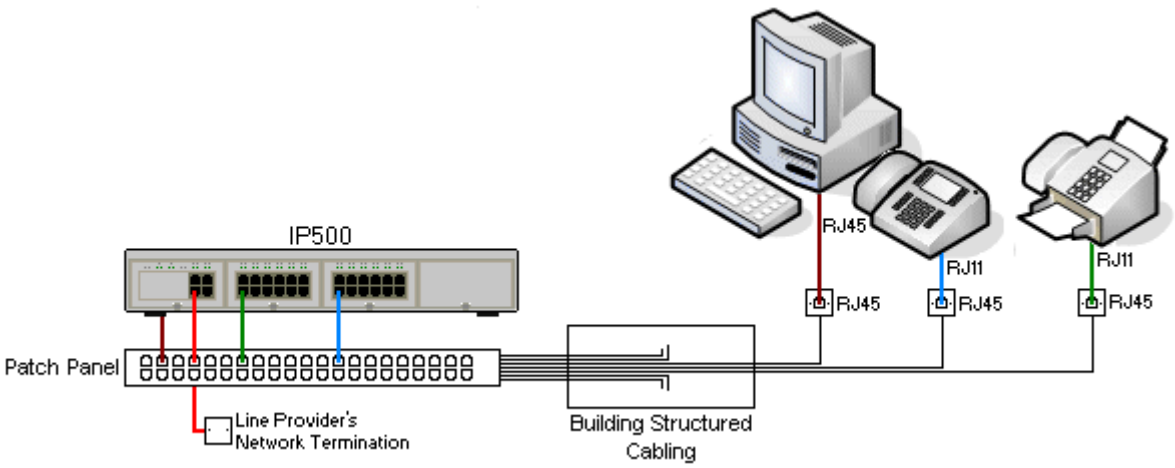
- COSA ANÁLOGA 267
  Se utiliza para la conexión de troncales analógicas externas.
- AUDIO 268
  Se utiliza para la entrada de una fuente externa de música en espera.
- BRI 269
  Se utiliza para la conexión de troncales BRI (tarjeta de troncales Quad BRI). En los modos estándar de IP Office también se pueden utilizar para dispositivos terminales ISDN (modo So8).
- BST (RJ21) 270 y BST (RJ45) 270
  Conexiones para teléfonos de las series M y T compatibles con IP Office. También para el sistema Digital Mobility Solution compatible con los teléfonos de las series 4100 y 7400. Ver compatible Teléfonos digitales Avaya BST 39.
- E/P CC 271
  Entrada de alimentación desde fuente de alimentación externa.
- SD 274
  Conexión de teléfonos de estación digital de Avaya compatibles con IP Office.
- RS232/DTE 278
  Se utiliza para el mantenimiento de la unidad de control bajo la guía de Avaya. En módulos de expansión no utilizados.
- FE 272
  Puertos de falla de energía de emergencia encontrados en la tarjeta base ETR6.
- ETR 272
  Solo se admite en la unidad de control IP500 V2 que se ejecuta en IP Office Basic Edition - Modo PARTNER® o IP Office Basic Editions.
- EXPANSIÓN 273
  Se utiliza para la interconexión de módulos de expansión externos y unidades de control.
- O/P EXT. 191
  Se utiliza para controlar sistemas de relés externos. El puerto proporciona dos controles conmutables (encendido, apagado y pulso).
- ⏚
  Se utiliza para la conexión de tierra funcional o de protección si es necesario.
- LAN 274
  Puertos LAN Ethernet de 10/100 Mbps.
- FP 275
  La alimentación analógica falla en los puertos.
- TELÉFONO 196 (MACETA) 276
  Puertos de extensión de teléfonos analógicos. En unidades más antiguas, estos puertos están etiquetados como puertos POT.
- PRI 277
  Puertos troncales PRI.

¿Comentarios sobre este documento? infodev@avaya.com

13.12.1 Cables

Los sistemas IP Office están diseñados principalmente para su uso dentro de un sistema de cableado estructurado RJ45 que utiliza cableado de par trenzado sin blindaje (UTP) CAT3 y enchufes RJ45.

Un sistema de cableado estructurado es aquel en el que los cables van desde un panel de conexión central RJ45 en la sala de comunicaciones/datos hasta los enchufes RJ45 individuales en las ubicaciones de los usuarios. Todos los hilos de cada cable entre el panel de conexión y el enchufe del escritorio están conectados directamente. Esta disposición permite que los dispositivos conectados en el panel de conexiones se intercambien para que coincidan con el tipo de dispositivo que debe conectarse en el enchufe del usuario. Por ejemplo, convertir un enchufe de usuario en un puerto de teléfono y otro enchufe de usuario en un puerto LAN de computadora, sin necesidad de volver a cablear los cables entre el panel de conexión y la ubicación del usuario.



- **Instalaciones tradicionales de cableado IDC Punchdown**
  Cuando sea necesario, el conector RJ45 del extremo remoto puede quitarse de los cables de IP Office y conectarse a los sistemas de cableado tradicionales mediante conectores de bloque perforado. Este tipo de instalación debe ser realizada por un técnico de cableado con experiencia.

- **Conexiones troncales**
  La mayoría de los puertos troncales de IP Office utilizan conectores RJ45 para aceptar un cable RJ45 a RJ45. Sin embargo, la conexión en el extremo del proveedor de la línea puede requerir el uso de un tipo de enchufe diferente para que coincida con el equipo del proveedor de la línea.

- **Conectores telefónicos RJ11**
  Muchos teléfonos utilizan enchufes RJ11 y se suministran con cables RJ11 a RJ11. Los enchufes RJ11 se pueden insertar en los enchufes RJ45 y, en muchos casos, la conexión funcionará. Sin embargo, esto no se recomienda ni se admite, ya que el bloqueo de la conexión no es realmente positivo y puede desconectarse. UnCable RJ45 a RJ11 [271]está disponible para estas conexiones.

Cables IP Office estándar

Los siguientes son cables estándar de Avaya disponibles para usar con los sistemas IP Office. La longitud máxima se aplica si el cable estándar de Avaya se reemplaza por un cable alternativo.

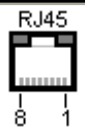
Cable	Descripción	Código SAP	Estándar Longitud	Máximo Longitud
Cable DTE de 9 vías 278	Se conecta al puerto RS232 DTE de la unidad de control. Enchufe tipo D de 9 vías a enchufe tipo D de 9 vías.	–	2m/6'6''.	2m/6'6''.
Cableado estructurado Cable de línea DS 271	Se conecta desde enchufes RJ45 a teléfonos analógicos y DS con enchufe RJ11.	TT700047871	4m/13'2''.	Ver tabla abajo.
Cable troncal BRI/PRI 269	Conecta los puertos troncales BRI/PRI al punto de terminación de red del proveedor de línea. RJ45 a RJ45. Rojo.	700213440	3m/9'10''.	–
Interconexión de expansión Cable 273	Conecta la unidad de control a los módulos de expansión. RJ45 a RJ45. Azul. Se puede reemplazar por un cable de interconexión amarillo (2 m (6'6") - 700472871) suministrado con elExpansión de 4 puertos IP500 212tarjeta al usar esa tarjeta.	700213457	1m/3'3''.	1m/3'3''.
Cable de LAN 274	Se conecta desde puertos LAN de IP Office a dispositivos IP. RJ45 a RJ45. Gris.	700213481	3m/9'10''.	100m/328'.

La siguiente tabla detalla las distancias totales máximas de cable para DS y extensiones analógicas que utilizan diferentes grosores de cable. El cableado debe ser un cable de par trenzado sin blindaje de categoría 1 o superior.

Teléfono	Par trenzado sin blindaje (UTP) - 50nf/Km		
	AWG22 (0,65 mm)	AWG24 (0,5 mm)	AWG26 (0,4 mm)
Serie 1400	1200m/3937'	1000m/3280'.	670m/2200'
Serie 9500	1200m/3937'	1000m/3280'	670m/2200'
BST	580m/1900'	365m/1200'	228m/750'
Teléfonos analógicos	1000m/3280'	1000m/ 3280'	400m/1312'
Teléfonos ETR	305m/1000'	305m/1000'	122m/400'

13.12.2 Puerto ANALÓGICO

Estos puertos son puertos de troncales analógicas. Las tarjetas de troncales analógicas IP500 solo admiten troncales de inicio en bucle. losTroncal analógico [229] ATM16 El módulo admite troncales de inicio por bucle y de inicio por tierra, conmutables dentro de la configuración de IP Office.

COSA ANÁLOGA	Alfiler	Descripción
	1	No utilizado.
	2	No utilizado.
	3	No utilizado.
	4	Anillo.
	5	Consejo.
	6	No utilizado.
	7	No utilizado.
	8	No utilizado.

- **Corriente descolgada:**25 mA.
- **IMPORTANTE**
  En todas las instalaciones de IP Office, cualquier módulo que se utilice para conexiones de troncales analógicas debe estar conectado a untierra funcional [35].
- **ADVERTENCIA**
  Dentro de la República de Sudáfrica y en áreas de alto riesgo de rayos, cualquier módulo que use conexiones troncales analógicas debe estar conectado a untierra protectora [35]y paraequipo de protección contra sobretensiones [36].

13.12.3 Puerto de AUDIO

Este puerto se encuentra en la parte posterior de todas las unidades de control de IP Office. Se utiliza para la entrada de una fuente de sonido de música en espera externa. Tenga en cuenta que si IP Office cargó un archivo de sonido interno de música en espera, se ignorará cualquier entrada de este zócalo.

El puerto es un conector jack estéreo de 3,5 mm adecuado para su uso con los cables de audio más estándar y la conexión a la toma de salida de "auriculares" de la mayoría de los sistemas de audio.

El uso de una toma de 'auriculares' permite un ajuste de volumen simple. La conexión a través de un enchufe 'Line Out' puede requerir equipo adicional para ajustar el nivel de volumen.

Número de pin	Descripción
Común	Común
Izquierda	Entrada de audio: canal izquierdo.
Derecha	Entrada de audio - Derecha - Canal.

- Impedancia de entrada: 10k /canal. Señal de CA máxima: 200 mV rms.

13.12.4 Puerto BRI (So)

Para IP Office 4.2+, las tarjetas secundarias de troncales IP500 BRI se pueden cambiar del modo To a So.

Oficina de PI			Cable	Terminal RDSI	
RJ45	Alfiler	BRI		ALFILER	RJ45
	1	–	Blanco/Naranja	1	
	2	–	Naranja/Blanco	2	
	3	⬅ Rx-A	Blanco verde	3	
	4	➡ Tx-B	Azul blanco	4	
	5	➡ Tx-A	Blanco azul	5	
	6	⬅ Rx-B	Verde blanco	6	
	7	–	Blanco/Marrón	7	
	8	–	Cafe Blanco	8	

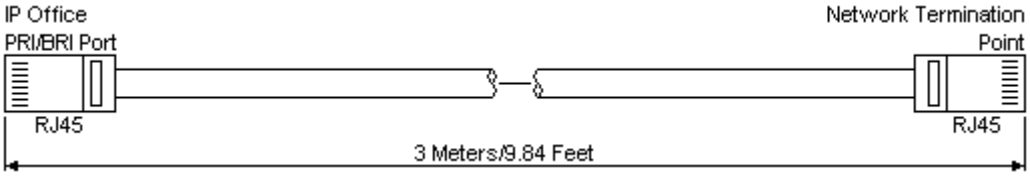
- **Resistencias de terminación**
  Se requieren resistencias de terminación de 100 ohmios en los pares de cables de transmisión y recepción en cada extremo del bus S.
  - Para IP Office 4.2+, los puertos individuales de una tarjeta secundaria IP500 BRI se pueden cambiar al modo So. Esto se hace configurando el**Subtipo de línea**a***S-autobús***en la configuración de IP Office. En este caso, se deben agregar resistencias de terminación en el extremo de IP Office además de las del otro extremo de la conexión S-bus.
    - La adición de la terminación necesaria en el extremo de IP Office se puede realizar mediante un cable convertidor IP500 BRI So (700458649). Este cable corto (25 cm/10") incluye tanto las resistencias de terminación necesarias como el cruce de cables.
  - Muchos dispositivos terminales ISDN incluyen resistencias de terminación. Si este no es el caso, se deben conectar resistencias de 100 ohmios (+/-5 %) entre el par de cables de recepción y el par de cables de transmisión en la caja de conexiones inmediatamente antes del último terminal ISDN en el S-bus.

13.12.5 Puerto BRI (Hacia)

Estos puertos son puertos de interfaz BRI A para la conexión a servicios troncales BRI externos.

Cable troncal PRI/BRI

Este cable se utiliza para conectar desde los puertos troncales BRI/PRI de IP Office al equipo de terminación de red del proveedor de línea. Si ese equipo no usa enchufes RJ45, es posible que sea necesario pelar y volver a cablear el cable o usar un cable alternativo. A continuación se detallan las asignaciones de pines de señal y los colores de los cables apropiados.



Oficina de PI				Cable	La red Terminación	
BRI	RJ45	BRI	PRI		ALFILER	RJ45
RJ45 8 1	1	–	⬅ Rx-A	Blanco/Naranja	1	RJ45 8 1
	2	–	⬅ Rx-B	Naranja/Blanco	2	
	3	➡ Tx-A	–	Blanco verde	3	
	4	⬅ Rx-A	➡ Tx-A	Azul blanco	4	
	5	⬅ Rx-B	➡ Tx-B	Blanco azul	5	
	6	➡ Tx-B	–	Verde blanco	6	
	7	–	–	Blanco/Marrón	7	
	8	–	–	Cafe Blanco	8	

- Suministro: Con estos cables no se suministran tarjetas de troncales BRI/PRI.
- Color de cable: rojo.
- Código SAP: 700213440.
- Longitud estándar: 3 m/9'10".
- Largo Máximo: 5m/16'5''.
- Aunque no se usan, los pines 7 y 8 están conectados para facilitar la construcción.

13.12.6 Puerto BST (RJ21)

Estos puertos se encuentran enEstación Digital IP500 16A/30A 233módulos de expansión externos. Son compatibles con IP500 V2 sistemas que ejecutan IP Office versión 7.0 y superior. Ver compatibleTeléfonos digitales Avaya BST 39.

1er Conector RJ21

Puerto		Alfiler	Cable
1	Consejo	26	Blanco azul
	Anillo	1	Azul blanco
2	Consejo	27	Blanco/Naranja
	Anillo	2	Naranja/Blanco
3	Consejo	28	Blanco verde
	Anillo	3	Verde blanco
4	Consejo	29	Blanco/Marrón
	Anillo	4	Cafe Blanco
5	Consejo	30	Blanco/Pizarra
	Anillo	5	Pizarra/Blanco
6	Consejo	31	Rojo azul
	Anillo	6	Azul rojo
7	Consejo	32	Naranja roja
	Anillo	7	Rojo naranja
8	Consejo	33	Rojo verde
	Anillo	8	Verde rojo
9	Consejo	34	Rojo marrón
	Anillo	9	Rojo marrón
10	Consejo	35	Rojo/Pizarra
	Anillo	10	Pizarra/Rojo
11	Consejo	36	Azul negro
	Anillo	11	Azul negro
12	Consejo	37	Negro/Naranja
	Anillo	12	Naranja/Negro
13	Consejo	38	Verde negro
	Anillo	13	Verde/Negro
14	Consejo	39	Marrón oscuro
	Anillo	14	Marrón/Negro
15	Consejo	40	Negro/Pizarra
	Anillo	15	Pizarra/Negro
dieciséis	Consejo	41	Amarillo azul
	Anillo	dieciséis	Azul amarillo
No utilizado		42	Amarillo naranja
		17	Naranja amarillo
		43	Violeta/Pizarra
		08	Pizarra/Violeta

2do conector RJ21

Puerto		Alfiler	Cable
17	Consejo	26	Blanco azul
	Anillo	1	Azul blanco
18	Consejo	27	Blanco/Naranja
	Anillo	2	Naranja/Blanco
19	Consejo	28	Blanco verde
	Anillo	3	Verde blanco
20	Consejo	29	Blanco/Marrón
	Anillo	4	Cafe Blanco
21	Consejo	30	Blanco/Pizarra
	Anillo	5	Pizarra/Blanco
22	Consejo	31	Rojo azul
	Anillo	6	Azul rojo
23	Consejo	32	Naranja roja
	Anillo	7	Rojo naranja
24	Consejo	33	Rojo verde
	Anillo	8	Verde rojo
25	Consejo	34	Rojo marrón
	Anillo	9	Rojo marrón
26	Consejo	35	Rojo/Pizarra
	Anillo	10	Pizarra/Rojo
27	Consejo	36	Azul negro
	Anillo	11	Azul negro
28	Consejo	37	Negro/Naranja
	Anillo	12	Naranja/Negro
29	Consejo	38	Verde negro
	Anillo	13	Verde/Negro
30	Consejo	39	Marrón oscuro
	Anillo	14	Marrón/Negro
No utilizado		40	Negro/Pizarra
		15	Pizarra/Negro
		41	Amarillo azul
		dieciséis	Azul amarillo
		42	Amarillo naranja
		17	Naranja amarillo
		43	Violeta/Pizarra
		08	Pizarra/Violeta

13.12.7 Puerto BST (RJ45)

Estos puertos se encuentran en elMódulos de expansión de estación digital IP500 16B/30B 236.Son compatibles con IP500 V2 sistemas que ejecutan IP Office versión 9.0 y superior. Ver compatibleTeléfonos digitales Avaya BST 39.

¿Comentarios sobre este documento? infodev@avaya.com

13.12.8 Puerto I/P de CC

Se encuentra en todas las unidades de control y módulos de expansión de IP Office. Se utiliza para la conexión desde el exterior[unidad de fuente de alimentación](#) 30 suministrado con la unidad de control o el módulo.

- No se debe utilizar ningún otro tipo de fuente de alimentación con el módulo o módulo a menos que Avaya lo indique específicamente.
- Los cables de alimentación no deben fijarse a la superficie del edificio ni atravesar paredes, techos, suelos ni aberturas similares.

13.12.9 Puertos DS (RJ45)

Estos puertos se utilizan para la conexión desde un sistema de cableado estructurado RJ45 a teléfonos de estación digital compatibles con IP Office. Los puertos DS son proporcionados por[Tarjetas de estación digital IP500](#) 218,[Tarjetas combinadas de cajero automático IP500](#) 214,[IP500 BRI Tarjetas combinadas](#) 216y[Estación digital IP500](#) 231módulos de expansión externos.

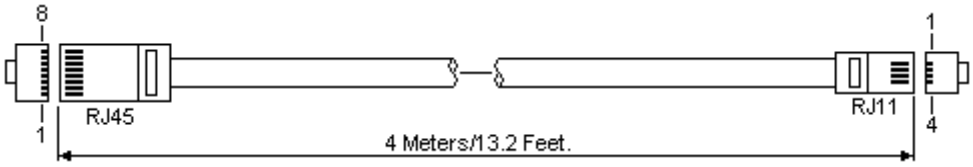
Aunque los cables RJ11 a RJ11 suministrados con algunos teléfonos se pueden conectar directamente a los puertos RJ45, incluidos los de los módulos de IP Office, esto no se recomienda ya que el bloqueo de la conexión no es positivo y puede desconectarse.

- Los puertos DS de los módulos de expansión externos se pueden conectar a[extensiones fuera del edificio](#) 36.Si este es el caso, la conexión debe realizarse mediante dispositivos de protección adecuados en cada extremo y mediante la protección primaria de cada edificio. Además, el módulo de la estación digital debe estar conectado a una tierra de protección.
- Los puertos DS en tarjetas base dentro de la unidad de control no deben conectarse a extensiones fuera del edificio.

Cable de línea de cableado estructurado

Este es un cable RJ45 a RJ11 adecuado para la conexión desde un puerto RJ45 de un sistema de cableado estructurado a un teléfono DS. También se puede utilizar para extensiones telefónicas analógicas de dos hilos.

Este cable no es adecuado para la conexión de una fuente de alimentación Avaya 1151D1/B2 a un teléfono DS con un módulo complementario EU24 o XM24. En esos casos, se deben utilizar los cables suministrados con la fuente de alimentación y el módulo adicional.



Oficina de PI			Teléfono	
Puerto DS	Alfiler	Descripción	Alfiler	Puerto
RJ45 8 1	1	No utilizado.	–	RJ11 6 1
	2	No utilizado.	1	
	3	No utilizado.	2	
	4	Señal 1.	3	
	5	Señal 2.	4	
	6	No utilizado.	5	
	7	No utilizado.	6	
	8	No utilizado.	–	

- Código SAP: T700047871.

13.12.10 Puerto EF

Estos puertos se encuentran en la tarjeta base ETR6. Son puertos de troncales analógicas que solo se pueden usar cuando la tarjeta está equipada con una tarjeta secundaria de troncales analógicas IP500. Cuando falla la energía, los puertos EF se conectan al puerto troncal 12.

13.12.11 Puerto ETR

Los puertos ETR (Enhanced Tip and Ring) son proporcionados por la tarjeta base ETR6. Se pueden utilizar para la conexión de dispositivos telefónicos analógicos DTMF y teléfonos ETR de Avaya.

- La paginación a equipos de paginación externos no es compatible a través de los puertos ETR6. Es compatible a través de puertos POT.

13.12.12 Puerto EXPANSIÓN

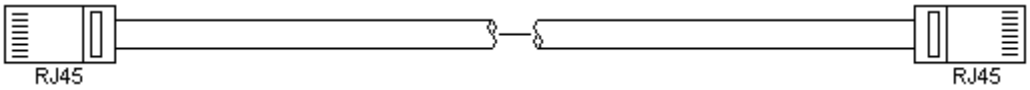
Este tipo de puerto se encuentra en la parte posterior de las unidades de control de IP Office y los módulos de expansión externos. Se utiliza para conectar los módulos de expansión externos a la unidad de control principal de IP Office.

La conexión entre estos puertos solo debe realizarse mediante un cable de interconexión de expansión de Avaya. No se debe utilizar ningún otro tipo de cable.

- Cada módulo de expansión externo se suministra con un cable de interconexión de expansión azul de 1 metro (3'3''). este cable deber utilizarse cuando se conecta a puertos de expansión en la parte trasera de una unidad de control.
- Cuando se conecta a puertos de expansión en una tarjeta de expansión de 4 puertos IP500, se puede usar un cable de interconexión de expansión amarillo de 2 metros (6'6") en lugar del cable azul estándar. Se suministran 4 cables amarillos con la tarjeta de expansión de 4 puertos IP500 tarjeta.

Cable de interconexión de expansión

El cable de interconexión de expansión se utiliza para vincular los puertos de expansión entre la unidad de control de IP Office y los módulos de expansión externos.



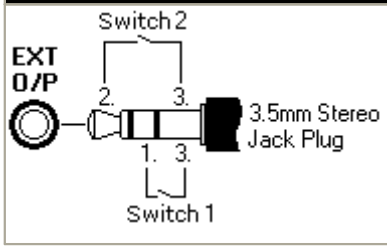
- Suministro: Normalmente se suministra un cable con cada módulo de expansión externo.
- Código SAP: cable azul de 1 m (3'3") - 700213457, cable amarillo de 2 m (6'6") - 700472871.

13.12.13 Puerto EXT O/P

Estos puertos se encuentran en la parte posterior de todas las unidades de control de IP Office. Se utilizan para la conexión a relés de conmutación externos. El puerto utiliza un conector jack estéreo estándar de 3,5 mm para la conexión.

IP Office puede abrir (resistencia alta), cerrar (resistencia baja) o pulsar (cerrar durante 5 segundos y luego abrir) dos interruptores dentro del puerto. Cualquiera de los interruptores se puede operar por separado. Estos interruptores están destinados a la activación de relés externos en sistemas como los sistemas de apertura de puertas.

- **PRECAUCIÓN:**
  En las instalaciones en las que este puerto esté conectado a un dispositivo externo al edificio, la conexión debe realizarse a través de un protector contra sobretensiones MDS2 y debe proporcionarse una conexión a tierra de protección en la unidad de control de IP Office. Cuando use el MDS2 en el puerto Ext O/P, use solo las tomas de Línea 1 y Equipo 1, no use las tomas de Línea 2 o Equipo 2.

O/P EXT.	Alfiler	Descripción
	1	interruptor 1
	2	interruptor 2
	3	0 voltios (tierra/chasis)

- Capacidad de conmutación: 0.7A.
- Voltaje máximo: 55V CC
- Resistencia en estado: 0,7 ohmios.
- Corriente de cortocircuito: 1A.
- Capacidad de corriente del circuito inverso: 1.4A.
- Asegúrese de que los pines 1 y 2 estén siempre en un voltaje positivo con respecto al pin 3.

Los conectores jack de audio estéreo de 3,5 mm se venden con frecuencia como módulos sellados precableados. Puede ser necesario usar un multímetro para determinar las conexiones de cableado de un enchufe disponible. Normalmente 3 (común a ambos relés) es la pantalla del cable.

13.12.14 Puerto LAN

Estos puertos se encuentran en las unidades de control de IP Office. Se utilizan para la conexión a IP LAN y dispositivos IP.

Todos los puertos LAN de IP Office son de detección automática de 10/100 Mbps. Los puertos son puertos cruzados MDI full-duplex de 10/100 Mbps con detección automática. Forman un conmutador Ethernet de capa 3 administrado.

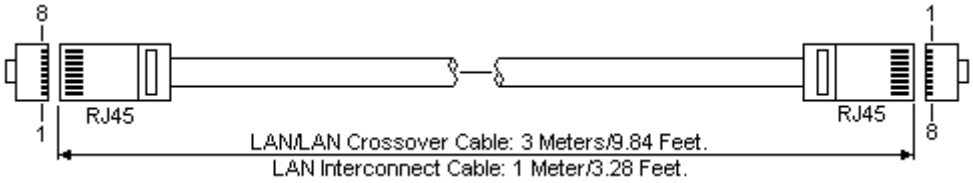
El puerto WAN no es compatible con los sistemas que se ejecutan en el modo IP Office Essential Edition.

Los LED se utilizan de la siguiente manera:

- Verde: Encendido = conectado, Intermitente = Actividad.
- Amarillo: Encendido = 100 Mbps, Apagado = 10 Mbps.

Cables LAN

Estos son cables UTP CAT5 para la conexión de varios dispositivos IP dentro del sistema IP Office.



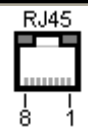
Oficina de PI							
LAN	**Alfiler**	**MDIX (Normal)**	**IDM (Transversal)**	**Cable**	**Estándar/ Interconectar**	**Transversal**	
RJ45 8 1	1	⬅ Rx-A.	➡ Tx-A.	Blanco/Naranja	1	3	RJ45 8 1
	2	⬅ Rx-B.	➡ Tx-B.	Naranja/Blanco	2	6	
	3	➡ Tx-A.	⬅ Rx-A.	Blanco verde	3	1	
	4	No utilizado.	No utilizado.	Azul blanco	4	4	
	5	No utilizado.	No utilizado.	Blanco azul	5	5	
	6	➡ Tx-B.	⬅ Rx-B.	Verde blanco	6	2	
	7	No utilizado.	No utilizado.	Blanco/Marrón	7	7	
	8	No utilizado.	No utilizado.	Cafe Blanco	8	8	

- **Código SAP:**
  - **Cable LAN - GRIS: 700213481.** Cable LAN recto estándar.
  - **Cable cruzado LAN - Negro: 700213473.** Cable cruzado LAN.

13.12.15 Puerto PF

Estos puertos se encuentran en la parte trasera delMódulo de expansión Analog Trunk 16 229.Son puertos de extensión analógicos que pueden usarse junto con troncales analógicas de inicio en bucle durante una falla de energía en el sistema IP Office. Ver tambiénPuertos de emergencia y fallas de energía 47.

Todos los teléfonos conectados a estos puertos deben estar claramente etiquetados como extensiones de corte de energía de acuerdo con los requisitos normativos nacionales y locales correspondientes.

FP	Alfiler	Descripción
	1	No utilizado.
	2	El pin 2 está conectado internamente al pin 5 a través de un condensador de timbre.
	3	No utilizado.
	4	Anillo.
	5	Consejo.
	6	El pin 6 está conectado internamente al pin 5 a través de un condensador de timbre.
	7	No utilizado.
	8	No utilizado.

- Tamaño mínimo del cable: AWG 26.
- Longitud máxima del cable:
  - AWG26: 500m / 1640'.
  - AWG24, AWG22: 1000m / 3280'.

13.12.16 Puerto TELÉFONO (POT)

Estos puertos son puertos de extensión analógicos. En las unidades IP Office más antiguas, estos puertos estaban etiquetados como puertos POT en lugar de puertos PHONE.

Los puertos TELÉFONO en los módulos de expansión Teléfono V1/V2 se pueden conectar a extensiones fuera del edificio 36.Si este es el caso, la conexión debe realizarse a través de dispositivos de protección adecuados (Caja de barrera de IP Office) en cada extremo y a través de la protección primaria de cada edificio. Además, el módulo del teléfono debe estar conectado a una tierra de protección.

Los puertos de TELÉFONO en las unidades de control de IP Office no deben conectarse a extensiones fuera del edificio.

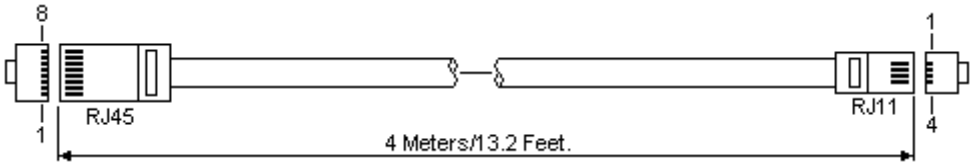
TELÉFONO	Alfiler	Descripción
	1	No utilizado.
	2	No utilizado.
	3	No utilizado.
	4	Anillo.
	5	Consejo.
	6	No utilizado.
	7	No utilizado.
	8	No utilizado.

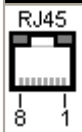
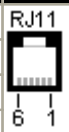
- REN: 2
- Corriente descolgada: 25mA.
- Voltaje del anillo:
  - Unidad de control IP500 V2, módulos telefónicos IP500: 49 V rms.
- Tamaño mínimo del cable: AWG 26.
- Longitud máxima del cable:
  - AWG26: 0,5 km / 1640 pies.
  - AWG24, AWG22: 1 km / 3280 pies.

Estos puertos no incluyen un condensador de llamada. Por lo tanto, para la conexión a teléfonos analógicos de 4 hilos donde esto sea un requisito (normalmente en el Reino Unido y Nueva Zelanda), la conexión debe realizarse a través de un enchufe maestro que contenga condensadores de llamada.

Cable de línea de cableado estructurado

Este es un cable RJ45 a RJ11 adecuado para la conexión desde un puerto RJ45 de un sistema de cableado estructurado a un teléfono DS. También se puede utilizar para extensiones telefónicas analógicas de dos hilos.



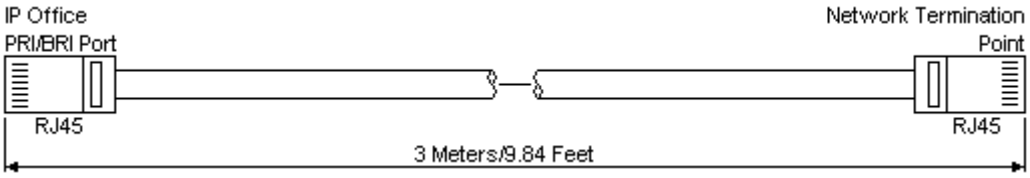
Oficina de PI			Teléfono	
Puerto DS	Alfiler	Descripción	Alfiler	Puerto
	1	No utilizado.	–	
	2	No utilizado.	1	
	3	No utilizado.	2	
	4	Señal 1.	3	
	5	Señal 2.	4	
	6	No utilizado.	5	
	7	No utilizado.	6	
	8	No utilizado.	–	

13.12.17 Puerto PRI

Estos puertos se utilizan para la conexión a servicios troncales PRI, incluidos E1, T1 y E1-R2.

Cable troncal PRI

Este cable se utiliza para conectarse desde los puertos troncales PRI de IP Office al equipo de terminación de red del proveedor de línea. Si ese equipo no usa enchufes RJ45, es posible que sea necesario pelar y volver a cablear el cable o usar un cable alternativo. A continuación se detallan las asignaciones de pines de señal y los colores de los cables apropiados.



Oficina de PI			Cable	Terminación de red	
RJ45		PRI		ALFILER	RJ45
RJ45 8 1	1	⬅ Rx-A	Blanco/Naranja	1	RJ45 8 1
	2	⬅ Rx-B	Naranja/Blanco	2	
	3	–	Blanco verde	3	
	4	➡ Tx-A	Azul blanco	4	
	5	➡ Tx-B	Blanco azul	5	
	6	–	Verde blanco	6	
	7	–	Blanco/Marrón	7	
	8	–	Cafe Blanco	8	

- Suministro: Las tarjetas de troncales PRI no se suministran con estos cables.
- Color de cable: rojo.
- Código SAP: 700213440.
- Longitud estándar: 3 m/9'10".

13.12.18 Puerto RS232 (DTE)

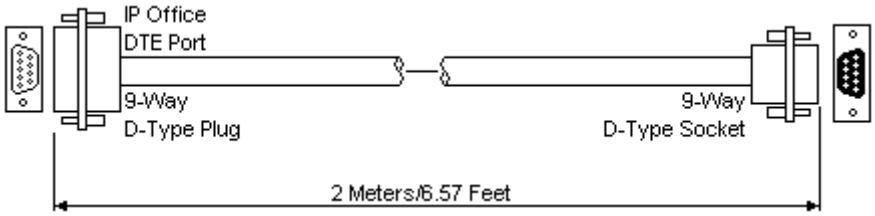
Estos puertos se encuentran en la parte posterior de todas las unidades de control de IP Office y módulos de expansión externos. Los puertos similares en los módulos de expansión externos solo los usa Avaya.

Los puertos RS232 DTE se pueden utilizar para una serie de[procesos de mantenimiento del sistema](#) 198.Un programa de terminal asíncrono como HyperTerminal también es necesario. Configure esto para la operación a través de un puerto serie de PC, de la siguiente manera:

- **Bits por segundo:**38400
- **Bits de datos:**8
- **Paridad:**Ninguna
- **Bits de parada:**1
- **Control de flujo:**Ninguna
- **Configuración | Emulación:**TTY

Cables DTE

Estos cables se utilizan para el mantenimiento y diagnóstico del sistema bajo la guía de Avaya. También se pueden utilizar para la conexión de equipos adaptadores de terminales serie RS232 a la unidad de control de IP Office. El cable requerido depende de la unidad de control de IP Office. Este cable es un "Cable serial directo DB9 hembra a DB9 macho".



IP Office de 9 vías RS232 Puerto DTE	Señal	PC/Terminal Adaptador
3	⬅ Recibir datos	3
2	➡ Dato transmitido	2
7	⬅ RTS (Solicitud de envío)	7
8	➡ CTS (Borrar para enviar)	8
6	➡ DSR (Conjunto de datos listo)	6
5	⬬ Terrestre	5
1	➡ DCD (Detección de portador de datos)	1
4	⬅ DTR (Terminal de datos listo)	4
9	➡ RI (indicador de anillo)	9

13.13 Licencias

Esta sección cubre las licencias utilizadas en los sistemas IP Office IP500 V2 que ejecutan la versión 10.0 de IP Office. No incluye detalles de las licencias utilizadas para otros tipos de sistemas IP Office como Server Edition.

El sistema IP Office requiere licencia para algunas funciones, consulteLicencias 279.El archivo de licencia se puede cargar manualmente oprecargado en la tarjeta SD del sistema 78.

¿Cómo se licencia el sistema?

- Se carga en el sistema un archivo XML que contiene el conjunto completo de licencias PLDS. El archivo de licencia es único para el número de serie de la clave de función de la tarjeta SD del sistema instalada en el sistema.
    - El ID de host PLDS utilizado para el archivo de licencia debe coincidir con el que se muestra en los 12 dígitos.**Identificación PLDS**impreso en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra con**FK**o**FK SN**. Para esas tarjetas agregue el prefijo***11***para obtener la identificación PLDS de la tarjeta.

Requisitos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una**Edición esencial**licencia del sistema para la versión específica de IP Office que desea ejecutar.

Actualización de licencias

A partir de la versión 10.0 de IP Office, el archivo de licencia XML de PLDS es específico de la versión. Para que un sistema se actualice a una nueva versión principal del software IP Office, se requiere un nuevo archivo de licencia específico para la versión de destino. Esto se aplica incluso si el archivo contiene el mismo conjunto de licencias.

13.13.1 Licencias de edición del sistema

Estas licencias se utilizan para establecer el rango de funciones que admite el sistema IP Office.

- **Edición esencial:**
  El sistema requiere esta licencia para ejecutarse en el modo IP Office Essential Edition. Hasta que se ingrese, el sistema funciona como un sistema IP Office Basic Edition.
    - Esta licencia es también un requisito previo para la**Edición preferida**licencia.
    - Esta licencia permite el correo de voz integrado con hasta 2 conexiones simultáneas y 15 horas de almacenamiento.
- **Puertos de correo de voz adicionales de Essential Edition:**
  Esta licencia permite dos conexiones adicionales de correo de voz incorporado y 5 horas adicionales de almacenamiento. Se pueden agregar múltiples licencias para un máximo de hasta 6 conexiones y 25 horas de almacenamiento.
- **Edición preferida (Voicemail Pro):**
  Esta licencia permite la compatibilidad con Voicemail Pro como servidor de correo de voz de IP Office con 4 puertos de correo de voz. los **Edición preferida**La licencia permite que el servidor de correo de voz brinde los servicios que se enumeran a continuación. Para IP Office versión 8.0 y superior, un**Edición esencial**La licencia es un requisito previo para esta licencia en los sistemas IP500 V2.
    - Buzones para todos los usuarios y grupos de búsqueda.
    - Anuncios para usuarios y grupos de búsqueda.
    - Flujos de llamadas personalizables.
    - Grabación de llamadas a buzones.
    - Campañas.
    - Lectura de correo electrónico TTS para usuarios con licencia para **Trabajador móvil**o**Usuario de poder**perfiles. También requiere licencias TTS.
    - Uso de**Conferencia Encuéntrame**funciones
    - Secuencias de comandos básicas visuales*(Solo Voicemail Pro basado en Windows)*

    1. un**Edición preferida** 279La licencia del sistema es un requisito previo para cualquier licencia de perfil de usuario que no sea**Usuario Básico**.

        - En una Red Comunitaria Pequeña, el**Edición preferida**La licencia del sistema central se comparte automáticamente con otros sistemas en la red, lo que permite licencias de perfil de usuario en esos otros sistemas. Sin embargo, cada sistema que admita un servidor Voicemail Pro, por ejemplo, para el correo de voz distribuido, aún requiere su propio **Edición preferida**licencia.
- **Sistema de Sucursales**
  Esta licencia habilita la compatibilidad con funciones de sucursales empresariales. Estos se relacionan con un sistema IP Office que se utiliza como un conmutador de sitio de sucursal en una red Avaya Aura. Adicional**Troncal SM**se requieren licencias para las líneas SM configuradas entre la sucursal y Avaya Aura.

¿Comentarios sobre este documento? infodev@avaya.com

13.13.2 Licencias de actualización

Los sistemas IP Office existentes que se actualizan a la versión 11.0 de IP Office requieren una licencia de actualización de software.

- **!Advertencia: Requisitos de licencia de actualización**
  En un sistema nuevo, cuando se realiza la primera llamada, el nivel de software que se está ejecutando se escribe en la memoria permanente de la unidad de control. Cualquier actualización posterior a una versión superior requiere la adición de la**Edición esencial** licencia para la versión de destino. Sistemas actualizados sin esa visualización de licencia *"No hay licencia disponible"*en algunos teléfonos y no permitirá ninguna función de telefonía.

- **!Nota: Sistemas Server Edition**
  Las unidades de control IP500 V2 configuradas como sistemas de sistema de expansión IP500 V2 se licencian y actualizan a través de los menús de administración web de Server Edition. Consulte la documentación de Server Edition.

13.13.3 Licencias troncales

Las siguientes licencias de troncales pueden ser utilizadas por un sistema IP Office Essential Edition.

- **IP500 Universal PRI (canales adicionales)**
  Estas licencias se utilizan para habilitar canales B adicionales por encima de los 8 básicos en una tarjeta IP500 PRI-U. La tarjeta IP500 PRI-U admite los modos PRI E1, T1 y E1-R2. El sistema IP Office admite 8 canales B sin licencia en cada puerto IP500 PRI-U instalado. Los canales B adicionales, hasta la capacidad de los puertos instalados y el modo PRI seleccionado, requieren licencias. Estos canales adicionales consumen licencias según los canales adicionales configurados como en servicio desde el puerto 9 de la ranura 1 hacia arriba. Los canales D no se ven afectados por las licencias. La licencia está disponible en variantes de 2, 8 y 22 canales que se pueden combinar para obtener el número total de canales necesarios.

- **Canales troncales SIP**
  Estas licencias se utilizan para configurar el número máximo de llamadas de troncales SIP simultáneas admitidas. Las licencias son consumidas por llamadas en curso en un canal SIP. Para soporte SIP, el sistema también requiereRecursos de VCM 224. La licencia está disponible en variantes de 1, 5, 10 y 20 canales que se pueden combinar para obtener el número total de canales necesarios.

- **Redes de voz IP500**
  Estas licencias permiten la compatibilidad con troncales IP SCN, QSIG y H323. Para soporte de red de voz, el sistema también requiereRecursos de VCM 221.

- **Canales troncales SM**
  Estas licencias se utilizan para habilitar líneas SM para la conexión a una red Avaya Aura. El sistema IP Office también requiere un **Sistema de Sucursales**licencia.

13.13.4 Licencias de teléfono/punto final

El uso de teléfonos H323 y SIP con IP Office está controlado por las siguientes licencias. Se utilizan diferentes licencias para los teléfonos IP de Avaya y los teléfonos que no son de Avaya, incluidos los softphones que no son de Avaya.

Para los softphones IP, los requisitos de licencia varían según la aplicación en particular y no se tratan aquí. Consulte la documentación específica de la aplicación. Sin embargo, la mayoría de las aplicaciones de softphone de Avaya no requieren una licencia para terminales IP de Avaya.

De manera predeterminada, las licencias de punto final las consume cada teléfono IP que se registra en el sistema en el orden en que se registran los teléfonos. Sin embargo, es posible reservar una licencia para una extensión en particular para garantizar que ese teléfono siempre obtenga una licencia primero si está disponible. Esto se hace a través de la**Licencia de reserva**ajuste de los ajustes de la extensión en la configuración del sistema. Las licencias se liberan si el teléfono se cancela a menos que se reserve.

- **Advertencia**
  Los teléfonos IP de Avaya sin licencia aún pueden registrarse, pero están limitados a realizar llamadas de emergencia solamente (***marcar emergencia***llamadas de código corto). El usuario asociado se trata como si hubiera cerrado sesión y el teléfono puede mostrar *"No hay licencia disponible"*y*"Solo llamadas de emergencia"*.Si una licencia está disponible, se asigna primero a cualquier teléfono DECT sin licencia y luego a cualquier otro teléfono IP de Avaya sin licencia en el orden en que se registraron los teléfonos.

- **Licencia de terminales IP de Avaya**
  Estas licencias se utilizan para licenciar teléfonos IP físicos de Avaya adicionales. Esto incluye todos los teléfonos 1600, 9600, DECT R4, Spectralink y VPN compatibles.
- **Licencia de terminales IP de terceros**
  Estas licencias se utilizan para admitir teléfonos IP que no son de Avaya, incluidas las extensiones SIP. Las licencias disponibles se utilizan en el orden de registro del teléfono. Si no hay licencias disponibles, el teléfono no puede registrarse. Esta licencia se llamaba anteriormente la **Puntos finales de IP**licencia.
- **Licencia de Softphone de Avaya**
  Esta licencia se utiliza para permitir el soporte paraComunicador de Avaya 256oCliente del lugar de trabajo de Avaya IX 254por un usuario cuyo El perfil con licencia normalmente no admite esas aplicaciones como parte de la licencia del perfil.

¿Comentarios sobre este documento? infodev@avaya.com

13.13.5 Licencias de usuario

Las funciones disponibles para un usuario básico se pueden mejorar mediante la adición de licencias de usuario. Una vez que estas licencias están presentes en la configuración del sistema, los perfiles correspondientes se pueden aplicar a los usuarios seleccionados a través de su**Usuario | Usuario | Perfil** ajuste en la configuración del sistema.

Tenga en cuenta que para todos los perfiles que no sean**Usuario Básico**, a**Edición preferida**la licencia del sistema es un requisito previo para las licencias de usuario requeridas.

	Usuario Básico	Oficina Trabajador	teletrabajador	Móvil Trabajador	Usuario de poder
Servicios del portal one-X	–	✓	✓	–	✓
Opciones de teletrabajador	–	–	✓	–	✓
Servicios Web UMS	–	✓	✓	–	✓
Funciones de movilidad	–	–	–	✓	✓
TTS para lectura de correo electrónico[4]	–	–	–	✓	✓
Trabajador remoto[2]	–	–	✓	–	✓
Comunicador de Avaya[3]	✓[7]	✓	✓	–	✓
Cliente del lugar de trabajo de Avaya IX	✓[5]	✓	✓	✓[5]	✓
Colaboración web[6]	–	✓	✓	–	✓
Programación de conferencias	–	–	–	–	✓

1. un**Edición preferida**[279]La licencia del sistema es un requisito previo para cualquier licencia de perfil de usuario que no sea**Usuario Básico**.

   - En una Red Comunitaria Pequeña, el**Edición preferida**La licencia del sistema central se comparte automáticamente con otros sistemas en la red, lo que permite licencias de perfil de usuario en esos otros sistemas. Sin embargo, cada sistema que admita un servidor Voicemail Pro, por ejemplo, para el correo de voz distribuido, aún requiere su propio **Edición preferida**licencia.

2. La versión 8.0 admite usuarios que utilizan extensiones H323 remotas. Se admiten hasta 4 usuarios básicos en las extensiones remotas del sistema. Se admiten usuarios remotos adicionales si tienen licencia y están configurados para un ***teletrabajador***o ***Usuario de poder***perfil del usuario.

3. Solicite que las aplicaciones one-X Portal for IP Office y Voicemail Pro también estén instaladas para funciones avanzadas.

4. TTS para lectura de correo electrónico también requiere que el sistema de correo de voz tenga una licencia para la cantidad de sesiones TTS simultáneas requeridas.

5. Compatible conCliente del lugar de trabajo de Avaya IX[254]modo independiente con una licencia de Softphone de Avaya.

6. También requiere un**Colaboración web**licencia.

7. Compatible conComunicador de Avaya[256]modo básico con una licencia de Softphone de Avaya.

Licencias de usuario

- **Licencia de teletrabajador**
  Estas licencias establecen el número de usuarios que pueden tener su perfil configurado como***teletrabajador***. Para los usuarios con esta opción, se habilitan ajustes adicionales en la configuración de los siguientes servicios: one-X Portal for IP Office con opción Telecommuter, Avaya Communicator y UMS Web Services. A**Edición preferida**licencia del sistema[279]requisito previo para esta licencia.

- **Licencia de trabajador móvil**
  Estas licencias establecen el número de usuarios que pueden tener su perfil configurado como***Trabajador móvil***. Para usuarios con esta opción, se habilitan configuraciones adicionales en la configuración para los siguientes servicios: Funciones de movilidad y TTS para lectura de correo electrónico. Para IP Office versión 8.0 y superior, todas las funciones de movilidad están habilitadas para todos los usuarios por el **Edición esencial**licencia. A **Edición preferida**licencia del sistema[279]es un requisito previo para esta licencia.

- **Licencia de trabajador de oficina**
  Estas licencias establecen el número de usuarios que pueden tener su perfil configurado como***Empleado de oficina***. Para los usuarios con esta opción, se habilitan ajustes adicionales en la configuración de los siguientes servicios: Portal one-X para IP Office (sin funciones de teletrabajador) y servicios web UMS. A**Edición preferida**licencia del sistema[279]es un requisito previo para esta licencia.

- **Licencia de perfil de usuario avanzado**
  Estas licencias establecen el número de usuarios que pueden tener su perfil configurado como***Usuario de poder***. Para el usuario con esta opción, los mismos servicios adicionales que para Teleworker y Mobile Worker están habilitados para el usuario. A**Edición preferida** licencia del sistema[279]es un requisito previo para esta licencia.

Otras licencias de usuario

Además de las licencias de perfil de usuario anteriores, están disponibles las siguientes licencias de usuario individuales:

- **Recepcionista:**
  Esta licencia se utiliza para habilitar la compatibilidad con la aplicación IP Office SoftConsole. Esta licencia solo puede ser utilizada por usuarios configurados para**Recepcionista**en la configuración de IP Office. Se admite un máximo de 4 recepcionistas. Esta licencia se llamaba anteriormente**SoftConsole**. Cada usuario configurado como usuario consume una instancia de esta licencia. **Recepcionista**.

- **Colaboración web**
  Esta licencia se puede utilizar para habilitar el soporte para elAplicación de colaboración web 260.Una instancia de licencia es requerido para cada usuario configurado para la colaboración web. Compatible con usuarios con licencia como**Empleado de oficina**, **teletrabajador**o**Usuario de poder**.

13.13.6 Licencias de Voicemail Pro

Voicemail Pro se habilita mediante la adición de las siguientes licencias.

- **Edición preferida (Voicemail Pro):**
  Esta licencia permite la compatibilidad con Voicemail Pro como servidor de correo de voz de IP Office con 4 puertos de correo de voz. los **Edición preferida**La licencia permite que el servidor de correo de voz brinde los servicios que se enumeran a continuación. Para IP Office versión 8.0 y superior, un**Edición esencial**La licencia es un requisito previo para esta licencia en los sistemas IP500 V2.

  - Buzones para todos los usuarios y grupos de búsqueda.
  - Anuncios para usuarios y grupos de búsqueda.
  - Flujos de llamadas personalizables.
  - Grabación de llamadas a buzones.
  - Campañas.
  - Lectura de correo electrónico TTS para usuarios con licencia para **Trabajador móvil**o**Usuario de poder**perfiles. También requiere licencias TTS.
  - Uso de**Conferencia Encuéntrame**funciones
  - Secuencias de comandos básicas visuales*(Solo Voicemail Pro basado en Windows)*

  1. un**Edición preferida**[279]La licencia del sistema es un requisito previo para cualquier licencia de perfil de usuario que no sea**Usuario Básico**.

     - En una Red Comunitaria Pequeña, el**Edición preferida**La licencia del sistema central se comparte automáticamente con otros sistemas en la red, lo que permite licencias de perfil de usuario en esos otros sistemas. Sin embargo, cada sistema que admita un servidor Voicemail Pro, por ejemplo, para el correo de voz distribuido, aún requiere su propio **Edición preferida**licencia.

- **Puertos de correo de voz adicionales de Preferred Edition**
  La licencia requerida para la compatibilidad con el servidor Voicemail Pro (Preferred Edition (Voicemail Pro)) también habilita 4 puertos de correo de voz. Estas licencias se pueden usar para agregar puertos de correo de voz adicionales hasta la capacidad máxima del sistema IP Office (IP500 V2 = 40). Esta licencia se llamaba anteriormente**Voicemail Pro adicional (puertos)**. Estas licencias están disponibles en variantes de 2, 4, 8 y 16 puertos que se pueden combinar para obtener el número total de puertos necesarios.

- **Administrador de medios**
  Permite el uso de Media Manager en un IP Office Application Server para brindar un archivo a largo plazo de las grabaciones de llamadas. En una Red Comunitaria Pequeña, cada Oficina de PI requiere su propia licencia.

- **Mensajería en red VMPro**
  Habilita la funcionalidad VPNM (mensajería en red de Voicemail Pro) dentro de Voicemail Pro. Esto permite el intercambio de mensajes con sistemas Voicemail Pro remotos y sistemas Avaya Interchange.

- **VMPro TTS (genérico)**
  Esta licencia heredada permite el uso de instalaciones de texto a voz utilizando software TTS de terceros con Voicemail Proen un servidor Windows . Una licencia por instancia simultánea de uso de TTS. Tenga en cuenta que la licencia de IP Office Advance Edition también habilita 8 puertos de TTS genéricos, pero solo se pueden usar con acciones de Leer texto.

- **VMPro TTS (ScanSoft)**
  Esta licencia heredada permite el uso de funciones de texto a voz utilizando el software TTS suministrado por Avaya con Voicemail Pro. en un servidor Windows . Una licencia por instancia simultánea de uso de TTS.

- **VMPro TTS profesional**
  Esta licencia permite el uso de funciones de texto a voz proporcionadas por Voicemail Proen un servidor basado en Linux . Una licencia por instancia simultánea de uso de TTS.

- **Servicios Web UMS**
  Estas licencias se utilizan para habilitar la compatibilidad con los servicios de correo de voz de UMS para los usuarios configurados en el***Usuario Básico***perfil. Otros usuarios están habilitados para UMS a través de su perfil de usuario con licencia. Estas licencias también se utilizan para otorgar licencias a grupos de búsqueda para servicios de correo de voz UMS. Cada licencia habilita 1 usuario.

13.13.7 Licencias de prueba

Se pueden solicitar licencias de prueba. Cada uno es válido durante 60 días a partir de la fecha de emisión y solo se puede emitir una vez para un número de serie de tarjeta SD del sistema en particular. Aparte de esa restricción, las licencias de prueba funcionan igual que las licencias completas.

13.13.8 Licencias CTI

- **Enlace CTI Pro:**
  Habilita la funcionalidad CTI Link Pro (TAPI Link Pro y DEVLink Pro).
- **Usuario de onda:**
  Permite la transmisión de archivos WAV, utilizando TAPILink Pro, para aplicaciones de voz de terceros. Esta es una licencia por usuario. Tenga en cuenta que las llamadas TAPI WAV usan canales de datos del sistema tomados de los mismos grupos que se usan para los puertos de correo de voz. El número máximo de llamadas de usuario TAPI WAV y usuarios de correo de voz simultáneos está determinado por el tipo de unidad de control de IP Office; IP500 V2 =40.

13.13.9 Otras licencias

- **Correo de voz de Audix:**
  Permite que IP Office use un sistema Intuity Audix o Modular Messaging remoto para el correo de voz en lugar de requerir un servidor de correo de voz local.
- **Tunelización IPSec:**
  Permite que IP Office inicie y finalice túneles IPSec y L2TP.
- **Selección del centro de contacto de Avaya**
  Esta licencia es necesaria para el soporte de Avaya Contact Center Select.

13.14 Compatibilidad de hardware/software

Esta página resume los componentes de hardware y software admitidos en diferentes versiones del software principal de IP Office. Puede obtener información adicional sobre otros productos de Avaya, incluidas las versiones de software compatibles, en el**Matriz de compatibilidad de productos de Avaya** sitio web (https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml).

- **Unidades de control** 285
  - **Módulos de expansión externos** 287
  - **Tarjetas base y troncales** 288
- **Plataformas de servidor** 289
- **Los telefonos** 290
- **Aplicaciones** 295

13.14.1 Unidades de control y componentes de la unidad de control

Unidades de control

Unidad de control	Código material	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
Edición para oficina pequeña	–	–	–	–	–	–	–	–	–	–	–	–
IP403	700350382	–	–	–	–	–	–	–	–	–	–	–
IP406 V1	700210776	–	–	–	–	–	–	–	–	–	–	–
IP406 V2	700359946	✓[1]	✓[1]		–	–	–	–	–	–	–	–
IP412	700350408	✓	✓	✓	–	–	–	–	–	–	–	–
IP500	700417207	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP500 V2	700476005	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. Para que una unidad de control IP406 V2 ejecute el software IP Office versión 4.0 o superior hasta la versión 6.1 de IP Office, la unidad de control debe ser PCS 8 o superior.

Módulos de expansión externos

Módulo	Código material	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
cajero automático IP40016[3]	700211360	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 DS16	700184807	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP400 DS30	700184880	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP400 DS16 V2[3]	700359839	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 DS30 V2[3]	700359847	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Teléfono IP400 8	700184773	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Teléfono IP400 16	700184781	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Teléfono IP400 30	700184799	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Teléfono IP400 8	700359896	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Teléfono IP400 16 V2[3]	700359904	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Teléfono IP400 30 V2[3]	700359912	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 So8	700185077	–	–	–	–	–	–	–	–	–	–	–
IP400 WAN3[1]	–	–	–	–	–	–	–	–	–	–	–	–
IP400 WAN3 10/100[1]	700262009	✓	✓	✓	–	–	–	–	–	–	–	–
cajero automático IP50016[2]	700449473	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 So8	700449515	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP500 DS16	700449499	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS30	700426216	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS16A (RJ21)	700500699	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS30A (RJ21)	700500698	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS16B	700501585	–	–	–	–	–	✓[5]	✓	✓	✓	✓	✓
IP500 DS30B	700501586	–	–	–	–	–	✓[5]	✓	✓	✓	✓	✓
IP500 DS16B2	700511093	–	–	–	–	–	–	–	✓[4]	✓[4]	✓	✓
IP500 DS30B2	700511094	–	–	–	–	–	–	–	✓[4]	✓[4]	✓	✓
Teléfono IP500 16 V2	700449507	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Teléfono IP500 30 V2	700426224	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. No compatible con los sistemas IP500 e IP500 V2.
2. Solo en América del Norte, a menos que se acepte en el país de destino.
3. Estas variantes de IP400 todavía son compatibles con IP Office versión 9.1 y superior.
4. Originalmente solo se admitía en R10.1. Se agregó más soporte en R9.1 SP12 y R10.0 SP5.
5. Service Pack 9 y superior.

Base y Tarjetas

Tarjetas base	Código material	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
Teléfono IP500 2	700431778	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Teléfono IP500 8	700417231	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Estación digital IP500 8	700417330	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Portatarjetas IP500[6]	700417215	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP500 VCM 32[6]	700417389	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 VCM 64[6]	700417397	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 VCM 32 V2[6]	700504031	–	–	–	–	–	✓	✓	✓	✓	✓	✓
IP500 VCM 64 V2[6]	700504032	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Expansión de 4 puertos IP500[6]	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 ETR6[1][2]	700476039	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tarjeta combinada IP500 ATM4[1]	700476013	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
"PCS04 296 y más alto[5]	700476013	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tarjeta combinada IP500 ATM4 V2[1]	700504556	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Tarjeta combinada IP500 BRI BRI[1]	700476021	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 TCM 8[1]	700500758	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
Módulo de comunicaciones unificadas v1[1][6]	700501442	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Módulo de comunicaciones unificadas v2[1][6]	700507449	–	–	–	–	–	–	–	✓	✓	✓	✓

Tarjetas de troncales	Código material	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
Tarjeta de troncales Alog IP500	700417405	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
"PC10 296 y más alto[4]	700417405	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tarjeta de troncales IP500 Alog V2[1][3]	700503164	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Tarjeta de troncales IP500 BRI 4	700417413	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tarjeta de troncales IP500 BRI 8	700417421	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 PRI-1U	700417439	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 PRI-2U	700417462	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 T1(J) PRI Doble	700509377	–	–	–	–	–	–	–	✓	✓	✓	✓

1. Solo sistemas IP500 V2.
2. Solo se admite en los modos IP Office Basic Edition - PARTNER® Mode o IP Office Basic Edition (U-Law) que se ejecutan en una configuración regional de América del Norte.
3. Compatible con 8.1 Feature Pack 1 y superior.
4. Estas tarjetas son compatibles con IP Office versión 4.0 y superior. Sin embargo, las tarjetas PCS10 y superiores solo se admiten en sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) o 8.0 y superior. Consulte la sugerencia técnica 237 de IP Office.
5. Estas tarjetas son compatibles con la versión 6.0 y posteriores de IP Office. Sin embargo, las tarjetas PCS04 y superiores solo se admiten en sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) u 8.0 y superior. Consulte la sugerencia técnica 237 de IP Office.
6. No compatible con los sistemas en modo IP Office Basic Edition.

13.14.2 Plataformas de servidor

Para R11.0.4.2 y versiones posteriores, las plataformas Avaya enviadas actualmente son los modelos R230 y R640.

Plataforma de servidor	Código material	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
DL120G7 SRVR salida a bolsa R8+	269810	–	–	–	–	–	✓	✓	✓	✓	✓	✓
DL120G7 SRVR IPO R8+ FRANCIA TELECOM	270391	–	–	–	–	–	✓	✓	✓	✓	✓	✓
DL120G7 SRVR IPO R8.1+ SE EXP	270395	–	–	–	–	–	✓	✓	✓	✓	✓	✓
SERVIDOR R210 II XL OFICINA IP UNIFICADA COMUNICACIONES	302786	–	–	–	–	–	✓	✓	✓	✓	✓	✓
R210 II XL SERVIDOR IP OFFICE FRANCE TELECOM	302787	–	–	–	–	–	✓	✓	✓	✓	✓	✓
SERVIDOR R210 II XL EDICIÓN SERVIDOR IP OFFICE EXPANSIÓN	302788	–	–	–	–	–	–	✓	✓	✓	✓	✓
R210 II XL SERVIDOR IP OFICINA CENTRO DE CONTACTO SERVIDOR	306626	–	–	–	–	–	–	–	✓	✓	✓	✓
SERVIDOR R220 II XL OFICINA IP UNIFICADA COMUNICACIONES	380223	–	–	–	–	–	–	–	✓	✓	✓	✓
R220 II XL SERVIDOR IP OFFICE FRANCE TELECOM	380224	–	–	–	–	–	–	–	✓	✓	✓	✓
SERVIDOR R220 II XL EDICIÓN SERVIDOR IP OFFICE EXPANSIÓN	380225	–	–	–	–	–	–	–	✓	✓	✓	✓
R220 II XL SERVIDOR IP OFICINA CENTRO DE CONTACTO	380226	–	–	–	–	–	–	–	✓	✓	✓	✓
R230 XL SRVR salida a bolsa UC	390081	–	–	–	–	–	–	–	–	–	–	✓
R230 XL SRVR OPI FRANCE TELECOM	390082	–	–	–	–	–	–	–	–	–	–	✓
R230 XL SRVR IPOCC	390083	–	–	–	–	–	–	–	–	–	–	✓
DL360G7 SRVR IPO R8.1+ PRIMARIO	270393	–	–	–	–	–	✓	✓	✓	✓	✓	✓
R620 SRVR IPO SE PRIMARIO	306961	–	–	–	–	–	–	✓	✓	✓	✓	✓
R630 SRVR OPI SE/UC	383542	–	–	–	–	–	–	✓	✓	✓	✓	✓
R630 SRVR IPOCC	383555	–	–	–	–	–	–	✓	✓	✓	✓	✓
R640 SRVVR P3 salida a bolsa	700514262	–	–	–	–	–	–	–	–	–	✓	✓

13.14.3 Teléfonos

- Serie 1000 290 · Serie 3600 290 · Serie 4600 291 · Serie 9600 292 · Serie J100 293
- Serie 1100 290 · Serie 3700 290 · Serie 5400 291 · Serie B100 292 · Serie K100 293
- Serie 1200 290 · Serie 3800 291 · Serie 5600 291 · Serie D100 293 · Serie M 293
- Serie 1400 290 · Serie 3900 291 · Serie 6400 292 · Serie E100 293 · Serie T 293
- Serie 1600 290 · Serie 4100 291 · Serie 7400 292 · Serie H100 293 · Serie T3 294
- Serie 2400 290 · Serie 4400 291 · Serie 9500 292 · Serie H200 293 · Serie IP T3 294

Serie 1000

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
1010	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1040	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 1100/1200

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
1120E	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1140E	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1220	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1230	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 1400

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
1403	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1408	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1416	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 1600

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
1603[1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603-I	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603SW	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603SW-I	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1608[1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1608-I	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1616[1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1616-I	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. 4.2 Q4 '08+.

Serie 2400

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
2402D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2410D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2420	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 3600

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
3616	✓	✓	✓	✓	✓	✓	–	–	–	–	–
3620	✓	✓	✓	✓	✓	✓	–	–	–	–	–
3626	✓	✓	✓	✓	✓	✓	–	–	–	–	–
3641	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3645	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 3700

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
3701	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Página1306 de 3226.

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
3711	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
3720	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3725	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3730[1]	–	–	–	–	–	–	–	✓	✓	✓	✓
3735[1]	–	–	–	–	–	–	–	✓	✓	✓	✓
3740	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
3745	–	–	–	–	–	–	–	–	✓	✓	✓
3749	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

1. Compatible desde 9.1 SP11, 10.0 SP4.

Serie 3800/3900

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
3810	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
3910	–	✓	✓	✓	✓	✓	✓	✓	✓	–	–
3920	–	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Serie 4100

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
4135	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4136	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4145	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4145EX	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4146	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4146EX	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Serie 4400

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
4406D	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4412D	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4424D	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Serie 4600

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
4601	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4602IP	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4602SW	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4606	–	–	–	–	–	–	–	–	–	–	–
4610SW	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4612	–	–	–	–	–	–	–	–	–	–	–
4620	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4621	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4624	–	–	–	–	–	–	–	–	–	–	–
4625	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Serie 5400

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
5402	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5410	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5420	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Serie 5600

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
5601	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5602IP	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5602SW	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Página1307 de 3226.

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
5610 SW	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5620	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5621	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Serie 6400

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
6408D	✓	✓	✓	–	–	–	–	–	–	–	–
6416D	✓	✓	✓	–	–	–	–	–	–	–	–
6424D	✓	✓	✓	–	–	–	–	–	–	–	–

Serie 7400

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
7420	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7430	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7434	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7439	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7440	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7444	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7449	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Serie 9500

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
9504	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
9508	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Serie 9600

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
9608	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9608G	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9611	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9620		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9620L	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9620C	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9621G	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9621GS	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9630		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9630G	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9640	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9640G	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9641G	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9641GS	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9650	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9650C	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. Service Pack de la versión 8.0 2012 Q1 y superior.

Serie B100

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
B149*(cosa análoga)*	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
B159*(cosa análoga)*	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
B169*(DECT vía estación base analógica o SIP)*	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
B179*(SORBO)*	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
B199*(SORBO)*	–	–	–	–	–	–	–	–	–	–	✓

Serie D100

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
D160	–	–	–	–	–	✓[1]	✓	✓	✓	✓	✓

1. Compatible con 8.1 Feature Pack 1 y superior.

Serie E100

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
E129	–	–	–	–	–	–	✓	✓	✓	✓	✓
E159	–	–	–	–	–	–	✓	✓	✓	✓	✓
E169	–	–	–	–	–	–	✓	✓	✓	✓	✓

Serie H100

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
H175	–	–	–	–	–	–	–	–	✓	✓	✓

Serie H200[1]

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
H229	–	–	–	–	–	–	–	–	–	–	✓
H239	–	–	–	–	–	–	–	–	–	–	✓
H249	–	–	–	–	–	–	–	–	–	–	✓

1. Compatible con R11.0 SP1.

Serie J100

NB: El soporte no incluye las variantes 3PCC Open SIP de estos teléfonos.

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
J129[1]	–	–	–	–	–	–	–	–	✓	✓	✓
J139[3]	–	–	–	–	–	–	–	–	–	–	✓
J159[4]	–	–	–	–	–	–	–	–	–	–	✓
J169[2]	–	–	–	–	–	–	–	–	–	–	✓
J179[2]	–	–	–	–	–	–	–	–	–	–	✓

1. Compatible con R10.0 SP2.
2. Compatible con versiones anteriores que utilizan el firmware H323. Referirse a *"Notas de instalación de la extensión SIP de IP Office"*.
3. Compatible con R11.0 SP1.
4. Compatible con R11.0.4.2.

Serie K100 (teléfonos Vantage)

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
K155	–	–	–	–	–	–	–	–	–	–	✓[1]
K165	–	–	–	–	–	–	–	–	–	–	✓
K175	–	–	–	–	–	–	–	–	–	–	✓

1. Compatible con R11.0 SP1.

Serie M

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
M7100	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7100N	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7208	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7208N	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7310	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7310N	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7324	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7324N	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Serie T

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
T7000	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7100	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7208	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
T7316	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7316E	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7406	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7406E	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
UCA	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Serie T3/T3IP

Teléfono	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
T3 compacto	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
T3 clásico	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Confort T3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Compacto IP T3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
T3 IP clásico	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Comodidad IP T3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–

13.14.4 Aplicaciones

NB: Algunas aplicaciones particulares requieren servidores y licencias adicionales para operar con el sistema IP Office. Esta tabla simplemente indica qué aplicaciones son compatibles con los usuarios de IP500 V2.

Solicitud	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
Registros de detalles de llamadas (CDR)	–	–	–	–	–	–	–	–	–	–	–
Centro de conferencias	✓	–	–	–	–	–	–	–	–	–	–
Centro de negocios compacto	–	–	–	–	–	–	–	–	–	–	–
Registrador de contactos	–	–	–	–	–	✓	✓	✓	✓	✓	–
ContactoTienda	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Reportero de llamadas de clientes	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Centro de contacto compacto	✓	–	–	–	–	–	–	–	–	–	–
Administrador de migración de datos	–	–	–	✓	✓	✓	✓	–	–	–	–
Servidor delta	✓	–	–	–	–	–	–	–	–	–	–
Comunicador de Avaya para ventanas	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Comunicador de Avaya para iPad	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Comunicador de Avaya para Web	–	–	–	–	–	–	–	✓	✓	✓	✓
Cliente del lugar de trabajo de Avaya IX	–	–	–	–	–	–	–	–	–	–	✓
Centro de contacto de IP Office	–	–	–	–	–	–	✓	✓	✓	✓	✓
Reportero de contacto integrado	–	–	–	–	–	–	–	–	–	✓	–
Gerente	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Administrador de medios	–	–	–	–	–	–	–	–	–	✓	✓
MS-CRM	✓	–	–	–	–	–	–	–	–	–	–
Administrador de teléfono	✓	✓	✓	✓	✓	✓	–	–	–	–	–
" Pro	✓	✓	✓	✓	✓	✓	–	–	–	–	–
Softphone profesional	✓	✓	✓	✓	✓	✓	–	–	–	–	–
one-x móvil	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Preferido de one-X Mobile	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Portal one-X	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Asistente de llamadas	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
Complemento de Lync	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Complemento de Outlook	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Complemento de Salesforce	–	–	–	–	✓	✓	✓	✓	–	–	–
Cliente web de IP Office	–	–	–	–	–	–	–	–	–	–	✓
Llamada saliente exprés	–	–	–	–	–	✓	✓	✓	–	–	–
SoftConsole	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Aplicación de estado del sistema	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Monitoreo del sistema	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Enlace TAPI Lite	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Enlace TAPI Pro	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mensajería integrada	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Softphone de vídeo (Mac)	–	–	–	–	✓	✓	✓	✓	✓	✓	–
" (ventanas)	–	✓	✓	✓	✓	✓	✓	✓	–	–	–
Correo de voz ligero	–	–	–	–	–	–	–	–	–	–	–
Buzón de voz profesional	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaboración web	–	–	–	–	–	–	–	✓	✓	✓	✓

13.15 Niveles PCS

Cada elemento del hardware de IP Office tiene un nivel de estado de cambio de producto (PCS). Esto generalmente se incluye en la etiqueta del prefijo de hardware con**PC**.

El nivel de PCS aumenta cada vez que se realiza un cambio significativo en los componentes de esa pieza de hardware. Por ejemplo, el nivel de PCS puede aumentar cuando se reemplaza un componente por uno de un proveedor diferente.

Normalmente, los cambios en un nivel de PCS no son importantes y los elementos del mismo hardware pero con diferentes niveles de PCS siguen siendo idénticos en funcionamiento y pueden intercambiarse. Sin embargo, hay algunas excepciones que se enumeran a continuación.

Restricciones de nivel de PCS

- **Tarjeta de troncales analógicas IP500 V1**
  Estas tarjetas son compatibles con IP Office versión 4.0 y superior. Sin embargo, las tarjetas PCS10 y superiores solo se admiten en sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) o 8.0 y superior. Consulte la sugerencia técnica 237 de IP Office.
- **Tarjeta combinada IP500 ATM4 V1**
  Estas tarjetas son compatibles con la versión 6.0 y posteriores de IP Office. Sin embargo, las tarjetas PCS04 y superiores solo se admiten en sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) u 8.0 y superior. Consulte la sugerencia técnica 237 de IP Office.
- **Unidad de control IP500 V2**
  Para admitir la versión 9.1 o superior de IP Office, las unidades PCS 14 o anteriores primero deben instalar la versión 8.1(65) (o superior 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1 o superior. Se debe tener cuidado para asegurarse de que no se realicen llamadas antes de la actualización final; de lo contrario, el sistema requerirá una licencia de actualización.

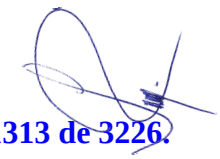
13.16 TAA

Los artículos etiquetados como TAA cumplen con los requisitos de la Ley de Acuerdos Comerciales, que es un requisito previo para las compras federales en los Estados Unidos de América. A menos que se indique lo contrario, las variantes de equipo TAA son física y funcionalmente iguales a las variantes que no son TAA.

		Código SAP
Unidad de control	UNIDAD DE CONTROL IPO IP500 V2 TAA 205	700501510
Tarjetas base	IPO IP500 TARJETA EXTN DGTL STA 8 TAA 218	700501512
	IPO IP500 V2 COMB TARJETA ATM TAA 214	700501513
	IPO IP500 VCM 32 TAA 221	700501518
	IPO IP500 VCM 32 TAA V2 221	700504033
Tarjetas de la hija del tronco	IPO IP500 TRNK BRI 4 UNI TAA 226	700501515
	IPO IP500 TRNK PRI UNVRSL SNGL TAA 227	700501514
	IPO IP500 TRNK PRI UNVRSL DUAL TAA 227	700501517
Módulos de expansión externos	IPO IP500 EXP MOD ANLG TRNK 16 TAA 229	700501511
	IPO IP500 EXP MOD DGTL STA 16 TAA 231	700501516
Teléfonos	**Teléfono de escritorio IP 9608 TAA Global**	700501428, 700507947
	Teléfono de escritorio IP 9608G TAA Global	700507946
	Teléfono de escritorio IP 9611G TAA Global	700501429, 700507948
	Teléfono de escritorio IP 9621G TAA Global	700500254, 700506516
	Teléfono de escritorio IP 9641G TAA Global	700501431, 700506519

Capítulo 14.

Declaraciones de seguridad



14. Declaraciones de seguridad

Los módulos de oficina IP500 de Avaya están destinados a ser instalados por "personal de servicio" y es responsabilidad del personal de servicio asegurarse de que todos los equipos interconectados subsidiarios estén cableados correctamente y también cumplan con los requisitos de seguridad de IEC60950 o UL60950, según corresponda.

- La marca CE adherida a este equipo significa que el módulo cumple con las directivas 1999/5/EC (R&TTE), 89/336/EEC (EMC) y 72/23EEC (LVD).
- Las declaraciones de conformidad (DoC) para los productos IP500 están disponibles en el DVD de la aplicación IP Office.
- Este símbolo de advertencia se encuentra en la base de los módulos IP500.
- Referirse aMódulos de interfaz troncal 299para obtener información sobre qué variantes de módulos de interfaz de troncales están instaladas en qué país.

En Finlandia, Noruega y Suecia, se debe conectar un conductor de conexión a tierra de protección al punto de conexión a tierra de protección en la parte posterior de la unidad de control IP500 V2. VerToma de tierra 93para más información. Además, el servidor debe estar ubicado en un lugar de acceso restringido donde se haya aplicado la conexión equipotencial, por ejemplo, en un centro de telecomunicaciones.

14.1 Protección contra rayos/símbolos de peligro

Pararrayos

Los pararrayos de los edificios deben verificarse de la siguiente manera:

1. Verifique los pararrayos, en el punto de entrada del cable troncal al edificio donde se encuentra Avaya IP Office, prestando especial atención a la puesta a tierra de los pararrayos. Informe cualquier problema, por escrito, a la compañía telefónica.
2. Los equipos que están diseñados para conectarse mediante cableado interno generalmente no están protegidos contra rayos. Por lo tanto, el cableado de extensión de Avaya IP Office no debe salir del edificio. Para instalaciones donde los teléfonos y/u otros dispositivos estándar (tip/ring) están instalados en otro edificio, entonces se requiere protección contra rayos (verInstalaciones Telefónicas Fuera de Edificio 36).

Símbolo de peligro

El símbolo de peligro de descarga eléctrica tiene por objeto alertar al personal sobre peligros eléctricos o daños en el equipo. También se deben observar las siguientes precauciones al instalar equipos telefónicos:

1. Nunca instale cableado telefónico durante una tormenta eléctrica.
2. Nunca instale conectores telefónicos en lugares húmedos a menos que el conector esté diseñado específicamente para lugares húmedos.
3. Nunca toque cables telefónicos o terminales sin aislamiento a menos que la línea telefónica haya sido desconectada en la interfaz de red.
4. Siempre tenga cuidado cuando trabaje con líneas telefónicas.

14.2 Módulos de interfaz troncal

Para garantizar la validación de las aprobaciones, solo los siguientes tipos de tarjetas de interfaz troncal deben instalarse en las siguientes unidades de control de IP Office.

EE. UU./Canadá						
Producto	**Patio BRI**	**PRI E1**		**PRI T1**		**Cosa análoga Tronco Tarjeta**
		Único	**Doble**	**Único**	**Doble**	
IP500 V2	✗	✗	✗	✓	✓	✓
IP500	✗	✗	✗	✓	✓	✓

Resto del mundo						
Producto	**Patio BRI**	**PRI E1/E1R2**		**PRI T1**		**Cosa análoga Tronco Tarjeta**
		Único	**Doble**	**Único**	**Doble**	
IP500 V2	✓	✓	✓	✗	✗	✓
IP500	✓	✓	✓	✗	✗	✓

notas

- Los troncales E1R2 solo se admiten en CALA y Corea.

14.3 Información adicional y actualizaciones de productos

Se puede obtener más información, incluidas las actualizaciones del Manual de referencia y del producto, en los distribuidores y distribuidores de Avaya o en el sitio web de Avaya:http://www.avaya.com .

Esta guía también está disponible en el sitio web de soporte de Avaya:http://soporte.avaya.com .

Números de teléfono de soporte

Para obtener ayuda y soporte iniciales, comuníquese con su distribuidor/proveedor. Los siguientes puntos de contacto son para socios autorizados de Avaya.

Solo en los EE. UU.

Avaya ofrece una línea de ayuda al cliente de árbol de peaje las 24 horas del día:

- Nombre: Organización de soporte técnico de Avaya (TSO)
- Línea de atención al cliente: 1 800 628-2888
- Dirección: 8744 Lucent Blvd., Highlands Ranch, Colorado, 80129 EE. UU.
- URL:http://soporte.avaya.com
  Si necesita ayuda para instalar, programar o usar su sistema, llame a la línea de ayuda oa su representante de Avaya. Se pueden aplicar cargos por consulta.

Fuera de los EE. UU.

Si necesita ayuda para instalar, programar o usar su sistema, comuníquese con su representante de Avaya.

- URL:http://soporte.avaya.com

14.4 Clasificación de seguridad portuaria

Los sistemas Avaya IP Office tienen los siguientes puertos que se clasifican de la siguiente manera:

Nombre del puerto	Descripción del puerto	Clasificación de puertos
Puerto PRI	Conexión PRI RDSI (NET)	TNV (Operando dentro de los límites de SELV)
puertos BRI	Conexión RDSI BRI (NET)	TNV (Operando dentro de los límites de SELV)
Puertos analógicos	Troncal analógico de dos hilos	TNV3
Puertos de falla de energía	Troncal analógico de dos hilos	TNV3
Puerto RS232 DTE	Conexión de datos asíncrona.	SELV
Puertos telefónicos analógicos	Puertos de extensión telefónica	TNV2
Puertos telefónicos digitales	Puertos de extensión telefónica	SELV
Puertos LAN	Conexión 10/100 BaseT a LAN.	SELV
Puertos de expansión	Conector del módulo de expansión.	SELV
Puerto de audio	Conector para Música en Espera.	SELV
Puerto de control externo	Conector para Control de Circuitos Auxiliares.	SELV
Puerto de entrada de CC	Conector para alimentación de entrada de CC.	SELV

Los circuitos de interconexión deben seleccionarse para proporcionar conformidad continua con los requisitos de EN 609050:1992/A3:1995, cláusula 2.3 para circuitos SELV y con los requisitos de la cláusula 6 para circuitos TNV, después de las conexiones entre equipos.

Traducido del inglés al español - www.onlinedoctranslator.com

14.5 Directiva EMC

889/336/EEC (Directiva EMC) CISPR 22:1993 incluyendo A1 + A2, AS/NZ 3548:1995 (ROW)

- **ADVERTENCIA**
  Este es un producto de clase A. En un entorno doméstico, este producto puede causar interferencias de radio, en cuyo caso se puede solicitar al usuario que tome las medidas adecuadas.

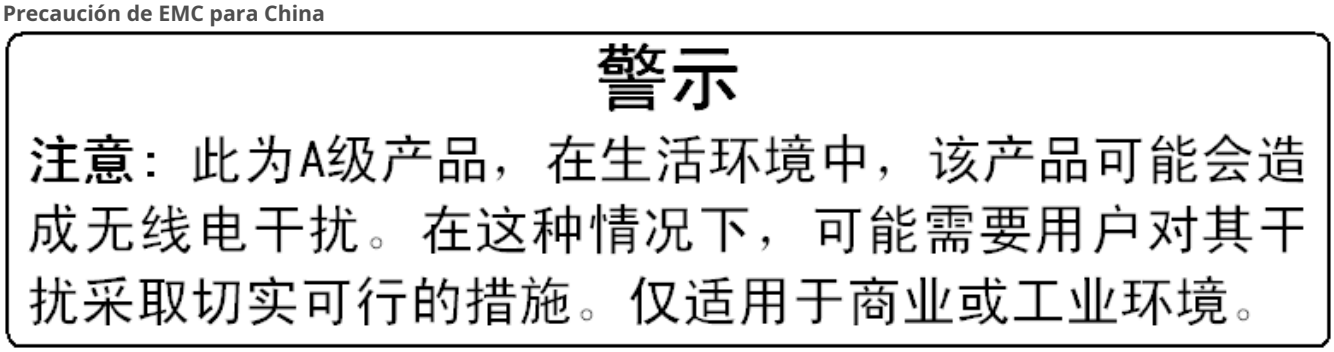
Comisión Federal de Comunicaciones (FCC)

Este equipo ha sido probado y se encontró que cumple con los límites para un dispositivo digital de Clase A, de conformidad con la Parte 15 de las Reglas de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias dañinas cuando el equipo funciona en un entorno comercial. Este equipo genera, usa y puede irradiar energía de radiofrecuencia y, si no se instala y usa de acuerdo con el manual de instrucciones, puede causar interferencias dañinas en las comunicaciones por radio. Es probable que la operación de este equipo en un área residencial cause interferencia dañina, en cuyo caso el usuario deberá corregir la interferencia por su propia cuenta.

Departamento Canadiense de Comunicaciones (DOC)

''AVISO: Este equipo cumple con las especificaciones técnicas aplicables de equipos terminales de Industry Canada. Esto es confirmado por el número de registro. La abreviatura, IC, antes del número de registro significa que el registro se realizó sobre la base de una Declaración de conformidad que indica que se cumplieron las especificaciones técnicas de Industry Canada. No implica que Industry Canada haya aprobado el equipo".

Precaución de EMC para China



14.6 Instrucciones reglamentarias de uso

14.6.1 Australia

Conexión

La conexión de los productos de IP Office debe realizarse a través de un módulo de aislamiento de línea con una etiqueta de cumplimiento de telecomunicaciones.

Interfaz BRI

Durante la configuración, asegúrese de que el número de emergencia "000" no esté bloqueado, realizando lo siguiente:

- Código corto: 000
- Número de teléfono: 000;
- Función: DialEmergency

En las conexiones a TS013, no se utilizarán las siguientes capacidades portadoras:

- 7kHz Audio, Video, Información Digital Restringida.

Si se utiliza un tipo de número desconocido en el número de la persona que llama, la red utilizará la CLI predeterminada.

El sistema debe estar configurado para conexión Punto a Multipunto para cumplir con los requisitos de Austel para conectarse a circuitos TS013.

Como IP Office no es compatible con la marcación de emergencia después de una pérdida de energía, se debe reconocer el siguiente aviso de advertencia:

- **ADVERTENCIA**
  Este equipo no funcionará cuando falle la alimentación de red.

Interfaz PRI

Durante la configuración, asegúrese de que el número de emergencia "000" no esté bloqueado, realizando lo siguiente:

- Código corto: 000
- Número de teléfono: 000;
- Función: DialEmergency

- **ADVERTENCIA**
  Este equipo no funcionará durante un corte de energía eléctrica.

14.6.2 Canadá

Este equipo cumple con las especificaciones técnicas aplicables de equipos terminales de Industry Canada. Esto es confirmado por el número de registro. La abreviatura, IC, antes del número de registro significa que el registro se realizó sobre la base de una Declaración de conformidad que indica que se cumplieron las especificaciones técnicas de Industry Canada.

No implica que Industry Canada haya aprobado el equipo.

''AVISO: El número de equivalencia de timbre (REN) para este equipo terminal es 1. El REN asignado a cada equipo terminal proporciona una indicación del número máximo de terminales que se pueden conectar a una interfaz telefónica. La terminación en una interfaz puede consistir en cualquier combinación de dispositivos sujeta únicamente al requisito de que la suma de los números de equivalencia de timbre de todos los dispositivos no exceda de cinco”.

14.6.3 China

AVAYA

700433220
February 2007
Copyright© 2007, Avaya Inc. All Rights Reserved

所有在中华人民共和国境内进口或销售的电子信息产品必须附上本文件
Include this document with all Electronic Information Products imported or sold in the People's Republic of China

部件名称 (Part Name)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 (Metal Parts)	×	○	○	○	○	○
电路模块 (Circuit Modules)	×	○	○	○	○	○
电缆及电缆组件 (Cables & Cable Assemblies)	×	○	○	○	○	○
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	○
电路开关/断路器 (Circuit Switch/Breakers)	○	○	○	○	○	○
电源组件 (Power Assemblies)	×	○	○	○	○	○
显示器 (LCD, Monitor)	○	○	○	○	○	○
玻璃 (Glass)	○	○	○	○	○	○

○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363 2006 标准规定的限量要求以下。
Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363 2006 standard.

×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363 2006 标准规定的限量要求。
Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363 2006 standard.

本表显示，所附的亚美亚电子信息产品中，从生产日期起，可能包含这些物质。注意：所附产品可能包含或不含以上所列的某些组件。
This table shows where these substances may be found in Avaya's electronic information products, as of the date of manufacture of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

除非有另外特别的标注,此标志将作为所附产品及零部件的环保使用期标志. 某些产品会有一个不同的环保使用期(例如,电话机)并贴在其产品上.此环保使用期限只适用于产品在产品手册中所规定的条件下使用

The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain products have a different EFUP (for example, telephones) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

14.6.4 Japón

El juego de cables de alimentación incluido en el envío o asociado con el producto está diseñado para usarse únicamente con dicho producto. No utilice el juego de cables para ningún otro propósito. Cualquier uso no recomendado podría provocar incidentes peligrosos como incendios, descargas eléctricas y funcionamiento defectuoso.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります

Si se trata de un dispositivo de Clase A:

Este es un producto Clase A basado en el estándar del Consejo de Control Voluntario de Interferencias por Equipos de Tecnología de la Información (VCCI). Si este equipo se utiliza en un entorno doméstico, es posible que se produzcan interferencias de radio, en cuyo caso, es posible que el usuario deba tomar medidas correctivas.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるように要求されることがあります

Si se trata de un dispositivo de Clase B:

Este es un producto de Clase B basado en el estándar del Consejo de Control Voluntario de Interferencias de Equipos de Tecnología de la Información (VCCI). Si se utiliza cerca de un receptor de radio o televisión en un entorno doméstico, puede provocar interferencias de radio. Instale y utilice el equipo de acuerdo con el manual de instrucciones.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい

14.6.5 Unión Europea

1. No se deben bloquear las llamadas al 999 y al 112. Si lo hace, invalidará la aprobación.
2. Todas las conexiones en el MDF deberán ser identificables mediante un etiquetado adecuado.
3. La marca CE que se muestra en el equipo de IP Office indica el cumplimiento de los sistemas con las directivas EMC, LVD y R&TTE y los reglamentos técnicos comunes para ISDN de tarifa primaria y básica.
4. Todos los puertos para la conexión de otros aparatos que no sean de telecomunicaciones tienen un estado de seguridad de voltaje extra bajo de seguridad (SELV).

Declaraciones de conformidad de la Unión Europea

Avaya Inc. declara que el equipo especificado en este documento que lleva la marca "CE" (Conformité Europeénne) cumple con la Directiva de equipos terminales de radio y telecomunicaciones de la Unión Europea (1999/5/EC), incluida la Directiva de compatibilidad electromagnética (2004/108/ CE) y la Directiva de Baja Tensión (2006/95/CE).

Se pueden obtener copias de estas Declaraciones de conformidad (DoC) comunicándose con su representante de ventas local y están disponibles en el siguiente sitio web: http://support.avaya.com/DoC.

Directiva sobre baterías de la Unión Europea

Avaya Inc. es compatible con la Directiva sobre baterías de la Unión Europea 2006/66/EC. Ciertos productos de Avaya Inc. contienen baterías de litio. Estas baterías no son piezas reemplazables por el cliente o en campo. No desarmar. Las baterías pueden suponer un peligro si no se manipulan correctamente.

14.6.6 Nueva Zelanda

La concesión de un Telepermiso para cualquier elemento de equipo terminal indica únicamente que Telecom ha aceptado que el elemento cumple con las condiciones mínimas para la conexión a su red. No indica respaldo del producto por parte de Telecom, ni proporciona ningún tipo de garantía. Sobre todo, no garantiza que ningún artículo funcione correctamente en todos los aspectos con otro equipo con permiso Tele de una marca o modelo diferente, ni implica que ningún producto sea compatible con todos los servicios de red de Telecom.

14.6.7 Notificación de la FCC

Este equipo cumple con la Parte 68 de las normas de la FCC y los requisitos adoptados por el Consejo Administrativo de Accesorios de Terminales (ACTA). En la parte trasera de este equipo hay una etiqueta que contiene, entre otra información, un identificador de producto en el formato US:AAAEQ##TXXX. Si se solicita, este número debe proporcionarse a la compañía telefónica.

El REN se utiliza para determinar la cantidad de dispositivos que se pueden conectar a la línea telefónica. Los REN excesivos en la línea telefónica pueden provocar que los dispositivos no suenen en respuesta a una llamada entrante. En la mayoría de las áreas, pero no en todas, la suma de REN no debe exceder 5.0. Para estar seguro de la cantidad de dispositivos que se pueden conectar a una línea, según lo determinado por los REN totales, comuníquese con la compañía telefónica local. Para los productos aprobados después del 23 de julio de 2001, el REN de este producto forma parte del identificador del producto que tiene el formato US:AAAEQ##TXXX. Los dígitos representados por ## son el REN sin punto decimal (por ejemplo, 03 es un REN de 0,3). Para productos anteriores, el REN se muestra por separado en la etiqueta.

Medios de conexión

La conexión de este equipo a la red telefónica se muestra en la siguiente tabla.

Puerto	FIC	SOC	Gato USOC	REN
IP500 PRI 1U, IP500 PRI2U	04DU9.BN, 04DU9.DN, 04DU9.IKN, 04DU9.ISN	6,0 años	RJ48C	N / A
IP500 ATM4U	OL13A, OL13B, OL13C, 02AC2, 02LA2, 02LB2, 02LC2, 02LR2, 02LS2	9.0Y	RJ45S	0.1B
cajero automático IP50016	OL13A, OL13B, OL13C, 02AC2, 02GS2, 02LA2, 02LB2, 02LC2, 02LR2, 02LF2 02GS2, 02LS2	9.0Y	RJ45S	0.1B

Si este equipo causa daño a la red telefónica, la compañía telefónica le notificará con anticipación que es posible que se requiera la interrupción temporal del servicio. Pero si el aviso previo no es práctico, la compañía telefónica notificará al cliente lo antes posible. Además, se le informará sobre su derecho a presentar una queja ante la FCC si lo considera necesario.

La compañía telefónica podrá realizar cambios en sus instalaciones, equipos, operaciones o procedimientos que puedan afectar el funcionamiento del equipo. Si esto sucede, la compañía telefónica le avisará con anticipación para que realice las modificaciones necesarias para mantener el servicio sin interrupciones.

Si tiene problemas con este equipo, para obtener información sobre reparación o garantía, comuníquese con el Centro de servicio técnico al 1-800-242-2121 o comuníquese con su representante local de Avaya. Si el equipo está causando daños a la red telefónica, la compañía telefónica puede solicitarle que desconecte el equipo hasta que se resuelva el problema.

El enchufe y el conector que se utilicen para conectar este equipo al cableado y la red telefónica de las instalaciones deben cumplir con las reglas y los requisitos aplicables de la Parte 68 de la FCC adoptados por ACTA.

La conexión al servicio de línea compartida está sujeta a tarifas estatales. Comuníquese con la comisión estatal de servicios públicos, la comisión de servicios públicos o la comisión de corporaciones para obtener información.

Equipos con Discado Directo Interno (“DID”):

Permitir que este equipo se opere de tal manera que no brinde una supervisión de respuesta adecuada es una violación de la Parte 68 de las reglas de la FCC.

La supervisión de respuesta adecuada es cuando:

A. Este equipo devuelve la supervisión de respuesta a la red telefónica pública conmutada (PSTN) cuando las llamadas DID son:

- contestado por la estación llamada,
- respondido por el asistente,
- enrutado a un anuncio grabado que puede ser administrado por el usuario del equipo local del cliente (CPE).
- Enrutado a un indicador de marcación

B. Este equipo devuelve señales de supervisión de respuesta en todas las llamadas (DID) reenviadas a la PSTN. Las excepciones permitidas son:

- No se responde una llamada.
- Se recibe un tono de ocupado.
- Se recibe un tono de reorden.

Avaya certifica que este equipo registrado es capaz de proporcionar a los usuarios acceso a proveedores interestatales de servicios de operador mediante el uso de códigos de acceso. La modificación de este equipo por agregadores de llamadas para bloquear los códigos de marcación de acceso es una violación de la Ley de Consumidores de Operadores Telefónicos de 1990.

Marcadores automáticos:

Al programar números de emergencia y (o) realizar llamadas de prueba a números de emergencia:

1. Permanezca en la línea y explique brevemente al despachador el motivo de la llamada.
2. Realice dichas actividades fuera de las horas pico, como temprano en la mañana o tarde en la noche.

Restricción de peaje y equipos de enrutamiento de menor costo:

El software contenido en este equipo para permitir el acceso de los usuarios a la red debe actualizarse para reconocer los códigos de área de red recién establecidos y los códigos de intercambio a medida que se ponen en servicio.

Si no se actualizan los sistemas de las instalaciones o el equipo periférico para reconocer los nuevos códigos a medida que se establecen, se restringirá el acceso del cliente y de los empleados del cliente a la red ya estos códigos.

FCC Parte 68 Declaraciones de conformidad del proveedor

Avaya Inc. en los Estados Unidos de América certifica por la presente que el equipo descrito en este documento y que lleva un número de identificación de etiqueta TIA TSB-168 cumple con las Reglas y Regulaciones de la FCC 47 CFR Parte 68, y el Consejo Administrativo de Conexión de Terminales (ACTA) criterios técnicos adoptados.

Avaya afirma además que el equipo terminal equipado con teléfono de Avaya descrito en este documento cumple con el Párrafo 68.316 de las Reglas y Regulaciones de la FCC que definen la Compatibilidad con Audífonos y se considera compatible con los audífonos.

14.6.8 Cumplimiento de las normas de la FCC

Configuración de ganancia de transmisión y recepción para PRI/T1 y puertos analógicos

Los ajustes de ganancia están controlados por contraseña para uso exclusivo del personal de instalación calificado y no deben estar disponibles para el usuario final. La configuración de ganancia predeterminada de 0dB garantiza el cumplimiento de la sección 68.308(b)(5) de la parte 68 de la FCC y la sección 4.5.2.5 de TIA/EIA-IS-968. "Mediante amplificación de transmisión desde puertos para la conexión de equipos registrados por separado o desde otros puertos de conexión a la red". El ajuste de la configuración de ganancia por parte de personal no calificado puede resultar en una violación de las reglas de la FCC. El personal calificado puede ajustar la configuración de ganancia por encima de estos niveles solo cuando:

1. La medición se realiza para garantizar que los niveles de potencia enviados a la línea en cada interfaz de red conectada no excedan los niveles máximos especificados en FCC parte 68 sección 68.308(b) y TIA/EIA-IS-968 Sección 4.5 para ese tipo de interfaz específico .
2. Cuando se realicen ajustes de ganancia fuera de los valores predeterminados, se deben tomar precauciones para garantizar que la conexión del equipo terminal sea controlada por personal de instalación calificado.
3. Para cumplir con el índice de sonoridad objetivo de recepción a distancias superiores a 2,7 km de la oficina central, en las troncales analógicas se debe establecer una ganancia de recepción de 1,5 dB.

Capítulo 15.

Historia del documento

15. Historial del documento

Fecha	Tema	Resumen de cambios
15 de noviembre de 2017	33a	Actualización para la versión 11.0 de IP Office.
14 de febrero de 2018	33b	· Conversión a la herramienta de creación HMv7. · Eliminación de Integrated Contact Reporter.
26 de abril de 2018	33c	· Corrección a la visualización de encabezados de tablas en las salidas.
10 de mayo de 2018	33d	· Equinox no es compatible con macOS 10.10. · IE10 solo se admite en Windows Server 2012.
16 de mayo de 2018	33e	· Adición del servidor Dell R630.
18 de mayo de 2018	33f	· Avaya Communicator for Windows dejó de ser compatible de forma incorrecta en R11.0. · Licencia de sistema de modo avanzado de Clarified Communicator para IP500 V2. · Se corrigió el error en las propiedades de título HTML/metadatos de salida de PDF.
22 de mayo de 2018	33g	· Tablas divididas que causaban una carga de HTML excesivamente lenta.
20 de agosto de 2018	33h	· Simplifique la nota de instalación de .NET de la suite de administración. · Actualización para R110.0 SP1. Adición de compatibilidad con teléfonos de las series J139, K155 y H200. · Se eliminó la declaración incorrecta del soporte de Equinox en los teléfonos K100.
21 de agosto de 2018	33i	· Vuelva a publicar para corregir la imagen que falta (SVG) y los encabezados de las tablas en blanco.
13 de septiembre de 2018	33j	· Corrija las fuentes de alimentación admitidas para los módulos actuales. · H229 incorrecto listado como analógico. Movido a teléfonos IP SIP. · La música interna en espera no es compatible con la Edición básica. · La salida HTML de la Edición básica se etiquete incorrectamente como Edición esencial.
9 de octubre de 2018	33k	· Más de dos JBM24 requieren fuente de alimentación principal para el teléfono en lugar de PoE.
6 de noviembre de 2018	33l	· Corrección a la tabla de soporte de Equinox. · Actualizaciones para la versión 11.0 SP2: oEquinox escritorio/modo de control compartido.
30 de enero de 2019	34a	· Actualizaciones para 11.0.3.0/11.0.4.0: · Soporte para módulo JEM24 y J179 Bluetooth.
15 de febrero de 2019	34b	· Sección Novedades actualizada para 11.0.4.0.
7 de agosto de 2019	34c	· Corrección. Equinox on Vantage ahora es compatible a partir de 11.0.4.0.
20 de noviembre de 2019	35a	· Actualizaciones para R11.0.4.2.0: oCompatibilidad con firmware J100 4.0.3 y teléfonos J159. o Cambio de marca de Equinox a Avaya IX Workplace.
27 de noviembre de 2019	35b	· Restablecimiento y actualización de detalles de montaje en pared/rack.
3 de diciembre de 2019	35c	· Nota adicional. Capacidad máxima de extensión de DS en los modos de IP Office Basic Edition.
4 de diciembre de 2019	35d	· Retire los teléfonos E159/E169. Ahora soporte de fin de servicio de Avaya.
9 de diciembre de 2019	35e	· Corregir enlaces perdidos.
6 de enero de 2020	35f	· Actualice el enlace de la base de conocimientos de IP Office.

© 2020 AVAYA Todos los derechos reservados.

Aviso

Si bien se han realizado esfuerzos razonables para garantizar que la información de este documento sea completa y precisa en el momento de la impresión, Avaya no asume ninguna responsabilidad por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información de este documento sin la obligación de notificar a ninguna persona u organización sobre dichos cambios.

Descargo de responsabilidad de la documentación

"Documentación" hace referencia a la información publicada por Avaya en diversos medios que pueden incluir información sobre productos, instrucciones de funcionamiento y especificaciones de rendimiento que Avaya generalmente puede poner a disposición de los usuarios de sus productos y servicios alojados. La documentación no incluye materiales de marketing. Avaya no será responsable de ninguna modificación, adición o eliminación de la versión original publicada de la documentación, a menos que Avaya haya realizado dichas modificaciones, adiciones o eliminaciones. El usuario final acepta indemnizar y eximir de responsabilidad a Avaya, a los agentes, servidores y empleados de Avaya frente a todos los reclamos, juicios, demandas y juicios que surjan de, o en relación con, modificaciones, adiciones o eliminaciones posteriores a esta documentación, en la medida en que lo haga End Usuario.

Descargo de responsabilidad del enlace

Avaya no es responsable del contenido o la confiabilidad de los sitios web vinculados a los que se hace referencia en este sitio o la documentación proporcionada por Avaya. Avaya no es responsable de la precisión de la información, declaración o contenido proporcionado en estos sitios y no respalda necesariamente los productos, servicios o información descritos u ofrecidos en ellos. Avaya no garantiza que estos enlaces funcionen todo el tiempo y no tiene control sobre la disponibilidad de las páginas enlazadas.

Garantía

Avaya proporciona una garantía limitada para el hardware y el software de Avaya. Consulte su contrato de venta para establecer los términos de la garantía limitada. Además, el lenguaje de la garantía estándar de Avaya, así como la información sobre el soporte para este producto mientras está en garantía, está disponible para los clientes de Avaya y otras partes a través del sitio web de soporte de Avaya: https://support.avaya.com/helpcenter/getGenericDetails?detailId= C20091120112456651010 en el enlace "Garantía y ciclo de vida del producto" o en el sitio sucesor designado por Avaya. Tenga en cuenta que si adquirió los productos de un socio de canal autorizado de Avaya fuera de los Estados Unidos y Canadá, dicho socio de canal de Avaya le proporciona la garantía y no Avaya.

"Servicio alojado" hace referencia a una suscripción de servicio alojado que adquiere de Avaya o de un socio de canal autorizado de Avaya (según corresponda) y que se describe con más detalle en Hosted SAS u otra documentación de descripción del servicio con respecto al servicio alojado aplicable. Si compra una suscripción al Servicio alojado, es posible que la garantía limitada anterior no se aplique, pero puede tener derecho a servicios de soporte en relación con el Servicio alojado, como se describe más adelante en los documentos de descripción del servicio para el Servicio alojado correspondiente. Comuníquese con Avaya o con el socio de canal de Avaya (según corresponda) para obtener más información.

Servicio alojado

LO SIGUIENTE SE APLICA SI COMPRA UNA SUSCRIPCIÓN AL SERVICIO ALOJADO DE AVAYA O DE UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA), LOS TÉRMINOS DE USO PARA LOS SERVICIOS ALOJADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO BAJO EL ENLACE Los "Términos de uso de Avaya para los servicios alojados" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, Y SON APLICABLES A CUALQUIER PERSONA QUE ACCEDA O UTILICE EL SERVICIO ALOJADO. AL ACCEDER O UTILIZAR EL SERVICIO ALOJADO, O AL AUTORIZAR A OTROS A HACERLO, USTED, EN NOMBRE DE USTED Y DE LA ENTIDAD PARA LA QUE LO ESTÁ HACIENDO (EN ADELANTE DENOMINADO INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA LOS TÉRMINOS DE USO. SI USTED ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR DICHA ENTIDAD A ESTOS TÉRMINOS DE USO. SI USTED NO TIENE TAL AUTORIDAD, O SI NO DESEA ACEPTAR ESTOS TÉRMINOS DE USO, NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEMPRE QUE PARA CIERTOS SERVICIOS ALOJADOS SI CORRESPONDE, PUEDE TENER LA OPORTUNIDAD DE UTILIZAR LICENCIAS FLEX, QUE SERÁN FACTURADO SEGÚN EL USO REAL POR ENCIMA DEL NIVEL DE LICENCIA DEL CONTRATO. CONTACTE A AVAYA O AL SOCIO DEL CANAL DE AVAYA PARA OBTENER MÁS INFORMACIÓN SOBRE LAS LICENCIAS PARA EL SERVICIO ALOJADO CORRESPONDIENTE, LA DISPONIBILIDAD DE CUALQUIER LICENCIA FLEX (SI CORRESPONDE), PRECIOS E INFORMACIÓN DE FACTURACIÓN, Y OTRA INFORMACIÓN IMPORTANTE RELACIONADA CON EL SERVICIO ALOJADO. NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEMPRE QUE PARA CIERTOS SERVICIOS ALOJADOS SI CORRESPONDE, PUEDE TENER LA OPORTUNIDAD DE UTILIZAR LICENCIAS FLEX, QUE SERÁN FACTURADO SEGÚN EL USO REAL POR ENCIMA DEL NIVEL DE LICENCIA DEL CONTRATO. CONTACTE A AVAYA O AL SOCIO DEL CANAL DE AVAYA PARA OBTENER MÁS INFORMACIÓN SOBRE LAS LICENCIAS PARA EL SERVICIO ALOJADO CORRESPONDIENTE, LA DISPONIBILIDAD DE CUALQUIER LICENCIA FLEX (SI CORRESPONDE), PRECIOS E INFORMACIÓN DE FACTURACIÓN, Y OTRA INFORMACIÓN IMPORTANTE RELACIONADA CON EL SERVICIO ALOJADO. NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEMPRE QUE PARA CIERTOS SERVICIOS ALOJADOS SI CORRESPONDE, PUEDE TENER LA OPORTUNIDAD DE UTILIZAR LICENCIAS FLEX, QUE SERÁN FACTURADO SEGÚN EL USO REAL POR ENCIMA DEL NIVEL DE LICENCIA DEL CONTRATO. CONTACTE A AVAYA O AL SOCIO DEL CANAL DE AVAYA PARA OBTENER MÁS INFORMACIÓN SOBRE LAS LICENCIAS PARA EL SERVICIO ALOJADO CORRESPONDIENTE, LA DISPONIBILIDAD DE CUALQUIER LICENCIA FLEX (SI CORRESPONDE), PRECIOS E INFORMACIÓN DE FACTURACIÓN, Y OTRA INFORMACIÓN IMPORTANTE RELACIONADA CON EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEMPRE QUE PARA CIERTOS SERVICIOS ALOJADOS SI CORRESPONDE, PUEDE TENER LA OPORTUNIDAD DE UTILIZAR LICENCIAS FLEX, QUE SERÁN FACTURADO SEGÚN EL USO REAL POR ENCIMA DEL NIVEL DE LICENCIA DEL CONTRATO. CONTACTE A AVAYA O AL SOCIO DEL CANAL DE AVAYA PARA OBTENER MÁS INFORMACIÓN SOBRE LAS LICENCIAS PARA EL SERVICIO ALOJADO CORRESPONDIENTE, LA DISPONIBILIDAD DE CUALQUIER LICENCIA FLEX (SI CORRESPONDE), PRECIOS E INFORMACIÓN DE FACTURACIÓN, Y OTRA INFORMACIÓN IMPORTANTE RELACIONADA CON EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEM

Licencias

LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, BAJO EL ENLACE "TÉRMINOS DE LICENCIA DE SOFTWARE DE AVAYA (Productos de Avaya)" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, SON APLICABLES A CUALQUIER PERSONA QUE DESCARGUE , UTILIZA Y/O INSTALA EL SOFTWARE DE AVAYA, COMPRADO DE AVAYA INC., CUALQUIER AFILIADO DE AVAYA O UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA) EN VIRTUD DE UN ACUERDO COMERCIAL CON AVAYA O UN SOCIO DE CANAL DE AVAYA. A MENOS QUE AVAYA ACORDE LO CONTRARIO POR ESCRITO, AVAYA NO EXTENDERÁ ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE CUALQUIER PERSONA QUE NO SEA AVAYA, UNA AFILIADA DE AVAYA O UN SOCIO DE CANAL DE AVAYA; AVAYA SE RESERVA EL DERECHO DE TOMAR ACCIONES LEGALES CONTRA USTED Y CUALQUIER OTRA PERSONA QUE UTILICE O VENDA EL SOFTWARE SIN LICENCIA. AL INSTALAR, DESCARGAR O UTILIZAR EL SOFTWARE O AUTORIZAR A OTROS A HACERLO, USTED,

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el cual el alcance de la licencia se detalla a continuación. Cuando la documentación del pedido no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de Sistema Designado. El número aplicable de licencias y unidades de capacidad para las que se otorga la licencia será uno (1), a menos que se especifique un número diferente de licencias o unidades de capacidad en la documentación u otros materiales disponibles para Usted. "Software" hace referencia a los programas informáticos en código objeto, proporcionados por Avaya o un socio de canal de Avaya, ya sea como productos independientes, preinstalados en productos de hardware y cualquier mejora, actualización, parche, corrección de errores o versión modificada de los mismos. "Procesador designado" significa un único dispositivo informático independiente. "Servidor" hace referencia a un Procesador designado que alberga una aplicación de software a la que acceden varios usuarios. "Instancia" significa una única copia del Software que se ejecuta en un momento determinado: (i) en una máquina física; o (ii) en una máquina virtual de software implementada ("VM") o implementación similar.

Tipos de licencia

Licencia de sistema(s) designado(s) (DS). El Usuario final puede instalar y usar cada copia o una Instancia del Software solo en una cantidad de Procesadores designados hasta la cantidad indicada en el pedido. Avaya puede solicitar que los Procesadores designados se identifiquen en el pedido por tipo, número de serie, clave de función, Instancia, ubicación u otra designación específica, o que el Usuario final los proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este objetivo.

Licencia de Usuario Concurrente (CU). El Usuario final puede instalar y utilizar el Software en varios Procesadores designados o en uno o más Servidores, siempre que solo el número de Unidades con licencia acceda y utilice el Software en un momento dado. Una "Unidad" hace referencia a la unidad en la que Avaya, a su exclusivo criterio, basa el precio de sus licencias y puede ser, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o correo de voz a nombre de una persona. o función corporativa (por ejemplo, webmaster o servicio de asistencia), o una entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software. Las Unidades pueden vincularse a un Servidor específico e identificado oa una Instancia del Software.

Licencia de base de datos (DL). El Usuario final puede instalar y utilizar cada copia o una Instancia del Software en un Servidor o en varios Servidores, siempre que cada uno de los Servidores en los que se instala el Software se comunique con no más de una Instancia de la misma base de datos.

Licencia de CPU (CP). El Usuario final puede instalar y usar cada copia o Instancia del Software en una cantidad de Servidores hasta la cantidad indicada en el pedido, siempre que la capacidad de rendimiento de los Servidores no supere la capacidad de rendimiento especificada para el Software. El usuario final no puede volver a instalar ni operar el software en servidores con una mayor capacidad de rendimiento sin el consentimiento previo de Avaya y el pago de una tarifa de actualización.

Licencia de usuario nominal (NU). Usted puede: (i) instalar y usar cada copia o Instancia del Software en un solo Procesador o Servidor Designado por Usuario Designado autorizado (definido a continuación); o (ii) instalar y usar cada copia o Instancia del Software en un Servidor, siempre que solo los Usuarios designados autorizados accedan y usen el Software. “Usuario designado” significa un usuario o dispositivo que ha sido expresamente autorizado por Avaya para acceder y utilizar el Software. A discreción exclusiva de Avaya, un "Usuario designado" puede ser, entre otros, designado por nombre, función corporativa (por ejemplo, webmaster o servicio de asistencia técnica), una cuenta de correo electrónico o correo de voz en nombre de una persona o función corporativa, o un entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software.

Licencia Shrinkwrap (SR). Usted puede instalar y usar el Software de acuerdo con los términos y condiciones de los acuerdos de licencia aplicables, como la licencia "shrinkwrap" o "clickthrough" que acompaña o se aplica al Software ("Licencia Shrinkwrap").

Software de la herencia de Nortel

“Software Heritage Nortel” significa el software que fue adquirido por Avaya como parte de su compra de Nortel Enterprise Solutions Business en diciembre de 2009. El software Heritage Nortel es el software incluido en la lista de productos Heritage Nortel que se encuentra en https://support. .avaya.com/LicenseInfo bajo el enlace "Heritage Nortel Products" o el sitio sucesor designado por Avaya. Para el software Heritage Nortel, Avaya le otorga al Cliente una licencia para usar el software Heritage Nortel proporcionado en virtud del presente únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la Documentación, y únicamente como integrado, para ejecución en, o para comunicación con equipos Avaya. Los cargos por el software Heritage Nortel pueden basarse en el grado de activación o uso autorizado según se especifica en un pedido o factura.

Derechos de autor

Salvo que se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, la documentación, el software, el servicio alojado o el hardware proporcionado por Avaya. Todo el contenido de este sitio, la documentación, el Servicio alojado y el producto proporcionado por Avaya, incluida la selección, disposición y diseño del contenido, es propiedad de Avaya o de sus otorgantes de licencias y está protegido por derechos de autor y otras leyes de propiedad intelectual, incluida la ley sui generis. derechos relativos a la protección de las bases de datos. No puede modificar, copiar, reproducir, volver a publicar, cargar, publicar, transmitir o distribuir de ninguna manera ningún contenido, en su totalidad o en parte, incluido cualquier código y software, a menos que Avaya lo autorice expresamente. La reproducción, transmisión, difusión, almacenamiento o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede ser un delito,

virtualización

Lo siguiente se aplica si el producto se implementa en una máquina virtual. Cada producto tiene su propio código de pedido y tipos de licencia. Tenga en cuenta que cada Instancia de un producto se debe licenciar y pedir por separado. Por ejemplo, si el cliente usuario final o el socio de canal de Avaya desea instalar dos instancias del mismo tipo de productos, entonces se deben pedir dos productos de ese tipo.

Componentes de terceros

"Componentes de terceros" significa que ciertos programas de software o partes de los mismos incluidos en el Software o el Servicio alojado pueden contener software (incluido el software de código abierto) distribuido bajo acuerdos de terceros ("Componentes de terceros"), que contienen términos relacionados con los derechos de uso de ciertos partes del Software ("Términos de terceros"). Según sea necesario, la información sobre el código fuente del sistema operativo Linux distribuido (para aquellos productos que tienen el código fuente del sistema operativo Linux distribuido) y la identificación de los titulares de derechos de autor de los componentes de terceros y los términos de terceros que se aplican está disponible en los productos, la documentación o en el sitio web de Avaya. en: https://support.avaya.com/Copyright o en el sitio sucesor designado por Avaya. Los términos de la licencia de software de código abierto proporcionados como Términos de terceros son consistentes con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del software de código abierto. Los Términos de terceros prevalecerán sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables en la medida en que estos Términos de licencia de software le impongan mayores restricciones que los Términos de terceros aplicables.

Lo siguiente se aplica si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO TIENE LICENCIA BAJO LA LICENCIA DE CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS POR LOS QUE NO RECIBE REMUNERACIÓN PARA (i) CODIFICAR VÍDEO EN CUMPLIMIENTO CON EL ESTÁNDAR AVC (“AVC VIDEO”) Y/O (ii) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL DE MPEG LA, LLC CONSULTE HTTP://WWW.MPEGLA.COM.

Proveedor de servicio

LO SIGUIENTE SE APLICA AL ALOJAMIENTO DE PRODUCTOS O SERVICIOS DE AVAYA POR PARTE DEL SOCIOS DE CANAL DE AVAYA. EL PRODUCTO O EL SERVICIO ALOJADO PUEDE UTILIZAR COMPONENTES DE TERCEROS SUJETOS A TÉRMINOS DE TERCEROS Y REQUIERE QUE UN PROVEEDOR DE SERVICIOS TENGA UNA LICENCIA INDEPENDIENTE DIRECTAMENTE DEL PROVEEDOR DE TERCEROS. EL ALOJAMIENTO DE PRODUCTOS DE AVAYA POR PARTE DE UN SOCIO DE CANAL DE AVAYA DEBE SER AUTORIZADO POR ESCRITO POR AVAYA Y SI DICHOS PRODUCTOS ALOJADOS UTILIZAN O INTEGRAN DETERMINADO SOFTWARE DE TERCEROS, INCLUYENDO, ENTRE OTROS, SOFTWARE O CÓDECS DE MICROSOFT, EL SOCIO DE CANAL DE AVAYA DEBE OBTENER CUALQUIER LICENCIA CORRESPONDIENTE DE FORMA INDEPENDIENTE ACUERDOS, A CARGO DEL SOCIO DE CANAL DE AVAYA, DIRECTAMENTE DEL PROVEEDOR TERCERO CORRESPONDIENTE.

CON RESPECTO A LOS CÓDECS, SI EL SOCIO DE CANAL DE AVAYA ALOJA CUALQUIER PRODUCTO QUE UTILICE O INTEGRA EL CÓDEC G.729, EL CÓDEC H.264 O EL CÓDEC H.265, EL SOCIO DE CANAL DE AVAYA RECONOCE Y ACEPTA QUE EL SOCIO DE CANAL DE AVAYA ES RESPONSABLE DE CUALQUIER Y TODAS LAS TARIFAS Y/O REGALÍAS RELACIONADAS. EL CÓDEC G.729 TIENE LICENCIA DE SIPRO LAB TELECOM INC. CONSULTE WWW.SIPRO.COM/CONTACT.HTML. EL CÓDEC H.264 (AVC) TIENE LICENCIA BAJO LA LICENCIA DE LA CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS EN LOS QUE NO RECIBE REMUNERACIÓN PARA: (I) CODIFICAR VÍDEO DE CONFORMIDAD CON EL ESTÁNDAR AVC (“AVC VIDEO ”) Y/O (II) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO CON LICENCIA PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. INFORMACIÓN ADICIONAL PARA H.

De acuerdo con las leyes

El cliente reconoce y acepta que es responsable de cumplir con las leyes y reglamentaciones aplicables, incluidas, entre otras, las leyes y reglamentaciones relacionadas con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude y los derechos de interpretación musical en el país. o territorio donde se utiliza el producto Avaya.

Prevención del fraude de llamadas

El "fraude interurbano" es el uso no autorizado de su sistema de telecomunicaciones por parte de una parte no autorizada (por ejemplo, una persona que no es un empleado corporativo, agente, subcontratista o que no trabaja en nombre de su empresa). Tenga en cuenta que puede haber un riesgo de fraude de llamadas asociado con su sistema y que, si ocurre, puede resultar en cargos adicionales sustanciales para sus servicios de telecomunicaciones.

Intervención de fraude de llamadas de Avaya

Si sospecha que está siendo víctima de fraude de llamadas y necesita asistencia o soporte técnico, llame a la línea directa de intervención de fraude de llamadas del Centro de Servicio Técnico al +1-800-643-2353 para los Estados Unidos y Canadá. Para obtener números de teléfono de soporte adicionales, consulte el sitio web de soporte de Avaya: https://support.avaya.com o el sitio sucesor designado por Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de soporte de seguridad de Avaya en la sección Políticas de seguridad y soporte de https://support.avaya.com/security. Las sospechas de vulnerabilidades de seguridad de productos de Avaya se manejan según el Flujo de soporte de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Descarga de documentación

Para obtener las versiones más recientes de la documentación, consulte el sitio web de soporte de Avaya: https://support.avaya.com, o el sitio sucesor designado por Avaya.

Comuníquese con el soporte de Avaya

Consulte el sitio web de soporte de Avaya: https://support.avaya.com para obtener avisos y artículos sobre productos o servicios alojados, o para informar un problema con su producto o servicio alojado de Avaya. Para obtener una lista de números de teléfono de soporte y direcciones de contacto, vaya al sitio web de Soporte de Avaya: https://support.avaya.com (o el sitio sucesor designado por Avaya), desplácese hasta la parte inferior de la página y seleccione Contactar con Avaya. Apoyo.

Índice

A

Cosa análoga
- Cajas de barrera de teléfono 189
- Teléfono Región Disponibilidad 39, 249
- Puerto 264, 267

Solicitud
- Centro de llamadas 45
- Registro de llamada 45
- CD/DVD 42
- TIC 45
- Mantenimiento 43
- Gerente 253
- Monitor 255
- SoftConsole 257
- Aplicación de estado del sistema 257
- TAPI 258
- Usuario 44
- Mensaje de voz 44
- Correo de voz Pro 259

Evaluaciones
- La red 40
- VoIP 40

Audio
- Conversión de códec 41
- Puerto 264

Puerto de audio 267

Disponibilidad de Equipo 12

B

Respaldo
- Tarjeta SD 149

Cajas de barrera
- Teléfono analógico 189
- Montaje en bastidor 190

Tarjeta básica
- Teléfono analógico 22, 209
- Estación digital 22, 209
- Portador de tarjetas heredado 22, 209
- VCM 22, 209

BRI
- (Entonces) Puerto 268
- (Troncal) Puerto 269
- Puerto 264

C

Cable
- Requisitos de acceso 53
- Requisitos de autorización 53

cabos
- Distancias máximas de cable 33, 265
- IP Office estándar 33, 265

Cableado
- Protección contra rayos 36, 187

Aplicación de registro de llamadas 45

Estado de llamadas
- Solicitud 43

Tarjetas
- Base de teléfono analógico 213
- IP500 Base de estación digital 218
- IP500 IP500 VCM 221

Roca del castillo 192

Canales
- Compresión 41

Reloj 107

Centro de negocios compacto
- Aplicación 45

Centro de contacto compacto
- Aplicación 45

Canales de compresión 41

Centro de conferencias
- Solicitud 44

Configuración
- Crear nuevo 76
- Borrar 170

Conexiones
- Toma de tierra 35
- fuera del edificio 36, 187

ContactoTienda
- Solicitud 44

Unidad de control
- IP406 V2 18
- IP412 18
- Unidad del sistema IP500 18
- Montaje en bastidor 37
- SOE 18
- Montaje en pared 37

Copiar
- Tarjeta SD 152

País
- Idiomas 42
- Regiones admitidas 42

Crear configuración 76

D

Tarjetas de hija
- Troncal analógico 25, 224
- Troncal BRI 25, 226
- Troncal PRI 227
- Troncal PRI-U 25
- Tronco 25

E/P CC
- Puerto 264

Puerto I/P DCI 271

DECT
- Teléfono 39, 249
- Disponibilidad de región 39, 249

Aplicación DevLink 45

SD
- YO ROBO 188
- Teléfono 39, 188, 249
- Puerto 264, 271
- Disponibilidad de región 39, 249

DTE Puerto 198
- Requisito de cable 278
- RS232 278
- Ajustes 278

mi

Correo de voz integrado
- Solicitud 44

Precauciones de EMC
- Departamento Canadiense de Comunicaciones 301
- EMC Precaución para China 301
- Requisitos ambientales de la Comisión 301

Federal de Comunicaciones 51

Disponibilidad de equipos 12

Expansión
- Puerto 264

Módulos de expansión
- Troncal analógico IP400 16 241

Página1331 de 3226.

Módulos de expansión
IP400 Digital Station V2 243
IP400 Phone V2 245
IP500 Analog Trunk 16 229
IP500 Digital Station 26, 231
Teléfono IP500 26, 238 IPO
500 Troncal analógico IPO 26
500 BRI So8 26 Puerto de
expansión 273
Exportación de ajustes 77
O/P EXT.
Puerto 264
EXT O/P Puerto 191, 273
Números de extensión
Intercambio 186
Módulos de expansión externos 26

F

Unidades defectuosas 12
Normas de la FCC 307
Servidor de claves de funciones
Solicitud 43
Teclas de funciones
Paralela 21
De serie 21
Tarjeta electrónica 21
USB 21
Excepción de cortafuegos 260

GRAMO

Información general
Cursos de formación 46
Sitios web 46
Unidades de Control de Puesta a Tierra 35

H

H323
Los telefonos 39, 249
Disponibilidad de región 39, 249
Símbolos de peligro 298
Sustancias peligrosas 12
Declaración de homologación
298 HP OpenView 192

yo

Importación de ajustes 77
Operación de IP Office en
Australia 302
Canadá 302
Porcelana 303
unión Europea 304
Nueva Zelanda 304
Estados Unidos 305
IP500
Tarjeta base de teléfono analógico Tarjeta 22, 209
secundaria de troncal analógica Tarjeta 25
secundaria de troncal BRI Tarjeta base de 25
estación digital Tarjeta heredada Tarjeta 22, 209
base de operador Tarjeta secundaria de 22, 209
troncal PRI-U Botón de reinicio 197 25
Tarjeta Hija Tronco 25
Tarjeta base VCM 22, 209
Instalación IP500
Aplicaciones de administración 64
Tarjeta 82
Comprobar LED de tarjeta 95
Administrador de conexión 67
Documentación 60
puesta a tierra 93
Montaje en bastidor 89
Administrador de inicio 68
Herramientas 59
Desembalaje 60

L

LAN
Puerto 264
Puerto LAN 274
Licencias
Gerente 253
Monitor 255
SoftConsole 257
Aplicación de estado del 257
sistema TAPI 258
Correo de voz Pro 259
Licencias
Base de PC 21
Sin PC 21
Protección Aclarante 298
Protección Aclarante 36, 187

METRO

Mantenimiento
Aplicaciones 43
Gerente
Solicitud 43
Calidad del reloj 107
Componentes 253
Requisitos de licencia 253
Requisitos de la computadora 253
Prefijo marcando 109
Baúles 105
Actualización de software 180
Tarjeta de memoria
Eliminación 142
Módulos
Interfaz troncal 299
Monitor
Solicitud 43
Componentes 255
Requisitos de licencia 255
Requisitos de la computadora 255
Protocolos 260
MS-CRM
Solicitud 44

norte

Evaluaciones de red 40
Nueva configuración 76

O

fuera del edificio
Conexiones 36, 187

PAGS

Clave de función paralela 21
Licencias basadas en PC 21
Licencias sin PC 21
FP
Puerto 264
Puerto PF 275
Teléfono (POT)
Puerto 264
Teléfono (POT) Puerto 276

Puerto
Cosa análoga 264, 267
Asignado 260
Audio 264, 267
BRI 264
BRI (entonces) 268
BRI (Troncal) 269
E/P CC 264
E/P DCI 271
Puerta 191
SD 264, 271
Expansión 264, 273
O/P EXT. 191, 264, 273
Oficina de PI 260
LAN 264, 274
FP 264, 275
Teléfono (POT) 264, 276
PRI 264, 277
RS232/DTE 264
DTE RS323 278
Clasificación de seguridad 300
USB 264
Usó 260
PÁLIDO 264
Fuentes de alimentación
1151C1 30
1151C2 30
Cordones 31
Fuente de alimentación tipo 40w 30
Tipo PSU con conexión a tierra de 45 W 30
Fuente de alimentación ininterrumpida tipo 30
PSU con conexión a tierra de 60 W 32
PRI
Puerto 264
PRI Puerto 277
Protocolos 260
R
Unidades de control de montaje en bastidor
Disponibilidad de 37 regiones
Teléfono analógico 39, 249
Teléfono DECT 39, 249
Teléfono DS 39, 249
Teléfono H323 39, 249
Remover
Tarjeta SD 142
Requisitos
Acceso a cables 53
Separación de cables 53
ambiental 51
Espacio 53
Montaje en pared 51
Restaurar
Tarjeta SD 150
RoHS 12
RS232/DTE
Puerto 264
S
Declaración de seguridad 298
Tarjeta SD
Respaldo 149
Copiar 152
Eliminación 142
Restaurar 150
Configuraciones de seguridad
Defecto 173
Configuración de la tecla de
función serial 21
Formatos de archivo CSV 77
Exportador 77
Importador 77
Tecla de función de tarjeta inteligente
21 SNMP 192
Habilitación 195
Instalación 193
Puerto 195
responder 195
Envío de trampas 195
MIB de SNMP
Solicitud 43
SoftConsole
Solicitud 44
Componentes 257
Requisitos de licencia 257
Requisitos de la computadora 257
Software
Borrar software principal 199
Requisitos de espacio 53
Declaración
Homologación 298
Seguridad 298
Soportado
Idioma 42
locales 42
Estado del sistema
Solicitud 43
Aplicación de estado del sistema
Componentes 257
Requisitos de licencia 257
Requisitos de la PC 257
T
TAPI
Componentes 258
Requisitos de licencia 258
Requisitos de la PC 258
Aplicación de controlador WAV 45
TAPI Link Lite
Solicitud 44
Aplicación TAPIlink Pro 45
Cursos de formación 46
Módulos de interfaz troncal 299
tu
USB
Clave de funciones 21
Puerto 264
V
Canales de compresión de voz 41
Voicemail Lite
Solicitud 44
Correo de voz Pro
Solicitud 44
Componentes 259
Requisitos de licencia 259
Requisitos de la PC 259
Evaluaciones VoIP 40
W
Unidades de control de montaje en pared
37 Requisitos de montaje en pared 51

PÁLIDO

Puerto 264

Sitios web 46

¿Comentarios sobre este documento? infodev@avaya.com

© 2020 Avaya Inc. Todos los derechos reservados.

IP Office™ Platform 10.1

Deploying Avaya IP Office™ Platform IP500 V2

© 2017 AVAYA Reservados todos los derechos.

Aviso
Si bien se hicieron esfuerzos razonables para asegurar que la información contenida en este document esté completa y sea exacta en el momento de su impresión, Avaya no se responsabiliza por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información contenida en este documento sin la obligación de notificar a ninguna persona u organización dichos cambios.
Para leer toda la información de apoyo técnico, consulte el documento en su totalidad, Avaya Support Notices for Hardware Documentation, documento número 03–600759.
Para leer toda la información de apoyo técnico, consulte el documento en su totalidad, Avaya Support Notices for Software Documentation, documento número 03–600758.
Para encontrar este documento en nuestro sitio web, solo visite http://www.avaya.com/support y busque el número de documento en el cuadro Búsqueda.

Exención de responsabilidad con respecto a la documentación
“Documentación” hace referencia a la información publicada por Avaya en diversos medios, que puede incluir información del producto, instrucciones operativas y especificaciones de rendimiento, que Avaya suele poner a disposición de los usuarios de sus productos. La documentación no incluye material publicitario. Avaya no es responsable de ninguna modificación, incorporación ni eliminación en la version original publicada de la presente documentación a menos que dichas modificaciones, incorporaciones o eliminaciones hayan sido efectuadas por Avaya. El usuario final acuerda indemnizar y eximir de toda responsabilidad a Avaya, agentes de Avaya y empleados con respecto a todo reclamo, acción judicial, demanda y juicio que surgiere de o en relación con modificaciones, incorporaciones o eliminaciones posteriores en esta documentación realizadas por el usuario final.

Exención de responsabilidad con respecto a los vínculos
Avaya no asume la responsabilidad del contenido ni la fiabilidad de los enlaces a los sitios Web incluidos en cualquier punto de este sitio o en documentación proporcionada por Avaya. Avaya no es responsible de la confiabilidad de ninguna información, instrucción ni contenido proporcionado en estos sitios y no necesariamente aprueba los productos, los servicios o la información descritos u ofrecidos por los mismos. Avaya no garantiza que estos vínculos funcionarán todo el tiempo ni tiene control de la disponibilidad de las páginas vinculadas.

Garantía
Avaya ofrece una garantía limitada para sus “productos” de hardware y software. Consulte su contrato de compraventa para establecer las condiciones de la garantía limitada. Asimismo, el idioma de la garantía estándar de Avaya, así como la información relativa al soporte técnico para este producto durante el período de vigencia de la garantía está disponible en el sitio Web: del soporte técnico de Avaya: http://support.avaya.com. Tenga en cuenta que si ha adquirido los productos de un socio de canal autorizado por Avaya fuera de Estados Unidos y Canadá, la garantía es proporcionada por el mencionado socio de canal de Avaya y no por Avaya. “Software” significa programas de computadora en código objeto proporcionado por Avaya o un Channel Partner de Avaya, ya sea como productos independientes o preinstalados en productos de hardware, y cualquier mejora, actualización, corrección de falla o versions modificadas.

Licencias
LOS TÉRMINOS DE LICENCIA DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, SE APLICAN A CUALQUIER PERSONA QUE DESCARGUE, USE Y/O INSTALE SOFTWARE DE AVAYA, ADQUIRIDO A AVAYA INC., CUALQUIER SUBSIDIARIA DE AVAYA, O UN SOCIO DE CANAL AUTORIZADO DE AVAYA (SEGÚN SEA APLICABLE) BAJO UN ACUERDO COMERCIAL CON AVAYA O CON UN SOCIO DE CANAL AUTORIZADO DE AVAYA. A MENOS QUE AVAYA ACUERDE LO CONTRARIO POR ESCRITO, AVAYA NO OTORGA ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE ALGUIEN DISTINTO A AVAYA, UNA SUBSIDIARIA DE AVAYA O UN SOCIO DE CANAL AUTORIZADO DE AVAYA, RESERVÁNDOSE AVAYA EL DERECHO A EJERCER ACCIONES LEGALES EN SU CONTRA O EN CONTRA DE TERCEROS QUE USEN O VENDAN EL SOFTWARE SIN UNA LICENCIA. AL INSTALAR, DESCARGAR O USAR EL SOFTWARE DE AVAYA, O AL AUTORIZAR A TERCEROS A HACERLO, USTED, EN NOMBRE PROPIO Y EN NOMBRE DE LA ENTIDAD PARA LA CUAL ESTÁ INSTALANDO, DESCARGANDO O USANDO EL SOFTWARE (EN ADELANTE REFERIDOS INDISTINTAMENTE COMO “USTED” O “USUARIO FINAL”), ACEPTA OBLIGARSE DE CONFORMIDAD CON LO DISPUESTO POR ESTOS TÉRMINOS Y CONDICIONES Y CREAR UN CONTRATO OBLIGATORIO ENTRE USTED Y AVAYA INC. O LA AFILIADA DE AVAYA APLICABLE (“AVAYA”).

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el que el alcance de la licencia se detalla a continuación. Donde la documentación de la orden no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de sistema designado. La cantidad correspondiente de licencias y unidades de capacidad para la que se otorga la licencia será uno (1), a menos que una cantidad diferente de licencias o unidades de capacidad se especifique en la documentación u otros materiales disponibles para el usuario final. “Procesador designado” significa un dispositivo informático independiente único. “Servidor” significa un Procesador designado que aloja una aplicación de software a la que pueden acceder varios usuarios.

Tipos de licencia
Licencia de sistemas designados (DS). El usuario final puede instalar y utilizar cada copia del software solo en la cantidad de procesadores designados indicada en la orden. Avaya puede exigir que se identifique el procesador designado por tipo, número de serie, tecla de función, ubicación u otra designación específica o que el usuario final lo proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este propósito.

Licencia de usuarios simultáneos (CU). El usuario final puede instalar y utilizar el software en múltiples procesadores designados o uno o más servidores, siempre y cuando sólo las unidades con licencia accedan y utilicen el software en un momento dado. Una “unidad” se refiere a la unidad en la que Avaya, a su exclusivo criterio, fundamenta el precio de sus licencias y puede ser incluso, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o de correo de voz en nombre de una persona o function corporativa (por ejemplo, administrador web o centro de asistencia técnica) o una entrada de directorio en la base de datos administrative utilizada por el software que permite que un usuario se conecte con el software. Las unidades pu8eden vincularse con un servidor específico identificado.

Licencia de la base de datos (DL). El usuario final puede instalar y utilizar cada copia del software en un servidor o en múltiples servidores siempre que cada servidor en el cual el software esté instalado se comunique con no más de una única instancia de la misma base de datos.

Licencia de CPU (CP). El usuario final puede instalar y utilizar cada copia del software hasta la cantidad de servidores que indica la orden, siempre que la capacidad de rendimiento de los servidores no exceda la capacidad de rendimiento especificada para el software. El usuario final no puede instalar nuevamente ni operar el software en servidores con una capacidad de rendimiento más grande sin el consentimiento previo de Avaya y sin pagar una tarifa por la actualización.

Licencia del usuario identificado (NU). El cliente puede: (i) instalar y utilizar el software en un solo procesador designado o servidor por usuario identificado autorizado (se define a continuación); o (ii) instalar y utilizar el software en un servidor siempre y cuando únicamente los usuarios identificados autorizados obtengan acceso a él y lo utilicen. “Usuario identificado” se refiere a un usuario o dispositivo que ha sido expresamente autorizado por Avaya para tener acceso al software y utilizarlo. A entera discreción de Avaya, un “usuario identificado” puede ser incluso, entre otros, designado por nombre, función corporative (por ejemplo, administrador web o centro de asistencia técnica), una cuenta de correo electrónico o de correo de voz a nombre de una persona o función corporativa o una entrada de directorio en la base de datos administrative utilizada por el software que permite que un usuario se conecte con el software.

Licencia Shrinkwrap (SR). El cliente puede instalar y utilizar el software de acuerdo con los terminus y condiciones de los contratos de licencia vigentes, como por ejemplo, las licencias “shrinkwrap” o “clickthrough” que acompañan o se aplican al software (“licencia Shrinkwrap”).

Heritage Nortel Software
“Heritage Nortel Software” significa el software que adquirió Avaya como parte de la compra de Nortel Enterprise Solutions Business en diciembre de 2009. El Heritage Nortel Software actualmente disponible para licencia de Avaya es el software contenido en la lista de productos Heritage Nortel Products ubicada en http://support.avaya.com/LicenseInfo en el vínculo “Heritage Nortel Products”. Para Heritage Nortel Software, Avaya otorga al cliente una licencia para utilizar Heritage Nortel Software proporcionado en virtud del presente documento únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el objetivo especificado en la documentación y solamente como se incorpora, ejecuta o (en caso de que la documentación correspondiente permita la instalación en un equipo que no sea Avaya) para comunicación con equipo Avaya. Los cargos por Heritage Nortel Software se podrían basar en el alcance de activación o el uso autorizado según se especifique en una orden o factura.

Copyright
Excepto donde se indique expresamente lo contrario, no se debería hacer uso de los materiales de este sitio, de la documentación, del software ni del hardware proporcionados por Avaya. Todo el contenido de este sitio, la documentación y el Producto proporcionados por Avaya, incluida la selección, la disposición y el diseño del contenido, son propiedad de Avaya o de sus licenciantes y están protegidos por las leyes de derecho de autor y otras leyes de propiedad intelectual, incluidos los derechos de su género relacionados con la protección de las bases de datos. No debe modificar, copiar, reproducir, reeditar, cargar, publicar, transmitir ni distribuir de ninguna manera el contenido, en su totalidad o en parte, incluidos los códigos y el software, a menos que posea una autorización expresa de Avaya. La reproducción, transmisión, difusión, almacenamiento y/o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede considerarse un delito penal o civil según la ley vigente.

Virtualización
Cada vAppliance tendrá su propio código de pedido. Tenga en cuenta que cada instancia de vAppliance debe pedirse por separado. Si el cliente usuario final o el socio de canal de Avaya prefieren la instalación de dos vAppliances del mismo tipo, se deben solicitar dos vAppliances del mismo tipo.
Cada Producto tiene su propio código de pedido. Tenga en cuenta que cada instancia de un product debe tener una licencia y pedirse por separado. ""Instancia"" significa una copia única del software. Por ejemplo, si el cliente usuario final o el socio de canal de Avaya prefieren instalar dos instancias del mismo tipo de producto, se deben solicitar dos productos del mismo tipo.
Componentes de terceros
“Componentes de terceros” significa que ciertos programas de software y partes de este incluidos en el producto pueden contener software (incluido el software de código abierto) distribuido según contratos de terceros (“componentes de terceros”), que incluyen condiciones sobre los derechos a utilizar ciertas partes del software (“Términos y condiciones de terceros”). La información con respecto al código fuente de SO Linux distribuido (para aquellos productos que tienen código fuente de SO Linux distribuido) y que identifique a los titulares de derechos de autor de componentes de terceros y las condiciones de terceros que se aplican está disponible en la documentación o en el sitio web de Avaya: http://support.avaya.com/Copyright. Acepta las condiciones de terceros para tales tipos de componentes de terceros.

Nota para el proveedor de servicio
El producto podría utilizar componentes de terceros con términos y condiciones de terceros que no le permitan funcionar como host y podría necesitar licencias independientes para dicho objetivo.

Prevención del fraude telefónico
El fraude telefónico se refiere al uso no autorizado de su sistema de telecomunicaciones por parte de un participante sin autorización (por ejemplo, una persona que no es un empleado, agente ni subcontratista corporativo o no trabaja en nombre de su compañía). Tenga en cuenta que pueden existir riesgos de Fraude telefónico asociados con su sistema y que, en tal caso, esto puede generar cargos adicionales considerables para sus servicios de telecomunicaciones.

Intervención en fraude telefónico de Avaya
En el caso de que sospeche que es víctima de fraude telefónico y que necesite asistencia o soporte técnico, llame a la línea directa de Intervención de Fraude Telefónico del Centro de Servicio Técnico al +1-800-643-2353 para Estados Unidos y Canadá. Para obtener números de teléfono de soporte técnico adicionales, vaya al sitio web de soporte técnico de Avaya: http://support.avaya.com.

Marcas comerciales
Las marcas comerciales, logotipos y marcas de servicio (“Marcas”) que aparecen en este sitio, la Documentación y los Productos proporcionados por Avaya son marcas registradas o no registradas de Avaya, sus subsidiarias y otros terceros. Los usuarios no tienen permiso de usar dichas Marcas sin previo consentimiento por escrito de Avaya o dichos terceros que puedan ser propietarios de la Marca. Ningún contenido de este sitio, la Documentación ni los Productos deben considerarse como otorgamiento, por implicación, impedimento o de alguna otra forma, una licencia ni derecho para usar las Marcas sin la autorización expresa por escrito de Avaya o del tercero correspondiente.

Avaya es una marca registrada de Avaya Inc.

Todas las demás marcas son propiedad de sus respectivos dueños. Linux® es una marca commercial registrada de Linus Torvalds en EE. UU. y en otros países.

Descarga de documentación:
Para obtener las versiones más actualizadas de la documentación, visite el sitio web de soporte técnico de Avaya: http://support.avaya.com.

Contacto con el soporte de Avaya
Visite el sitio web del soporte técnico de Avaya: http://support.avaya.com para obtener avisos y artículos sobre productos o para informar acerca de algún problema con su producto Avaya. Para obtener una lista de números de teléfono y direcciones de contacto de soporte, visite el sitio web de soporte técnico de Avaya: http://support.avaya.com, desplácese hasta el final de la página y seleccione Contacto con el soporte de Avaya.

Contenido

1. Panorama general del sistema

1.1 Cambios en esta versión 12
1.2 Documentación adicional 12
1.3 Disponibilidad del equipo 13
1.4 Reparación 13
1.5 RoHS 13
1.6 Modos de IP Office 14
1.6.1 Tarjetas SD de sistema 14
1.6.2 Capacidad general 14
1.6.3 Resumen del soporte técnico de hardware 16
1.6.4 Resumen del soporte técnico de funciones 18
1.7 La unidad de control 20
1.8 Componentes del sistema IP500 V2 21
1.9 Tarjeta System SD 23
1.10 Licencias 23
1.11 Tarjetas de la unidad de control 24
1.11.1 Tarjetas base IP500 24
1.11.2 Tarjetas de troncales IP500 27
1.12 Módulos de expansión externos 29
1.12.1 Módulos de expansión externos IP500 30
1.12.2 Módulos de expansión externos IP400 31
1.12.3 Conexión de módulos de expansión externos 32
1.13 Suministros y cables de energía 33
1.13.1 Suministros de energía 33
1.13.2 Cables de suministro de energía 34
1.13.3 Suministro de energía de respaldo 35
1.13.4 Cableado y cables 36
1.13.5 Puesta a tierra 38
1.13.6 Protección contra rayos/Conexiones fuera del edificio 39
1.14 Montaje de pared y en bastidor 40
1.15 Teléfonos IP Office 41
1.16 VoIP 42
1.16.1 Canales de compresión de voz 43
1.17 Localidades de país compatibles 45
1.18 Aplicaciones de software IP Office 45
1.18.1 Aplicaciones de programación 46
1.18.2 Aplicaciones de usuario 47
1.18.3 Aplicaciones de correo de voz 47
1.18.4 Aplicaciones para registro de llamadas 48
1.18.5 Aplicaciones para centros telefónicos 48
1.18.6 Aplicaciones CTI 48
1.19 Capacitación 49
1.20 Sitios Web 49
1.21 Puertos de emergencia y para cortes de energía 50

2. Información general de la instalación

2.1 Requerimientos ambientales 53
2.2 Requisitos de espacio 54
2.2.1 Unidad de control 54
2.2.2 Módulos de expansión externos 55
2.2.3 Montaje en pared 56
2.2.4 Requisitos de espacio para montaje en bastidor 57
2.3 Herramientas y piezas requeridas 58
2.4 Documentación 59
2.5 Desembalaje 59

3. Instalación del software de administración

3.1 Descarga del software 63
3.2 Instalación de las aplicaciones de administración 64
3.3 Conexión de la PC de instalación 67
3.4 Inicio de IP Office Manager 68
3.5 Iniciando System Status Application 69
3.6 Iniciando System Monitor 70
3.7 Inicio de IP Office Web Manager 71

4. Preparación de la tarjeta SD de sistema

4.1 Actualización del firmware de tarjeta 75
4.2 Creación de un archivo de configuración sin conexión 76
4.3 Inserción de un archivo de configuración predeterminado 77
4.4 Inserción de un archivo de licencia 77
4.5 Incorporación de certificados de seguridad 77
4.6 Inserción de un archivo protector de pantalla para la serie 9600 78
4.7 Inserción de música en los archivos de espera 78

5. Instalación de las tarjetas de la unidad de control

5.1 Ajuste de tarjetas auxiliares IP500 81
5.2 Inserción de tarjetas base IP500 82

6. Instalación del sistema físico

6.1 Montaje en pared 85
6.1.1 Kit de montaje en pared V2/V3 86
6.2 Montaje en bastidor 87
6.3 Conexión de módulos de expansión externos 88
6.4 Puesta a tierra 90
6.5 Inicio del sistema 91
6.6 Comprobación de las luces LED 92
6.7 Conexión de teléfonos 95
6.7.1 Teléfonos analógicos 95
6.7.2 Teléfonos ETR 95
6.7.3 Teléfonos estación digital DS 95
6.7.4 Teléfonos IP/SIP 95
6.7.5 Teléfonos TCM/BST 96

7. Configuración básica mediante Manager

7.1 Conexión de red 99
7.2 Configuración inicial 101
7.3 Numeración de las extensiones 103
7.4 Deshabilitación de las troncales no utilizadas 104
7.5 Configuración de la fuente de reloj para troncales digitales 106
7.6 Configuración de los prefijos de troncales 108
7.7 Selección de modo de puerto DS16B/30B 109
7.8 Carga del archivo de licencia 111
7.9 Guardado de la configuración 112

8. Configuración básica mediante IP Office Web Manager

Página1341 de 3226.

8.1 Conexión de red 115
8.2 Configuración inicial 117
8.3 Carga del archivo de licencia 119
8.4 Deshabilitación de las troncales no utilizadas 120
8.5 Configuración de la fuente de reloj para troncales digitales 121
8.6 Configuración de los prefijos troncales 123
8.7 Guardado de la configuración 124

9. Seguridad del sistema

9.1 Cambio de la configuración de seguridad predeterminada 127
9.2 Cambio de contraseña de usuario remoto 129
9.3 Deshabilitación de la compatibilidad con líneas troncales SIP 129
9.4 Deshabilitación de la compatibilidad con teléfonos H.323 129

10.Ingreso

10.1 Ingreso 133

11.Administración de la tarjeta SD

11.1 Inicio desde tarjetas SD 138
11.2 Creación de una tarjeta SD de IP Office 140
11.3 Visualización del contenido de la tarjeta 142
11.4 Creación de copia de seguridad en la carpeta de respaldo 143
11.4.1 Crear copia de seguridad en la carpeta de respaldo IP Office Manager 143
11.4.2 Crear copia de seguridad en la carpeta de respaldo mediante System Status Application 143
11.4.3 Crear copia de seguridad en la carpeta de respaldo mediante un teléfono del sistema 143
11.4.4 Crear copia de seguridad en la carpeta de respaldo mediante IP Office Web Manager 144
11.5 Restauración del sistema desde la carpeta de respaldo 145
11.5.1 Restauración del sistema desde la carpeta de respaldo mediante IP Office Manager 145
11.5.2 Restauración del sistema desde la carpeta de respaldo mediante System Status Application 145
11.5.3 Restauración del sistema desde la carpeta de respaldo mediante un teléfono del sistema 145
11.5.4 Restauración del sistema desde la carpeta de respaldo mediante IP Office Web Manager 146
11.6 Creación de copia de seguridad en la tarjeta SD opcional 147
11.6.1 Creación de copia de seguridad en la tarjeta opcional SD mediante IP Office Manager 147
11.6.2 Creación de copia de seguridad en la tarjeta SD opcional mediante System Status Application 147
11.6.3 Creación de copia de seguridad en la tarjeta SD opcional mediante IP Office Web Manager 147
11.6.4 Creación de copia de seguridad en la tarjeta SD opcional mediante un teléfono del sistema 147
11.7 Restauración de la configuración desde una tarjeta opcional 149
11.7.1 Restauración del sistema desde la tarjeta SD opcional mediante IP Office Manager 149
11.7.2 Restauración del sistema desde la tarjeta SD opcional mediante un teléfono del sistema 149
11.8 Carga del software desde una tarjeta SD opcional 150
11.8.1 Carga del software desde la tarjeta SD opcional mediante IP Office Manager 150
11.8.2 Carga del software desde la tarjeta SD opcional mediante un teléfono del sistema 150
11.9 Creación de una copia de seguridad en una PC 151
11.10 Restauración desde una PC 151
11.11 Actualización del software de la tarjeta 152
11.12 Extracción y apagado de la tarjeta de memoria 153
11.12.1 Apagado de una tarjeta mediante IP Office Manager 153
11.12.2 Apagado de una tarjeta mediante System Status Application 153
11.12.3 Apagado de una tarjeta mediante IP Office Web Manager 153
11.12.4 Apagado de una tarjeta mediante un teléfono del sistema 153
11.13 Inicio de la tarjeta de memoria 155
11.13.1 Inicio de una tarjeta mediante IP Office Manager 155
11.13.2 Inicio de una tarjeta mediante System Status Application 155
11.13.3 Inicio de una tarjeta mediante IP Office Web Manager 155
11.13.4 Inicio de una tarjeta mediante un teléfono del sistema 155

12.Procesos adicionales

12.1 Cambio de un sistema IP Office Basic Edition al modo estándar 159
12.2 Automatización del cambio a modo estándar 160
12.3 Desactivación de un sistema 161
12.3.1 Apagado de un sistema mediante IP Office Manager 161
12.3.2 Apagado de un sistema mediante System Status Application 162
12.3.3 Apagado de un sistema mediante un teléfono del sistema 162
12.3.4 Apagado de un sistema mediante el botón AUX 162
12.3.5 Apagado de un sistema mediante IP Office Web Manager 162
12.4 Reinicio de un sistema 163
12.4.1 Reinicio de un sistema mediante IP Office Manager 163
12.4.2 Reinicio de un sistema mediante IP Office Web Manager 164
12.4.3 Reinicio de un sistema mediante el botón Restablecer 164
12.4.4 Apagado de un sistema mediante un teléfono del sistema 164
12.5 Modificación de los componentes 165
12.5.1 Reemplazo de un componente por otro igual 166
12.5.2 Reemplazo por equipos de mayor capacidad 166
12.5.3 Reemplazo por equipos de menor capacidad 166
12.5.4 Inserción de un componente nuevo 166
12.5.5 Extracción permanente 167
12.5.6 Reemplazo por un tipo diferente 167
12.6 Devolver la configuración a valores predeterminados 168
12.6.1 Devolver la configuración a valores predeterminados mediante IP Office Manager 168
12.6.2 Devolver la configuración a valores predeterminados mediante IP Office Web Manager 168

Página1342 de 3226.

12.6.3 Devolver la configuración a valores predeterminados mediante el botón Restablecer..... 169
12.6.4 Devolver la configuración a valores predeterminados mediante depuración..... 170
12.6.5 Devolver la configuración a valores predeterminados mediante un teléfono del sistema.. 171
12.6.6 Devolver la configuración a valores predeterminados mediante carga por reinicio..... 171
12.7 Definición de la configuración de seguridad predeterminada..... 172
12.7.1 Devolver la seguridad a valores predeterminados mediante IP Office Manager..... 173
12.7.2 Devolver la seguridad a valores predeterminados mediante IP Office Web Manager.. 173
12.7.3 Devolver la seguridad a valores predeterminados mediante el puerto RS232..... 174
12.7.4 Devolver la seguridad a valores predeterminados mediante carga por reinicio..... 175
12.8 Carga de una configuración..... 176
12.8.1 Creación de un archivo de configuración sin conexión..... 177
12.8.2 Carga de una configuración mediante IP Office Manager..... 178
12.8.3 Carga de una configuración mediante IP Office Web Manager..... 178
12.8.4 Carga de una configuración en una tarjeta SD del sistema..... 178
12.9 Acualización de sistemas..... 179
12.9.1 Actualizar mediante el asistente de actualización..... 180
12.9.2 Actualización remota de la tarjeta SD del sistema mediante Manager..... 182
12.9.3 Actualización local de la tarjeta SD del sistema mediante Manager..... 183
12.9.4 Actualización mediante una tarjeta SD opcional..... 184
12.9.5 Actualización mediante IP Office Web Manager..... 185
12.10 Intercambio de usuarios de extensiones..... 187
12.11 Instalaciones telefónicas fuera del edificio..... 188
12.11.1 Teléfonos DS..... 189
12.11.2 Caja de protección para teléfonos analógicos..... 190
12.11.3 Cajas de protección para montaje en bastidor..... 191
12.12 Uso del puerto de salida externo..... 192
12.12.1 Conexión de puerto..... 192
12.13 Módulo BRI So8..... 194
12.13.1 Ejemplo 1: Terminal ISDN..... 194
12.13.2 Ejemplo 2: Conferencia de video..... 195
12.14 SNMP..... 197
12.14.1 Instalación de los archivos MIB de IP Office..... 198
12.14.2 Habilitación de SNMP y soporte para encuestas..... 200
12.14.3 Habilitación de envío de trampas SNMP..... 200
12.15 Botón Restaurar..... 201
12.16 Botón AUX..... 201
12.17 Mantenimiento del puerto RS232..... 202
12.18 Borrado del software principal..... 203
12.18.1 Borrado del software principal mediante el botón Restablecer..... 203
12.18.2 Borrado del software principal mediante depuración..... 204
12.18.3 Borrado del software principal mediante la carga por reinicio..... 205
12.19 Activación de IP Office Web Manager..... 206

13.Componentes del sistema

13.1 Unidad de control IP500 V2..... 209
13.2 Tarjetas SD del sistema IP500 V2..... 212
13.3 Tarjetas base IP500..... 213
13.3.1 Tarjeta de expansión de cuatro puertos..... 216
13.3.2 Teléfono analógico..... 217
13.3.3 Tarjeta combinada ATM..... 219
13.3.4 Tarjeta combinada BRI..... 221
13.3.5 Unified Communications Module..... 223
13.3.6 Estación digital..... 224
13.3.7 Tarjeta ETR6..... 226
13.3.8 Estación digital TCM8..... 228
13.3.9 VCM..... 229
13.4 Tarjetas auxiliares de troncales IP500..... 231
13.4.1 Tarjeta de troncales analógicas..... 233
13.4.2 Tarjetas de líneas troncales BRI..... 235
13.4.3 Tarjetas de troncales PRI..... 236
13.5 Módulos de expansión externos IP500..... 238
13.5.1 Troncal analógica de 16 líneas..... 240
13.5.2 BRI So8..... 243
13.5.3 DS16/30..... 245
13.5.4 DS16A/30A..... 247
13.5.5 DS16B/30B, DS16B2/30B2..... 250
13.5.6 Teléfono 16/30..... 252
13.6 Módulos de expansión IP400..... 254
13.6.1 Troncal analógica de 16 líneas..... 255
13.6.2 Estación digital V2..... 257
13.6.3 Teléfono V2..... 259
13.7 Kits de montaje..... 261
13.7.1 Kits de montaje en pared IP500..... 261
13.7.2 Kit de montaje en bastidor con cajas de protección..... 261
13.8 Teléfonos..... 262
13.9 Complementos del teléfono..... 263
13.10 Aplicaciones..... 264
13.10.1 IP Office Application Server..... 265
13.10.2 Contact Recorder for IP Office..... 265
13.10.3 IP Office Manager..... 267
13.10.4 Monitor..... 267
13.10.5 one-X Portal for IP Office..... 267
13.10.6 Avaya Communicator..... 269
13.10.7 SoftConsole..... 270
13.10.8 IP Office Video SoftPhone..... 270
13.10.9 System Status Application..... 272
13.10.10 TAPI..... 273
13.10.11 Voicemail Pro..... 274
13.10.12 Colaboración web..... 275
13.10.13 Puertos IP Office..... 275
13.11 Resumen del sistema operativo..... 276
13.11.1 Compatibilidad con Windows..... 276
13.11.2 Compatibilidad con Apple MacOS..... 277
13.11.3 Compatibilidad con Linux..... 277
13.11.4 Soporte de navegador..... 277

Página1343 de 3226

13.12 Puertos físicos 279
13.12.1 Cables 280
13.12.2 Puerto ANALÓGICO 282
13.12.3 Puerto AUDIO 282
13.12.4 Puerto BRI (So) 283
13.12.5 Puerto BRI (To) 284
13.12.6 Puerto BST (RJ21) 285
13.12.7 Puerto BST (RJ45) 285
13.12.8 Puerto DC I/P 286
13.12.9 Puertos DS (RJ45) 286
13.12.10 Puerto EF 287
13.12.11 Puerto ETR 287
13.12.12 Puerto Expansión 288
13.12.13 Puerto EXT O/P 288
13.12.14 Puerto LAN 289
13.12.15 Puerto PF 290
13.12.16 Puerto PHONE (POT) 291
13.12.17 Puerto PRI 292
13.12.18 Puerto RS232 (DTE) 293
13.13 Licencias 294
13.13.1 Licencias de edición del sistema 294
13.13.2 Licencias de actualización 296
13.13.3 Licencias para troncales 296
13.13.4 Licencias para teléfonos/terminales 297
13.13.5 Licencias de usuario 298
13.13.6 Licencias de Voicemail Pro 300
13.13.7 Licencias de prueba 301
13.13.8 Licencias CTI 301
13.13.9 Otras licencias 301
13.14 Compatibilidad con hardware y software 302
13.15 Niveles PCS 310
13.16 TAA 310

14.Declaraciones de seguridad

14.1 Protección contra rayos/símbolos de peligro 312
14.2 Módulos de interfaz de troncales 313
14.3 Información adicional y actualizaciones de productos 314
14.4 Clasificación de seguridad de los puertos 314
14.5 Directiva EMC 315
14.6 Instrucciones regulatorias para su uso 316
14.6.1 Australia 316
14.6.2 Canadá 316
14.6.3 China 317
14.6.4 Japón 318
14.6.5 Unión Europea 318
14.6.6 Nueva Zelanda 319
14.6.7 Notificación de la FCC 320
14.6.8 Cumplimiento de las normas de la FCC 322
Índice 323

Capítulo 1.

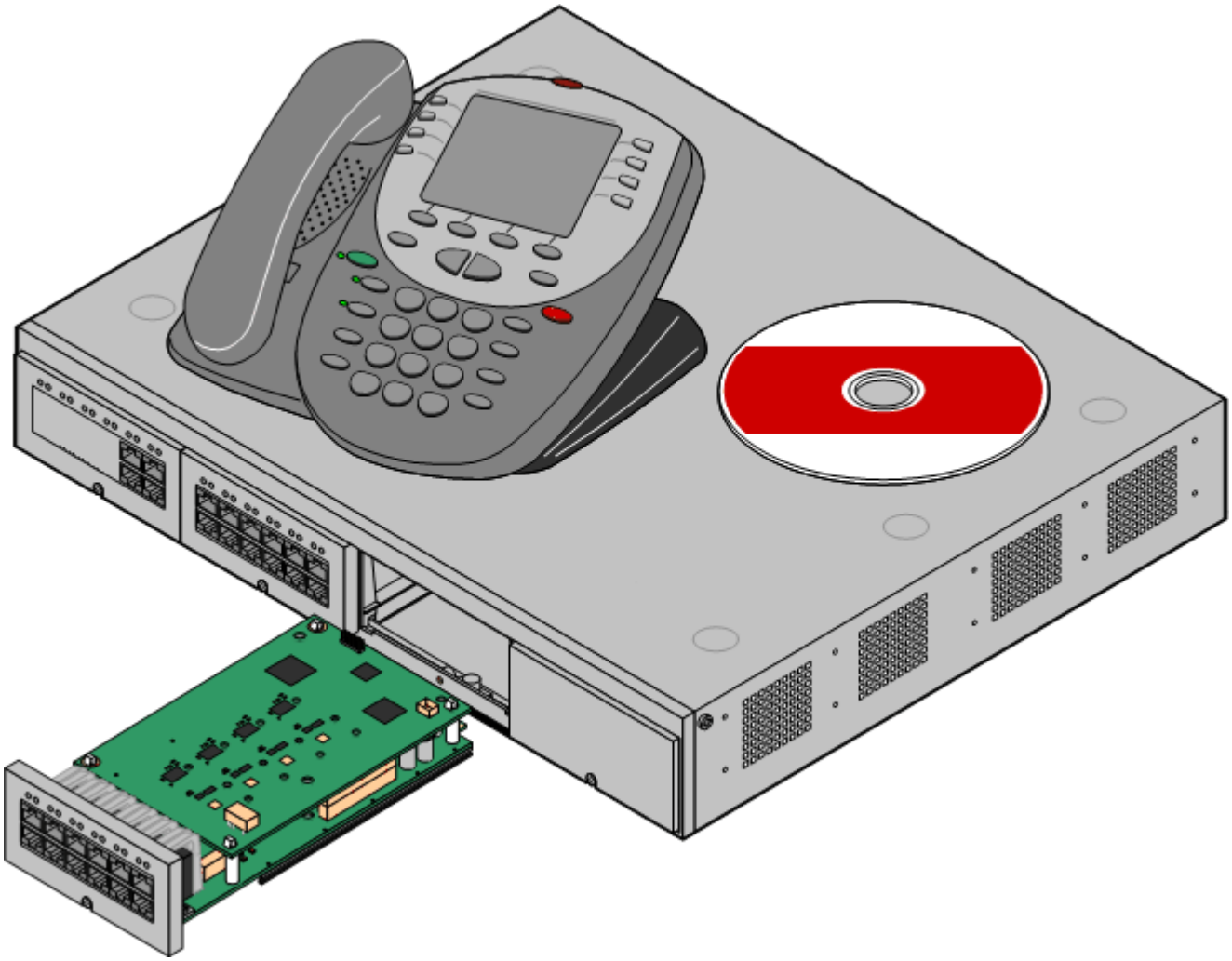
Panorama general del sistema

1. Panorama general del sistema

El objetivo de este documento es asistirlo en la instalación de un sistema IP Office que se ejecuta en el modo estándar de IP Office (IP Office Essential Edition o IP Office Preferred Edition) usando una unidad de control IP500 V2.

Esta documentación no cubre la instalación de los sistemas IP Office Basic Edition, IP Office Basic Edition - modo Norstar o IP Office Basic Edition - modo PARTNER®, cada uno de los cuales tiene su propia documentación de instalación por separado. Tampoco cubre la adición de un sistema IP500 V2 como un sistema IP500 V2 Expansion sistema en una red Server Edition. Por lo tanto, las notas sobre compatibilidad de hardware para IP500 V2 en este manual se siguen aplicando al uso de Server Edition, a menos que se indique lo contrario.

- Los instaladores familiarizados con la instalación de versiones previas deben consultar la sección Cambios para la versión 10.1 12.



- El sistema IP Office es un sistema de comunicaciones de convergencia de voz y datos. Por lo tanto, solo debe ser instalado por personas con experiencia en telefonía y redes de datos IP.
- Los técnicos instaladores deben estar capacitados para trabajar con sistemas IP Office. Mediante Avaya University 49 (AU), Avaya ofrece un rango de cursos de capacitación, incluyendo capacitación específica para la implementación e instalación de IP Office. También ofrece programas de certificación para que los técnicos instaladores reciban distintos niveles de acreditación en el sistema IP Office.
- Es responsabilidad de quien lo instala comprobar que todo el trabajo de instalación se realice en cumplimiento con los reglamentos y requerimientos locales y nacionales. Es asimismo su responsabilidad determinar correctamente los requerimientos del cliente antes de realizar la instalación, con el fin de asegurar que la instalación cumple con estos requerimientos.
- Es necesario que lea y comprenda esta documentación antes de la instalación. También debe obtener y leer los Boletines técnicos de Avaya relacionados con versiones de software y hardware recientes, a fin de asegurar que esté familiarizado con cualquier cambio realizado a los equipos y software de IP Office.
- Avaya IP Office IP 500 V2 también es conocido como "Unidad de control IPO IP500 V2", "IP Office IP 500 v2", "IPO IP500 v2", "IP 500 V2", "IP500 V2", "Conjunto de unidad de sistema IPO 500v2" o "IP Office 500 v2". A lo largo de este documento se usa el término IP500 V2.

1.1 Cambios en esta versión

A continuación se presenta un resumen de los cambios más importantes que afectan la instalación de IP500 V2 con la versión 10.1 de IP Office.

- **Compatibilidad con IP500 DS16B2 y DS30B2**
  Los módulos de expansión externa IP500 DS16B y DS30B han sido sustituidos por los módulos DS16B2 y DS30B2, respectivamente. Los módulos nuevos admiten la misma funcionalidad que los módulos anteriores.

1.2 Documentación adicional

Este manual solo abarca la instalación básica del sistema necesaria para lograr un sistema IP500 V2 que se pueda configurar. Las aplicaciones de IP Office y productos accesorios, como también los teléfonos IP, están fuera del alcance de este manual.

Si esas aplicaciones y productos van a ser parte de la instalación del sistema, se debería conseguir, leer y entender la documentación separada para cada producto, antes de la instalación.

- **Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín Técnico de IP Office referente a la versión de software de IP Office que desea instalar. El boletín contiene información importante que puede haberse omitido en este manual. Puede encontrar los Boletines Técnicos de IP Office en el sitio Web de soporte técnico Avaya *(http://support.avaya.com)*.

Para descargar la documentación:

1. Vaya a ***https://support.avaya.com***.
2. Seleccione **Soporte por producto** y luego **Documentación**.
3. Introduzca ***IP Office*** en el cuadro **Introducir el nombre del producto** y seleccione la opción correcta del menú desplegable.
4. Use el menú desplegable **Elegir versión** para seleccionar la versión de IP Office requerida.
5. Seleccione los tipos de documentos requeridos en la lista y haga clic en **INTRO**.

1.3 Disponibilidad del equipo

Los códigos SAP y los detalles de los artículos específicos en estos documentos se proporcionan como referencia únicamente. Los artículos disponibles en cualquier localidad en específico deben confirmarse en la lista de precios local de Avaya IP Office para dicha localidad. La lista de precios local puede incluir también artículos adicionales relativos a los requerimientos de instalación para dicho lugar.

Esta documentación cubre el equipo compatible con IP Office 10.1. Esto incluye el equipo que es compatible pero que ya no está disponible como nuevo de Avaya.

1.4 Reparación

IP Office no contienen componentes que puedan recibir servicio o reparaciones. Si se sospechan fallas en una unidad, la unidad entera debe ser reemplazada.

Las unidadesde control de IP Office no deben abrirse bajo ninguna circunstancia, excepto para introducir tarjetas base IP500 80.

1.5 RoHS

RoHS es una directiva de la Unión Europea, y significa Restricción de ciertas sustancias peligrosas en equipos eléctricos y electrónicos. Varios otro países han implementado legislaciones similares o están por implementarlas. Avaya ha decidido actualizar su rango global de productos para cumplir con los requerimientos de la directiva RoHS.

Las acciones emprendidas varían.

- En algunos cosas, el equipo ha sido descontinuado y Avaya ya no lo tiene disponible.
- En algunos casos, los productos manufacturados recientemente se han diseñado en cumplimiento con RoHS y conservan su código SAP anterior.
- En otros casos, el equipo ha sido reemplazado por una alternativa en cumplimiento con RoHS y tienen nuevos códigos SAP.
- Los códigos SAP en este documentos incluyen los equipos en cumplimiento con RoHS a menos que se especifique lo contrario.

1.6 Modos de IP Office

Los sistemas IP Office se pueden ejecutar en varios modos. Para la versión 10.0 de IP Office, solo son compatibles los siguientes modos para unidades de control IP500 V2:

Modos IP Office Basic Edition

Los siguientes modos operativos se conocen en conjunto como modo IP Office básico.

- **IP Office Basic Edition**
  Este es el modo predeterminado de funcionamiento para unidades de control IP500 V2.
- **IP Office Basic Edition - modo Norstar**
  Este modo opera igual que el modo IP Office Basic Edition. Este modo se vende en locales de Oriente Medio y África del Norte.
- **IP Office Basic Edition - modo PARTNER®**
  Este modo opera igual que el modo IP Office Basic Edition. Este modo se vende en locales en Norteamérica.

Modo estándar de IP Office

Los siguientes modos operativos se conocen en conjunto como modo estándar de IP Office.

- **IP Office Essential Edition**
  Para IP Office versión 10.1, los sistemas IP500 V2 se ejecutan en este modo si se agrega una licencia **Essential Edition** a la configuración. Los sistemas configurados en este modo sin una licencia no admitirán funciones de telefonía.
- **IP Office Preferred Edition**
  Este modo es similar a IP Office Essential Edition, pero agrega compatibilidad a la aplicación Voicemail Pro. Este modo se activa al agregar una licencia **Preferred Edition (Voicemail Pro)** a un sistema que ya cuenta con licencia para **Essential Edition**.

Otros modos

- **Server Edition**
  En este documento no se analiza este modo especial. Consulte la documentación separada de Server Edition. Un sistema IP500 V2 puede usarse en una red Server Edition como IP500 V2 Expansion sistema. Por lo tanto, las notas sobre compatibilidad de hardware para la unidad de control IP500 V2 en este manual se siguen aplicando al uso de Server Edition, a menos que se indique lo contrario.
  - **IP Office™ Platform Select**
    Este modo activa funciones adicionales en sistemas Server Edition.

1.6.1 Tarjetas SD de sistema

La unidad de control IP500 V2 debe estar equipada con una tarjeta SD del sistema. El modo predeterminado del sistema lo determina el tipo de tarjeta SD del sistema presente. Al usar IP Office Manager y agregar licencias, el modo del sistema se puede cambiar.

Las distintas tarjetas SD del sistema son:

- **Tarjeta SD de IP Office U-Law**
  Un sistema equipado con este tipo de tarjeta operará en modo predeterminado en telefonía U-Law y en Sistema clave IP Office Basic Edition . Diseñado para localidades en Norteamérica.
- **Tarjeta SD de IP Office A-Law**
  Un sistema equipado con este tipo de tarjeta operará en modo predeterminado en telefonía A-Law y en sistema PBX IP Office Basic Edition . Diseñado para localidades fuera de Norteamérica.

1.6.2 Capacidad general

La siguiente tabla es solo un resumen. Las combinaciones exactas de puertos de extensión, para troncales y usuarios también dependen de variaciones locales en el hardware compatible. Por ejemplo, las troncales BRI no están disponibles en los sitios norteamericanos.

		IP Office Basic Edition - modo PARTNER®	IP Office Basic Edition - modo Norstar	IP Office Basic Edition	IP Office Essential Edition IP Office Preferred Edition
Extensiones	Extensiones máximas	100 [1]	100 [1]	100 [1]	384
Líneas troncales	Troncales máximas:	64	64	64	[5]
	- Troncales analógicas máximas:	32	32	32	204

Página1350 de 3226.

		IP Office Basic Edition - modo PARTNER®	IP Office Basic Edition - modo Norstar	IP Office Basic Edition	IP Office Essential Edition IP Office Preferred Edition
	- Canales BRI máximos [3]	–	12	12	32
	- Canales PRI máximos [4]	24	30	30	240
	- Canales SIP máximos [2]	20	20	20	[5]
	- Canales H323 IP máximos	–	–	–	[5]

1. 100 extensiones en el modo de numeración con tres dígitos. 48 extensiones en el modo de numeración con dos dígitos.
   - Para modos IP Office Basic Edition, el sistema asume que la unidad de control base está siempre completa con un máximo de 32 extensiones, ya sean reales, fantasmas o una combinación, a la que asigna números de extensiones en secuencia. Esto se realiza antes de asignar los números de extensión a cualquier extensión real en los módulos de expansión externa conectados, hasta el límite de extensiones del sistema. Si no se excedió el límite de extensiones del sistema, todos los números de extensión restantes se asignarán a extensiones fantasma adicionales.
2. En todos los modos, se requieren los recursos de hardware para compresión de voz para la compatibilidad con SIP.
3. Los sistemas de modo IP Office Basic Edition no admiten ambas troncales BRI y PRI en el mismo sistema. También están restringidos a 12 canales BRI independientemente del hardware BRI instalado. Los sistemas de modo IP Office admiten ambas troncales BRI y PRI en el mismo sistema.
4. Los sistemas de modo IP Office Basic Edition se limitan a una tarjeta PRI de puerto único.
5. La capacidad depende de las licencias, los recursos de compresión de voz y el ancho de banda disponibles.

1.6.3 Resumen del soporte técnico de hardware

Observe que aún en los casos donde se indica que existe soporte, la disponibilidad y compatibilidad de los equipos permanece sujeta a las restricciones locales. La tabla a continuación es un resumen de IP Office versión 10.1, consulte Compatibilidad con hardware y software 302 para obtener un resumen más histórico y un listado de los teléfonos compatibles.

	Modos IP Office Basic Edition	Modos IP Office estándar
Unidad de control IP500 V2	✓	✓
Tarjetas base IP500		
Tarjeta de estación digital IP500	✓ 3	✓ 3
Teléfono analógico IP500 2/8	✓ 4	✓ 4
Tarjeta TCM8 IP500	✓ 4	✓ 4
Tarjetas 32/64 VCM IP500	–	✓ 2
Expansión de 4 puertos IP500	–	✓ 1
Producto combinado BRI IP500[2][4]	✓ 2	✓ 2
Producto combinado ATM IP500[2]	✓ 2	✓ 2
Producto combinado ATM IP500 V2[2]	✓ 2	✓ 2
IP500 ETR6[1][6]	✓ 3	–
Unified Communications Module[6]	–	✓
Tarjetas auxiliares de troncales		
Tarjeta de troncales analógicas	✓	✓
Tarjeta de troncales analógicas V2	✓	✓
Tarjetas de troncales BRI [4]	✓	✓
Tarjeta de troncales PRI [4][5]	✓ 1	✓ 4
Módulos de expansión		
Cantidad de módulos[3]	8	12
Estación digital 16/30	✓	✓
Estación digital 16A/30A	✓	✓
Estación digital 16B/30B	✓	✓
Teléfono 8/16/30	✓	✓
Troncal analógica de 16 líneas	✓	✓
BRI So8	–	✓
Tipos de teléfonos		
Teléfonos ETR *(Puertos ETR)*	✓	–
Teléfonos BST *(puertos BST)*	✓	✓
Teléfonos DS *(puertos DS)*	✓	✓
Teléfonos IP H323 *(LAN)*	–	✓
Teléfonos IP SIP *(LAN)*	–	✓
DECT R4 *(LAN)*	–	✓
DECT DMS *(puertos BST)*	✓	✓
Tipos de correo de voz		
Embedded Voicemail	✓	✓
Voicemail Pro	–	✓

1. La tarjeta ETR6 solo es compatible con sistemas IP500 V2 en los modos IP Office Basic Edition - modo PARTNER® o IP Office Basic Edition U-Law.
2. solo se admiten dos tarjetas combinadas en una unidad de control, sin importar el tipo de tarjeta combinada.
3. Pueden agregarse módulos de expansión externos, siempre y cuando no se exceda el límite total de extensiones y troncales. En modos estándar de IP Office Basic Edition, se admite un máximo de un módulo de troncal analógica de 16 puertos.
4. Los sistemas en modo IP Office Basic Edition no admiten la combinación de líneas troncales BRI y PRI, y solo admiten un máximo de 12 canales BRI.

5. Los sistemas de modo IP Office Basic Edition solo admiten una tarjeta PRI de puerto único.

1.6.4 Resumen del soporte técnico de funciones

La tabla a continuación es solo un resumen general. Para información más detallada, consulte la documentación de instalación de la aplicación específica.

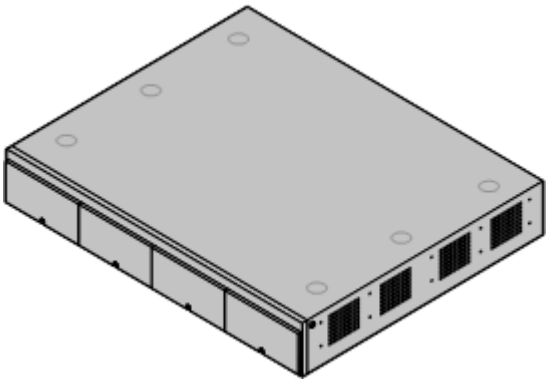
		IP Office Basic Edition			IP Office Essential Edition	IP Office Preferred Edition
		PARTNER Mode	Norstar Mode	Quick Mode		
Aplicaciones Admin	**Administración basada en teléfonos**	✓	✓	✓	–	–
	IP Office Web Manager	✓	✓	✓	✓	✓
	IP Office Manager	✓	✓	✓	✓	✓
	Supervisar (System Monitor)	✓	✓	✓	✓	✓
	System Status Application	✓	✓	✓	✓	✓
Aplicaciones	**one-X Portal for IP Office**	–	–	–	–	✓
	one-X Mobile	–	–	–	–	✓
	Avaya Communicator	–	–	–	–	✓
	SoftConsole	–	–	–	✓	✓
	TAPI (1st Party)	–	–	–	✓	✓
	TAPI (3rd Party)	–	–	–	✓	✓
	Voicemail Pro	–	–	–	–	✓
	Contact Recorder for IP Office	–	–	–	–	✓

Localidades		Canadá, México, Estados Unidos.	Bahréin, Egipto, Kuwait, Marruecos, Omán, Pakistán, Qatar, Arabia Saudita, Sudáfrica, Turquía, Emiratos Árabes Unidos.	Argentina, Australia, Bahréin, Bélgica, Brasil, Canadá, Chile, China, Colombia, República Checa, Dinamarca, Egipto, Finlandia, Francia, Alemania, Grecia, Hong Kong, Hungría, Islandia, India, Irlanda, Italia, Japón, Corea, Kuwait, Malasia, México, Marruecos, Países Bajos, Nueva Zelanda, Noruega, Omán, Paquistán, Perú, Filipinas, Polonia, Portugal, Catar, Rusia, Arabia Saudita, Singapur, Sudáfrica, España, Suecia, Suiza, Taiwán, Turquía, Emiratos Árabes Unidos, Reino Unido, Estados Unidos, Venezuela.		
Idiomas de correo de voz	**Embedded Voicemail**	• **Árabe**, **cantonés**, **danés**, **holandés**, **inglés (Reino Unido)**, **inglés (EE. UU.)**, **finlandés**, **francés**, **francés (Canadá)**, **alemán**, **hebreo**, **italiano**, **japonés**, **coreano**, **mandarín**, **noruego**, **polaco**, **portugués**, **portugués (Brasil)**, **ruso**, **español**, **español (Argentina)**, **español (América Latina)**, **español (México)**, **sueco**, **turco**.				
	Voicemail Pro	–	–	–	–	Como se describió anteriormente, además de: **Griego**, **húngaro**. Excepto: **Árabe**, **español (México)**.

1.7 La unidad de control

La base de todo sistema IP Office es la unidad de control. La unidad de control almacena la configuración del sistema y controla la operación del sistema. Cada unidad de control se puede personalizar con la introducción de distintas tarjeta base 24 en las que también se pueden agregar tarjetas auxiliares de troncales 27. Los módulos de expansión externos 29 también se pueden conectar para agregar puertos de extensión y de troncales adicionales.

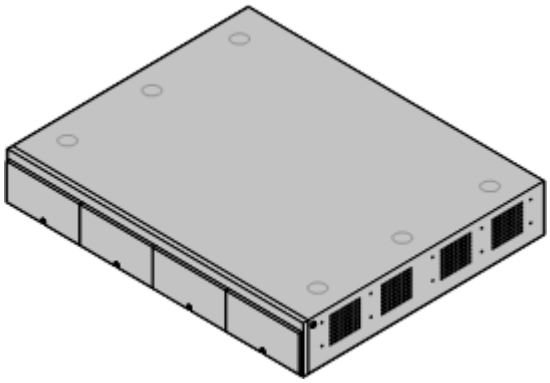
El IP Office versión 10.1 es compatible con las siguientes unidades de control IP Office. Otros tipos anteriores de unidades de control de IP Office no son compatibles con IP Office versión 10.1 y esta documentación no las contempla.



- **Unidad de control IP500 V2** 209
  Esta unidad de control incluye cuatro ranuras en la parte delantera para tarjetas base IP500. Tiene una fuente de alimentación interna y usa una tarjeta SD de sistema obligatoria. Incluye un conmutador LAN con dos puertos Ethernet (Capa 3 administrada) en la parte posterior.
  - El tipo de tarjeta SD de sistema que se coloque predetermina el modo de operación 14 del sistema.
    - **IP Office Basic Edition**
    - **IP Office Basic Edition - modo PARTNER®**
    - **IP Office Basic Edition - modo Norstar**
    - **IP Office Essential Edition**

1.8 Componentes del sistema IP500 V2

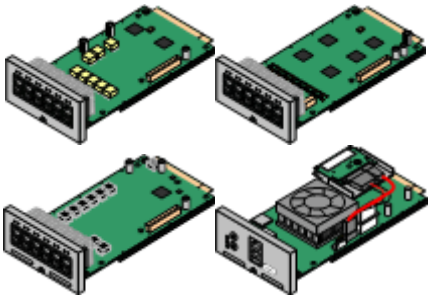
Los siguientes son los componentes típicos de un sistema basado en una unidad de control IP500 V2.



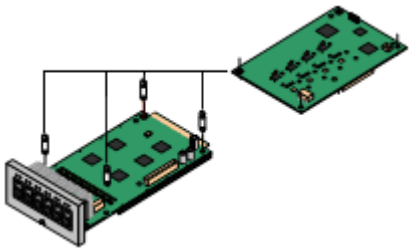
VK00nDd15SDvXoxkw9cR9x_jOXr_AWz9

- **Unidad de sistema IP500 V2 de IP Office** 209
  La unidad de control contiene la configuración principal y realiza el enrutamiento y conmutado de las llamadas telefónicas y el tráfico de datos. Cada unidad de control contiene cuatro ranuras para tarjetas base opcionales para soportar los puertos de troncales y extensiones telefónicas.
  - **Tarjeta SD Avaya** 23
    Esta tarjeta contiene el firmware y otros archivos que usa el sistema cuando se inicia. Es obligatorio tener una tarjeta System SD Avaya para que el sistema funcione correctamente. La tarjeta también brinda almacenamiento para el correo de voz integrado.

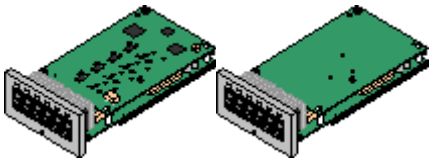
- **Claves de licencias** 301
  Distintas funciones y aplicaciones requieren ingresar una clave de licencia en la configuración del sistema. Cada clave es una cadena de texto de 32 caracteres exclusiva para la función que se activará y el número de serie del servidor que emite la licencia. En la mayoría de los casos, es el número de serie de la tarjeta System SD que está instalada en el sistema.



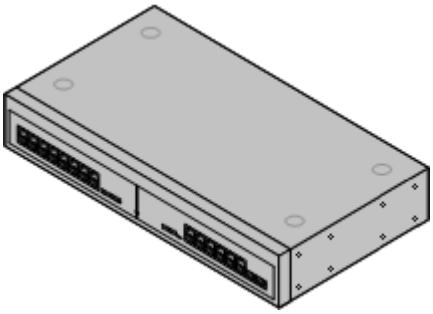
- **Tarjetas base IP500** 24
  La unidad de control IP500 V2 incluye ranuras para hasta cuatro tarjetas base IP500. Puede utilizarlas para agregar puertos para extensiones analógicas, extensiones digitales, canales de compresión de voz y otros recursos.
  - **Tarjeta base de estación digital IP500** 224
  - **Tarjeta base de teléfono analógico IP500** 217
  - **Tarjeta base de VCM IP500** 229
  - **Tarjeta base de expansión de cuatro puertos IP500** 216
  - **Tarjeta base TCM8 IP500** 228
  - **Tarjeta base ETR6 IP500** 226
  - **Unified Communications Module** 223



- **Tarjetas auxiliares de troncales IP500** 27
  Muchas de las tarjetas base IP500 pueden equiparse con una tarjeta auxiliar IP500 a fin de admitir distintos tipos de conexiones de troncales.
  - **Tarjeta de troncales analógicas IP500** 233
  - **Tarjeta de troncales analógicas IP500 V2** 233
  - **Tarjeta de troncales BRI IP500** 235
  - **Tarjeta de troncales PRI IP500** 236



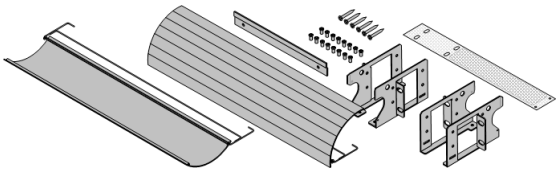
- **Tarjetas combinadas IP500** 24
  Estas tarjetas son tarjetas base y auxiliar previamente emparejadas. Proporcionan seis puertos de estación digital, dos puertos de teléfono analógico, diez canales de compresión de voz y ya sea cuatro puertos troncales analógicos o cuatro canales BRI (dos puertos). La tarjeta de troncales auxiliar no se puede extraer ni reemplazar por una tarjeta de otro tipo.
  - **Tarjeta combinada BRI IP500** 221
  - **Tarjeta combinada ATM IP500** 219
  - **Tarjeta combinada ATM IP500 V2** 219



- **Módulos de expansión externos IP500** 29
  Se pueden agregar puertos adicionales con ayuda de algunos módulos de expansión externos IP500.
  - Los sistemas que funcionan en modos estándar de IP Office admiten ocho módulos de expansión externos o 12 si la unidad de control se instala con una tarjeta base de expansión de cuatro puertos IP500.

- **Suministros de energía** 33
  La unidad de control IP500 está equipada con una unidad interna de suministro de energía. Cada módulo de expansión externo incluye una unidad externa de suministro de energía. También pueden requerirse unidades de suministro de energía adicionales para los teléfonos IP y algunos complementos del teléfono.
- **Cables de energía** 34
  Dependiendo de la localidad, es necesario solicitar distintos cables de energía para cada unidad de control, módulo de expansión externo y para cualquier teléfono o dispositivo que emplee unidades de suministro de energía externas.

- **Cables** 36
  El sistema está diseñado principalmente para ser conectado a un sistema de cableado estructurado por medio de cables UTP CAT3. Este método permite que el tráfico telefónico y de datos compartan la misma infraestructura de cableado, además que simplifica los movimientos o traslados de equipo.



- **Kits de montaje** 40
  La unidad de control puede emplearse como una unidad independiente, con módulos de expansión externos apilados encima. Con ayuda de los kits de montaje en bastidor opcionales, también puede montar en bastidor la unidad de control y sus módulos de expansión externos. En forma alterna, con un kit opcional de montaje en pared, puede montar en la pared la unidad de control IP500. Los módulos de expansión externos IP500 también pueden montarse en la pared.

- **Protectores contra picos y cajas de protección** 39
  En instalaciones que incluyen extensiones hacia otros edificios, es necesario instalar equipo de protección adicional. Este equipo puede también ser necesario en áreas donde el riesgo de rayos es alto.

- **Teléfonos** 41
  Los sistemas IP Office son compatibles con diversos teléfonos digitales e IP de Avaya, además de teléfonos analógicos.

- **DVD de aplicación** 45
  Puede ordenar las aplicaciones de IP Office, disponibles en varios discos DVD. Además, puede descargarlos de la sección IP Office en el sitio web de soporte técnico Avaya *(http://support.avaya.com)*.

1.9 Tarjeta System SD

El sistema IP Office requiere una Tarjeta System SD Avaya 212 para funcionar. Esta tarjeta tiene el firmware y otros archivos que el sistema carga cuando se enciende. Una vez que el sistema está en funcionamiento, la tarjeta System SD guarda una copia de la configuración del sistema, el archivo de licencia y, si se utiliza, los archivos del buzón de voz integrado. La tarjeta se inserta en la ranura System SD en la parte trasera de la unidad de control antes de iniciar el sistema.

Si el sistema usa un archivo XML PLDS como licencia, el número de serie de clave de funciones de la tarjeta SD es el único valor que se utiliza para la emisión y validación de las licencias.

Configuración de nivel de software original del sistema

Para una nueva unidad de control de IP Office, la versión del software de IP Office que carga desde la tarjeta SD del sistema cuando inicia por primera vez se convierte en la base o nivel de software original. El valor se graba en la memoria permanente de la unidad de control y no se puede cambiar.

Por lo tanto, es importante verificar que se haya cargado la tarjeta System SD con la versión correcta del software antes de que se inicie el sistema por primera vez. Esto se realiza mediante el uso de IP Office Manager para cargar el nivel requerido de software en la tarjeta SD 75.

1.10 Licencias

El sistema IP Office requiere licencia para algunas funciones. Consulte Licencias 294. El archivo de licencia puede cargarse manualmente o cargarse previamente en la tarjeta SD del sistema 77.

¿Cómo se le agrega una licencia al sistema?

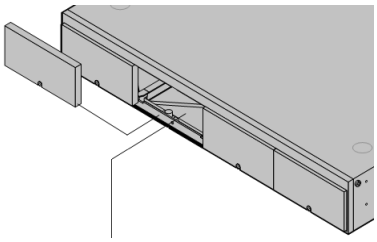
- Se carga al sistema un archivo XML que contiene el conjunto completo de licencias PLDS. El archivo de licencia es exclusivo para el número de serie de clave de la función de la tarjeta System SD instalada en el sistema.
    - La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.

Requerimientos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una licencia de sistema **Essential Edition** para la versión de IP Office específica que desea ejecutar.

1.11 Tarjetas de la unidad de control

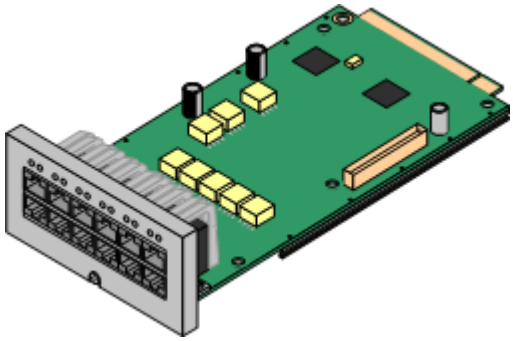
1.11.1 Tarjetas base IP500



La unidad de control de IP500 V2 tiene 4 ranuras para la inserción de las tarjetas base de IP500. Las ranuras están numeradas de 1 al 4, de izquierda a derecha. Por lo general se les puede utilizar en el orden que sea sin embargo, en caso de exceder la capacidad del tipo de tarjeta en particular, la tarjeta en la ranura de la extrema derecha será desactivada.

Cada tarjeta base incluye un panel delantero integrado con los puertos para las conexiones de cable. Típicamente los primeros ocho puertos de la izquierda se utilizan para conectar dispositivos de extensiones. Los cuatro puertos a la izquierda se utilizan para conectar troncales cuando se ha conectado una tarjeta auxiliar de troncales 27 a la tarjeta base.

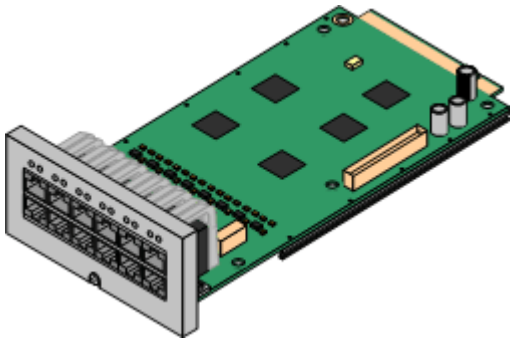
Tarjeta base de estación digital IP500 224



Esta tarjeta proporciona ocho puertos 8 DS (estación digital) para la conexión de teléfonos digitales Avaya.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500 27 que utiliza los puertos de la tarjeta base para realizar conexiones de troncales.
- **Máximo:** 3 tarjetas por unidad de control.
  - Las conexiones para teléfonos 4100, 7400, serie M y serie T utiliza la tarjeta IP500 TCM8 Digital Station.

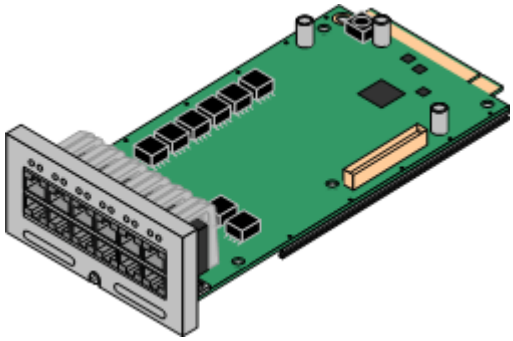
Tarjeta base de teléfono analógico IP500 217



La tarjeta esta disponible en dos variantes, proporcionando ya sea 2 u 8 puertos de teléfono analógico.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500 27 que utiliza los puertos de la tarjeta base para realizar conexiones de troncales.
- **Máximo:** Cuatro por unidad de control.
  - Los puertos de troncales analógicas no incluyen un capacitor de timbre. En sitios donde existe este requerimiento, debe realizarse la conexión mediante un enchufe Maestro que contenga capacitores de timbre.
  - Si está equipada una tarjeta auxiliar de troncales analógicas IP500, durante los cortes de energía el puerto 8 se conecta al puerto de troncales analógicas 12.

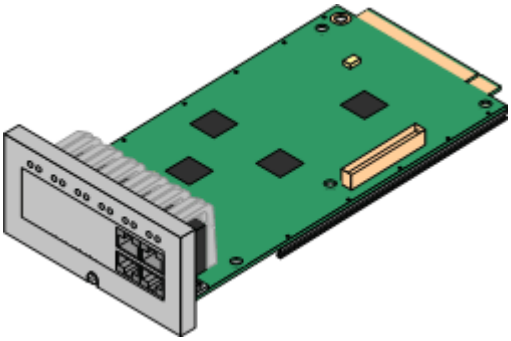
Tarjeta de estación digital TCM8 IP500 228



Esta tarjeta proporciona ocho puertos BST (estación digital) para la conexión de los teléfonos Avaya 4100, 7400, serie M y serie T.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500 27 que utiliza los puertos de la tarjeta base para realizar conexiones de troncales.
- **Máximo:** 4 por unidad de control por unidad de control IP500 V2.

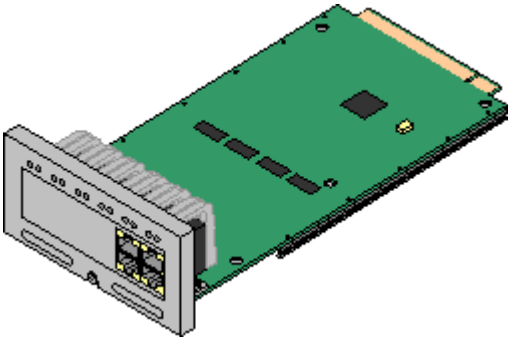
Tarjeta base de VCM IP500 229



Esta tarjeta está disponible en variantes que soportan 32 o 64 canales de compresión de voz para el uso con llamadas VoIP.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500 27 que utiliza los puertos de la tarjeta base para realizar conexiones de troncales.
- **Máximo:** Dos por unidad de control

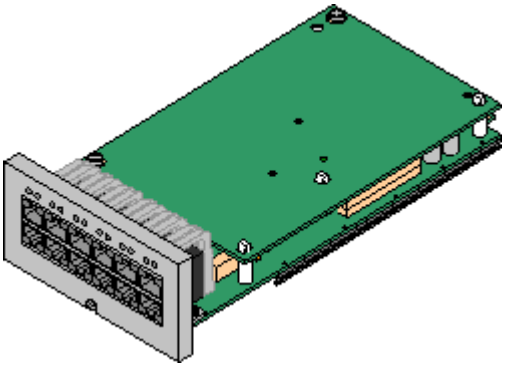
Tarjeta base de expansión de cuatro puertos IP500 216



Esta tarjeta agrega cuatro puertos de expansión adicionales a los módulos de expansión externos. La tarjeta trae incluidos cuatro cables de interconexión amarillos de 2m.

- Esta tarjeta no admite ninguna tarjeta auxiliar de troncales IP500.
- **Máximo:** 1 por unidad de control (solamente en la ranura 4 del lado derecho).
- **Módulos de expansión compatibles:** Los siguientes módulos de expansión externos son compatibles:
  - Módulo de troncales analógicas IP500
  - Módulo BRI So8 IP500
  - Módulo de estación digital IP500
  - Módulo de estación digital A IP500
  - Módulo de estación digital B IP500
  - Módulo Phone IP500

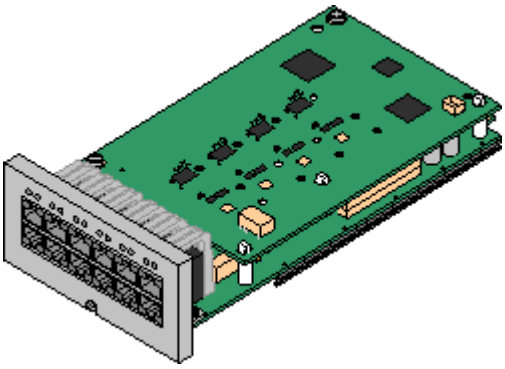
Tarjeta combinada BRI IP500 221



Esta tarjeta proporciona seis puertos de estación digital (1-6), dos puertos de extensiones analógicas (7-8) y dos puertos de troncales BRI (9-10, cuatro canales). La tarjeta también ofrece 10 canales de compresión de voz.

- **Máximo:** 2 tarjetas combinadas por unidad de control IP500 V2, sin importar el tipo.
  - Las tarjetas combinadas IP500 están equipadas previamente con una tarjeta auxiliar de troncales que no se puede extraer ni cambiar por otra tarjeta auxiliar de troncales de otro tipo o capacidad.
  - Los sistemas IP Office Basic Edition - modo Norstar y IP Office Basic Edition están limitados a un máximo de 12 canales BRI que usan tarjetas combinadas BRI o tarjetas auxiliares troncales BRI.

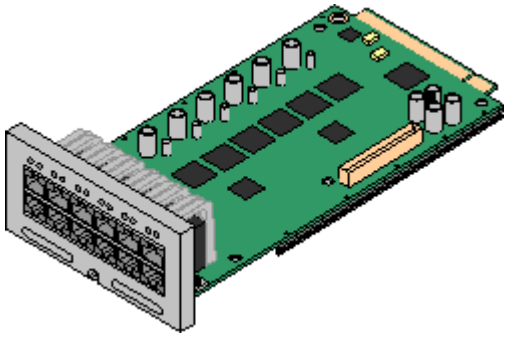
Tarjeta combinada ATM IP500/Tarjeta combinada ATM IP500 V2 219



Esta tarjeta proporciona seis puertos de estación digital (1-6), dos puertos de extensiones analógicas (7-8) y dos puertos de troncales analógicas (9-12). La tarjeta también ofrece 10 canales de compresión de voz.

- **Máximo:** 2 tarjetas combinadas por unidad de control IP500 V2, sin importar el tipo.
  - Las tarjetas combinadas IP500 están equipadas previamente con una tarjeta auxiliar de troncales que no se puede extraer ni cambiar por otra tarjeta auxiliar de troncales de otro tipo o capacidad.
  - Los puertos de troncales analógicas no incluyen un capacitor de timbre. En sitios donde existe este requerimiento, debe realizarse la conexión mediante un enchufe Maestro que contenga capacitores de timbre.
  - Durante cortes de energía, el puerto 8 del teléfono se conecta al puerto para troncales analógicas 12.

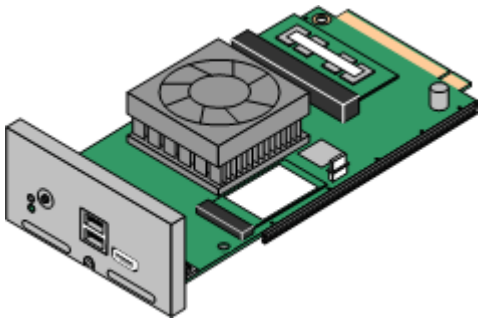
Tarjeta base ETR6 IP500 226



Esta tarjeta solo es compatible en una unidad de control IP500 V2 que funciona en IP Office Basic Edition - modo PARTNER® o IP Office Basic Edition. Proporciona seis puertos ETR para la conexión de teléfonos ETR. También se proporcionan dos puertos de extensiones analógicas para su uso de emergencia con la tarjeta de troncales analógicas.

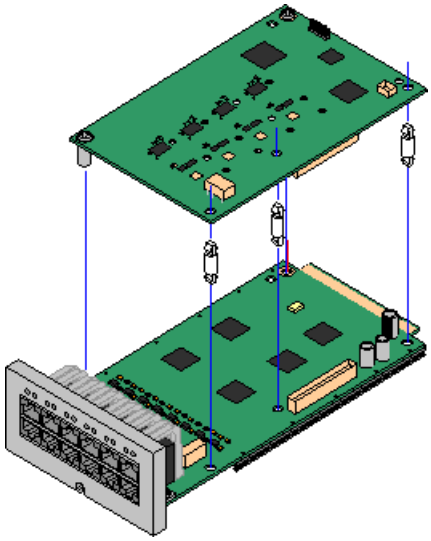
- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500, la cual utiliza los puertos de la tarjeta base para la conexión de troncales..
- **Máximo:** 3 por unidad de control IP500 V2.
- Los puertos de troncales analógicas no incluyen un capacitor de timbre. En sitios donde existe este requerimiento, debe realizarse la conexión mediante un enchufe Maestro que contenga capacitores de timbre.
- Si está equipada una tarjeta auxiliar de troncales IP500, durante los cortes de energía los puertos 7 y 8 se conectan al puerto de troncales analógicas 12. Sin embargo, durante la operación normal los puertos analógicos 7 y 8 no son utilizables.

Unified Communications Module 223



Esta tarjeta funciona como un servidor Linux incorporado para las aplicaciones one-X Portal for IP Office y/o Voicemail Pro.

1.11.2 Tarjetas de troncales IP500

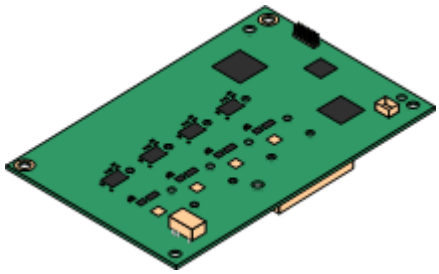


Muchos tarjetas base IP500 [24] pueden equiparse con tarjetas auxiliares de troncales IP500 para admitir la conexión de troncales a la tarjeta base.

Cada tarjeta auxiliar está equipada con los pilares de soporte requeridos para su instalación, así como una tarjeta para identificar la presencia de la tarjeta auxiliar en la parte de adelante de la tarjeta base después de la instalación.

- Las tarjetas combinadas IP500 están pre-equipadas con una tarjeta auxiliar de troncales que no puede ser extraída ni cambiada por otro tipo de tarjeta auxiliar de troncales.

Tarjeta de troncales analógicas IP500/Tarjeta de troncales analógicas IP500 V2 [233]

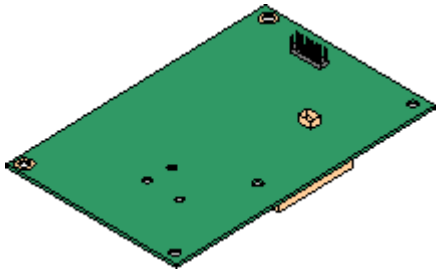


Estas tarjetas permiten que la tarjeta base admita cuatro troncales analógicas de inicio por bucle.

  - Los puertos de troncales analógicas no incluyen un capacitor de timbre. En sitios donde existe este requerimiento, debe realizarse la conexión mediante un enchufe Maestro que contenga capacitores de timbre.
  - Si está instalada la tarjeta base con puertos de teléfono analógico, durante un corte de energía el puerto de teléfono 8 se conecta al puerto de las troncales analógicas 12.

- **Máximo:** 4 tarjetas por unidad de control. La tarjeta de troncales analógicas IP500 V2 solo se admite en el IP500 V2.

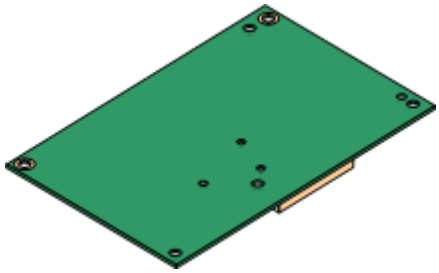
Tarjeta de troncales PRI-U IP500 [236]



Esta tarjeta permite que la tarjeta base admita dos conexiones con troncales PRI. La tarjeta está disponible en variantes de puerto individual o dual. La tarjeta puede configurarse para troncales E1 PRI, T1 de hurto de bits, T1 PRI o E1R2 PRI. También está disponible una variante T1(J) para uso en Japón.

- **Máximo:** Cuatro por unidad de control.
- El sistema IP Office admite 8 canales B sin licencia en cada puerto PRI-U IP500 instalado. Los canales B adicionales, hasta donde lo permiten la capacidad de los puertos instalados y el modo PRI seleccionado, requieren que se agreguen licencias tipo **IP500 Universal PRI (Canales adicionales)** [296] a la configuración. Estos canales adicionales consumen licencias con base en los canales adicionales que sean configurados como en servicio, desde el puerto 9 de la ranura 1 en adelante. Los canales D no son afectados por las licencias.

Tarjeta de enlace BRI de IP500 [235]



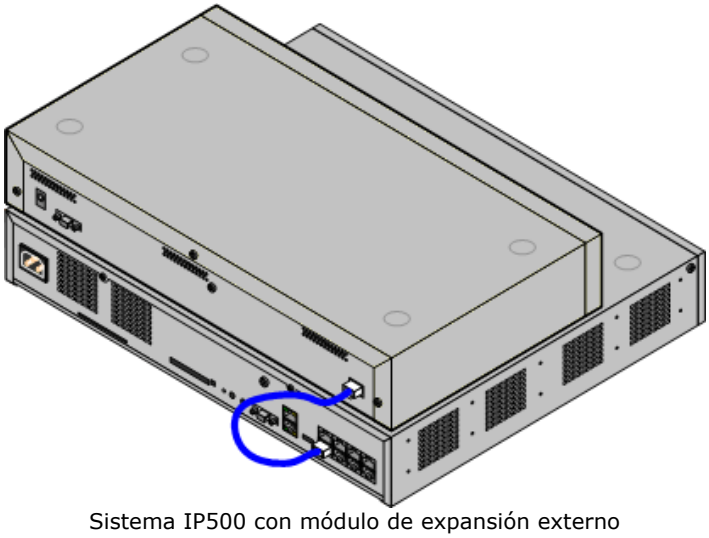
Esta tarjeta permite que la tarjeta base admita hasta cuatro conexiones de troncales BRI, con cada troncal suministrando canales digitales 2B+D. Esta tarjeta está disponible en variantes de 2 puertos (4 canales) y 4 puertos (8 canales).

- **Máximo:** 4 tarjetas por unidad de control.
- **Conexión S-Bus**: La tarjeta puede ser alternada del modo de troncales To al modo So. Este modo requiere de resistores de terminación adicionales y de un cable de interconexión cruzada ISDN, consulte la sección Puerto BRI (So) [283].

- Los sistemas IP Office Basic Edition - modo Norstar y IP Office Basic Edition están limitados a un máximo de 12 canales BRI que usan tarjetas combinadas BRI o tarjetas auxiliares troncales BRI.

1.12 Módulos de expansión externos

Estos módulos pueden equiparse para agregar puertos adicionales a los sistemas IP Office. La cantidad de módulos de expansión externos admitidos depende del tipo de unidad de control. Cada módulo utiliza una unidad de suministro de energía 33 externa, incluida con el módulo. El cable de energía 34 específico de la localidad para el PSU debe solicitarse por separado.



Sistema IP500 con módulo de expansión externo

- Los sistemas que funcionan en modos estándar de IP Office admiten ocho módulos de expansión externos o 12 si la unidad de control se instala con una tarjeta base de expansión de cuatro puertos IP500.
  - Cada módulo de expansión externo incluye un cable de interconexión para expansiones azul de 1 metro (3'3"). Este cable sedebe usar cuando se conecte a puertos de expansión en la parte trasera de una unidad de control.
  - Al realizar la conexión con los puertos de expansión de una tarjeta IP500 4-Port Expansion card, puede utilizar el cable de interconexión para expansiones amarillo de dos metros (6'6") en vez del cable azul estándar. La tarjeta de expansión de 4 puertos IP500 contiene cuatro cables amarillos.

Módulos de expansión externos IP500

Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y un cable de interconexión azul de 1m. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Variante	País	Código SAP
Teléfonos digitales (no IP)		
Estación Digital 16 IPO 500 245	Todos	700449499
Estación Digital 30 IPO 500 245	Todos	700426216
IPO 500 Digital Station 16A (RJ21) 247	Todos	700500699
IPO 500 Digital Station 30A (RJ21) 250	Todos	700500698
Estación digital IPO 500 16B 250	Todos	700501585
Estación digital IPO 500 30B 250	Todos	700501586
Teléfonos analógicos		
Phone 16 IPO 500 252	Todos	700449507
Phone 30 IPO 500 252	Todos	700426224
Otros		
Troncal analógica IPO 500 de 16 puertos 240	EU	700449473
IPO 500 BRI So8 243	Todos	700449515

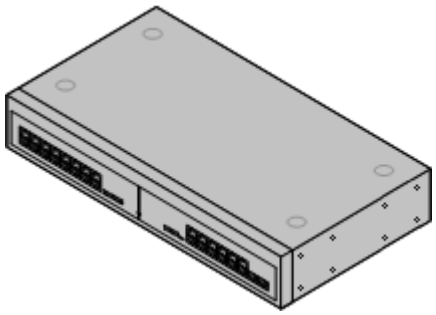
1.12.1 Módulos de expansión externos IP500

Los siguientes módulos de expansión externos IP500 son compatibles con la versión 10.1 de IP Office. Cada módulo utiliza una unidad de suministro de energía 33 externa, incluida con el módulo. El cable de energía 34 específico de la localidad para el PSU debe solicitarse por separado.

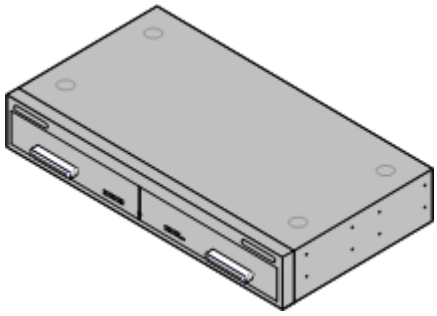
El módulo externo se puede apilar sobre la unidad de control. También se puede montar en la pared o en un rack con uno de los kits de montaje de IP Office 261.

- Los sistemas que funcionan en modos estándar de IP Office admiten ocho módulos de expansión externos o 12 si la unidad de control se instala con una tarjeta base de expansión de cuatro puertos IP500.

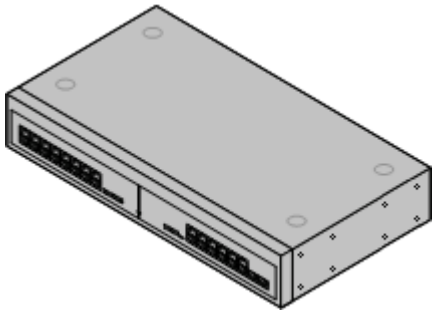
- **Módulos de estación digital IP500** 245
  Según la variante, ofrecen 16 o 30 puertos RJ45 DS 286 adicionales para teléfonos digitales Avaya DS 41 compatibles.



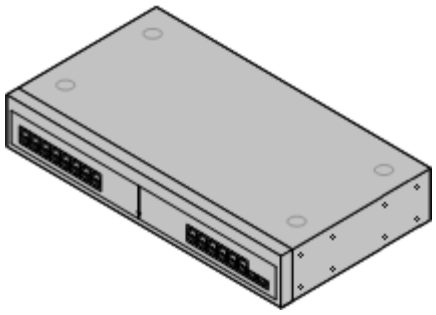
- **Módulos de Estación Digital A IP500** 247
  Según la variante, ofrecen puertos RJ21 para conectar 16 o 30 teléfonos digitales Avaya BST 41 adicionales. Compatibilidad solo en IP500 V2.



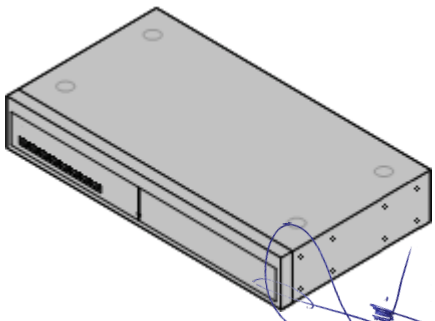
- **Módulos de estación digital B/B2 IP500** 250
  Según la variante, ofrecen 16 o 30 puertos RJ45 adicionales. Estos se pueden usar como puertos DS 286 para teléfonos digitales Avaya DS compatibles 41 o bien puertos BST 285 para teléfonos digitales Avaya BST compatibles 41. Sin embargo, el módulo sólo admite un tipo de puerto en cualquier momento. Para IP Office versión 10.1, los módulos DS16B/DS30B han sido reemplazados por los modelos DS16B2/DS30B2.



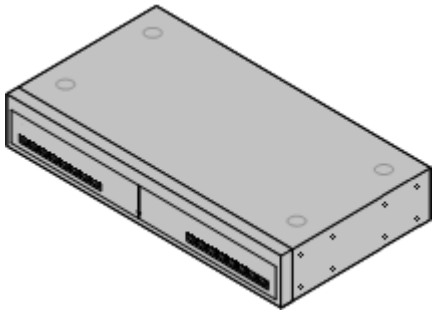
- **Módulos teléfono IP500** 252
  Según la variante, ofrecen 16 o 30 puertos TELÉFONO 291 para conectar teléfonos analógicos.



- **Módulo BRI So8 IP500** 243
  Proporciona ocho puertos BRI-So 283 para conectar dispositivos ISDN. Esta unidad no está diseñada para admitir troncales BRI.



- **Módulo de troncales analógicas IP500** 240
  Proporciona 16 puertos ANALÓGICOS 282 adicionales para conectar troncales analógicas. Es compatible con troncales de arranque por bucle y de arranque por tierra.
  - El uso con troncales de inicio por tierra requieren que el módulo de troncales y la unidad de control de IP Office estén conectados a tierra.
- En IP Office Basic Edition - modo PARTNER®, IP Office Basic Edition - modo Norstar y IP Office Basic Editions, solo se admite un módulo de troncales analógicas.

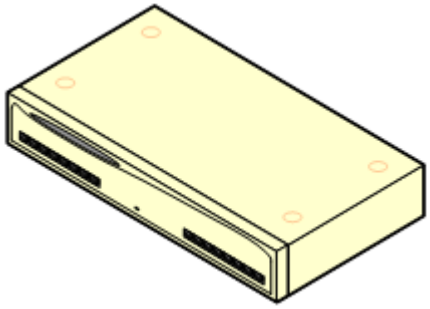


1.12.2 Módulos de expansión externos IP400

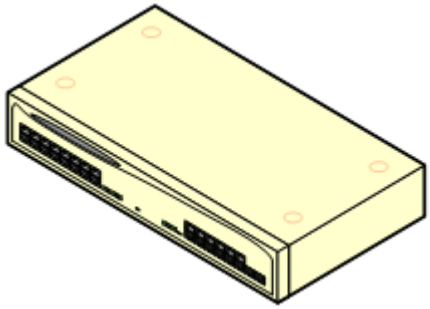
Los siguientes módulos de expansión externos IP400 son compatibles con la versión 10.1 de IP Office y pueden utilizarse con unidades de control IP500 V2. Cada módulo utiliza una unidad de suministro de energía 33 externa, incluida con el módulo. El cable de energía 34 específico de la localidad para el PSU debe solicitarse por separado.

Si se van a instalar en bastidor, estas unidades deben instalarse con el kit de montaje en bastidor IP400. Si se van a instalar en bastidor, estas unidades deben instalarse con el kit de montaje en bastidor IPO IP500. Estas unidades no pueden montarse en pared.

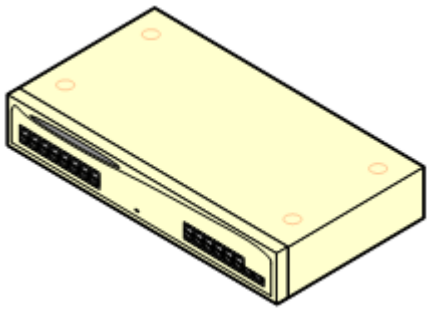
- **Módulo de troncales analógicas IP400 (ATM16)** 255
  Proporciona 16 puertos ANALÓGICOS 282 adicionales para conectar troncales analógicas. Es compatible con troncales de arranque por bucle y de arranque por tierra.
  - Disponible en múltiples variantes para distintas localidades.
  - El uso con troncales de inicio por tierra requieren que el módulo de troncales y la unidad de control de IP Office estén conectados a tierra.



- **Módulo de estación digital V2 IP400** 257
  Dependiendo de la variante, proporciona entre 16 y 30 puertos DS 286 adicionales para teléfonos digitales Avaya compatibles. 41. Esta versión reemplaza el módulo de estación digital anterior.



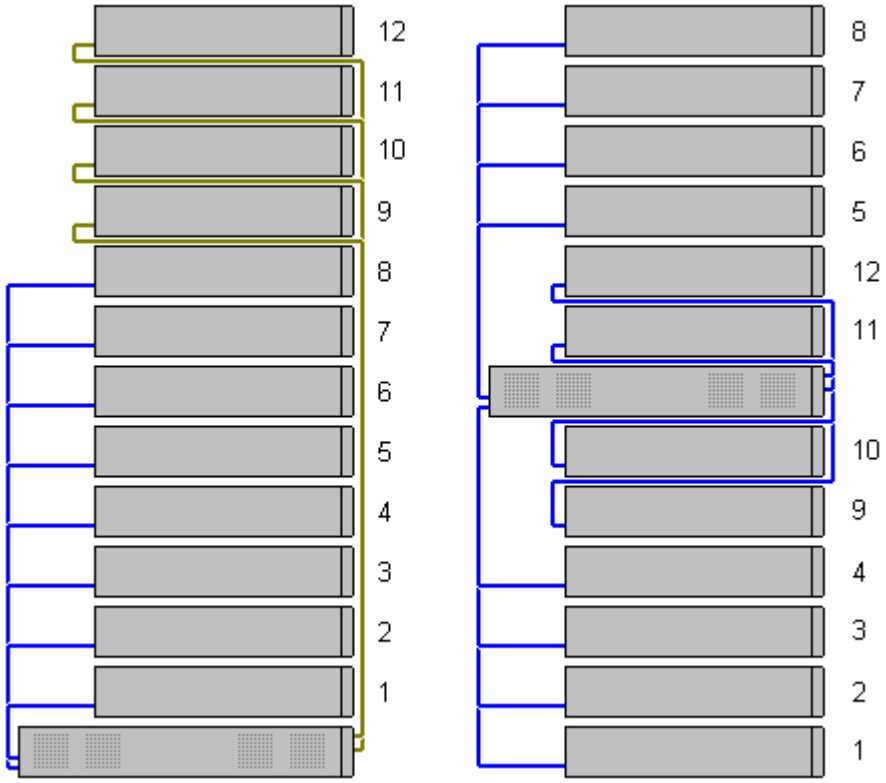
- **Módulo Phone V2 IP400** 259
  Dependiendo de la variante, proporciona entre 8, 16 y 30 puertos TELÉFONO 291 adicionales para teléfonos analógicos. Esta versión reemplaza el módulo Phone anterior. En IP Office 3.1, el módulo Phone V2 admite un mayor rango de opciones de indicación de mensaje en espera (MWI) que los módulos Phone V1.



1.12.3 Conexión de módulos de expansión externos

Los puertos de expansión integrados en una unidad de control se encuentran en la parte trasera de la unidad. Se puedan agregar cuatro puertos de expansión adicionales en la parte delantera de la unidad de control mediante la instalación de una tarjeta de expansión de cuatro puertos IP500.

- Cada módulo de expansión externo incluye un cable de interconexión para expansiones azul de 1 metro (3'3"). Este cable sedebe usar cuando se conecte a puertos de expansión en la parte trasera de una unidad de control.
- Al realizar la conexión con los puertos de expansión de una tarjeta IP500 4-Port Expansion card, puede utilizar el cable de interconexión para expansiones amarillo de dos metros (6'6") en vez del cable azul estándar. La tarjeta de expansión de 4 puertos IP500 contiene cuatro cables amarillos.



1.13 Suministros y cables de energía

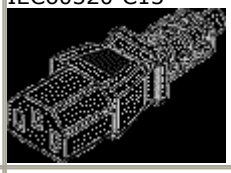
Todas las unidades de control de IP Office y módulos de expansión externos tienen ya sea una unidad interna de suministro de energía o están equipados con una unidad externa de suministro de energía

1.13.1 Suministros de energía

Las unidades de control IP500 V2 incluyen una fuente de alimentación interna y solo necesitan un cable de alimentación de energía específico para la localidad 34 y un enchufe de corriente que incluya interruptor. Observe que si el cable de energía incluye una terminal de tierra, el enchufe de corriente debe conectarse a una tierra de protección.

Los módulos de expansión externos incluyen una unidad externa de suministro de energía (PSU). Dichas unidades PSU incluyen un cable integrado de 1.5 metros para la conexión con la unidad de control o el módulo de expansión. No incluye el cable de energía 34 para la conexión de la PSU al enchufe de corriente, ya que éste varía según la localidad. Debe ordenar o conseguir localmente el cable de energía apropiado.

Se requieren fuentes de alimentación adicionales para los módulos complementarios EU24, XM24 y T3 DSS, y también pueden requerirlos los teléfonos IP de Avaya.

Área	Tipo	Utilizado con:	Tipo de conector
Unidades de control de IP Office y módulos de expansión externos	**PSU 40 W**	Analógica, Estación digital V1, Phone V1.	IEC60320 C7
	PSU 60W Aterrizada	Teléfono IP500 30, Estación digital IP500 30, Estación digital IP500 16A, Estación digital IP500 30A.	IEC60320 C13
Teléfonos IP y complementos del teléfono	**1151D1**	Todos los teléfonos con complementos XM24 Phone. Todos los teléfonos con complementos EU24/EU24BL Phone, excepto si se usa PoE Clase 3.	IEC60320 C13 
	1151D2		
	1600PWR 5V	PSU con clavija empleada con los teléfonos serie 1600 en IP cuando no se proporciona energía por medio de un PoE.	Distingas variantes por país.

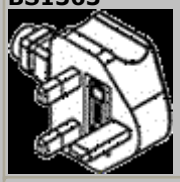
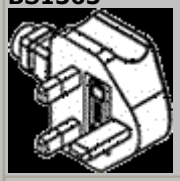
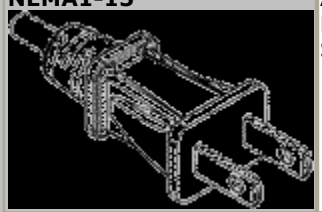
- La 1151D2 es igual que la 1151D1, excepto que incluye respaldo con baterías, las cuales se cargan durante la operación normal. La batería proporciona típicamente 15 minutos de respaldo con una carga máxima (20 Watts) y hasta ocho horas con una carga ligera (2 Watts).
- Los teléfonos IP Avaya pueden utilizar suministros de energía sobre Ethernet (PoE) tipo IEEE 802.3af. Consulte el Manual de instalación de teléfonos IP de IP Office para obtener la información completa.

1.13.2 Cables de suministro de energía

Cada unidad de control y módulo de expansión requiere un enchufe de salida de corriente con interruptor clasificado de 110-240V ac, 50-60Hz. La conexión de este enchufe de salida de corriente requiere de un cable de energía específico para la localidad que no viene incluido con la unidad, es necesario solicitarlo por separado. Observe que si el cable de energía incluye una terminal de tierra, el enchufe de corriente debe conectarse a una tierra de protección.

Los cables de energía no deben sujetarse a la superficie del edificio ni atravesar paredes, cielos rasos, pisos y otras aberturas similares. Deben tomarse medidas para la instalación a fin de evitar daños físicos al cable de suministro de energía, incluyendo el correcto enrutamiento del cable de suministro de energía y la disponibilidad de una conexión de corriente cerca del equipo fijo, o bien colocar éste cerca de una conexión de corriente.

Para las localidades que no se mencionan abajo, debe obtener localmente un cable de energía apropiado.

Tipo de cable de suministro de energía	Tipo de clavija para enchufe a la corriente	Localidades	Códigos SAP
Cables de energía aterrizados (IEC60320 C13) **Unidades de control** • IP500 V2. **Módulos de expansión externos IP500** • SO8 BRI • Estación digital 16/30 • Phone 16/30	**CEE7/7 (Schuko)** 	Europa y Sudáfrica.	700289762
	BS1363 	República Checa, Irlanda, Reino Unido.	700289747
	NEMA5-15P / CS22.2 No.42 	América del Norte, Centro y Sudamérica.	700289770
Cables de energía sin terminal de tierra (IEC60320 C7) **Módulos de expansión externos IP500** • Troncal analógica de 16 líneas	**CEE7/16 (Europlug)** 	Europa y Sudáfrica.	700213382
	BS1363 	República Checa, Irlanda, Reino Unido.	700213374
	NEMA1-15 	América del Norte, Centro y Sudamérica.	700213390
		Corea.	700254519

1.13.3 Suministro de energía de respaldo

Se recomienda el uso de una fuente de suministro continuo de energía (UPS) en todos los sistemas telefónicos. Incluso en lugares que rara vez se quedan si electricidad, es necesario desconectar la electridad ocasionalmente para realizar el mantenimiento de otros equipos. Asimismo, la mayor parte de las fuentes de suministro continuo de energía incluyen una unidad de acondicionamiento de energía eléctrica, que reduce los riesgos de sobretensiones y picos de voltaje transitorios.

La capacidad de los sistemas UPS y la carga total del equipo que el UPS soporte se miden por lo general en voltios-amperios (VA). Si la carga total del equipo se muestra en vatios (W), multiplique por 1.4 para obtener la carga en VA.

El cálculo de capacidad requerida por el UPS depende de varias elecciones.

- **¿Qué equipo colocará en el UPS?**
  No olvide incluir servidores tales como el servicio de correo de voz. Se recomienda que la carga total de una unidad UPS nueva no supere el 75% de su capacidad a fin de permitir la incorporación de nuevos equipos en el futuro.
- **¿Cuántos minutos de soporte UPS resultan necesarios?**
  El tiempo de ejecución de UPS es variable y depende del porcentaje de capacidad de la UPS que representa la carga total del equipo. Por ejemplo, un UPS con una capacidad de 1000 VA puede soportar una carga de 1000 VA (100%) por 5 minutos. Esta relación no es lineal, la misma UPS puede admitir una carga de 500VA (50%) por 16 minutos. Por consiguiente, mientras más bajo sea el porcentaje de capacidad máxima utilizado, más largo será el tiempo de ejecución de la UPS, por ejemplo, hasta 8 horas.
- **¿Con cuánta frecuencia se producen interrupciones de energía?**
  También debe incluir un espacio para el tiempo de recarga de la UPS. Para la mayoría de las UPS, la proporción entre la descarga y el tiempo de recarga completa es 1:10.
- **¿Cuántas tomas de salida tiene la unidad UPS?**
  Con múltiples unidades de UPS, es posible que sea necesario que cada pieza de equipo que se soporta tenga su propia toma de alimentación.

Valores de ejemplo

El factor dominante en el consumo de energía de un sistema IP Office son los teléfonos conectados a la unidad de control y los módulos de expansión externos. Esto no incluye teléfonos IP que requieren sus propias fuentes de alimentación aparte. Si se va a usar algún servidor en el sistema, también habrá que incluir en la evaluación los requisitos de dichos servidores. Igualmente, será necesario considerar compatibilidad para sistemas de módulo, como por ejemplo DECT.

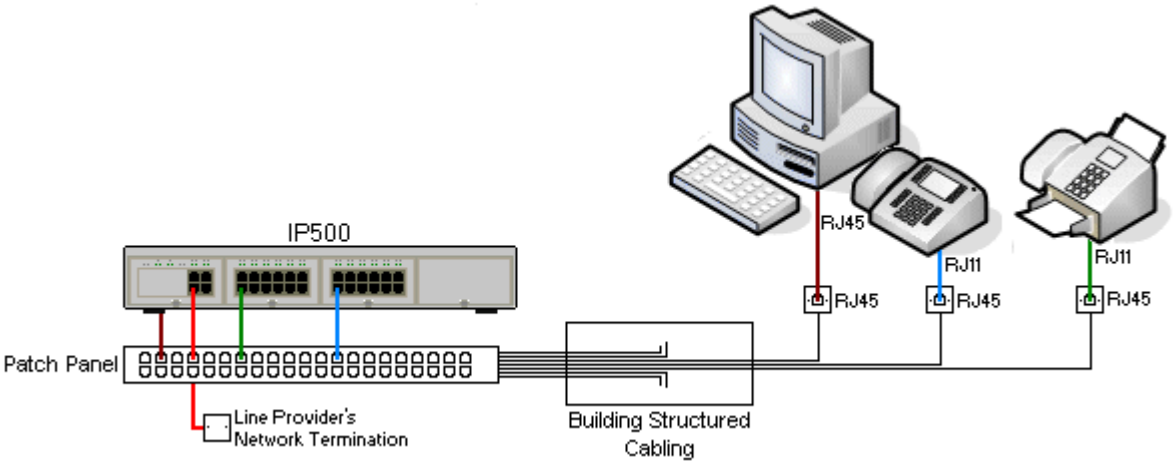
A continuación, presentamos las cifras correspondientes al peor de los casos probados usando unidades de control y módulos de expansión externos completamente llenos:

- **Unidad de control IP500 V2:** 115W.
- **Módulo de expansión externo de estación digital 16 IP500:** 31W.
- **Módulo de expansión externo de estación digital 30 IP500:** 56W.
- **Módulo de expansión externo de estación digital RJ21 IP500 DS16A:** 34W.
- **Módulo de expansión externo de estación digital RJ21 IP500 DS30A:** 60W.
- **Módulo de expansión externo de teléfono 16 IP500:** 25W.
- **Módulo de expansión externo de teléfono 30 IP500:** 45W.
- **Módulo de expansión externo de módulo de troncal analógica 16 IP500:** 8,8W.

1.13.4 Cableado y cables

Los sistemas IP Office están diseñados principales para ser utilizados con un sistema de cableado estructurado RJ45 que emplea cable de par trenzado sin blindar (UTP) tipo CAT3 y enchufes RJ45.

Un sistema de cableado estructurado es aquel donde los cables emergen de un panel central de conexiones RJ45 dentro de la sala de comunicaciones/datos hacia enchufes RJ45 individuales en la ubicación de los usuarios individuales. Todos los cables dentro de cada cable entre el panel de conexiones y el enchufe de escritorio están conectados directamente. Esta organización permite que los dispositivos conectados al panel de conexiones puedan intercambiarse para adecuarse al tipo de dispositivo que necesita estar conectado en el enchufe del usuario. Por ejemplo, un enchufe de usuario puede ser un puerto telefónico y otro enchufe un puerto LAN para computadora, sin que esto requiera que se vuelvan a tender los cables entre el panel de conexiones y la ubicación del usuario.



- **Instalaciones de cableado tradicional IDC con ponchadora**
  De ser necesario, la clavija RJ45 del extremo lejano de los cables IP Office puede ser descubierta y cableada para conectarse a sistemas de cableado tradicional que emplean conectores con ponchadora. Este tipo de instalación debe realizarla un técnico de cableado experimentado.
- **Conexiones troncales**
  La mayoría de los puertos de troncales de IP Office emplean conectores RJ45 para admitir cables con terminales tipo RJ45 a RJ45. Sin embargo, es posible que la conexión en el extremo del proveedor de la línea requiera del uso de una clavija de enchufe diferente, con el fin de adecuarse al equipo del proveedor de la línea.
- **Conectores telefónicos RJ11**
  Muchos teléfonos emplean enchufes RJ11 y traen incluidos cables con terminales tipo RJ11 a RJ11. Las clavijas de enchufe RJ11 pueden insertarse en los enchufes RJ45, y la conexión funcionará correctamente en muchos casos. Sin embargo, esta práctica no se recomienda ni es admisible, ya que la unión de conexión no es completamente positiva y puede desconectarse fácilmente. Para este tipo de conexiones, existe un cable con terminales tipo RJ45 a RJ11 286 disponible.

Cables de IP Office Standard

Los siguientes son los tipos de cables estándar de Avaya, disponibles para el uso en sistemas IP Office. La longitud máxima aplica también cuando el cable estándar de Avaya es reemplazado por un cable alternativo.

Cable	Descripción	Código SAP	Longitud estándar	Longitud máxima
Cable DTE de 9 terminales 293	Se conecta al puerto DTE de la unidad de control RS232. Con clavija de enchufe de 9 terminales tipo D a enchufe de 9 terminales tipo D	–	2m/6'6".	2m/6'6".
Cable de línea DS de cableado estructurado 286	Se conecta de los enchufes RJ45 a enchufes RJ11 y teléfonos DS y analógicos.	TT700047871	4m/13'2".	Consulte la tabla a continuación.
Cable de troncales BRI/PRI 284	Conecta los puertos de troncales BRI/PRI al punto de terminación de red del proveedor de línea. RJ45 a RJ45. Rojo.	700213440	3m/9'10".	–
Cable de interconexión para expansiones 288	Conecta la unidad de control a los módulos de expansión. RJ45 a RJ45. Azul. Puede reemplazarse por el cable de interconexión amarillo (2m - 700472871) incluido con la tarjeta IP500 4-Port Expansion 216, en casos donde se utilice esta tarjeta.	700213457	1m/3'3".	1m/3'3".
Cable LAN 289	Se conecta de los puertos LAN de IP Office a los dispositivos IP. RJ45 a RJ45. Gris.	700213481	3m/9'10".	100m/328'.

En la siguiente tabla se indican las distancias máximas totales de los cables para extensiones DS y analógicas utilizando cables de distintos espesores. Se debe usar cables de par trenzado no blindado Categoría 1 o superior.

Teléfono	Par trenzado no blindado (UTP) - 50 nf/km		
	AWG22 (0,65 mm)	AWG24 (0,5 mm)	AWG26 (0,4 mm)
Serie 1400	1.200m/3937'.	1.000m/3280'.	670m/2200'.
Serie 2400/5400	1.200m/3937'.	1.000m/3280'.	670m/2200'.
Serie 9500	1.200m/3937'.	1.000m/3280'.	670m/2200'.
Serie T3	1.000m/3280'.	1.000m/3280'.	400m/1310'.
BST	580m/1900'.	365 m/1200'.	228 m/750'
Teléfonos analógicos	1.000m/3280'.	1.000m/3280'.	400m/1640'.
Teléfonos ETR	305m/1000'.	305m/1000'.	122m/400'.

1.13.5 Puesta a tierra

Todas las unidades de control y módulos de expansión externos de IP Office deben estar conectados a una puesta a tierra funcional. Esto es cuando la unidad se conecta al suministro de energía con ayuda de un cable de energía con una terminal de tierra. El enchufe del suministro debe estar conectado a una puesta a tierra de protección.

El empleo de conexiones de tierra reduce la probabilidad de que ocurran problemas en la mayoría de los sistemas de telefonía y de datos. Esto es especialmente importante en edificios donde los múltiples componentes del equipo están conectados entre sí por largas longitudes de cable, por ejemplo, las redes de teléfonos y de datos.

En algunos casos, como en el caso de las troncales de arranque por tierra, además de fungir como medida de protección, la puesta a tierra es un requerimiento funcional para el equipo a operar. En otros casos, puede ser un requisito estipulado por los reglamentos locales o bien un paso de protección necesario, por ejemplo en áreas con alto riesgo de rayos.

- **PRECAUCIÓN**
  Durante la instalación, no suponga que los puntos de tierra están correctamente aterrizados. Pruebe los puntos de tierra antes de confiarles el equipo conectado a tierra.

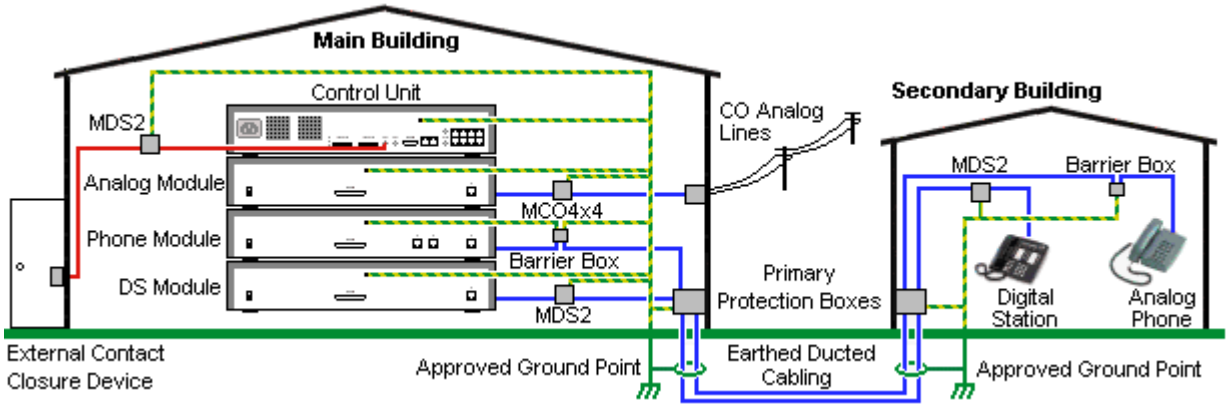
El punto de tierra en todas las unidades de control y módulos de expansión externos de IP Office está marcado con un símbolo o . Las conexiones de tierra hacia estos puntos deben realizarse con un cable sólido de 14 AWG con forro verde para una puesta a tierra funciona, o un forro verde y amarillo para la tierra de protección.

- **Equipo de protección adicional**
  Además de la puesta a tierra, es posible que sea necesario emplear equipo de protección en las siguientes situaciones. Consulte la sección Instalaciones telefónicas fuera del edificio 39.
  - En cualquier módulo de expansión externo Digital Station o Phones conectado a una extensión localizada en otro edificio.
  - En la República de Sudáfrica, en todos los módulos de expansión externos de troncales analógicas (ATM16) y en cualquier unidad de control que contenga tarjetas de troncales analógicas (ATM4/ATM4U).

1.13.6 Protección contra rayos/Conexiones fuera del edificio

Los siguientes son los únicos escenarios contemplados en los cuales las extensiones cableadas y dispositivos fuera del edificio principal pueden conectarse al sistema IP Office. En estos escenarios, debe equiparse asimismo protección adicional bajo la forma de puesta a tierra de protección y protectores contra picos.

- **PRECAUCIÓN**
  La instalación de protección adicional no elimina el riesgo de daños. Simplemente disminuye la probabilidad de que ocurran daños.



- Deben mantenerse separados los cables de distintos tipos, por ejemplos líneas de troncales, extensiones telefónicas, conexiones de tierra y energía.
- Todo el cableado entre edificios deben quedar encerrado dentro de ductos aterrizados. En forma ideal, estos ductos deben colocarse bajo tierra.
- Debe equiparse una caja de protección primaria en el punto donde los cables penetran al edificio. Esta protección debe ser de tipo de tres puntos (positivo, negativo y tierra). Típicamente, se trata de una protección de tubo de gas proporcionada por la compañía telefónica local. El cable de tierra debe ser lo suficientemente grueso para manejar todas las líneas afectadas por un choque indirecto al mismo tiempo.

Tipo de conexión	Tipo de dispositivo de protección	Requisito
Extensiones de teléfonos analógicos Módulo de expansión externos Phone (únicamente puertos POT 29 o TELÉFONO 29).	**Caja de protección IP Office** 190 Sólo admite una conexión. Máximo 16 con cualquier módulo de expansión.	• La conexión del módulo de expansión externo al teléfono debe ser por vía de un protector contra picos en cada extremo en el punto de protección principal de cada edificio. • Los módulos de expansión externos IP Office, la unidad de control y los dispositivos IROB deben estar conectados al punto de conexión de tierra de protección en su propio edificio. • La conexión entre edificios debe realizarse con ductos aterrizados, preferiblemente bajo tierra. El cable no debe estar expuesto al exterior en ningún punto.
Únicamente extensiones telefónicas DS Phone	**ITW Linx MDS2** 189 Es compatible con hasta 4 conexiones. Este dispositivo era llamado anteriormente Avaya 146E.	
Extensiones de teléfono BST	Ninguno	No admitida actualmente.
Troncales analógicas	**ITW Linx MCO4x4** 189 Admite hasta 4 líneas de dos hilos. Este dispositivo era llamado anteriormente Avaya 146C.	En las instalaciones en la República de Sudáfrica, es un requisito equipar las troncales analógicas con protección contra picos. En otras localidades donde se considera que el riesgo de rayos es alto, se recomienda adoptar protección adicional de las troncales analógicas entrantes.
Interruptor de salida externo	**ITW Linx MDS2** 189 Es compatible con hasta 4 conexiones. Este dispositivo era llamado anteriormente Avaya 146E.	Las conexiones de un puerto Ext O/P de IP Office hacia un dispositivo de relevadores externo debe hacerse mediante un protector contra picos. Cuando se utiliza el MDS2 en el puerto Ext O/P, utilice solo la Línea 1 y los conectores del Equipo 1. No utilice la Línea 2 ni los conectores del Equipo 2.

El rango de dispositivos towerMAX se encuentra en el sitio de ITWLinx (http://www.itwlinx.com).

1.14 Montaje de pared y en bastidor

Todas las unidades de control de IP Office están diseñadas para instalarse independientemente. En sistemas con módulos de expansión externos, la unidad de control y los módulos están diseñados para ser apilados.

Con ayuda de kits de montaje opcionales y adicionales, algunos sistemas pueden montarse en pared o en bastidor.

Unidad de control/expansión	Montaje en pared	Montaje en bastidor
Unidad de control IP500 V2	✓	✓
Módulos de expansión externos IP500	✓	✓

Montaje en pared

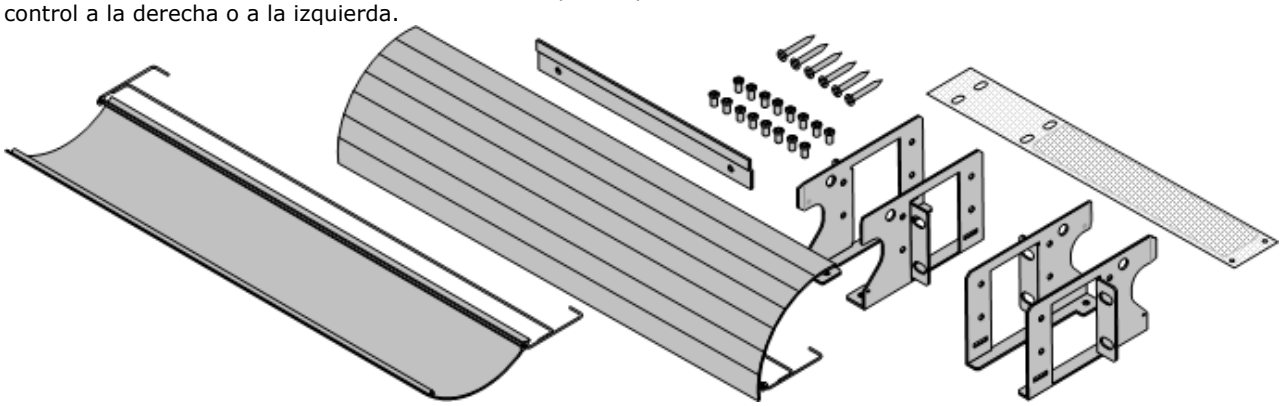
Las unidades de control IP500 V2 y los módulos de expansión externos IP500 pueden montarse en pared o bastidor. Para lograrlo, necesita un kit de montaje en pared, además de los aditamentos necesarios para fijarlos a la pared.

Además de los requerimientos ambientales 53 para el sistema IP Office, los siguientes requisitos adicionales aplican en la instalación en pared de una unidad:

- La superficie de la pared debe ser vertical, plana y estar libre de vibraciones. No se permite la fijación a paredes temporales.
- Debe utilizar únicamente los tornillos incluidos en el kit de montaje para fijar la unidad de control a los soportes.

El siguiente kit de montaje para pared y soporte está disponible actualmente:

- **IPO IP500 WALL MNTG KIT V3** *(Código SAP 700503160)*
  Este kit se puede usar para montaje en la pared y en bastidor de una unidad de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora el enrutamiento de los cables en la parte delantera y trasera de la unidad. En las unidades de control montadas en la pared, permite orientar las ranuras de la base de la unidad de control a la derecha o a la izquierda.

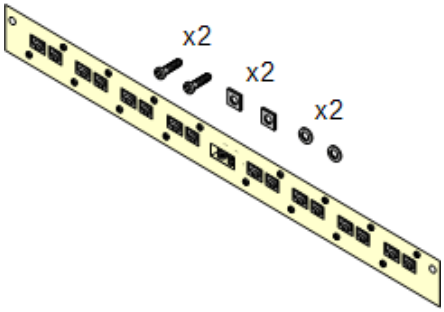


Montaje en bastidor

Todas las unidades de control de IP Office y módulos de expansión externos pueden montarse en bastidor en sistemas de bastidor estándar de 19". Cada unidad requiere un espacio de en la ranura dentro del bastidor. IPO IP500 RACK MNTG KIT V3 se usa para montar unidades en soporte.

En instalaciones donde los sistemas IP Office están montados en bastidor, deben tenerse en consideración el efecto de las condiciones dentro del gabinete del bastidor. Por ejemplo la temperatura dentro del bastidor puede ser superior a la temperatura de la sala, y el flujo de aire dentro del bastidor estará restringido. Los requerimientos ambientales 53 para las unidades IP Office individuales aplican igualmente dentro de un gabinete de bastidor.

Kit de montaje en bastidor con cajas de protección



- **Kit de montaje en bastidor con cajas de protección** *(SAP 700293905)*
  Deben utilizarse cajas de protección en las extensiones de teléfono analógicas fuera del edificio 39. Este soporte admite hasta ocho cajas de protección IP Office montadas en bastidor y simplifica el número de conexiones hacia el punto de tierra de protección en el bastidor. Debe utilizar este kit cuando se utilizan más de tres cajas de protección, y admite un máximo de 16 cajas de protección para un solo módulo de expansión externo.

1.15 Teléfonos IP Office

El IP Office versión 10.1 admite los siguientes teléfonos y complementos. La disponibilidad puede depender según la ubicación y puede ser objeto de restricciones locales.

Punto y anillo (Tip y ring) mejorados (puertos ETR)

Estos teléfonos solo son compatibles en una tarjeta ETR6 en un sistema IP500 V2. Solo son compatibles en sistemas IP Office Basic Edition - modo PARTNER® y IP Office Basic Edition que funcionan en una región de Norteamérica y compansión U-Law.

- **Serie ETR:** ETR6, ETR6D, ETR18, ETR18D, ETR34D *(Los teléfonos ETR 34D tiene un límite máximo de 2 por tarjeta y 4 en total)*
- **PARTNER DECT:** 3910, 3920

Teléfonos digitales Avaya DS (puertos DS)

Estas estaciones digitales se conectan a IP Office vía los puertos DS 286. Son compatibles en todos los modos IP Office.

- **Serie 1400:** 1403, 1408, 1416
- **Serie 9500:** 9504, 9508

Los siguientes teléfonos adicionales del puerto DS solo son compatibles en modo estándar de IP Office:

- **Serie 2400:** 2402, 2410, 2420.
- **Serie 3800:** Teléfono inalámbrico 3810 (solo son compatibles con los módulos de expansión externos).
- **Serie T3:** T3 Compact, T3 Classic, T3 Comfort.

Teléfonos digitales Avaya BST (puertos BST)

Estas estaciones digitales se conectan al sistema IP500 V2 IP Office mediante puertos BST.

- **Serie 4100:** 4135, 4136, 4145, 4145EX, 4146, 4146EX - Conexión a puertos BST de IP Office mediante un sistema Digital Mobility Solution.
- **Serie 7400:** 7420, 7430, 7434, 7439, 7440, 7444, 7449 - Conexión a puertos BST de IP Office mediante un sistema Digital Mobility Solution.
- **ACU:** Unidad de audioconferencia
- **Serie M:** M7100, M7100N, M7208, M7208N, M7310, M7310N, M7324, M7324N.
- **Serie T:** T7000, T7100, T7208, T7316, T7316E, T7406, T7406E

Teléfonos analógicos

Los teléfonos y dispositivos analógicos se conectan a los puertos TELÉFONO 291 en el sistema de IP Office. Sin embargo, debido a la gran variedad de teléfonos y dispositivos analógicos disponibles, no ofrecemos garantía de su funcionamiento. Es responsabilidad de la persona a cargo de instalar y dar mantenimiento al sistema IP Office para comprobar y verificar el funcionamiento del equipo analógico propuesto.

- **Serie 6200:** 6211, 6219, 6221 *(Norteamérica)*.
- **Serie B100:** B149, B159, B169.
- **Interquartz Gemini:** 9330-AV, 9335-AV, 9281-AV *(Europa, Medio Oriente, África, Asia-Pacífico)*.

Teléfonos IP:

Los teléfonos IP (SIP y H323) se conectan al sistema de IP Office mediante el puerto LAN o WAN RJ45. Estos dispositivos requieren una licencia para terminales IP Avaya y recursos de compresión de voz.

H323:

- **Serie 1600:** 1603IP/SW, 1608, 1608-I, 1616, 1616-I
- **Serie 3600:** 3616, 3620, 3626, 3641, 3645
- **Serie 3700:** 3701, 3711 - Conexión por medio de estaciones base DECT. 3720, 3725, 3730, 3735, 3740, 3745, 3749 - Conexión por medio de estaciones base DECT R4.
- **Serie 9600:** 9608, 9608G, 9611G, 9620L, 9620C, 9621G, 9630G, 9640, 9640G, 9641G, 9641GS, 9650, 9650C.
- **Serie T3 IP:** T3 IP Compact, T3 IP Classic, T3 IP Comfort.

SIP:

- **Serie 1000:** 1010, 1040
- **Serie 1100:** 1120E, 1140E
- **Serie 1200:** 1220, 1230
- **Serie B100:** B179.
- **Serie D100:** Estos auriculares DECT (hasta 8) usan una estación base que se conecta al sistema IP Office usando una línea troncal SIP y aparecen en el IP Office como extensiones.
- **E129:** Un teléfono SIP simple, el E129 admite respuesta automática, funcionamiento de auricular y manos libres.
- **E159, E169:** Teléfono SIP compatible con el acoplamiento de dispositivos móviles.
- **H175:** Teléfono SIP de video.
- **J129:** Teléfono SIP de escritorio simple. Compatible con IP Office versión 10.0 SP2.

1.16 VoIP

IP Office es un sistema de telefonía convergente que combina aspectos de los sistemas telefónicos PABX tradicionales y los sistemas de telefonía y datos IP. Esto opera en varios niveles.

- Los usuarios de los teléfonos individuales pueden controlar la operación de sus teléfonos mediante aplicaciones que se ejecutan en su PC.
- Puede enrutarse el tráfico de datos por la interfaz LAN hacia una interfaz de troncal de telefonía, por ejemplo a una conexión de marcación ISP.
- El tráfico de voz puede enrutarse por vínculos de datos internos y externos. Esta opción se conoce como voz sobre IP (VoIP).

El modo de operación VoIP puede incluir troncales SIP externas, troncales IP entre sistemas del cliente y/o teléfonos H.323 IP para los usuarios. En cualquier caso, deben considerarse los siguientes factores:

- La unidad de control IP Office debe estar equipada con canales de compresión de voz 43. Estos se utilizan cuando el dispositivo IP (troncal o extensión) necesita comunicarse con un dispositivo no IP (troncal o extensión), o bien con un dispositivo que emplea un códec distinto.
- Es obligatorio realizar una evaluación de red para todos los sistemas que emplean VoIP. Para la solución de problemas con VoIP, Avaya puede solicitar acceso a los resultados de la evaluación de red y puede rehusar proporcionar el soporte técnico si estos no están disponibles o no son satisfactorios.

Una evaluación de red incluye la determinación de la información siguiente:

- Una auditoría de red para verificar el equipo existente y evaluar sus capacidades, incluyendo su capacidad de cubrir las necesidades actuales y previstas para voz y datos.
- La determinación de los objetivos de red, incluyendo tipo de tráfico dominante, las opciones de tecnología, y los ajustes de objetivos de calidad de voz.
- La evaluación debe dejarle con la confianza que la red implementada tendrá la capacidad para el tráfico previsto de datos y voz, y que puede admitir H.323, DHCP, TFTP y amortiguadores de fluctuación en aplicaciones H.323.
- Un resumen de los objetivos esperados de la evaluación de red es:

Prueba	Objetivo de evaluación mínimo
Latencia	Menor a 150ms.
Pérdida de paquetes	Menor a 3%.
Duración	Monitoree las estadísticas una vez por minuto durante una semana entera.

1.16.1 Canales de compresión de voz

Las llamadas hacia y desde dispositivos IP pueden requerir la conversión al formato de códec de audio utilizado por el dispositivo IP. En los sistemas IP Office, esta conversión se realiza mediante canales de compresión de voz. Estos son compatibles con los códecs comunes de audio IP G.711, G.723 y G.729a. Para IP Office versión 8.0 y posteriores, las tarjetas combinadas VCM IP500 e IP500 también admiten G.722.

En unidades de control IP500 V2, pueden agregarse canales usando tarjetas VCM IP500 229 y tarjetas combinadas IP500 219.

Los canales de compresión de voz se usan de la siguiente manera.

Tipo de llamada	Uso de los canales de compresión de voz
Dispositivo IP a dispositivo no IP	Estas llamadas requieren de un canal de compresión de voz durante la duración de la llamada. Si no hay un canal disponible, la llamada recibe una indicación de ocupado.
Dispositivo IP a dispositivo IP	Los tonos de progreso de llamada (por ejemplo el tono de marcar, tono de marcar secundario, etc) no requieren canales de compresión de voz, con las siguientes excepciones: • La confirmación de código corto, campo ARS activado y tonos de entrada de código de cuenta requieren de un canal de compresión de voz. • Los dispositivos que utilizan G723 requieren de un canal de compresión de voz para todos los tonos excepto llamada en espera. Cuando se conecta una llamada: • Si los dispositivos IP utilizan el mismo códec de audio, no se utiliza el canal de compresión de voz. • Si los dispositivos utilizan distintos mismo códecs de audio, se requiere un canal de compresión de voz para cada uno.
Dispositivo no IP a dispositivo no IP	No se requieren canales de compresión de voz.
Música en espera	Proviene del bus TDM de IP Office y por tanto requiere un canal de compresión de voz cuando se reproduce en un dispositivo IP.
Recursos para conferencia y dispositivos IP	Los recursos de conferencia se administran desde el chip de conferencia, el cual se encuentra en el bus TDM de IP Office. Por tanto, se requiere un canal de compresión de voz para cada dispositivo IP incluidos en la conferencia. Esto incluye servicios que emplean recursos de conferencia como escucha, inctrusión de llamadas, grabación y monitoreo silencioso.
Llamadas de page a dispositivo IP	IP Office 4.0 y las versiones posteriores utilizan solamente G729a para las llamadas de page, por tanto sólo requieren un canal, pero también es compatible con pages compatibles con dispositivos G729a.
Dispositivos de servicios de correo de voz y dispositivos IP	Las llamadas a los servidores de correo de voz de IP Office son manejadas como llamadas de datos desde el bus TDM. Por tanto, todas las llamadas de un dispositivo IP a correo de voz requieren un canal decompresión de voz.
Llamadas de fax	Estas son llamadas de voz con un rango de frecuencia ligeramente más amplio que las llamadas de voz. IP Office soporta solamente las comunicaciones de fax por IP entre sistemas IP Office con la opción Transportar fax seleccionada. No es compatible actualimente con T38.
Llamadas de fax T38	IP Office 5.0 y versiones superiores es compatible con fax T38 en troncales SIP y extensiones SIP. Cada llamada de fax T38 emplea un canal VCM. En una pequeña red comunitaria, una llamada de fax T38 puede convertise en una llamada en líneas H323 SCN con ayuda del protocolo IP Office Fax Transport Support. Esta conversión emplea dos canales VCM. A fin de usar una conexión de fax T38, puede establecerse la **Clasificación de equipo** de una extensión analógica conectada a una máquina de fax puede definirse como ***Máquina de fax***. Además, está disponible una nueva función de código corto llamada **Marca fax**.

Nota: Los dispositivos T3 IP deben configurarse en el tamaño de paquete de 20 ms para que puedan aplicar las condiciones anteriores. Si se les deja configurados en tamaño de paquete de 10ms, será necesario un canal de compresión de voz para todos los tonos y llamadas por medios no directos.

Medición del uso de los canales

System Status Application puede usarse para visualizar el uso del canal de compresión de voz. En la sección **Recursos** aparece el número del canal en uso. También muestra la frecuencia con la que han ocurrido insuficientes canales disponibles, y la última vez que ocurrió este evento.

En las tarjetas VCM IP500, el uso del canal también es indicado por las luces LED (1 a 8) en la parte delantera de la tarjeta VCM IP500 229.

1.17 Localidades de país compatibles

Cuando una configuración del sistema nueva o predeterminada se abre por primera vez en IP Office Manager, el valor establecido en el campo **Región** siempre debe revisarse y cambiarse de ser necesario.

Los ajustes de localidad del sistema configuran factores como los patrones de timbrado predeterminados y los ajustes de visualización de llamada. La localidad también controla el lenguaje que el servidor de correo de voz utilizará para sus anuncios de manera predeterminada.

- Los países admitidos son: ***Argentina***, ***Australia***, ***Bahréin***, ***Bélgica***, ***Brasil***, ***Canadá***, ***Chile***, ***China***, ***Colombia***, ***República Checa***, ***Dinamarca***, ***Egipto***, ***Finlandia***, ***Francia***, ***Alemania***, ***Grecia***, ***Hong Kong***, ***Hungría***, ***Islandia***, ***India***, ***Irlanda***, ***Italia***, ***Japón***, ***Corea***, ***Kuwait***, ***Malasia***, ***Mediterráneo***, ***México***, ***Marruecos***, ***Países Bajos***, ***Nueva Zelanda***, ***Noruega***, ***Omán***, ***Pakistán***, ***Perú***, ***Filipinas***, ***Polonia***, ***Portugal***, ***Qatar***, ***Rusia***, ***Arabia Saudí***, ***Singapur***, ***Sudáfrica***, ***España***, ***Suecia***, ***Suiza***, ***Taiwán***, ***Turquía***, ***Emiratos Árabes Unidos***, ***Estados Unidos***, ***Venezuela***.

1.18 Aplicaciones de software IP Office

Las aplicaciones de IP Office vienen disponibles en varios discos DVD. Puede hacer el pedido de estos a un costo nominal que incluye el procesamiento y entrega. Los paquetes de instalación individuales para aplicaciones de IP Office también se pueden descargar 63 desde el sitio web de soporte técnico de Avaya en http://support.avaya.com.

Título	Discos	Descripción	Código SAP
Conjunto de DVD para administrador y usuario de la versión 10.1 de IP Office	2	Estos DVD contienen los paquetes de instalación de las principales aplicaciones de administración y para el usuario de IP Office. También contienen documentación para IP Office. • **DVD 1:** contiene la suite de aplicaciones de administración de IP Office, documentación de IP Office, aplicaciones de usuario de IP Office, IP Office Voicemail Pro. • **DVD 2:** Contiene la aplicación one-X Portal for IP Office.	700512892
Conjunto de DVD de TTS Voicemail Pro ScanSoft	2	Contiene motores de texto a voz para su uso con las funciones TTS de Voicemail Pro. Compatible con los mismos idiomas que los avisos pregrabados de Voicemail Pro, excepto el húngaro.	700478068
DVD de instalación de Server Edition para IP Office versión 10.1	2	DVD de instalación para servidores Server Edition e IP Office Application Server. El segundo DVD contiene material de código abierto que se usa para el primer DVD.	700511213
DVD para Virtualized IP Office Server Edition	1	DVD de instalación para servidores Virtualized Server Edition y Virtualized IP Office Application Server.	700511214
Conjunto de DVD de TTS para servidor Linux de IP Office	3	Contiene motores de texto a voz para usar con funciones TTS de Voicemail Pro basadas en Linux.	700502693

- Está permitido realizar copias de los DVD de Avaya IP Office DVD mencionados arriba. Sin embargo, es necesario conservar su contenido intacto, sin alteraciones, modificaciones ni adiciones. Avaya no admite responsabilidad alguna por daños o problemas que pudieran surgir del uso de dichas copias.

1.18.1 Aplicaciones de programación

Se utilizan las siguientes aplicaciones para programar y dar mantenimiento a un sistema de IP Office. Típicamente, funcionan en una PC conectada al sistema IP Office mediante la interfaz LAN. Estas aplicaciones se incluyen en el DVD de aplicaciones del administrador de IP Office y no requieren del ingreso de licencias.

Debido a la naturaleza de las aplicaciones, si se instala en una PC en el sitio del cliente, esto debe realizarse en una PC segura o en la PC de un usuario de confianza. Si se desea instalar también una PC de servidor de correo de voz con el sistema IP Office, puede usarse la misma PC para las aplicaciones de programación y de mantenimiento.

'En el caso de las aplicaciones de mantenimiento, éstas también pueden ejecutarse en forma remota si existe una ruta de conexión de datos hacia el sistema IP Office del cliente desde la ubicación de la persona que realizará el mantenimiento.

- ςερσι∫ν **IP Office Manager**
  Es importante que descargue e instale la versión actual de la suite de administración de IP Office, incluso IP Office Manager.
  - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincide con la versión de IP Office que requiere el sistema. Esto configura la versión del software IP Office cargado al momento de la recreación de la tarjeta SD del sistema 75.
  - Para el mantenimiento del sistema, la versión que se usa de IP Office Manager configura la versión de software de IP Office que se carga a un sistema cuando se actualiza el sistema 179.
  - Para la configuración del sistema, IP Office Manager es compatible con las versiones anteriores. IP Office Manager versión 10.1 es compatible con las versiones anteriores para configurar los sistemas que ejecutan software desde IP Office versión 6.0 en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión posterior del software
- **Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín Técnico de IP Office referente a la versión de software de IP Office que desea instalar. El boletín contiene información importante que puede haberse omitido en este manual. Puede encontrar los Boletines Técnicos de IP Office en el sitio Web de soporte técnico Avaya *(http://support.avaya.com)*.

Aplicaciones

- **IP Office Manager** 267
  Se utiliza esta herramienta para acceder a todas las partes de la configuración de IP Office. Pueden definirse distintos niveles de acceso para controlar cuáles partes de la configuración puede visualizar y modificar el usuario de IP Office Manager. También puede utilizar IP Office Manager para actualizar los archivos del software utilizado por el sistema IP Office.
- **IP Office Web Manager** 71
  Se puede acceder a la configuración para un sistema IP500 V2 a través de un navegador web mediante las mismas cuentas de usuario de servicio que se usan para IP Office Manager. Actualmente, para los sistemas de modo estándar de IP Office, IP Office Web Manager solo puede utilizarse para configurar usuarios, grupos y usuarios de servicio (cuentas de seguridad) y para realizar acciones de mantenimiento básicas. Por tanto, aún se requiere IP Office Manager para una instalación y un mantenimiento completo del sistema.
- **System Status Application** 272
  Puede usar esta aplicación para comprobar el estado actual de las líneas y extensiones de IP Office y para ver los registros de alarmas y eventos recientes. Funciona como una aplicación de Java.
- **MIB de SNMP** 197
  No son aplicaciones propiamente dichas. Puede utilizar los archivos MIB de SNMP de IP Office para el monitoreo por parte de aplicaciones SNMP de proveedores externos, como Castlerock y HP OpenView. Cuando se configura para la operación SNMP, el sistema IP Office puede enviar también alertas para problemas en potencia. Los sistemas IP Office también permiten enviar estas alertas a direcciones de correo electrónico para SMTP o Syslog.
  - Las alarmas que se pueden configurar para salir vía SNP pueden ser también enrutadas a correo electrónico SMTP y/o Syslog.
- **Monitor (SysMon)** 267
  Monitor es una herramienta que crea un trazo detallado de todas las actividades en el sistema IP Office. Como consecuencia, la interpretación de los datos de Monitor requiere de un gran conocimiento de protocolos de datos y telefonía. Sin embargo, todos los técnicos a cargo de la instalación y mantenimiento de IP Office deben saber cómo ejecutar Monitor cuando sea necesario, ya que Avaya puede solicitar copias de los trazos de Monitor para resolver problemas de soporte técnico.

1.18.2 Aplicaciones de usuario

IP Office admite varias aplicaciones que operan paralelamente con los teléfonos de usuarios. Estas aplicaciones son instaladas desde el DVD de aplicaciones de IP Office. El servidor one-X Portal for IP Office puede también instalarse como parte de una instalación del DVD de aplicaciones IP Office.

Algunas de ellas requieren ingresar licencias en la configuración de IP Office, con el fin de habilitar las funciones que ofrece y la cantidad permitida de usuarios simultáneos.

- **one-X Portal for IP Office** 267
  Esta aplicación se instala en la PC del servidor conectado al sistema IP Office. Los usuarios acceden al one-X Portal desde su PC con ayuda de un navegador Web. La aplicación permite a los usuarios controlar sus teléfonos, acceder a los mensajes de correo de voz, registros de llamadas y directorios telefónicos.
- **SoftConsole** 270
  Esta es una aplicación que requiere licencia. Se le ha diseñado para el uso de operadoras o recepcionistas del sistema telefónico. Muestra los detalles de llamadas dirigidas al usuario y le permite comprobar rápidamente el estado del destino requerido por la llamada, y transferir la misma. El usuario de SoftConsole tiene la capacidad de acceder a una serie de detalles sobre el estado de usuario y grupos dentro del sistema de IP Office. Se pueden ingresar licencias para hasta cuatro usuarios SoftConsole simultáneos.
- **Avaya Communicator** 269
  Esta es una aplicación de licencias que se ejecuta en diversos dispositivos Windows, iPad y Android. Dependiendo de la configuración, un usuario puede usarla en conjunto con su propio teléfono para controlar llamadas o bien como su teléfono.
- **TAPILink Lite** 273
  La interfaz de programas de aplicaciones de telefonía de Microsoft (TAPI) que permite las aplicaciones en cumplimiento con TAPI interactúen con el sistema IP Office mediante la instalación de un driver TAPI de IP Office. TAPILink Lite no requiere ingresar ninguna licencia en la configuración del sistema de IP Office. Permite realizar y responder llamadas con aplicaciones compatibles con TAPI (como Outlook). La parte de voz de las llamadas ocurre físicamente por el teléfono del usuario.

1.18.3 Aplicaciones de correo de voz

IP Office admite un amplio rango de aplicaciones para la grabación y reproducción de mensajes de correo de voz.

- **Embedded Voicemail**
  Embedded Voicemail admite la operación de buzón de correo de voz básico, operaciones sencillas de operadora automática y anuncios a grupos de búsqueda. En las unidades de control IP500 V2, Embedded Voicemail se incluye en la tarjeta SD Avaya instalada de manera predeterminada.
- **Voicemail Pro** 274
  Esta aplicación de correo de voz se instala en la PC del servidor conectado al sistema IP Office. Requiere ingresar varias licencias en la configuración de IP Office, con el fin de controlar las funciones que ofrece y la cantidad de conexiones simultáneas. Es posible personalizar el funcionamiento de Voicemail Pro para que proporcione servicios especiales.
- **ContactStore para IP Office** 265
  Voicemail Propuede usarse para grabaciones de llamadas manuales y automáticas. Estas grabaciones se colocan en los buzones de correo. Contact Store permite redirigir estas grabaciones hacia una base de datos en la PC ContactStore. Esto permite archivar las grabaciones y realizar búsquedas en las mismas en forma separada de los mensajes en el buzón de correo. Esta aplicación requiere que se ingrese una licencia en la configuración de IP Office.

1.18.4 Aplicaciones para registro de llamadas

Existe una amplia gama de aplicaciones de empresas externas que proporcionan servicios de registro de llamadas y contabilidad telefónica. Para admitir este tipo de sistemas, IP Office ofrece la salida SMDR.

- **Salida SMDR**
  En IP Office versión 5.0 y posteriores, la unidad de control IP Office produce salidas directas de registros SMDR hacia una dirección de IP específica. Esto se configura mediante IP Office Manager.

1.18.5 Aplicaciones para centros telefónicos

IP Office es compatible con una serie de soluciones del centro de contacto.

- **IP Office Contact Center**
  Esta aplicación es compatible con una variedad de módulos y permite enrutar llamadas a los agentes de acuerdo con una serie de factores.
- **Avaya Contact Center Select**
  Esta es una solución para centros de contacto grandes, con un máximo de 250 agentes.

1.18.6 Aplicaciones CTI

- **TAPILink Pro**
  Empleando el mismo software que TAPILink Lite, TAPILink Pro proporciona todas las funciones y operaciones de TAPILink Lite, pero además proporciona soporte para operaciones CTI de proveedores externos. Esto significa que un solo servidor puede controlar y monitorear cualquier cantidad de dispositivos telefónicos. Requiere el ingreso de una licencia CTI Link Pro. TAPILink Pro también proporciona la capacidad de monitorear y controlar grupos. Esto permite notificar a una aplicación cuando una llamada entra en cola de espera, así como redirigirla a otra ubicación.
- **Driver WAV TAPI**
  Proporciona soporte con base en software para el procesamiento de voz. La adquisición de la clave de licencia CTI Link Pro RFA también capacita cuatro puertos para procesamiento de voz, con la posibilidad de adquirir puertos adicionales en incrementos de 4 puertos. El driver TAPI-WAV sólo es compatible con TAPI 2.1; para TAPI 3.0, IP Office soporta la interfaz de Proveedor de Servicio de Medios (MSP), la cual Microsoft definió en TAPI 3.0.
- **DevLink Pro**
  Proporciona un torrente de eventos en tiempo real adicional a la interfaz SMDR proporcionada por IP Office SMDR (ver abajo). El torrente de eventos en tiempo real asume la forma de un registro de llamadas, emitido cada vez que el estado de cualquier de los extremos de la llamada tiene un cambio (típicamente cada llamada tiene dos puntos de terminación, pero en algunas circunstancias puede haber más, como en llamadas en conferencia o llamadas intrusas).

1.19 Capacitación

Avaya University ofrece un amplio rango de cursos de capacitación para IP Office y las aplicaciones relacionadas. Esto incluye los cursos necesarios para que los distribuidores de IP Office se conviertan en Asociados de Canal Autorizados de Avaya y para que técnicos individuales consigan la certificación en IP Office.

Puede encontrar la información relacionada con los cursos en el sitio Web de Avaya University (http://www.avaya-learning.com). Puede utilizar este sitio para comprobar la disponibilidad de los curso y reservar su lugar. También incluye cursos en línea y evaluaciones de curso en línea. Este sitio requiere que los usuarios creen un nombre y contraseña de usuario con el fin de mantener un registro de su capacitación personal.

1.20 Sitios Web

Puede encontrar información de apoyo para IP Office en varios sitios Web.

- **Avaya** *(http://www.avaya.com)*
  El sitio Web oficial de Avaya. La página principal proporciona acceso a sitios Web individuales de Avaya para los distintos países.
- **Avaya Enterprise Portal** *(http://partner.avaya.com)*
  Éste es el sitio Web oficial de todos los Socios de Negocios Avaya. Este sitio requiere del registro de un nombre y contraseña de usuario. Una vez que ha obtenido acceso, puede personalizar individualmente el portal del sitio para los productos y tipos de información que desea ver y sobre los que desea recibir notificaciones por correo electrónico.
- **Soporte técnico Avaya** *(http://support.avaya.com)*
  Contiene documentación y material de soporte adicional para los productos de Avaya, incluyendo IP Office. En el software, encontrará disponibles copias de las imágenes del CD IP Office, así como los archivos .bin actualizados del software nuclear.
- **Base de conocimientos Avaya IP Office** *(http://marketingtools.avaya.com/knowledgebase)*
  Acceso a una versión en línea periódicamente actualizada de la Base de conocimientos IP Office.
- **Avaya University** *(http://www.avaya-learning.com)*
  Este sitio proporciona acceso al amplio rango de cursos de capacitación de Avaya. Esto incluye cursos en línea, evaluaciones de curso y acceso a los detalles de los cursos en salón de clases. Este sitio requiere a los usuarios que se registren a fin de proporcionar al usuario los detalles de su registro de capacitación.
- **Avaya Community** *(http://www.aucommunity.com)*
  Éste es el foro oficial para los usuarios de productos Avaya. Sin embargo, no incluye un área separada para la discusión de problemas de IP Office.
- **Matriz de compatibilidad de productos Avaya** *(https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml)*
- **Documentación de matriz de puertos de productos Avaya** *(https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003)*
- **Otros sitios que no son propiedad de Avaya**
  Existen varios foros en la red externos para hablar sobre IP Office. Estos pueden representar una fuente útil de información sobre el uso de IP Office. Algunos de estos foros le requieren que se haga un miembro y se registre. Estos no son los foros oficiales de Avaya y Avaya no monitorea ni sanciona su contenido.
  - **Tek-Tips** *(http://www.tek-tips.com)*
  - **IP Office Info** *(http://www.ipofficeinfo.com)*
  - **Yahoo Groups** *(http://groups.yahoo.com/group/ipoffice)*
  - **PBX Tech** *(http://www.pbxtech.info/forumdisplay.php?f=8)*

1.21 Puertos de emergencia y para cortes de energía

Los sistemas IP Office pueden proporcionar dos tipos de puertos de extensiones analógicas para casos de corte de energía. En todos los casos, esto sólo funciona con troncales analógicas de arranque por bucle. Todos los teléfonos conectados a estos puertos deben estar correctamente marcados como extensiones para cortes de energía y de acuerdo con los requisito legales nacionales y locales.

Puertos conmutadores para cortes de energía

Durante la operación normal, estos puertos pueden utilizarse para realizar conexiones de teléfono analógico normales. Durante un corte de energía, los puertos se conectan directamente con un puerto de troncales analógicas.

Este tipo de puerto de corte de energía lo proporcionan las siguientes tarjetas:

- **Tarjeta Analog Phone 8 IP500**
  Cuando se instala una tarjeta Analog Phone 8 IP500 con una tarjeta auxiliar de troncales analógicas IP500, en casos de corte de energía el puerto 8 de extensión para cortes de energía se conecta al puerto de troncales analógicas 12.
- **Tarjeta combinada ATM IP500/Tarjeta combinada ATM IP500 V2**
  Con esta tarjeta, durante cortes de energía el puerto de extensión 8 se conecta al puerto 12 de troncales analógicas.

Puertos para cortes de energía únicamente para emergencias

No es posible utilizar estos puertos durante la operación normal. Durante un corte de energía, los puertos se conectan directamente con un puerto de troncales analógicas.

- **Tarjeta auxiliar de troncales analógicas IP500/Tarjeta auxiliar de troncales analógicas IP500 V2**
  Sin importar el tipo de tarjeta IP500 anfitriona, durante los cortes de energía los pins 4 y 5 del puerto 12 se conecta a los pins 7 y 8.
- **Tarjeta ETR6 IP500**
  En esta tarjeta, lo puertos de extensión 7 y 8 no se pueden utilizar durante la operación normal. Sin embargo, si está equipada una tarjeta auxiliar de troncales IP500, ambos puertos de extensión 7 y 8 se conectan al puerto de troncales analógicas 12 en caso de ocurrir un corte de energía.

Capítulo 2.

Información general de la instalación

2. Información general de la instalación

Este proceso de instalación tiene una estructura muy simple. Muchos pasos se pueden completar antes de la instalación real en la sede del cliente.

Resumen de proceso de instalación

1. **Preparar la instalación** 52
   a. **Requisitos del entorno** 53
      Controle que el área de la instalación cumpla con los requisitos de entorno del sistema.
   b. **Requisitos de espacio** 54
      Controle que el área de la instalación cumpla con los requisitos de espacio del sistema.
   c. **Herramientas y piezas requeridas** 58
      Compruebe que tenga las herramientas y piezas adicionales requeridas.
   d. **Documentación** 59
      Compruebe que ha obtenido y leído toda la documentación relevante.
   e. **Desembalaje** 59
      Verifique que el equipo requerido ha sido entregado y que no ha sufrido daños.
2. **Instalación del software de administración** 62
   Para la instalación del sistema necesita una PC con el software de administración de IP Office instalado. Debe incluirse una copia de IP Office Manager que coincida con el nivel requerido del software IP Office.
   a. **Descarga del software** 63
   b. **Instalación de las aplicaciones del administrador** 64
3. **Preparación de la tarjeta System SD** 74
   Actualice la tarjeta System SD a la versión requerida del software de IP Office. Además agregue todos los archivos disponibles como el archivo de licencia, la configuración preintegrada y el archivo de música en espera.
   - **ADVERTENCIA: Instalación de PCS14 y las unidades de control anteriores**
     PCS 310 Las unidades 14 o inferiores primero deben instalar la versión 8.1(65) (o posterior a 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1. Debe tomarse la precaución de comprobar que no se hagan llamadas antes de la actualización a la versión 10.0; de lo contrario, el sistema requerirá una licencia de actualización a 10.0 a pesar de que es "nuevo". El PCS de la unidad de control está impreso en la etiqueta que se encuentra en su parte posterior.
4. **Instale la tarjeta de la unidad de control** 80
   Conecte todas las tarjetas auxiliares de troncales a las tarjetas base IP500 e inserte las tarjetas base en la unidad de control.
5. **Instalación del sistema** 84
   a. **Montaje en pared** 85
      En caso de que la instalación sea en pared, asegure los soportes y sujete la unidad a la pared.
   b. **Montaje en bastidor** 87
      En caso de que la instalación sea en bastidor, asegure los soportes y sujete la unidad de control al bastidor.
   c. **Conexión de los módulos de expansión externos** 88
      Conecte los módulos de expansión externos a la unidad de control.
   d. **Conexión a tierra del sistema** 90
      Conecte los cables de tierra requeridos a la unidad de control y a los módulos de expansión externos.
   e. **Inicio del sistema** 91
      Inserte la tarjeta System SD y encienda el sistema.
   f. **Conexión de teléfonos** 95
      Conecte los teléfonos digitales Avaya.
6. **Configuración inicial** 98
   Comience la configuración básica del sistema mediante IP Office Manager.
7. **Protección del sistema** 126
   Cambie todas las contraseñas predeterminadas y deshabilite los servicios que no necesite.

2.1 Requerimientos ambientales

La ubicación planeada debe cumplir con los siguientes requisitos. Si se va a instalar el sistema en un bastidor, los siguientes son los requerimientos para el bastidor:

1. ☐ Temperatura: Funcionamiento de 5 °C a 40 °C (Almacenamiento de -40 °C a 70 °C).
2. ☐ Humedad relativa: Funcionamiento de 10% a 90% (Almacenamiento de 5% a 95%).
3. ☐ Compruebe que no haya materiales inflamables dentro del área.
4. ☐ Compruebe que no haya posibilidad de inundaciones.
5. ☐ Compruebe que no sea necesario mover primero otra maquinaria u equipo.
6. ☐ Verifique que la atmósfera no contenga polvo excesivo.
7. ☐ Verifique que se improbable que el área sufra cambios rápidos de temperatura y humedad.
8. ☐ Verifique la proximidad de fuertes campos magnéticos, fuentes de frecuencias de radio y otras interferencias eléctricas.
9. ☐ Compruebe la ausencia de químicos o gases corrosivos.
10. ☐ Compruebe que no existen vibraciones excesivas o potencialmente excesivas, especialmente sobre las superficies de montaje.
11. ☐ Compruebe que se hayan equipado los protectores y tierras de protección apropiadas en los teléfonos instalados en otros edificios (consulte la sección Instalaciones telefónicas fuera del edificio 39).
12. ☐ Compruebe que existe la iluminación adecuada para la instalación, programación del sistema y mantenimiento en el futuro.
13. ☐ Compruebe que existe suficiente espacio de trabajo para la instalación y el mantenimiento en el futuro.
14. ☐ Verifique que las actividades probables realizadas cerca del sistema no provocarán problemas, por ejemplo, el acceso y el mantenimiento de otros equipos en el área.
15. ☐ Las perforaciones de ventilación presentes en las unidades de IP Office no deben quedar cubiertas u obstruidas.
16. ☐ La superficie de instalación debe ser plana y horizontal, tanto para instalaciones independientes como montadas en bastidor.

Montaje en pared

Además de los requerimientos anteriores, las siguientes precauciones aplican a las unidad de IP Office que pueden instalarse con montaje en pared.

1. Las unidades deben montarse solamente sobre superficies de pared acabadas.
2. La superficie debe ser plana y vertical.
3. La orientación de la unidad debe ser como se muestra en la sección referente a Montaje en pared IP500 85.
4. Deben utilizarse los kits de montaje en pared de Avaya.

INSTRUCCIONES DE SEGURIDAD IMPORTANTES

Cuando utiliza el equipo telefónico, debe siempre seguir las precauciones básicas de seguridad para disminuir el riesgo de incendios, choques eléctricos y lesiones personales, incluyendo las siguientes:

1. Por ejemplo, no utilice es producto cerca de agua, cerca de una bañera, lavabo, tarja de cocina o tina de lavar, en sótanos húmedos o cerca de una piscina.
2. Evite utilizar los teléfonos (excepto por el tipo inalámbrico) durante tormentas eléctricas. Puede existir un riesgo remoto de recibir un choque eléctrico por un rayo.
3. No use el teléfono para reportar una fuga de gas en el área circundante a la misma.
4. Utilice solamente el cable de energía y las baterías indicadas en este manual.

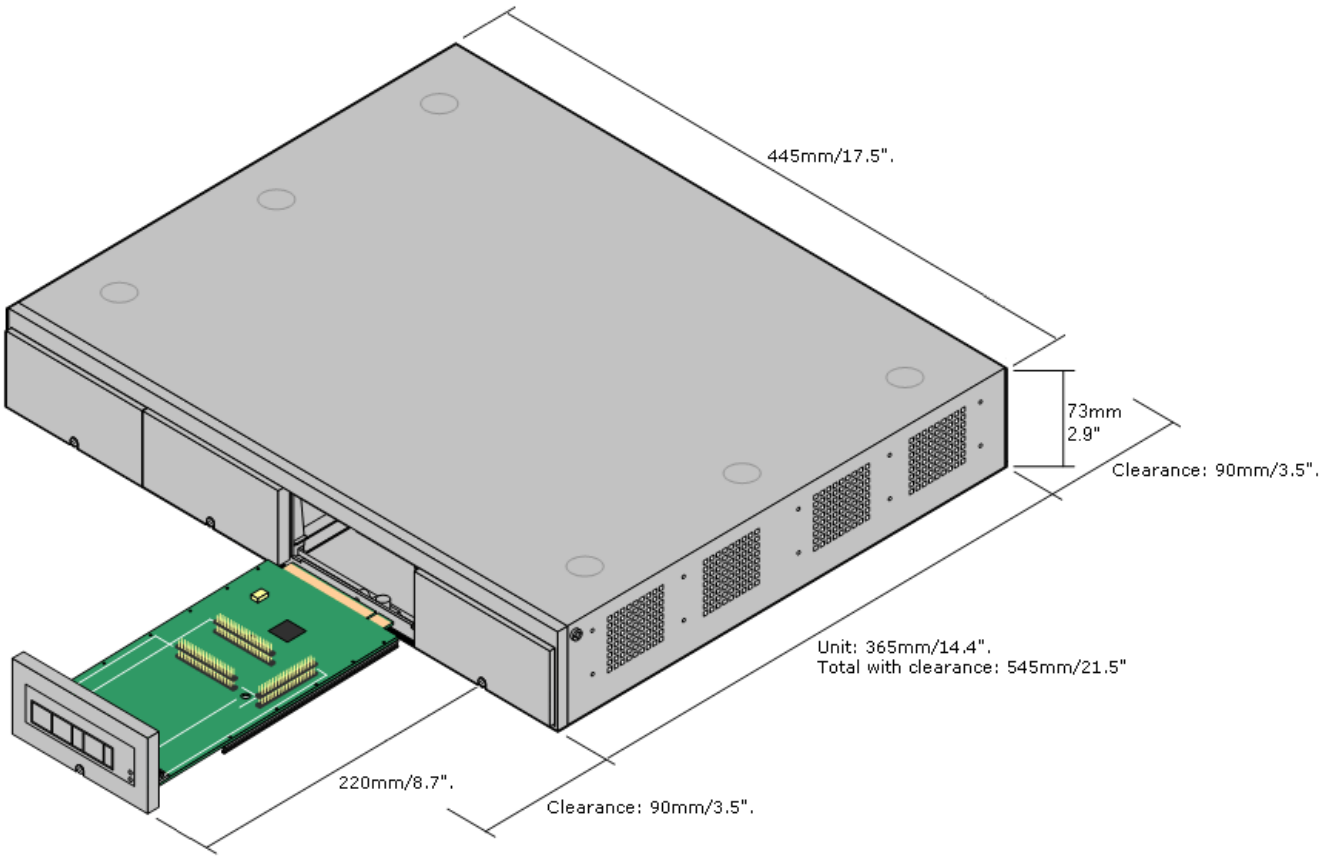
2.2 Requisitos de espacio

Las unidades de control y módulos IP Office están diseñados para instalarse ya sea en una torre independiente o en un sistema de bastidores de 19". La instalación en bastidor requiere de un kit de montaje en bastidor 40 por cada unidad de control y módulo de expansión.

- **Distancias de seguridad de los cables**
  Debe dejarse una distancia en las partes delantera y trasera de todos los módulos para acceder a los cables. En los sistemas IP500 V2, deje una distancia mínima de 90 mm (3,5 pies).
- **Distancia de seguridad adicional**
  Debe tenerse cuidado de asegurar que la colocación de los módulos no interrumpe el flujo de aire y otros factores que pueden afectar los requerimientos ambientales 53. Esto tiene especial importancia en las unidades de control IP500 V2, que tienen ranuras de ventilación laterales.
- **Acceso de cables**
  Los cables de energía no deben sujetarse a la superficie del edificio ni atravesar paredes, cielos rasos, pisos y otras aberturas similares. Deben tomarse medidas para la instalación a fin de evitar daños físicos al cable de suministro de energía, incluyendo el correcto enrutamiento del cable de suministro de energía y la disponibilidad de una conexión de corriente cerca del equipo fijo, o bien colocar éste cerca de una conexión de corriente.

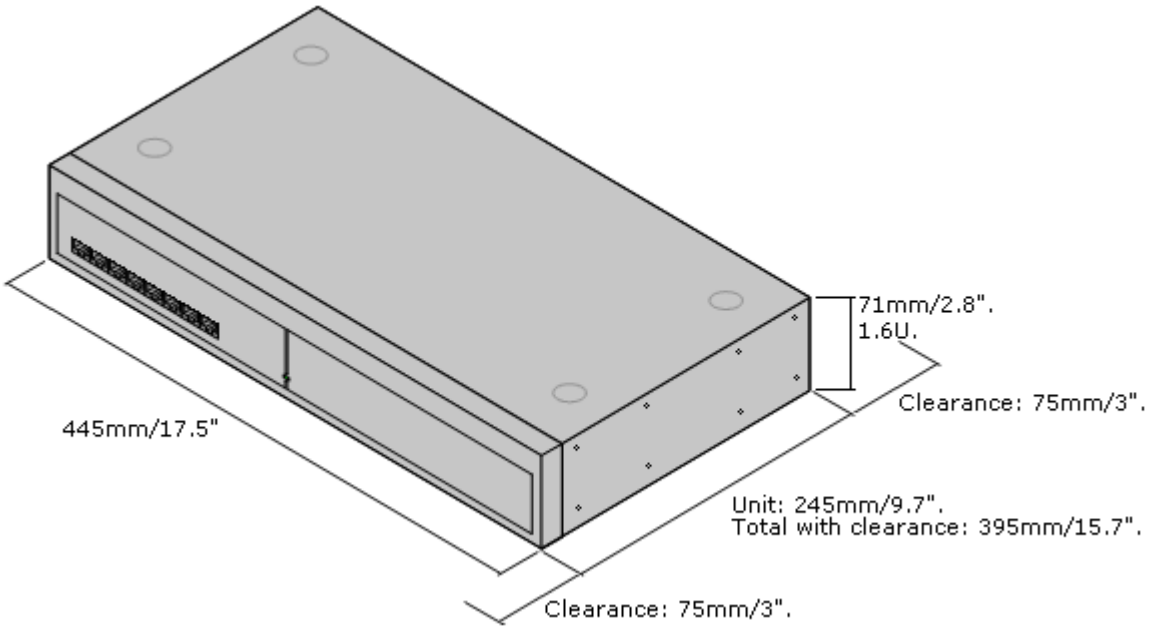
2.2.1 Unidad de control

Las ranuras para ventilación en la parte posterior y los costados de la unidad no deben quedar cubiertos ni obstruidos.



2.2.2 Módulos de expansión externos

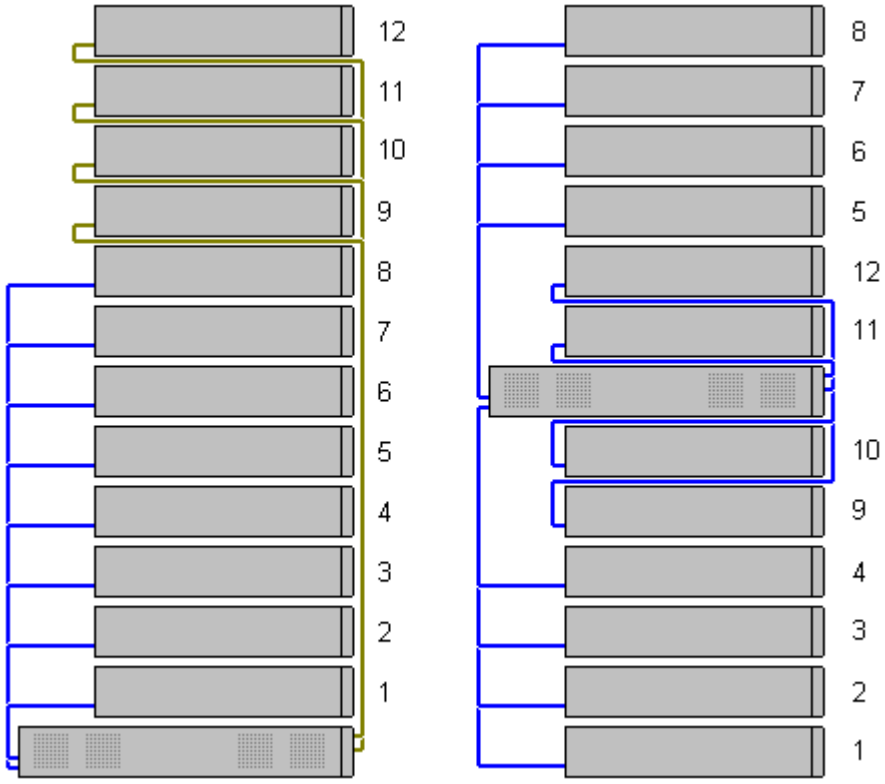
Las dimensiones siguientes aplican a todos los módulos de expansión externos de IP Office.



Para los sistemas autónomos, los módulos de expansión externos se pueden apilar sobre la unidad de control. Para ello y para los sistemas de montaje en bastidor, el siguiente diagrama muestra las opciones recomendadas para acomodar el largo del cable que conecta los módulos.

Los puertos de expansión integrados en una unidad de control se encuentran en la parte trasera de la unidad. Se puedan agregar cuatro puertos de expansión adicionales en la parte delantera de la unidad de control mediante la instalación de una tarjeta de expansión de cuatro puertos IP500.

- Cada módulo de expansión externo incluye un cable de interconexión para expansiones azul de 1 metro (3'3"). Este cable sedebe usar cuando se conecte a puertos de expansión en la parte trasera de una unidad de control.
- Al realizar la conexión con los puertos de expansión de una tarjeta IP500 4-Port Expansion card, puede utilizar el cable de interconexión para expansiones amarillo de dos metros (6'6") en vez del cable azul estándar. La tarjeta de expansión de 4 puertos IP500 contiene cuatro cables amarillos.



2.2.3 Montaje en pared

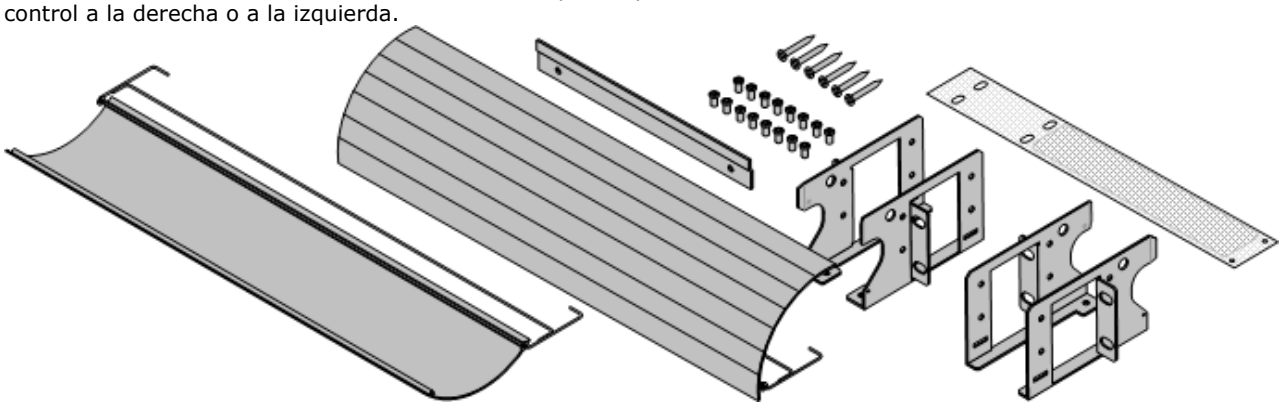
Las unidades de control IP500 V2 y los módulos de expansión externos IP500 pueden montarse en pared o bastidor. Para lograrlo, necesita un kit de montaje en pared, además de los aditamentos necesarios para fijarlos a la pared.

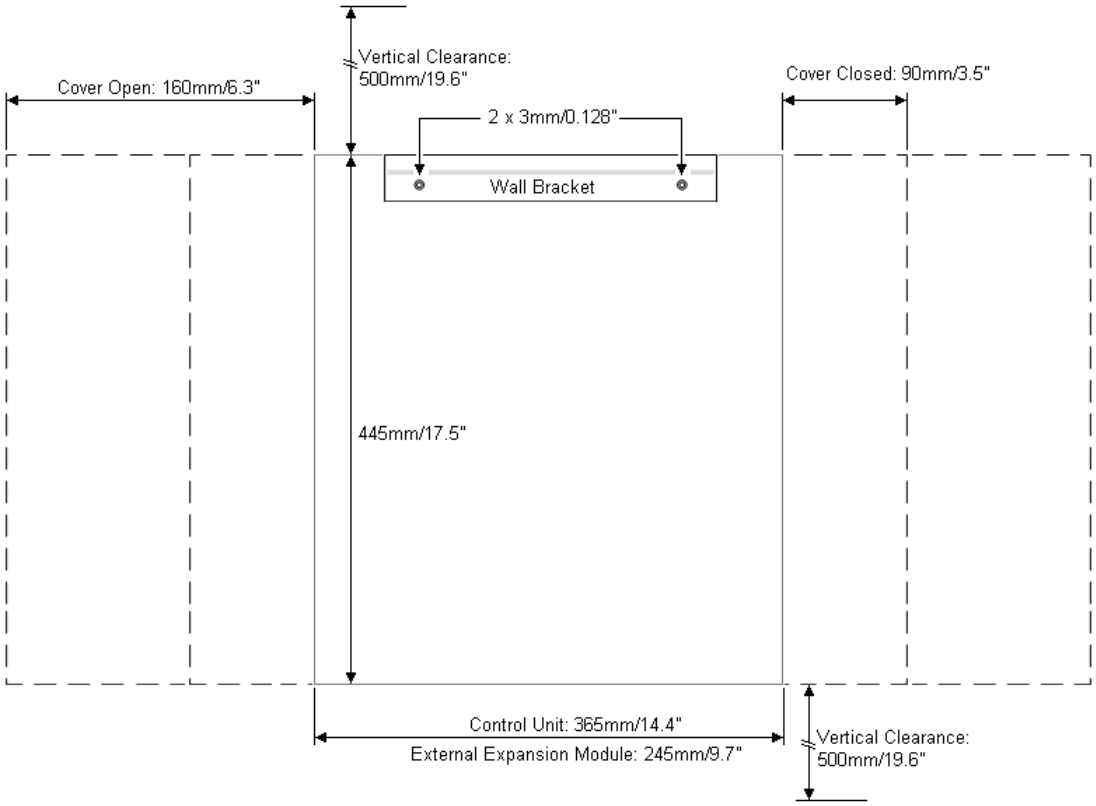
Además de los requerimientos ambientales 53 para el sistema IP Office, los siguientes requisitos adicionales aplican en la instalación en pared de una unidad:

- La superficie de la pared debe ser vertical, plana y estar libre de vibraciones. No se permite la fijación a paredes temporales.
- Debe utilizar únicamente los tornillos incluidos en el kit de montaje para fijar la unidad de control a los soportes.

El siguiente kit de montaje para pared y soporte está disponible actualmente:

- **IPO IP500 WALL MNTG KIT V3** *(Código SAP 700503160)*
  Este kit se puede usar para montaje en la pared y en bastidor de una unidad de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora el enrutamiento de los cables en la parte delantera y trasera de la unidad. En las unidades de control montadas en la pared, permite orientar las ranuras de la base de la unidad de control a la derecha o a la izquierda.



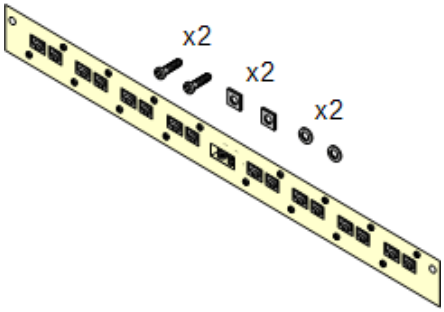


2.2.4 Requisitos de espacio para montaje en bastidor

Todas las unidades de control de IP Office y módulos de expansión externos pueden montarse en bastidor en sistemas de bastidor estándar de 19". Cada unidad requiere un espacio de en la ranura dentro del bastidor. IPO IP500 RACK MNTG KIT V3 se usa para montar unidades en soporte.

En instalaciones donde los sistemas IP Office están montados en bastidor, deben tenerse en consideración el efecto de las condiciones dentro del gabinete del bastidor. Por ejemplo la temperatura dentro del bastidor puede ser superior a la temperatura de la sala, y el flujo de aire dentro del bastidor estará restringido. Los requerimientos ambientales 53 para las unidades IP Office individuales aplican igualmente dentro de un gabinete de bastidor.

Kit de montaje en bastidor con cajas de protección

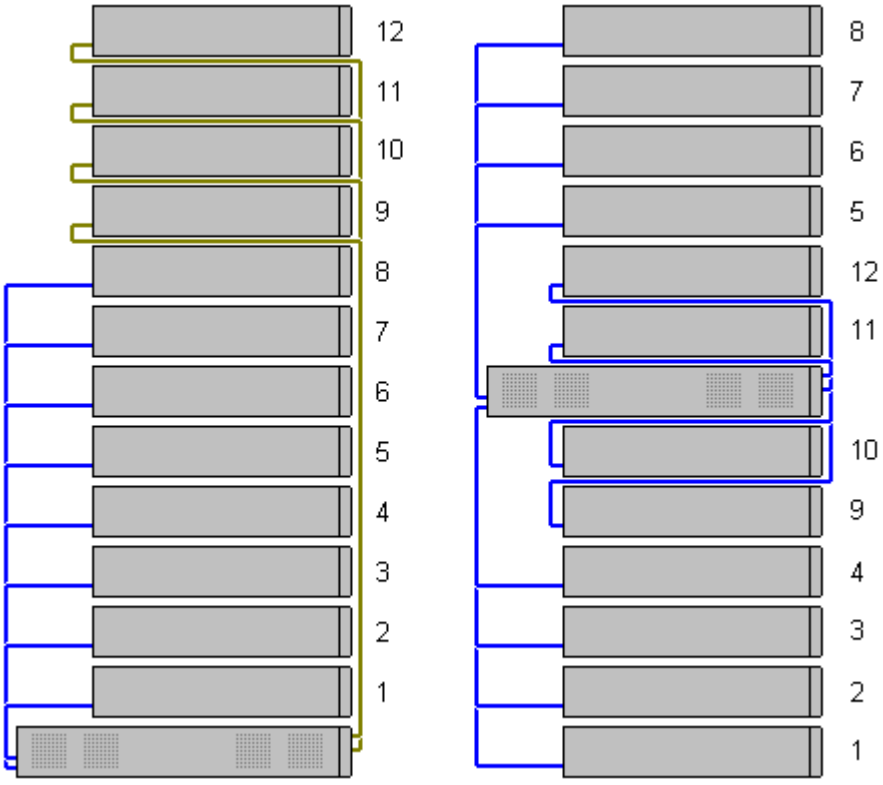


- **Kit de montaje en bastidor con cajas de protección** *(SAP 700293905)*
  Deben utilizarse cajas de protección en las extensiones de teléfono analógicas fuera del edificio 39. Este soporte admite hasta ocho cajas de protección IP Office montadas en bastidor y simplifica el número de conexiones hacia el punto de tierra de protección en el bastidor. Debe utilizar este kit cuando se utilizan más de tres cajas de protección, y admite un máximo de 16 cajas de protección para un solo módulo de expansión externo.

Posicionamiento de módulos en bastidor

Los puertos de expansión integrados en una unidad de control se encuentran en la parte trasera de la unidad. Se puedan agregar cuatro puertos de expansión adicionales en la parte delantera de la unidad de control mediante la instalación de una tarjeta de expansión de cuatro puertos IP500.

- Cada módulo de expansión externo incluye un cable de interconexión para expansiones azul de 1 metro (3'3"). Este cable sedebe usar cuando se conecte a puertos de expansión en la parte trasera de una unidad de control.
- Al realizar la conexión con los puertos de expansión de una tarjeta IP500 4-Port Expansion card, puede utilizar el cable de interconexión para expansiones amarillo de dos metros (6'6") en vez del cable azul estándar. La tarjeta de expansión de 4 puertos IP500 contiene cuatro cables amarillos.



2.3 Herramientas y piezas requeridas

El siguiente es un resumen general de las herramientas requeridas. Se requerirán herramientas y equipos adicionales para el montaje en pared y en bastidor, y para adaptar las conexiones del cable de tierra a los requerimientos locales.

Piezas de IP Office

Las piezas indispensables requeridas son:

- ☐ Unidad de control IP500 V2 209
- ☐ Tarjeta SD Avaya 212
- ☐ Archivo de licencia PLDS 294
  - La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.
- ☐ El archivo debe ser apropiado para la versión del software cuya licencia se otorga.
- ☐ El archivo debe contener una licencia **Essential Edition** apropiada para la versión IP Office que se desea.

Herramientas requeridas

- ☐ Destornillador de hoja plana de 5 mm
- ☐ Destornillador de cruz.
- ☐ Correa anti-estática para a muñeca y punto de tierra.
- ☐ Cable LAN Ethernet RJ45-RJ45.
- ☐ Destornillador de cruz M4.
- ☐ Herramientas adecuadas para sujetar la horquilla del cable.
- ☐ Si se va a montar en la pared, brocas y herramientas para la instalación de los aditamentos de pared.

Administración del sistema

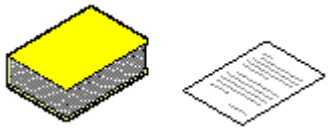
- ☐ PC Windows con:
  - ☐ Suite IP Office Admin instalada 64.
  - ☐ Puerto RJ45 Ethernet LAN.
  - ☐ Lector de tarjeta SD.

Piezas adicionales requeridas

Además del equipo IP Office que puede comprar a pedido, necesitará los siguientes artículos.

- ☐ Cable de cobre sólido de 14AWG para la conexión a tierra de unidades de control y módulos de expansión.
- ☐ Forro de cable en cumplimiento con los requerimientos locales para el cableado de tierra. Éste es por lo general verde para la tierra funcional y verde/amarillo para la puesta a tierra de protección.
- ☐ Si se va a montar en pared, los aditamentos e implementos adicionales para el tipo de pared y el kit de montaje utilizado.
- ☐ Amarres de cables y etiquetas para organizar e identificar los cables.

2.4 Documentación



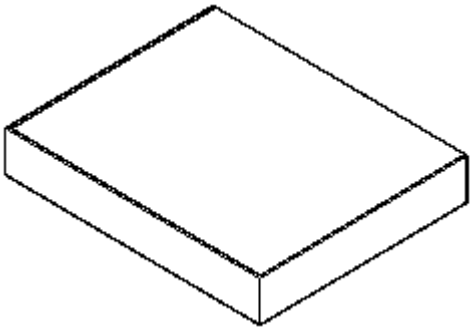
Asegúrese de leer este manual completo antes de comenzar la instalación. Incluya también la documentación de instalación de todos los demás equipos y aplicaciones que se van a instalar como parte del sistema IP Office.

La documentación de IP Office está disponible en los siguientes sitios Web.

- **Soporte técnico Avaya** *(http://support.avaya.com)*
  Contiene documentación y material de soporte adicional para los productos de Avaya, incluyendo IP Office. En el software, encontrará disponibles copias de las imágenes del CD IP Office, así como los archivos .bin actualizados del software nuclear.
- **Base de conocimientos Avaya IP Office** *(http://marketingtools.avaya.com/knowledgebase)*
  Acceso a una versión en línea periódicamente actualizada de la Base de conocimientos IP Office.

- **Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín Técnico de IP Office referente a la versión de software de IP Office que desea instalar. El boletín contiene información importante que puede haberse omitido en este manual. Puede encontrar los Boletines Técnicos de IP Office en el sitio Web de soporte técnico Avaya *(http://support.avaya.com)*.

2.5 Desembalaje



Utilice el siguiente procedimiento para desempacar los equipos proporcionadas por Avaya o por un vendedor o distribuidor de Avaya.

Información requerida

- ☐ **Lista de verificación del equipo**.
  Una lista de verificación de la instalación con las piezas y equipos ordenados para la instalación.

Procedimiento

1. ☐ **Compruebe en busca de daños de traslado**
   Antes de desempacar el equipo, compruebe en busca de señales de daños que pudieran haber ocurrido durante el tránsito. Si existe algún daño, hágalo del conocimiento del mensajero.
2. ☐ **Compruebe que le han entregado las piezas correctas**
   Verifique todas las cajas contra la factura de envío y asegúrese que ha recibido los artículos correctos. Informe sobre cualquier error u omisión al proveedor del equipo.
3. ☐ **Conserve todos los empaques y la documentación**
   Mientras desembala el equipo, conserve todo el material de empaque. Sólo se aceptan devoluciones de equipos defectuosos si están embalados en su embalaje original. Si realiza una instalación por etapas, el embalaje original también será de ayuda para volver a empacar el equipo para trasladarlo al sitio de instalación final.
4. ☐ **Asegúrese de observar las medidas de protección contra descargas de estática**
   Asegúrese de seguir las medidas de protección contra descargas estáticas en todo momento mientras maneja equipos con tableros de circuitos eléctricos expuestos.
5. ☐ **Verifique todas las partes**
   Realice una inspección visual de cada artículo y compruebe que incluya toda la documentación y artículos accesorios necesarios. Informe sobre cualquier error u omisión al proveedor del equipo.
6. ☐ **Compruebe toda la documentación**
   Asegúrese de leer y conservar toda la documentación incluida con el equipo.

Capítulo 3.

Instalación del software de administración

3. Instalación del software de administración

Para instalar y mantener un sistema IP Office, el usuario debe estar familiarizado con el uso de las siguientes aplicaciones.

- **IP Office Manager**
  Esta es una aplicación basada en Windows. IP Office Manager se usa para acceder todo de la configuración de IP Office. Pueden definirse distintos niveles de acceso para controlar cuáles partes de la configuración puede visualizar y modificar el usuario. También puede utilizar IP Office Manager para actualizar los archivos del software utilizado por el sistema IP Office.

  - çερσι ∫ν **IP Office Manager**
    Es importante que descargue e instale la versión actual de la suite de administración de IP Office, incluso IP Office Manager.

    - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincide con la versión de IP Office que requiere el sistema. Esto configura la versión del software IP Office cargado al momento de la recreación de la tarjeta SD del sistema 75.
    - Para el mantenimiento del sistema, la versión que se usa de IP Office Manager configura la versión de software de IP Office que se carga a un sistema cuando se actualiza el sistema 179.
    - Para la configuración del sistema, IP Office Manager es compatible con las versiones anteriores. IP Office Manager versión 10.1 es compatible con las versiones anteriores para configurar los sistemas que ejecutan software desde IP Office versión 6.0 en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión posterior del software

- **IP Office Web Manager**
  Luego de la instalación, se puede acceder a la configuración para un sistema IP500 V2 a través de un navegador web mediante las mismas cuentas de usuario de servicio que se usan para IP Office Manager.
- **System Status Application**
  System Status Application (SSA) es una herramienta de notificaciones que proporciona un amplio rango de información sobre el estado actual de un sistema IP Office. Reporta sobre los recursos disponibles y los componentes en el sistema, así como detalles de las llamada en progreso. Se muestran los detalles de las alarmas actuales y las alarmas anteriores. Cuando es necesario para la escalación de diagnóstico, la aplicación SSA tiene la capacidad de tomar una imagen instantánea del estado del sistema IP Office, incluyendo una copia de la configuración actual.
- **Monitor (System Monitor)**
  System Monitor es una herramienta que puede mostrar la actividad del sistema IP Office con muchos detalles. Como consecuencia, la interpretación de los datos requiere de un gran conocimiento de protocolos de datos y telefonía. Sin embargo, todos los técnicos a cargo de la instalación y el mantenimiento de IP Office deben saber cómo ejecutar Monitor para obtener datos ya que Avaya puede solicitar los datos de Monitor para resolver problemas de soporte técnico.

3.1 Descarga del software

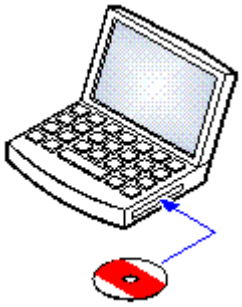
La suite de software de administración de IP Office está disponible en unDVD que está a la venta 45. Sin embargo, también se puede descargar el software desde la página web del soporte técnico de Avaya (http://support.avaya.com).

- ςερσι ∫ν **IP Office Manager**
  Es importante que descargue e instale la versión actual de la suite de administración de IP Office, incluso IP Office Manager.
  - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincide con la versión de IP Office que requiere el sistema. Esto configura la versión del software IP Office cargado al momento de la recreación de la tarjeta SD del sistema 75.
  - Para el mantenimiento del sistema, la versión que se usa de IP Office Manager configura la versión de software de IP Office que se carga a un sistema cuando se actualiza el sistema 179.
  - Para la configuración del sistema, IP Office Manager es compatible con las versiones anteriores. IP Office Manager versión 10.1 es compatible con las versiones anteriores para configurar los sistemas que ejecutan software desde IP Office versión 6.0 en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión posterior del software
- **Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín Técnico de IP Office referente a la versión de software de IP Office que desea instalar. El boletín contiene información importante que puede haberse omitido en este manual. Puede encontrar los Boletines Técnicos de IP Office en el sitio Web de soporte técnico Avaya *(http://support.avaya.com)*.

Para descargar el software de Avaya:

1. Vaya a ***http://support.avaya.com*** e inicie sesión.
2. Seleccione **Soporte por producto** y haga clic en **Descargas**.
3. Introduzca ***IP Office*** en el cuadro **Introducir el nombre del producto** y seleccione la opción correcta del menú desplegable.
4. Use el menú desplegable **Elegir versión** para seleccionar la versión de IP Office requerida.
5. Haga clic en **Descargas**. La página muestra las descargas disponibles más recientes.
6. Haga clic en **Ver descargas** para ver la lista completa de descargas.
7. Seleccione el paquete de software que desea descargar.
8. La página que se muestra en una nueva pestaña o ventana detalla las opciones de descarga de ese software. Para la instalación de IP500, descargue el paquete de administración completo, no los archivos binarios separados ni los paquetes de descarga de Admin lite.
9. También descargue los documentos detallados bajo el título **DOCUMENTOS RELACIONADOS**, si se muestran.

3.2 Instalación de las aplicaciones de administración



La suite IP Office Administration consiste de varias aplicaciones para la instalación y mantenimiento de IP Office.

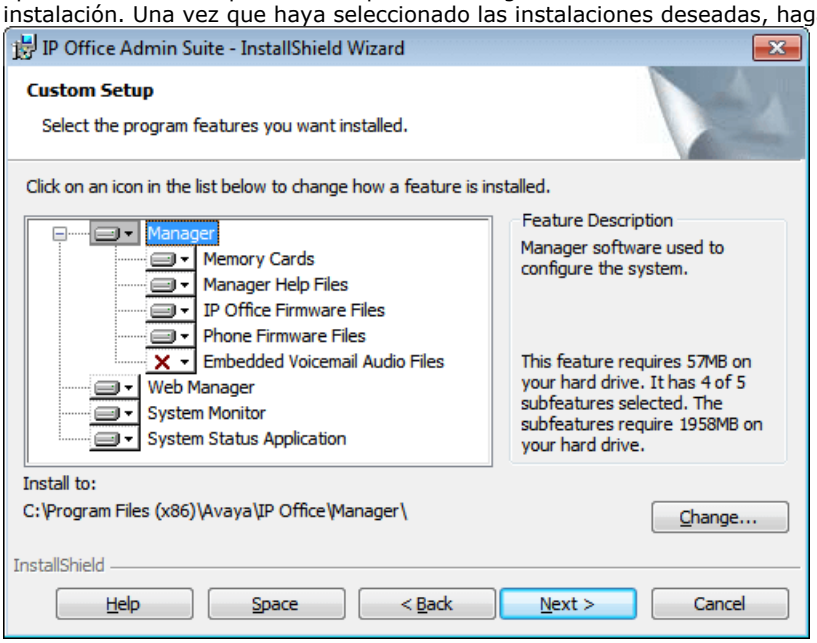
- ☐ **System Monitor** - *Instalar* ✓
- ☐ **IP Office Manager** - *Instalar* ✓
- ☐ **System Status Application** - *Instalar* ✓
- ☐ **Call Status** - *Opcional*
  Este software no es compatible con los sistemas con IP Office versión 7.0 ni sistemas posteriores. Se proporciona la información solamente para el mantenimiento de sistemas anteriores.

Requisitos

- ☐ **Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892)**
  En forma alternativa, puede descargar la suite de IP Office Administrator Applications del sitio de soporte de Avaya *(http://support.avaya.com)*.
- ☐ **Requerimientos de PC con Windows**
  Las siguientes especificaciones son los requerimientos mínimos para IP Office Manager. En caso de que se deseen instalar otras aplicaciones en la PC, es necesario cumplir con los requerimientos individuales. Las versiones de Windows que son compatibles están detalladas en la sección Sistemas operativos 278.
  - **Manager estándar:** CPU con Core i3, 4 GB de RAM, sistema operativo 32/64 bits
  - **Manager Server Edition:** CPU con Core i5, 6 GB de RAM, sistema operativo de 32/64 bits
  - **Select Manager Server Edition:** CPU con Core i5, 8 GB de RAM, sistema operativo de 64 bits
  - IP Office Manager solo se admite en Windows con una configuración de tamaño de fuente de 100%.

Para instalar las aplicaciones de administrador de IP Office:

1. Con ayuda de la opción **Agregar o eliminar programas** en el panel de control de Windows, compruebe que la PC no tenga ya instalada una versión de la suite IP Office Admin.
   - Si la respuesta es "sí" y la suite es de una versión anterior a IP Office versión 3.2, elimine la suite IP Office Admin existente mediante la opción Agregar/eliminar programas.
   - Si la suite existente es versión IP Office 3.2 o posteriores, es posible actualizarla sin necesidad de eliminar la instalación previa.
2. Inserte el DVD de IP Office Administrator Applications. Seleccione la opción para la suite de administración de IP Office. Aparecerá una ventana de la carpeta con los archivos de instalación para la suite administrativa.
3. Haga clic con el botón secundario en setup.exe y seleccione **Ejecutar como administrador**.
4. Seleccione el idioma en que se llevará a cabo el proceso de instalación, Esto no afecta el idioma utilizado por IP Office Manager cuando se ejecuta. Haga clic en **Siguiente >**.
5. Haga clic en **Siguiente>**.
6. Si está de acuerdo, haga clic sobre **Acepto los términos del contrato de licencia** y luego haga clic en **Siguiente >**.
7. De ser necesario, cambie el destino donde desea instalar las aplicaciones. Le recomendamos que acepte el destino predeterminado. Haga clic en **Siguiente >**.
8. La siguiente pantalla se emplea para seleccionar las aplicaciones que desea instalar. Al hacer clic en cada una, aparecerá una descripción de la aplicación. Haga clic en ▼ al lado de cada aplicación para modificar la selección de instalación. Una vez que haya seleccionado las instalaciones deseadas, haga clic en **Siguiente >**.

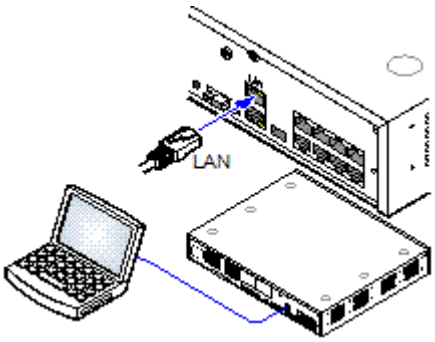


- **Manager**
  Instalar la aplicación IP Office Manager básica que se requiere para editar las configuraciones del sistema y cualquiera de las siguientes:
  - **Tarjetas de memoria**
    Instale los archivos necesarios para recrear una tarjeta System SD Avaya.
  - **Archivos de ayuda de Manager**
    Instale los archivos de ayuda de la aplicación en todos los idiomas disponibles. A menos que seleccione otros, se instala solo en inglés.
  - **Archivos del firmware de IP Office**
    Instale los archivos del firmware que usan los módulos de expansión externos de IP Office. Estos archivos se necesitan solo si IP Office Manager se utiliza para la actualización de sistemas.
  - **Archivos del firmware de teléfono**
    Instale los archivos del firmware que utilizan los diferentes teléfonos IP de Avaya que son compatibles con IP Office. Estos archivos se necesitan solo si IP Office Manager se utiliza para la actualización de sistemas.
  - **Archivos de audio del correo de voz integrado**
    Instale los avisos del correo de voz que usa el correo de voz integrado. Estos archivos se necesitan solo si IP Office Manager se utiliza para la actualización de sistemas.

- **Web Manager**
  Instale una copia de los archivos que deben cargarse en un sistema para que éste ejecute IP Office Web Manager.
- **System Monitor**
  Instale la aplicación System Monitor.
- **System Status Application**
  Instale la aplicación System Status Application.

9. Verifique que haya seleccionado como mínimo las aplicaciones **System Monitor** y **Manager**. Haga clic en **Siguiente >**.
10. Haga clic en **Instalar**. Si la instalación requiere otros componentes, como componentes Windows .Net2, siga las indicaciones para instalar esos componentes.
11. Si se le solicita, reinicie la PC.
12. Haga clic en **Finalizar**.

3.3 Conexión de la PC de instalación



Para la instalación, se recomienda que la unidad de control IP Office se inicie sin estar conectada a una red. Esto asegura que IP Office tome como predeterminado un conjunto de ajustes conocidos de dirección IP.

Si IP Office se inicia con conexión a una red con un servidor DHCP, la computadora de programación deberá estar conectada a la misma red ya sea como cliente DHCP o con una dirección IP válida para esa red.

Esta sección contempla la conexión de la PC de instalación directamente a la unidad de control de IP Office.

Requisitos

- ☐ **PC de administración IP Office**
  Una PC de Windows con la suite de aplicaciones de IP Office Administrator instalada 64.
- ☐ **Cable LAN**

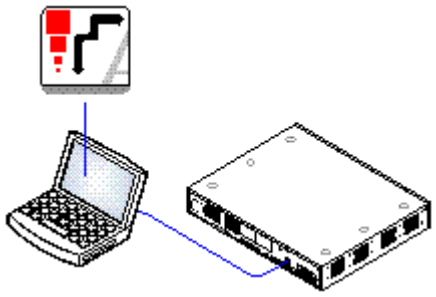
Para conectarse directamente a un sistema IP Office predeterminado:

1. La dirección predeterminada del puerto LAN de la unidad de control IP Office es 192.168.42.1/255.255.255.0. Para conectar directamente una PC, modifique las propiedades TCP/IP del puerto LAN de la PC como sigue:

Dirección IP fija	192.168.42.203
Máscara de subred	255.255.255.0
Gateway predeterminado	192.168.42.1.

   - Aunque puede configurarse la PC para actuar como un cliente DHCP, esto no se recomienda para realizar funciones más avanzadas, como las actualizaciones de firmware.
2. Conecte el cable LAN del puerto LAN de la PC al puerto LAN en la unidad de control de IP Office.
3. Compruebre que esté encendida la luz LED anaranjada en el puerto LAN de IP Office. Puede que la luz LED verde también esté parpadeando, ya que esto indica que existe tráfico en la conexión LAN.
4. Para probar la conexión antes de ejecutar IP Office Manager o System Status Application:
   - Seleccione **Inicio | Ejecutar** e ingrese ***cmd***.
   - En la ventana de comando que aparece, ingrese ping **192.168.42.1**. Los resultados deben mostrar una lista de las respuestas de ping del IP Office. Esto confirma que existe una comunicación básica entre la PC IP Office Manager e IP Office.
   - De no haber respuestas de ping, ingrese **ipconfig**. Los resultados deben mostrar la configuración de direcciones IP de la PC IP Office Manager, como se realizó anteriormente. En este caso, ingrese **exit** y compruebe la conexión del cable.
5. Ahora puede iniciar IP Office Manager 68, System Status 69 o System Monitor 70.

3.4 Inicio de IP Office Manager



IP Office Manager se usa para acceder a todas las partes de la configuración de IP Office. También puede utilizar IP Office Manager para actualizar los archivos del software utilizado por el sistema IP Office.

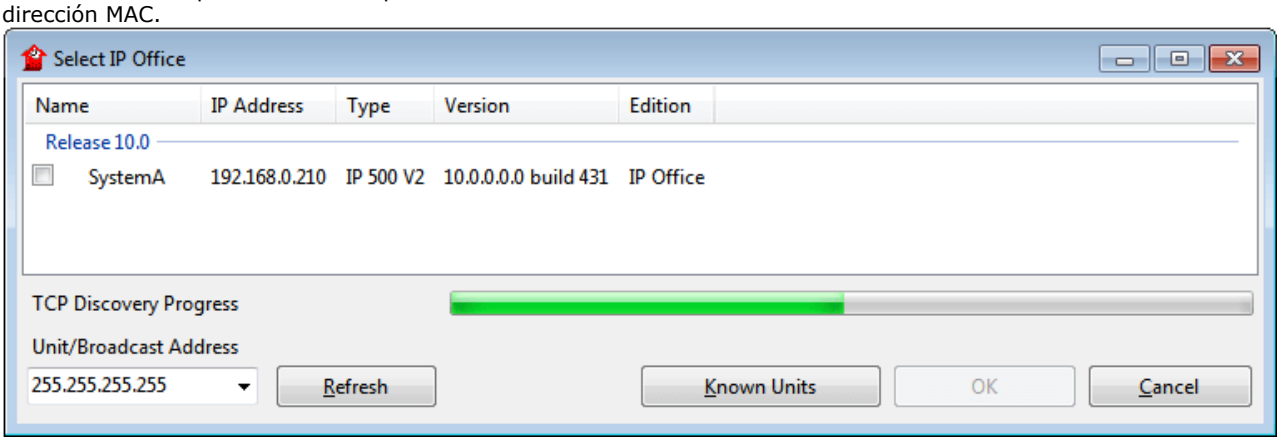
- ςερσι ∫ν **IP Office Manager**
  Es importante que descargue e instale la versión actual de la suite de administración de IP Office, incluso IP Office Manager.
  - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincide con la versión de IP Office que requiere el sistema. Esto configura la versión del software IP Office cargado al momento de la recreación de la tarjeta SD del sistema 75.
  - Para el mantenimiento del sistema, la versión que se usa de IP Office Manager configura la versión de software de IP Office que se carga a un sistema cuando se actualiza el sistema 179.
  - Para la configuración del sistema, IP Office Manager es compatible con las versiones anteriores. IP Office Manager versión 10.1 es compatible con las versiones anteriores para configurar los sistemas que ejecutan software desde IP Office versión 6.0 en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión posterior del software

Requisitos

- ☐ **PC de administración IP Office**
  Una PC de Windows con la suite de aplicaciones de IP Office Administrator instalada 64.
- ☐ **Cable LAN**

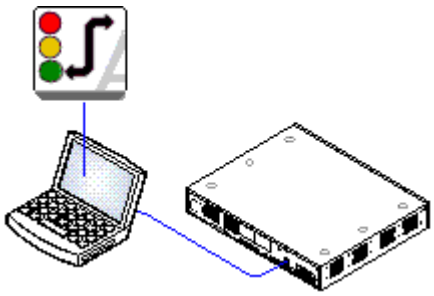
Para iniciar sesión en un sistema mediante IP Office Manager:

1. Seleccione **Inicio | Todos los programas | IP Office | Manager**.
2. Si la PC tiene instalado un software de firewall, puede recibir una notificación preguntando si desea permitir a este programa acceso a la red. Seleccione **Sí** o **Aceptar**.
3. Seleccione **Archivo | Abrir configuración** en la barra de menús.
4. Aparece la ventana **Seleccionar IP Office**. Después de algunos segundos, debe aparecer la unidad de control IP Office. El nombre predeterminado que se utiliza en una unidad de control IP Office recientemente instalada es su dirección MAC.



   - En caso que no se pueda encontrar el sistema requerido, puede modificar la dirección utilizada para la búsqueda. Ingrese o seleccione la dirección deseada en el campo **Dirección de la unidad/difusión** y luego haga clic en **Actualizar** para realizar una nueva búsqueda.
5. Haga clic en la casilla de verificación al lado del sistema y luego clic en **Aceptar**.
6. Aparecerá un cuadro con la solicitud de nombre y contraseña. El nombre y la contraseña deben coincidir con uno de los que se establecieron a través de las configuraciones de seguridad del sistema.

3.5 Iniciando System Status Application

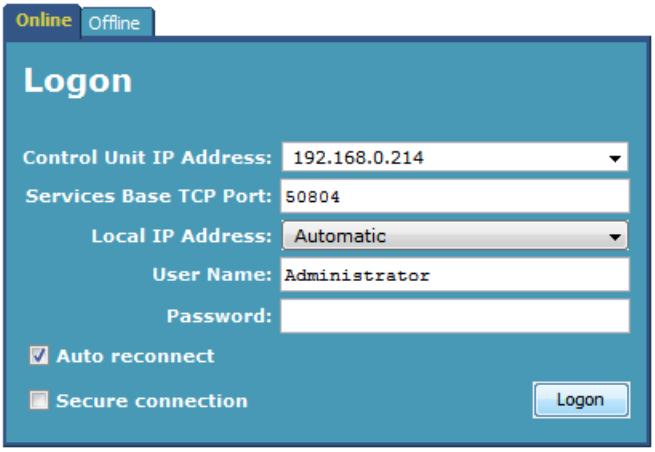


System Status Application (SSA) es una herramienta de notificaciones que proporciona un amplio rango de información sobre el estado actual de un sistema IP Office. Puede reportar sobre los recursos disponibles y los componentes en el sistema, así como detalles de las llamada en progreso. Registra los detalles de la cantidad de alarmas y la fecha y hora de las alarmas más recientes.

Cuando es necesario para la escalamiento de diagnóstico, la aplicación SSA tiene la capacidad de tomar una imagen instantánea del estado del sistema IP Office, incluyendo una copia de la configuración actual. El uso de la aplicación SSA requiere de un nombre y contraseña de usuario IP Office configurado para tener acceso a System Status en los ajustes de seguridad de IP Office.

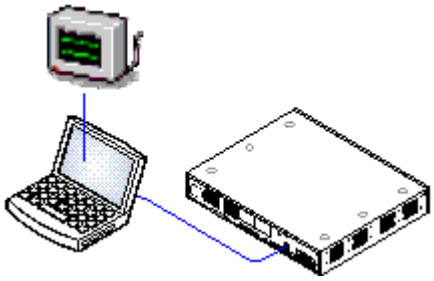
Para iniciar el estado del sistema:

1. Hay varios métodos que se pueden usar para iniciar System Status Application.
   - En una PC donde se ha instalado System Status 64, seleccione **Inicio | Programas | IP Office | System Status**.
   - Si IP Office Manager también está instalado en la PC y en ejecución, seleccione**Archivo | Avanzadas | System Status**.
   - En las unidades de control IP500 V2, inicie un navegador web e ingrese la dirección IP de la unidad de control. Seleccione el vínculo para **System Status**.
   - Si IP Office Web Manager ya está en ejecución, seleccione **Supervisión** y haga clic en **System Status**.
2. Una vez iniciado System Status, la aplicación solicitará los detalles del sistema IP Office al cual desea conectarse.



   - **Dirección IP de la unidad de control**
     Ingrese la dirección IP de la interfaz LAN de la unidad de control IP Office o utilice la lista desplegable para seleccionar una dirección utilizada anteriormente.
   - **Puerto TCP Services Base**
     Este debe coincidir con la configuración del puerto TCP Services Base en el sistema IP Office, configurado en los ajustes de seguridad del sistema. El valor predeterminado es 50804.
   - **Dirección IP local**
     Si la PC tiene asignada más de una dirección IP en su tarjeta de red o tarjetas múltiples de red, puede seleccionar la dirección que desea utilizar si es necesario.
   - **Nombre/contraseña de usuario**
     Ingrese un nombre y contraseña de usuario proporcionados para el uso de System Status. De manera predeterminada, este es el mismo nombre de usuario y contraseña usados con IP Office Manager. Este debe ser el nombre de un usuario de servicio IP Office configurado para tener acceso a System Status en los ajustes de seguridad de IP Office.
   - **Reconexión automática**
     Si selecciona esta opción, System Status intentará reconectarse con la misma configuración en caso de perder la conexión con IP Office.
   - **Conexión segura**
     Utiliza una conexión TLS cifrada al sistema. Si se selecciona y el sistema no está configurado para acceso seguro, System Status Application ofrece volver a intentar la conexión con acceso no seguro en lugar de ello.
3. Ingrese los detalles requeridos para IP Office y haga clic en**Iniciar sesión**.

3.6 Iniciando System Monitor



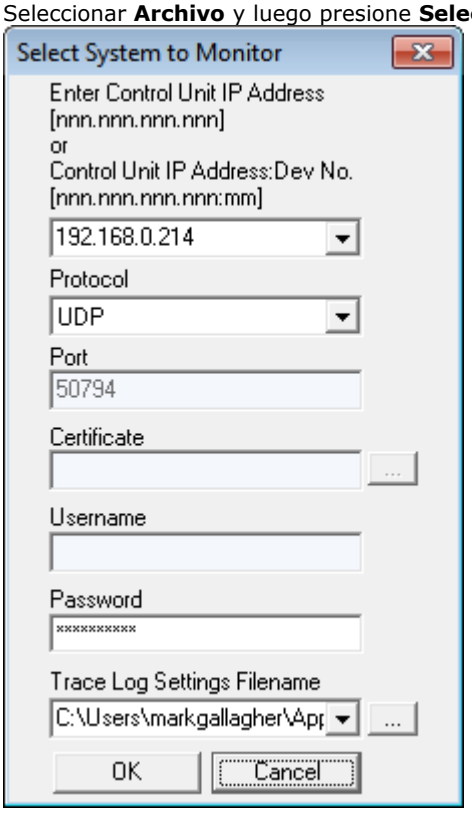
System Monitor es una herramienta que puede mostrar toda la actividad en el sistema IP Office en gran detalle. Como consecuencia, la interpretación de los datos de Monitor requiere de un gran conocimiento de protocolos de datos y telefonía. Sin embargo, todos los técnicos a cargo de la instalación y mantenimiento de IP Office deben saber cómo ejecutar Monitor cuando sea necesario, ya que Avaya puede solicitar copias de los trazos de Monitor para resolver problemas de soporte técnico.

Requisitos

- ☐ **PC de administración IP Office**
  Una PC de Windows con la suite de aplicaciones de IP Office Administrator instalada 64.
- ☐ **Cable LAN**

1. Para iniciar System Monitor

1. Seleccione **Inicio | Programas | IP Office | System Monitor**.
2. Seleccionar **Archivo** y luego presione **Select Unit (Seleccionar unidad)**.



3. Introduzca la **Dirección IP** y **Contraseña** del sistema que desea monitorear.
   - **Protocolo**
     El **Protocolo** predeterminado es ***UDP***. La aplicación también admite conexiones TCP, HTTP y HTTPS. Para obtener todos los detalles, consulte el manual "Uso de IP Office System Monitor".
   - **¿Cuál contraseña?**
     Mediante IP Office Manager, es posible configurar una **Contraseña de Monitor**. Si el sistema no tiene una **Contraseña de Monitor** configurada, System Monitor usa la **Contraseña del sistema**. Las columnas **Contraseña de Monitor** y **Contraseña del sistema** se configuran dentro de los ajustes de configuración de seguridad de un sistema.
4. Si desea que System Monitor se inicie con un conjunto de opciones de seguimiento guardadas anteriormente, use el botón del navegador **Trace Log Settings Filename (Nombre de archivo de configuración de registro de seguimiento)** para seleccionar el archivo de configuración de registro de seguimiento.
5. Haga clic en **Aceptar**.

3.7 Inicio de IP Office Web Manager

El acceso del navegador web al sistema se puede usar para actualizar IP Office Web Manager. Introduzca la dirección IP del sistema y luego seleccione el enlace **IP Office Web Manager**. Para obtener más información, consulte el Manual de IP Office Web Manager.

Para utilizar IP Office Web Manager se necesita que los archivos de la aplicación estén presentes en la tarjeta SD del sistema. Esto se realiza seleccionando la opción para incluir los archivos de Web Manager al momento de la recreación de la tarjeta SD del sistema 75.

Avaya es compatible con los siguientes navegadores para IP Office Web Manager:

- **Microsoft Internet Explorer 10** y **11**.
- **Microsoft Edge**
- **Mozilla Firefox**
- **Google Chrome**
- **Safari**

Para iniciar sesión en un sistema mediante IP Office Web Manager

1. Introduzca la dirección IP del sistema IP Office. En el menú que aparece, haga clic en **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
2. Aparece el menú para iniciar sesión en IP Office Web Manager.

3. Introduzca el nombre y la contraseña para la administración del sistema. Tanto el nombre como la contraseña predeterminados son ***Administrator***.

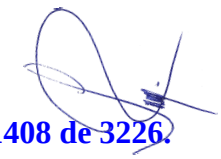
   - **Modo desconectado**
     Algunos cambios de configuración solo se pueden aplicar al sistema mediante un reinicio, por ejemplo, cambiar las configuraciones de línea. Para cambiar esas características necesita seleccionar el **Modo desconectado**. En ese modo, la parte superior de la ventana del navegador muestra un vínculo **Guardar en IP Office** que, cuando le hace clic, despliega un menú para reiniciar el sistema.

     - También puede cambiar a Modo desconectado después de iniciar sesión haciendo clic en y seleccionando **Modo desconectado**.

4. Haga clic en **Iniciar sesión**.

   a. Se le solicita que cambie todas las contraseñas predeterminadas.

   b. Para un sistema nuevo, aparece el menú de configuración inicial 101.



Capítulo 4.

Preparación de la tarjeta SD de sistema

4. Preparación de la tarjeta SD de sistema

Las nuevas unidades de control IP500 V2 no tienen instalado ningún firmware ni configuración. Al encenderla por primera vez, la unidad de control carga e instala el firmware necesario desde la tarjeta **SD del sistema** 212 Avaya instalada en la unidad de control. Luego crea una configuración predeterminada basada en las tarjetas físicas ya instaladas en la unidad de control y los módulos de expansión externos conectados a esta.

Puede realizar una cantidad de operaciones adicionales antes de instalar la tarjeta SD del sistema a fin de preconfigurar el sistema. Estas operaciones pueden acelerar en gran medida la instalación física en la sede del cliente ya que pueden hacerse por anticipado.

- **Actualización del firmware de tarjeta** 75
- **Inserción de un archivo de configuración** 77
- **Inserción de un archivo de licencia** 77
- **Incorporación de certificados de seguridad** 77
- **Inserción de un archivo protector de pantalla para la serie 9600** 78
- **Inserción de archivos de música en espera** 78

Las acciones adicionales que se pueden realizar en las tarjetas SD se describen en detalle en la sección Administración de la tarjeta SD 136.

4.1 Actualización del firmware de tarjeta

Puede utilizar IP Office Manager para actualizar un grupo de archivos en una tarjeta System SD para que coincidan con los requeridos para la versión particular de IP Office. Esto se puede utilizar para actualizar la tarjeta desde un sistema existente o para preparar la tarjeta para un sistema nuevo.

IP Office Manager actualiza la tarjeta con los archivos del firmware binario para la unidad de control, los módulos de expansión externos y los teléfonos. También incluye los archivos de avisos para el funcionamiento del correo de voz integrado y la opción para los archivos de la aplicación web manager.

Se conservan los archivos existentes como la configuración de sistema, el archivo de licencia PLDS, los mensajes del correo de voz integrado y los saludos.

- Para usar la tarjeta en una ranura de tarjeta **System SD** de una unidad de control, debe ser una tarjeta System SD Avaya. La tarjeta debe tener el formato correcto (puede hacerlo medianteIP Office Manager), aunque no es necesario cambiar el formato de una tarjeta en funcionamiento antes de usar la recreación para actualizar el contenido de la tarjeta.
- El origen de los archivos copiados a la tarjeta SD son las subcarpetas en la carpeta ***\Memory Cards*** en el directorio de aplicaciones de Manager **Directorio de trabajo** (por lo general ***C:\Program Files(x86)\Avaya\IP Office\Manager***). Sin embargo, si se cambia el **Directorio de trabajo** a una ubicación sin un conjunto adecuado de subcarpetas ***\Memory Cards***, el conjunto de archivos requerido no se copiará en la tarjeta SD.
    - **ADVERTENCIA: Instalación de PCS14 y las unidades de control anteriores**
      PCS 310 Las unidades 14 o inferiores primero deben instalar la versión 8.1(65) (o posterior a 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1. Debe tomarse la precaución de comprobar que no se hagan llamadas antes de la actualización a la versión 10.0; de lo contrario, el sistema requerirá una licencia de actualización a 10.0 a pesar de que es "nuevo". El PCS de la unidad de control está impreso en la etiqueta que se encuentra en su parte posterior.

Configuración del nivel de software de sistema inicial

Cuando la unidad de control realiza la primera llamada, la versión de software en funcionamiento se graba de forma permanente en la unidad de control. Esto pasa a ser el nivel base de la unidad de control cuando se consideren los requerimientos del sistema para las licencias de actualización, etc. Por lo tanto, para un sistema nuevo, es importante que actualice la tarjeta System SD a la versión de software requerida antes de iniciar el sistema.

Determinar el nivel de software de la tarjeta System SD

En la tarjeta SD, en la carpeta ***system/primary***, encuentre y abra el archivo ***filelist.txt***. La sección superior, al comienzo del archivo, termina con la versión del grupo de archivos que se copiaron anteriormente a la tarjeta. El resto del archivo detalla los archivos existentes.

Para actualizar/recrear una tarjeta System SD

1. Una vez iniciado, no interrumpa el proceso, por ejemplo, retirando la tarjeta SD. Este proceso toma alrededor de 20 minutos.
2. Inserte la tarjeta SD en la ranura del lector en la computadora IP Office Manager.
3. Mediante IP Office Manager, seleccione **Archivo | Avanzadas | Reproducir tarjeta SD de IP Office**.
4. Seleccione **IP Office A-Law** o **IP Office U-Law**. Esta selección afecta el modo de operación de los sistemas IP Office cuando sean devueltos a los ajustes predeterminados con esta tarjeta presente en la ranura de tarjetas **System SD**.
5. Navegue a la ubicación de la tarjeta y haga clic en **Aceptar**.
6. IP Office Manager indicará si desea incluir archivos IP Office Web Manager de Avaya como parte del proceso recreado. Esos archivos son necesarios si desea ejecutarIP Office Web Manager 71 para administrar el sistema IP Office en que se cargó la tarjeta o si desea utilizar integración 132.
7. IP Office Manager comenzará a crear carpetas en la tarjeta SD y a copiar a ellas los archivos requeridos. Este proceso toma alrededor de 20 minutos.
8. No extraiga la tarjeta SD durante este proceso. Espere hasta que IP Office Manager muestre un mensaje.

4.2 Creación de un archivo de configuración sin conexión

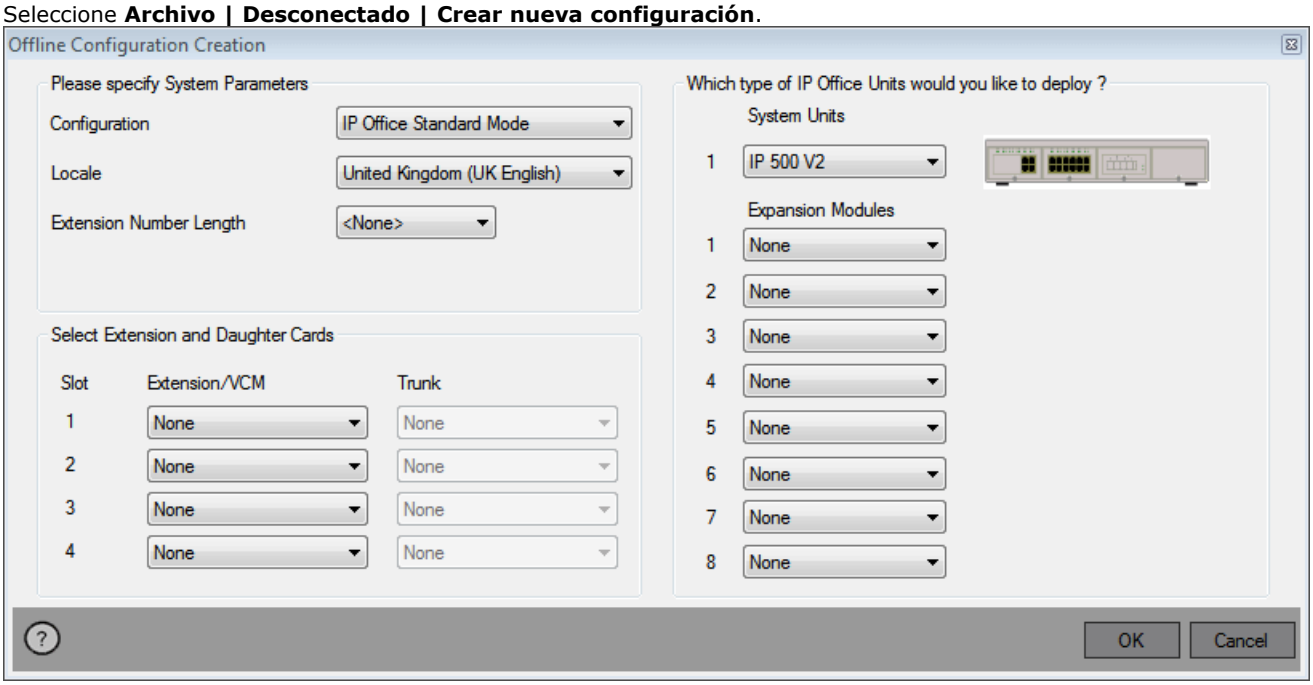
IP Office Manager se puede utilizar para crear una nueva configuración sin necesidad de conectarse a un sistema IP Office. Puede especificar durante el proceso la ubicación del sistema, el tipo de tarjetas de troncales que utiliza y el tipo de unidad de control y módulos de expansión que incluye.

Esto permite crear una configuración antes de instalar el sistema. El archivo de configuración se puede colocar en la tarjeta System SD antes de instalarla en el sistema. De lo contrario, la configuración puede cargarse en el sistema después de realizar la instalación inicial del sistema.

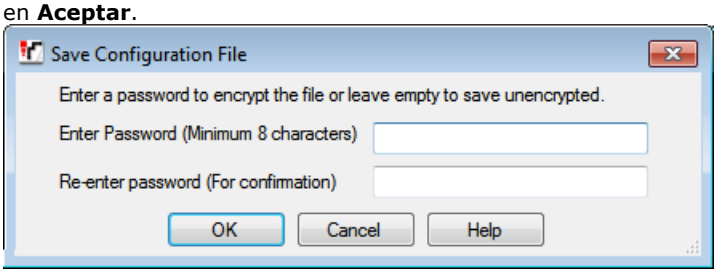
- La configuración creada debe coincidir con el equipo físico del sistema IP Office donde está cargada la configuración. De lo contrario, el sistema IP Office puede reiniciarse y experimentar otras dificultades.

Para crear un archivo de configuración sin conexión

1. Inicie IP Office Manager sin ninguna configuración cargada en IP Office Manager
2. Seleccione **Archivo | Desconectado | Crear nueva configuración**.



3. Seleccione el tipo de configuración que desea crear. El equipo y los ajustes se restringen a los compatibles en el modo seleccionado.
4. Cuando haya terminado el proceso, haga clic en **Aceptar**.
5. IP Office Manager creará y cargará la configuración.
6. Edite la configuración para adaptarse a los requerimientos del cliente. Esto puede incluir importar información desde archivos CSV preparados previamente.
    - Tenga en cuenta que ya que esta configuración se está realizando sin conexión, y sin licencias, puede configurar características que podrían convertirse en no compatibles una vez que la configuración se cargue en el sistema con conexión.
7. Cuando haya completado el proceso, seleccione **Archivo | Guardar configuración como**.
8. Cuando se le indique que ingrese una contraseña para encriptar el archivo, deje los campos en blanco y haga clic en **Aceptar**.



4.3 Inserción de un archivo de configuración predeterminado

IP Office Managerse puede usar para crear un archivo de configuración sin conexión 76. El archivo de configuración creado previamente se puede colocar en la tarjeta System SD del sistema antes de la instalación. Ese archivo se carga posteriormente, al iniciar el nuevo sistema IP Office.

- La configuración creada debe coincidir con el equipo físico del sistema IP Office donde está cargada la configuración. De lo contrario, el sistema IP Office puede reiniciarse y experimentar otras dificultades.

Para cargar una configuración sin conexión desarrollada previamente en una tarjeta SD del sistema

1. Mediante IP Office, cree una configuración fuera de línea que se adapte a las especificaciones del cliente, así como el equipo que se instalará en el IP Office.
2. Vuelva a nombrar el archivo de configuración ***config.cfg***.
3. Con ayuda de un lector de tarjeta, copie el archivo a la carpeta ***/system/primary*** en la tarjeta de memoria System SD.

4.4 Inserción de un archivo de licencia

El archivo XML que contiene las licencias PLDS del sistema se encuentra almacenado en la tarjeta SD del sistema Este archivo se puede agregar a la tarjeta System SD antes de la instalación. La licencia se importa automáticamente a la configuración del sistema cuando se inicia el sistema.

- La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.

Requerimientos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una licencia de sistema **Essential Edition** para la versión de IP Office específica que desea ejecutar.

Para cargar un archivo de licencia en una tarjeta SD del sistema

1. Cambie el nombre del archivo de licencia .XML que se le proporcionó a ***PLDSkeys.xml***.
2. Con ayuda de un lector de tarjeta, copie el archivo a la carpeta ***/system/primary*** en la tarjeta de memoria System SD.

4.5 Incorporación de certificados de seguridad

El sistema IP Office puede utilizar certificados de seguridad para validar las conexiones dentro del mismo sistema, con otras aplicaciones y con otros sistemas IP Office. También se pueden utilizar certificados para comunicaciones de telefonía IP.

Los certificados pueden instalarse en la tarjeta SD del sistema. Estos certificados se cargan posteriormente en el compartimiento de certificados del sistema cuando se lo inicia. La extensión del certificado debe indicar el tipo de codificación; los archivos con codificación PEM deben terminar en ***.pem***y los archivos con codificación DER deben terminar en ***.der***.

Para cargar un certificado que desea agregar:

1. Con ayuda de un lector de tarjeta, copie el archivo a la carpeta ***/system/primary/certificates/tcs/add*** en la tarjeta de memoria SD del sistema.

Para cargar un certificado que desea eliminar:

El mecanismo anterior puede adaptarse de manera que también elimine un certificado existente.

1. Con ayuda de un lector de tarjeta, copie el archivo a la carpeta ***/system/primary/certificates/tcs/remove*** en la tarjeta de memoria SD del sistema. Si existe un certificado que coincida en el compartimiento del sistema, se eliminará dicho certificado.

4.6 Inserción de un archivo protector de pantalla para la serie 9600

Durante períodos de inactividad, los teléfonos serie 9600 pueden suspenderse temporalmente y mostrar una imagen de protector de pantalla. Se encuentran presentes varios archivos ***.jpg*** en la carpeta de tarjetas ***/system/primary*** de manera predeterminada.

Puede reemplazar estos archivos con sus propios archivos de marcas. Con el fin de moverlos libremente alrededor de la pantalla, el tamaño de los archivos debe ser menor que el tamaño de la pantalla en los teléfonos serie 9600.

Teléfono	Tamaño máximo	Teléfono	Tamaño máximo	Teléfono	Tamaño máximo
9611	160x160	**9621G**	320x160	**9650**	320x240
9620	320x160	**9630**	320x240	**9650C**	320x240
9620L	320x160	**9640**	320x240		
9620C	320x160	**9641G**	320x240		

- Pantallas a color: La profundidad de color es de 16 bits. Una imagen a color por separado presentará la mejor apariencia.
- Pantallas monocromáticas: Logrará mejores resultados con una imagen de logotipo con una sola escala de grises. También admite dos niveles de escala de grises.
- Para invocar fondos transparentes en logotipos, utilice un color de fondo de 0,255,0 (el verde más brillante posible).

4.7 Inserción de música en los archivos de espera

En forma predeterminada, el sistema IP Office utilizará música interna durante los períodos en espera mediante la carga de un archivo de música desde la PC IP Office Manager. En sistemas IP500 V2, puede cargar un archivo en la tarjeta SD del sistema antes de instalarla en el IP Office.

El archivo debe estar en el siguiente formato y tener el nombre ***holdmusic.wav***.

Propiedad	Valor
Tipo de archivo	WAV
Tasa de bits	128kbps
Tamaño de la muestra de audio	16 bit
Canales	1 (mono)
Tasa de la muestra de audio	8 kHz
Formato de audio	PCM
Longitud	Hasta 90 segundos.

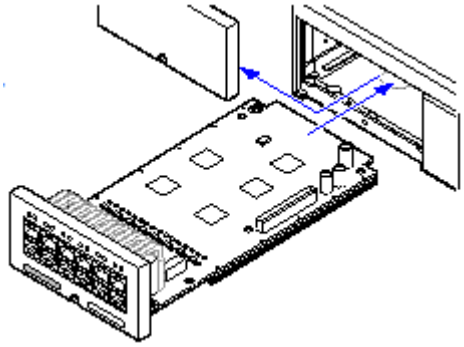
Para cargar un archivo de música en espera en una tarjeta SD del sistema

1. Renombrar archivo de música ***holdmusic.wav***.
2. Con ayuda de un lector de tarjeta, copie el archivo a la carpeta ***/system/primary*** en la tarjeta de memoria System SD.
3. Si el IP Office está configurado (o se planea para el futuro) para admitir archivos de música de espera adicionales (hasta tres archivos adicionales), copie estos archivos a este mismo destino. El nombre de los archivos adicionales debe coincidir con los especificados en la configuración de sistema de IP Office.

Capítulo 5.

Instalación de las tarjetas de la unidad de control

5. Instalación de las tarjetas de la unidad de control



Las tarjetas base y tarjetas auxiliares de troncales IP500 deben instalarse antes de encender la energía de la unidad de control. Asegúrese que las tarjetas se han conectado en el orden indicado por la configuración planeada o pre-construida.

Este proceso tiene 2 etapas:

1. Ajuste las tarjetas auxiliares troncales IP500 en las tarjetas básicas IP500. 81
2. Inserte las tarjetas básicas IP500 en la unidad de control. 82

⚠ Advertencias

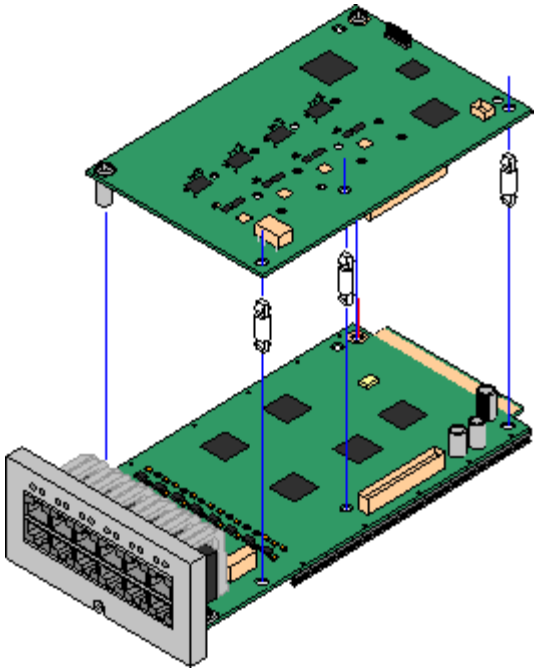
- Deben tomarse medidas de protección contra descargas estáticas antes de manipular los tableros de circuitos.
- No deben agregarse o extraerse tarjetas de una unidad de control mientras la energía está conectada.

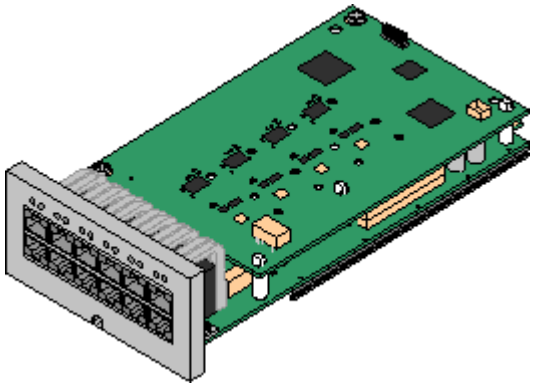
Notas generales

- Las tarjetas pueden insertarse dentro de las ranuras disponibles en cualquier orden. La única excepción es la tarjeta IP500 4-Port Expansion, la cual sólo puede insertarse en la ranura 4 del lado derecho.
- Se recomienda instalar las tarjetas de izquierda a derecha.
- Existen restricciones en cuanto a la cantidad compatible de tarjetas de ciertos tipos. Cuando se excede cierto límite, la tarjeta de ese tipo instalada al extremo derecho dejará de funcionar.
- Asegúrese de utilizar las etiquetas incluidas para identificar la tarjeta instalada en la unidad de control.

5.1 Ajuste de tarjetas auxiliares IP500

Las tarjetas auxiliares de troncales IP500 pueden instalarse en cualquier tarjeta base IP500, excepto por la Unified Communications Module y la tarjeta de expansión de cuatro puertos. En las tarjetas combinadas IP500, la tarjeta auxiliar hija es instalada con anterior y no es posible cambiarla.





⚠ Advertencias

- Deben tomarse las medidas correctas de protección contra descargas estáticas antes de manipular los tableros de circuitos.

Piezas y equipo requeridos

1. ☐ **Tarjeta base IP500**
2. ☐ **Tarjeta auxiliar de troncales IP500**
3. ☐ **3 pilares de soporte**
   Estos vienen incluidos con la tarjeta auxiliar de troncales.

Herramientas requeridas

1. ☐ Destornillador de hoja plana de 5 mm
2. ☐ Correa anti-estática para a muñeca y punto de tierra.

Procedimiento: Instalación de una tarjeta auxiliar de troncales

1. Compruebe que se hayan suministrado las tarjetas correctas.
2. Compruebe que lleva puesta la correa anti-estática para la muñeca y que está conectada a un punto de tierra adecuado.
3. En la base de la tarjeta, identifique la posición de tres orificios para los pilares de plástico para la tarjeta IP500. Éstas se encuentran sobre el mismo borde que el conector de tarjeta.
4. Acople los pilares de soporte a la tarjeta base IP500.
5. Si hay una cubierta metálica desprendible sobre el bloque de conectores en la tarjeta base, retírela.
6. Usando fuerza mínima y comprobando que los pins están en la posición correcta, empuje la tarjeta de troncales IP500 dentro de su bloque de conectores y los pilares de soporte.
7. Compruebe que el conector de la tarjeta se ha introducido en su sitio.
8. Con ayuda de las roldanas y tornillos incluidos, asegure los pilares de soporte metálicos a la tarjeta base.
9. La tarjeta auxiliar de troncales incluye un juego de etiquetas. Inserte la etiqueta apropiada en la parte delantera de la tarjeta base.

5.2 Inserción de tarjetas base IP500

Después de preparar todas las tarjetas base IP500 con la inserción de tarjetas auxiliares de troncales 81, la tarjeta base está lista para insertarla en la unidad de control.

⚠ Advertencias

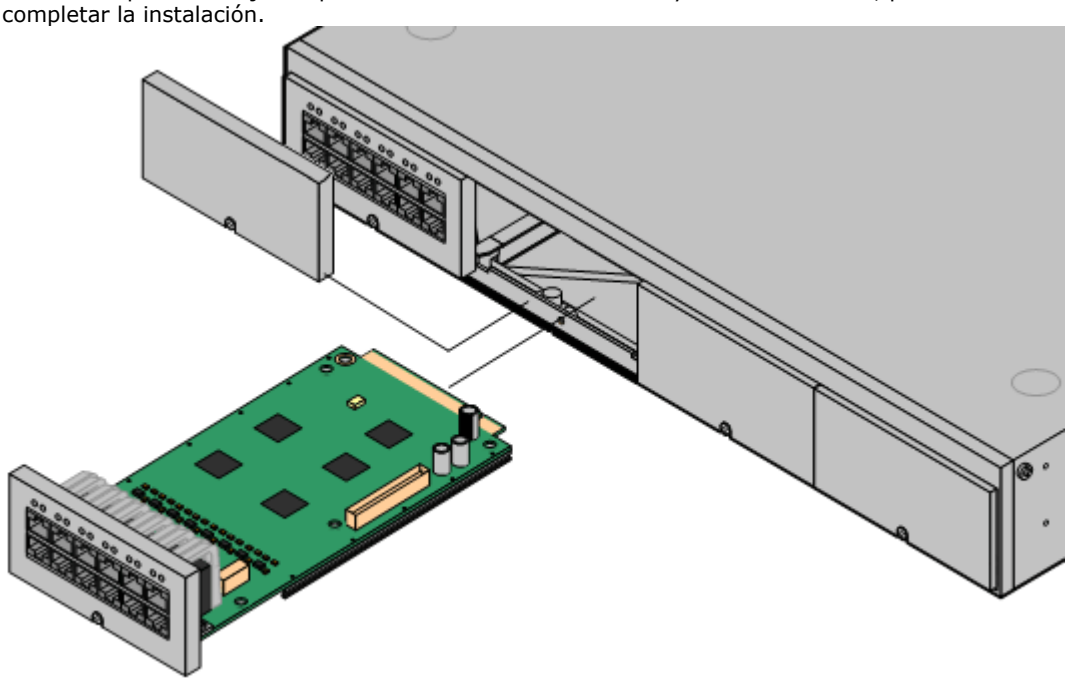
- Deben tomarse las medidas correctas de protección contra descargas estáticas antes de manipular los tableros de circuitos.
- No deben agregarse o extraerse tarjetas de una unidad de control mientras la energía está conectada.

Herramientas requeridas

- ☐ Destornillador de hoja plana de 5 mm
- ☐ Correa anti-estática para a muñeca y punto de tierra.

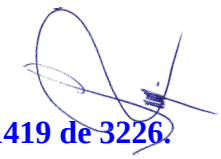
Instalación de una tarjeta IP500

1. Compruebe que no hay energía hacia la unidad de control (está apagada).
2. Con ayuda de un destornillador de punta plana, retire la cubierta de la ranura al frente de la unidad de control que se utilizará para las tarjetas que desea instalar. Esta cubierta ya no es necesaria, pero debe conservarla hasta completar la instalación.



3. Permitiendo que la tarjeta se apoye contra el fondo de la ranura, comience a deslizarla hacia el interior de la unidad de control. Una vez insertada a medias, compruebe que los rieles en la tarjeta se han acoplado con los bordes de la ranura, haciéndola girar despacio en una dirección. Si la tarjeta gira, retírela y comience a insertar de nuevo.
4. La tarjeta debe deslizarse hacia adentro libremente hasta estar casi completamente insertada. En este punto, aplique presión a la base en la parte delantera de la tarjeta para terminar de insertarla.
5. Con ayuda de un destornillador de punta plana, sujete la tarjeta.

Capítulo 6.
Instalación del sistema físico



6. Instalación del sistema físico

Después de la preparación para la instalación, en esta sección se describe la instalación en el lugar.

Resumen

1. **Preparar la instalación** 52
   a. **Requisitos del entorno** 53
      Controle que el área de la instalación cumpla con los requisitos de entorno del sistema.
   b. **Requisitos de espacio** 54
      Controle que el área de la instalación cumpla con los requisitos de espacio del sistema.
   c. **Herramientas y piezas requeridas** 58
      Compruebe que tenga las herramientas y piezas adicionales requeridas.
   d. **Documentación** 59
      Compruebe que ha obtenido y leído toda la documentación relevante.
   e. **Desembalaje** 59
      Verifique que el equipo requerido ha sido entregado y que no ha sufrido daños.
2. **Instalación del software de administración** 62
   Para la instalación del sistema necesita una PC con el software de administración de IP Office instalado. Debe incluirse una copia de IP Office Manager que coincida con el nivel requerido del software IP Office.
   a. **Descarga del software** 63
   b. **Instalación de las aplicaciones del administrador** 64
3. **Preparación de la tarjeta System SD** 74
   Actualice la tarjeta System SD a la versión requerida del software de IP Office. Además agregue todos los archivos disponibles como el archivo de licencia, la configuración preintegrada y el archivo de música en espera.
   - **ADVERTENCIA: Instalación de PCS14 y las unidades de control anteriores**
     PCS 310 Las unidades 14 o inferiores primero deben instalar la versión 8.1(65) (o posterior a 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1. Debe tomarse la precaución de comprobar que no se hagan llamadas antes de la actualización a la versión 10.0; de lo contrario, el sistema requerirá una licencia de actualización a 10.0 a pesar de que es "nuevo". El PCS de la unidad de control está impreso en la etiqueta que se encuentra en su parte posterior.
4. **Instale la tarjeta de la unidad de control** 80
   Conecte todas las tarjetas auxiliares de troncales a las tarjetas base IP500 e inserte las tarjetas base en la unidad de control.
5. **Instalación del sistema** 84
   a. **Montaje en pared** 85
      En caso de que la instalación sea en pared, asegure los soportes y sujete la unidad a la pared.
   b. **Montaje en bastidor** 87
      En caso de que la instalación sea en bastidor, asegure los soportes y sujete la unidad de control al bastidor.
   c. **Conexión de los módulos de expansión externos** 88
      Conecte los módulos de expansión externos a la unidad de control.
   d. **Conexión a tierra del sistema** 90
      Conecte los cables de tierra requeridos a la unidad de control y a los módulos de expansión externos.
   e. **Inicio del sistema** 91
      Inserte la tarjeta System SD y encienda el sistema.
   f. **Conexión de teléfonos** 95
      Conecte los teléfonos digitales Avaya.
6. **Configuración inicial** 98
   Comience la configuración básica del sistema mediante IP Office Manager.
7. **Protección del sistema** 126
   Cambie todas las contraseñas predeterminadas y deshabilite los servicios que no necesite.

6.1 Montaje en pared

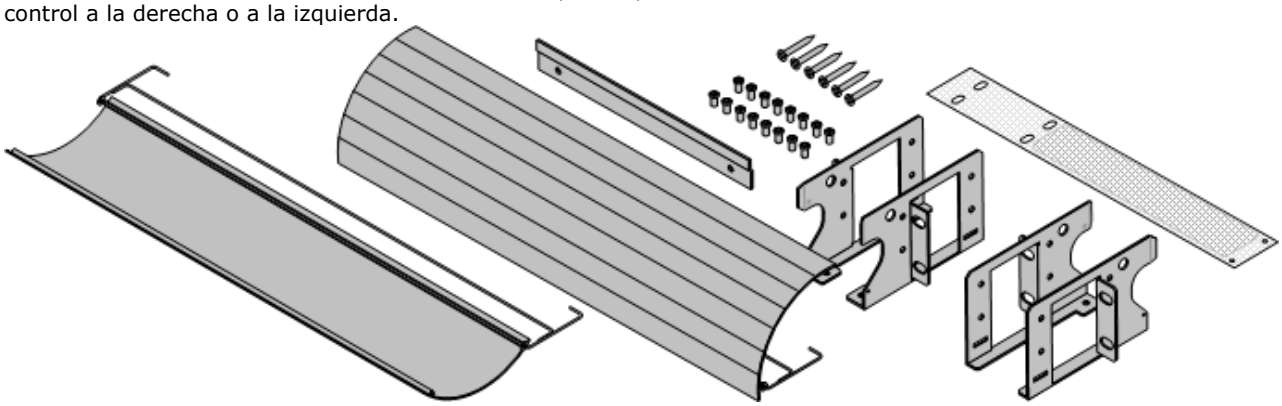
Las unidades de control IP500 V2 y los módulos de expansión externos IP500 pueden montarse en pared o bastidor. Para lograrlo, necesita un kit de montaje en pared, además de los aditamentos necesarios para fijarlos a la pared.

Además de los requerimientos ambientales 53 para el sistema IP Office, los siguientes requisitos adicionales aplican en la instalación en pared de una unidad:

- La superficie de la pared debe ser vertical, plana y estar libre de vibraciones. No se permite la fijación a paredes temporales.
- Debe utilizar únicamente los tornillos incluidos en el kit de montaje para fijar la unidad de control a los soportes.

El siguiente kit de montaje para pared y soporte está disponible actualmente:

- **IPO IP500 WALL MNTG KIT V3** *(Código SAP 700503160)*
  Este kit se puede usar para montaje en la pared y en bastidor de una unidad de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora el enrutamiento de los cables en la parte delantera y trasera de la unidad. En las unidades de control montadas en la pared, permite orientar las ranuras de la base de la unidad de control a la derecha o a la izquierda.



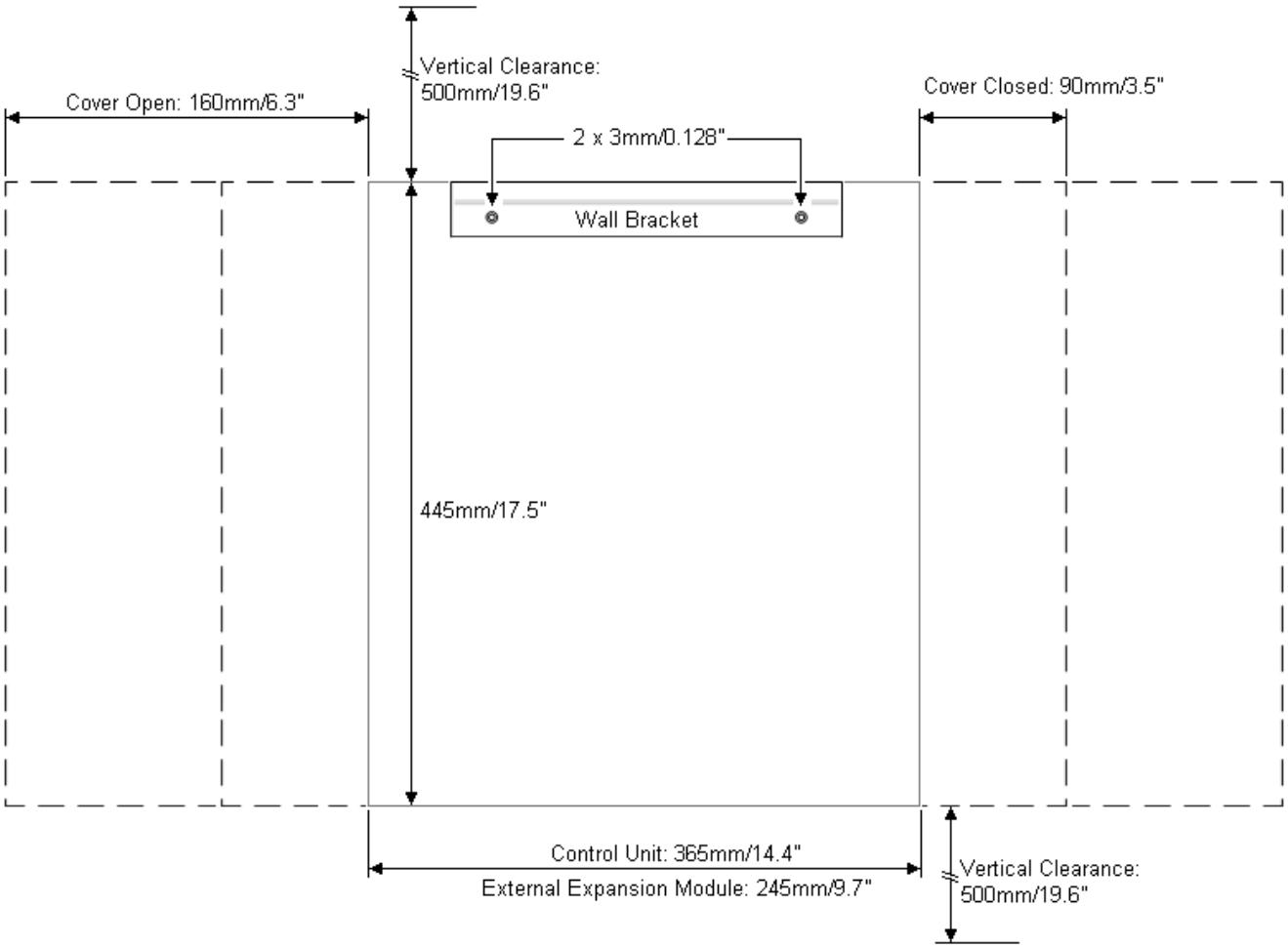
6.1.1 Kit de montaje en pared V2/V3

Estas notas se relacionan con **IPO IP500 RACK MNTG KIT V2** *(SAP 700500923)* e **IPO IP500 WALL MNTG KIT V3** *(SAP 700503160)*. Estos kits se pueden montar en pared o en bastidores de unidades de control IP500 V2 y módulos de expansión externos IP500.

Los kits incluyen todos los componentes necesarios para el montaje en pared en una superficie de madera terciada. El uso de cubiertas de cables es opcional.

Además de los requerimientos ambientales 53 para el sistema IP Office, los siguientes requisitos adicionales aplican en la instalación en pared de una unidad:

- La superficie de la pared debe ser vertical, plana y estar libre de vibraciones. No se permite la fijación a paredes temporales.
- Debe utilizar únicamente los tornillos incluidos en el kit de montaje para fijar la unidad de control a los soportes.
- La instalación debe hacerla solo una persona a cargo de servicio.
- Para unidades de control, la pantalla contra incendio de malla debe instalarse en el borde inferior de la unidad de control antes del montaje.
  - Para el kit V3, la pantalla de llamas se adosa a la parte extena de la unidad de control.
  - Para el kit V2, la pantalla de llamas se inserta dentro de la carcasa de la unidad de control. Para hacerlo usted debe esperar al menos 15 minutos después de sacar el cable de alimentación antes de instalar la pantalla contra incendio.
- Asegúrese de que el sistema esté apagado y que todas las unidades no estén conectadas a la electricidad. Apague el sistema usando un comando de apagado y luego corte la energía. No simplemente saque la unidad.
- Se requiere una superficie de montaje adecuada de madera contrachapada de al menos 19 mm (0.75 pulg) de espesor.
- Las instrucciones completas de instalación vienen incluidas con el kit.

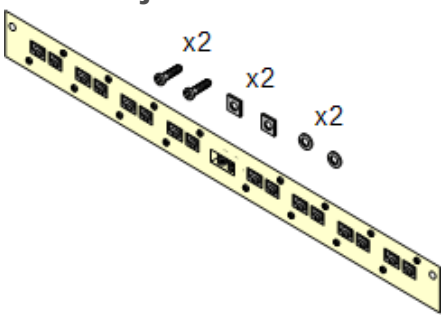


6.2 Montaje en bastidor

Todas las unidades de control de IP Office y módulos de expansión externos pueden montarse en bastidor en sistemas de bastidor estándar de 19". Cada unidad requiere un espacio de en la ranura dentro del bastidor. IPO IP500 RACK MNTG KIT V3 se usa para montar unidades en soporte.

En instalaciones donde los sistemas IP Office están montados en bastidor, deben tenerse en consideración el efecto de las condiciones dentro del gabinete del bastidor. Por ejemplo la temperatura dentro del bastidor puede ser superior a la temperatura de la sala, y el flujo de aire dentro del bastidor estará restringido. Los requerimientos ambientales 53 para las unidades IP Office individuales aplican igualmente dentro de un gabinete de bastidor.

Kit de montaje en bastidor con cajas de protección



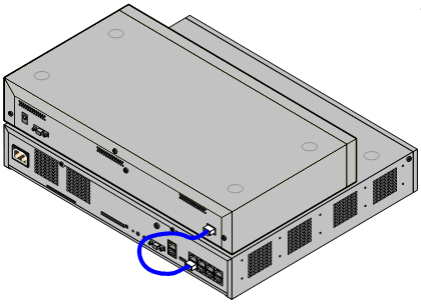
- **Kit de montaje en bastidor con cajas de protección** *(SAP 700293905)*
  Deben utilizarse cajas de protección en las extensiones de teléfono analógicas fuera del edificio 39. Este soporte admite hasta ocho cajas de protección IP Office montadas en bastidor y simplifica el número de conexiones hacia el punto de tierra de protección en el bastidor. Debe utilizar este kit cuando se utilizan más de tres cajas de protección, y admite un máximo de 16 cajas de protección para un solo módulo de expansión externo.

Requerimientos ambientales

Además de los requerimientos ambientales 53 para el sistema IP Office, los siguientes factores adicionales deben tomarse en consideración cuando se instala la unidad en un bastidor:

1. Posicionamiento del bastidor -- Asegúrese de cumplir con las instrucciones de seguridad del fabricante del bastidor. Por ejemplo, compruebe que as patas del bastidor se han bajado y se utilizaron soportes fijadores para evitar que se voltee.
2. Ambiente de operación elevado - Si la instalación se coloca en un aparato de bastidores con múltiples unidades, la temperatura ambiente de operación dentro del entorno del bastidor puede ser más elevada que la temperatura de la sala. Por tanto, debe tenerse consideración al instalar el equipo en un entorno compatible con la temperatura máxima ambiente (Tma) especificada por el fabricante.
   - ☐ Temperatura de operación: 5°C (40°F) a 40°C (104°F).
   - ☐ Humedad de operación: 10% a 95% sin condensación.
3. Flujo de aire reducido - La instalación del equipo en el bastidor debe ser tal que no comprometa la cantidad del flujo de aire necesaria para la operación segura del equipo. Debe conservarse una ventilación adecuada. Las rendijas de ventilación laterales en la unida de control IP500 no deben quedar cubiertas o bloqueadas.
4. Carga mecánica - La instalación del equipo en el bastidor debe realizarse de tal forma que no existan condiciones de riesgo debido a una carga mecánica dispareja.
5. Sobrecarga de los circuitos - Debe prestarse atención a las conexiones de los equipos al circuito de suministro y el efecto que puede tener sobrecargar de circuitos en la protección de sobrecorriente y el cableado de la alimentación. Se debe tener en consideración las clasificaciones inscritas en la placa de nombre del equipo para resolver esta cuestión.
6. Puesta a tierra confiable - Debe asegurarse una conexión de tierra confiable para el equipo montado en bastidor. Debe prestarse especial atención a las conexiones de suministro de energía aparte de las conexiones directas al circuito ramal (por ejemplo, el uso de tiras de contactos).
7. ⚠ Debe utilizar únicamente los tornillos incluidos en el kit de montaje para fijar la unidad de control a los soportes.

6.3 Conexión de módulos de expansión externos



Todo los módulos de expansión externos deben conectarse a la unidad de control antes de encender la unidad de control. Asegúrese que los módulos se han conectado en el orden indicado por la configuración planeada o pre-construida.

Los módulos de expansión externa se conectan a la unidad de control de IP Office con ayuda del cable de interconexión para expansiones. Cada módulo incluye un cable de conexión para expansión y su propia unidad de suministro de energía 33. Los cables de alimentación de energía específicos de la localidad 34 para la unidad de suministro de energía deben solicitarse por separado.

- Cada módulo de expansión externo incluye un cable de interconexión para expansiones azul de 1 metro (3'3"). Este cable sedebe usar cuando se conecte a puertos de expansión en la parte trasera de una unidad de control.
- Al realizar la conexión con los puertos de expansión de una tarjeta IP500 4-Port Expansion card, puede utilizar el cable de interconexión para expansiones amarillo de dos metros (6'6") en vez del cable azul estándar. La tarjeta de expansión de 4 puertos IP500 contiene cuatro cables amarillos.

Requerimientos de instalación

- ☐ Espacio para instalación por encima o debajo de la unidad de control IP Office existente. Consulte los Requerimientos de espacio del bastidor 57 para la colocación de varios módulos apilados.
- ☐ Enchufe para conexión de corriente con interruptor.
  El enchufe de corriente utilizado debe incluir un interruptor y cuando el cable de energía 34 contenga una conexión a tierra, ese enchufe debe contar con una conexión de tierra de protección.
- ☐ Puerto de EXPANSIÓN disponible en la unidad de control.
- ☐ Requisitos para la puesta a tierra
  - ☐ **Puesta a tierra funcional**
    Una conexión para puesta a tierra funcional 38 :
    - ☐ Se recomienda para todos los módulos.
    - ☐ La conexión de una tierra funcional es obligatoria para los módulos de troncales analógicas.
  - ☐ **Puesta a tierra de protección**
    Las conexiones de tierra para protección mediante equipos de protección contra picos 39 :
    - ☐ Son obligatorias para módulos de troncales analógicas en la República de Sudáfrica.
    - ☐ Son obligatorias para los módulos Digital Station y Phone conectados a extensiones fuera del edificio.
    - ☐ Son obligatorias para los módulos Digital Station V2 y Phone V2.

Herramientas requeridas

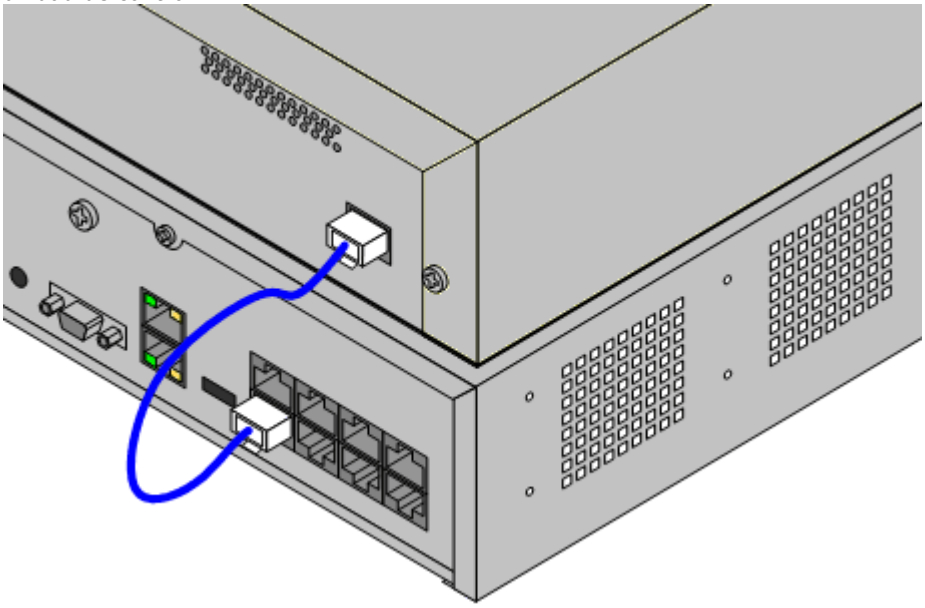
- ☐ PC IP Office Manager.
- ☐ Herramientas para montaje en bastidor 87 (opcional).

Piezas y equipo requeridos

- ☐ **Módulo de expansión externo**.
  Cada módulo trae incluido una unidad externa de suministro de energía apropiada, así como un cable de interconexión azul de 1m. La tarjeta IP500 4-Port Expansion incluye cables de interconexión amarillos de 2m, los cuales sólo deben utilizarse con dicha tarjeta.
- ☐ Cable de energía para la unidad de suministro de energía 34.
- ☐ Kit de montaje en bastidor 40 *(opcional)*.
- ☐ Kit de montaje en pared 85 *(Opcional, solamente para módulos de expansión externos IP500)*.
- ☐ Etiquetas para distinguir los cables.

Procedimiento

1. Los módulos de expansión externos no deben estar conectados a una unidad de control encendida. Si se agrega un módulo nuevo a un sistema existente, apague el sistema 161.
2. Si el sistema IP Office se va a instalar en un bastidor, conecte el kit de montaje en bastidor 87 al módulo de expansión.
3. Conecte el suministro de energía del módulo de expansión externo, pero aún no encienda la energía.
4. Conecte el cable de interconexión de la expansión del puerto EXPANSIÓN del módulo al puerto EXPANSIÓN en la unidad de control.



- **Nota**
  Se recomienda conectar los módulos desde el puerto 1 en adelante, utilizando cada puerto de manera secuencial..

5. Tome nota del puerto utilizado e incluya este dato en la etiqueta para el cable, así como otros registros del sistema.
6. Conecte todos los módulos de expansión externos que esté por agregar.
7. Ahora puede conectar el cable a tierra 90 para los módulos de expansión externos.

a. Una vez que se hayan conectado los módulos de expansión y colocado la toma a tierra, puede iniciar el sistema 91 . Asegúrese de que el módulo de expansión se haya iniciado antes que la unidad de control.

6.4 Puesta a tierra

El empleo de conexiones de tierra reduce la probabilidad de que ocurran problemas en la mayoría de los sistemas de telefonía y de datos. Esto es especialmente importante en edificios donde los múltiples componentes del equipo están conectados entre sí por largas longitudes de cable, por ejemplo, las redes de teléfonos y de datos.

Todas las unidades de control de IP Office y módulos de expansión externos deben conectarse a una conexión de tierra funcional. Esto es cuando la unidad se conecta al suministro de energía con ayuda de un cable de energía con una terminal de tierra. El enchufe del suministro debe estar conectado a una puesta a tierra de protección.

En algunos casos, como en el caso de las troncales de arranque por tierra, además de fungir como medida de protección, la puesta a tierra es un requerimiento funcional para el equipo a operar. En otros casos, puede ser un requisito estipulado por los reglamentos locales o bien un paso de protección necesario, por ejemplo en áreas con alto riesgo de rayos.

- ⚠ **PRECAUCIÓN**
  Durante la instalación, no suponga que los puntos de tierra están correctamente aterrizados. Pruebe los puntos de tierra antes de confiarles el equipo conectado a tierra.
- **Equipo de protección adicional**
  Además de la puesta a tierra, es posible que sea necesario emplear equipo de protección en las siguientes situaciones.
  - En cualquier módulo de expansión externo Digital Station o Phones conectado a una extensión localizada en otro edificio. Consulte la sección Instalaciones telefónicas fuera del edificio 39.
  - En la República de Sudáfrica, en todos los módulos de expansión externos de troncales analógicas (ATM16) y en cualquier unidad de control que contenga tarjetas de troncales analógicas (ATM4/ATM4U).

Herramientas requeridas

- ☐ Destornillador de cruz M4
- ☐ Herramientas adecuadas para sujetar la horquilla del cable.

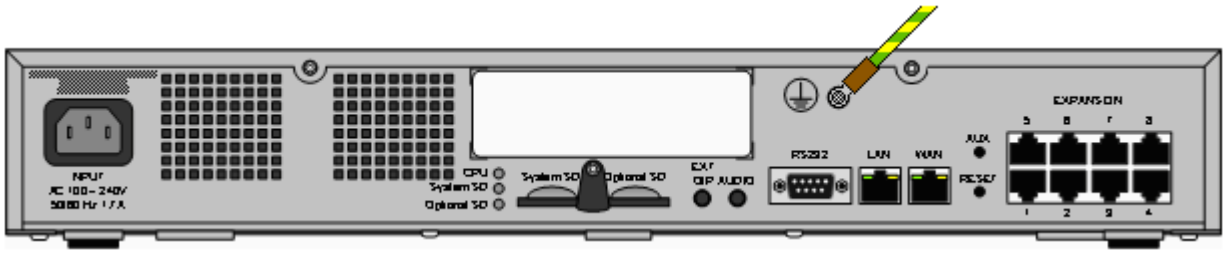
Piezas y equipo requeridos

- ☐ Cable de cobre sólido de 14AWG para la conexión a tierra.
- ☐ Forro de cable en cumplimiento con los requerimientos locales. Éste es por lo general verde para la tierra funcional y verde/amarillo para la puesta a tierra de protección.

El punto de tierra en todas las unidades de control y módulos de expansión de IP Office está marcado con un símbolo ⏚ o ⏚. Las conexiones de tierra hacia estos puntos deben realizarse con un cable sólido de 14 AWG con forro verde para una puesta a tierra funciona, o un forro verde y amarillo para la tierra de protección.

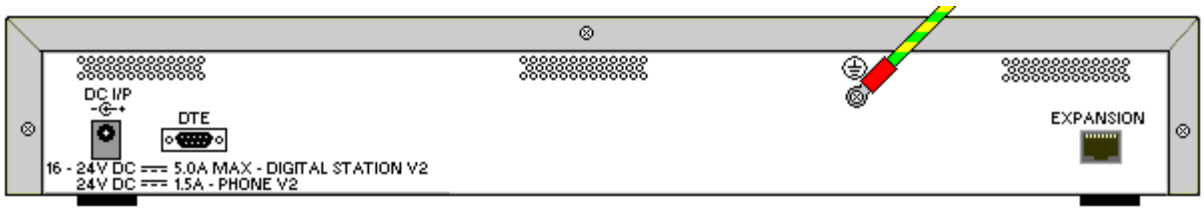
Unidad de control IP500 V2

En las unidades de control IP500 V2, el punto de tierra se encuentra sobre el puerto DTE RS232.



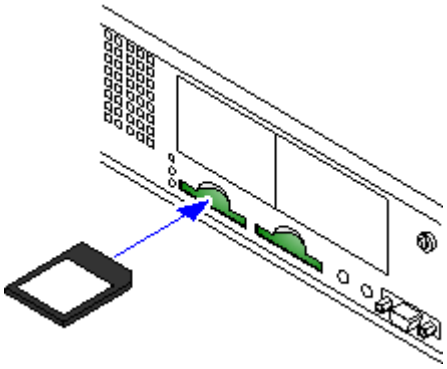
Módulos de expansión externos

En los módulos de expansión, el punto de tierra es un tornillo de 4 mm localizado del lado derecho o en la parte trasera del módulo.



- En algunos módulos de modelos anteriores, no existe el tornillo dedicado de punto de tierra. En estos casos, el tornillo superior central de fijación de la cubierta (3mm) pueden servir con punto de conexión de tierra alternativo. Debe agregar una roldana dentada para asegurar un buen contacto.

6.5 Inicio del sistema



1. Antes de que inserte la tarjeta System SD:
   a. Compruebe de que tiene el tipo correcto de tarjeta System SD Avaya 212.
   b. Compruebe que la tarjeta tenga instalado el nivel de software necesario. De ser necesario, actualice la tarjeta mediante IP Office Manager 75.
2. Cuando la unidad de control esté apagada o desconectada:
   a. Las ranuras de la tarjeta SD tienen un cobertor plástico. Afloje parcialmente el tornillo que sostiene el cobertor de modo que se pueda mover sin problemas de la ranura de tarjeta requerida.
   b. Inserte la tarjeta en la ranura **System SD** en la parte trasera de la unidad de control.
3. Suministre energía a todos los módulos de expansión externos.
4. Suministre energía a la unidad de control. El enchufe de corriente utilizado debe incluir interruptor y el enchufe debe contar asimismo con una conexión de tierra de protección.
5. La unidad de control carga el firmware desde la tarjeta System SD con la que se actualiza a sí misma y a sus componentes internos. Este proceso lleva aproximadamente un minuto. El final de este proceso lo indica la luz LED1 de cada tarjeta base parpadeando cada cinco segundos. La luz LED9 en cada tarjeta base equipada con una tarjeta auxiliar troncal también parpadea.
6. La unidad de control comienza con la actualización de los módulos de expansión externos si es necesario. Esto se indica mediante la luz LED central del módulo parpadeando de color rojo. El proceso queda completado cuando la luz LED queda encendida de color verde.
7. En caso que ya haya un archivo de configuración presente en la tarjeta System SD 77, el IP Office carga este archivo. Si no,los sistemas nuevos crean una configuración predeterminada y copian esa configuración en la tarjeta System SD.
8. Entonces debería ser posible utilizar IP Office Manager para acceder a la configuración de IP Office.

Luces LED del inicio de sistema de la unidad de control

Frente

Las luces LED en la parte trasera de la unidad de control siguen la secuencia a continuación durante el arranque normal. Observe que los tiempos proporcionados son solamente aproximados:

LED	4s	4s	12s	5s	2s	5s	5s	10s	10s	Terminado
CPU	Anaranjado	Verde	Verde	Verde Rojo	Verde	Verde	Verde	Verde	Verde	Verde
System SD	Anaranjado	Desactivado	Verde	Verde	Verde	Desactivado	Verde	Verde	Verde Parpadeo	Verde
Optional SD De estar presente.	Anaranjado	Desactivado	Verde	Verde	Verde	Desactivado	Desactivado	Verde	Verde	Verde

Parte trasera

En la parte delantera de la unidad de control, la luz LED1 de todas las tarjetas base IP500 instaladas se interpreta como sigue. También se utiliza LED9 para las tarjetas auxiliares de troncales instaladas.

LED	30s	30s	Terminado
LED1/LED9	Rojo	Rojo	Rojo
		Parpadeo rápido	Parpadeo cada cinco segundos

6.6 Comprobación de las luces LED

Luces LED de la unidad de control

LED	Descripción
Optional SD **System SD**	• **Apagado** = Apagado de la tarjeta. • **Verde encendido** = tarjeta presente. • **Verde parpadeando** = Tarjeta en uso. • **Anaranjado estable** = Reinicio inminente. • **Rojo parpadeando** = Tarjeta iniciándose o apagándose. • **Rojo parpadeando rápido** = tarjeta llena • **Rojo estable** = Falla de tarjeta/tipo incorrecto.
CPU	• **Alternado verde/rojo** = Iniciando sistema. • **Verde encendida** = Está bien. • **Roja encendida** = No hay software. • **Parpadeando en Rojo** = Error/ Apagado.

Luces LED de la tarjeta base

Nota: Las tarjetas no admitidas en el modo IP Office Basic Edition (expansión de cuatro puertos, VCM32 y VCM64) mostrarán una luz LED fija hasta que se obtenga una licencia para el sistema y se configure para Preferred Edition o superior.

Tarjeta base	Uso de indicadores LED 1 a 8
Todas las tarjetas	• Se utiliza la luz LED1 asimismo para indicar el estado de la tarjeta base: • **Rojo encendido** = Error/no compatible. • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
Teléfono analógico IP500	• Las extensiones de teléfono analógico no utilizan ninguna luz LED para indicar su estado.
Estación digital IP500	• **Destello verde** = Teléfono detectado. • **Verde encendida** = Teléfono activo.
IP500 TCM8	• **Verde encendida** = Teléfono detectado.
Combinación IP500	• Indicadores LED 1 a 6 • **Destello verde** = Teléfono detectado. • **Verde encendida** = Teléfono activo.
VCM IP500	• Las luces LED 1 a 8 no están etiquetadas. Se utilizan para indicar la utilización del canal de compresión de voz. Cada luz LED encendida representa un uso de 12.5% de la capacidad del canal de compresión de voz (capacidad total de la tarjeta, en vez de capacidad de la licencia).
Expansión de 4 puertos IP500	• Las luces LED 1 a 8 se utilizan para los puertos de expansión en la parte trasera de la unidad de control. Las luces LED 9 a 12 se utilizan para los puertos de expansión propios de la tarjeta.

Verde	**Encendido**	Módulo de expansión presente.
Rojo	**Parpadeando**	Iniciando sistema.
Rojo	**Encendido**	Error.
Anaranjado	**Parpadeo regular**	La tarjeta base está bien.

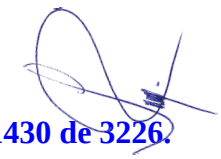
Luces LED de la tarjeta auxiliar de troncales

Tarjeta auxiliar de troncales	Uso de indicadores LED 9 a 12
Todas las tarjetas	• Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar: • **Rojo encendido** = Error • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
Troncal analógica	• **Verde encendida** = V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde parpadeando** = Línea en uso.
de troncales PRI	• **Apagado** = No troncal presente. • **Verde encendida** = Troncal presente.

Tarjeta auxiliar de troncales	Uso de indicadores LED 9 a 12
	• **Verde parpadeando** = Troncal en uso. • **Rojo/verde parpadeando rápido** (puerto 9) o **Verde parpadeando rápido** (puerto 10) = señal de indicación de alarma (AIS) desde el extremo remoto de la troncal. • **Rojo con parpadeo verde** (puerto 9) o **Parpadeo verde** (puerto 10) = Puerto en modo de bucle de retroceso (configurado con IP Office System Monitor).
Troncal BRI	• **Apagado** = No hay una troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso.

Luces LED del Módulo de expansión externa

Módulo	indicadores LED
Todos	El indicador LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **Rojo parpadeando** = Módulo iniciándose/Cargando firmware. • **Luz roja encendida** = Error. • **Luz verde encendida** = El módulo está bien. • **Verde parpadeando** = Módulo iniciándose/Cargando firmware (solo el módulo IP500 DS16A/30A).
Troncal analógica de 16 líneas	• Ninguno.
BRI So8	• **Verde encendida** = Conectado. • **Destello verde** = Actividad.
Estación digital 16/30	• **Destello verde** = Teléfono detectado. • **Verde encendida** = Teléfono activo.
Estación digital 16A/30A	• **Verde encendida** = Teléfono detectado.
Teléfono	• Ninguno.



6.7 Conexión de teléfonos

Durante el proceso de encendido inicial, IP Office crea automáticamente entradas de extensión y usuario para todos los puertos de extensión analógicos y digitales (DS y BST) en el sistema. Esto permite que los dispositivos se conecten sin requerir programación adicional.

- **ADVERTENCIA**
  Si el sistema ha sido actualizado desde una versión anterior del software de IP Office, todos los teléfonos tendrán las llamadas restringidas hasta que se haya ingresado una licencia de actualización. Para la versión 10.0 o posterior se necesita la licencia **Essential Edition** 294 específica de la versión correspondiente. Esta restricción de la marcación incluye la incapacidad para realizar llamadas de emergencia.
- Esta sección no contempla la instalación de teléfonos DECT, H323 y SIP. Para la instalación de estos dispositivos, consulte los manuales de instalación complementarios correspondientes.

6.7.1 Teléfonos analógicos

Conecte los teléfonos analógicos a sus puertos Teléfono 291 apropiados. Compruebe que aquellos teléfonos conectados a puertos para cortes de energía 50 queden correctamente etiquetados con esta información.

6.7.2 Teléfonos ETR

Conecte los teléfonos ETR en los puertos ETR 287 apropiados. No es necesario cargar firmware adicional a estos teléfonos.

6.7.3 Teléfonos estación digital DS

Conecte los teléfonos digitales a sus puertos DS 286 apropiados. Estos teléfonos pueden necesitar actualizar su firmware para coincidir con el software nuclear del sistema IP Office. El firmware apropiado se suministra con el software IP Office Manager y se copia en la tarjeta SD del sistema para sistemas IP500 V2.

Los teléfonos cargan automáticamente el firmware desde el sistema IP Office, de ser necesario.

- El proceso de actualización toma aproximadamente 10 minutos, período durante el cual el teléfono mostrará un mensaje de advertencia. No debe desconectarse el teléfono durante este proceso.
- Una vez que se ha actualizado un teléfono conectado a un puerto, IP Office no vuelve a comprobar si el teléfono conectado a dicho puerto necesita actualizarse de nuevo, excepto al reiniciar el sistema. Esto significa que no es posible actualizar múltiples teléfonos al intercambiar los teléfonos conectados a un mismo puerto.

6.7.4 Teléfonos IP/SIP

La instalación y configuración de teléfonos IP H323 y SIP que no se traten en este documento. Consulte el manual de instalación apropiado de IP Office para ver el tipo de teléfono que se va a instalar.

6.7.5 Teléfonos TCM/BST

Conecte todos los teléfonos BST a sus puertos BST correspondientes. No es necesario cargar firmware adicional a estos teléfonos.

Módulo DS30B

Los módulos de expansión externos IP500 DS16B y DS30B admiten puertos BST o DS. El tipo de puerto para el módulo completo se configura mediante IP Office Manager. Consulte la sección Selección de modo de puerto DS16B/30B 109.

Botones predeterminados

Para sistemas con puertos de teléfonos BST, cuando un teléfono se conecta primero al puerto, el botón de programación del usuario asociado se sobrescribe con la programación de botón predeterminada para el modelo de teléfono.

Si el nuevo sistema está siendo instalado con una configuración preestablecida que incluye la configuración del botón de usuario, la configuración automática de botones para coincidir con el tipo de teléfono sobrescribirá la configuración del botón de usuario. Esto puede evitarse añadiendo el siguiente código corto a los parámetros del usuario en la configuración predeterminada:

- **Código:** *DCP
- **Función:** Marcar
- **Número de teléfono:** 84000004,1,1,0
  La parte 4000004 de la cadena de arriba también puede usarse para ajustar los valores predeterminados para las siguientes configuraciones telefónicas:
  - El primer dígito configura el contraste del teléfono = 1 (bajo) a 9 (alto).
  - El último dígito configura el volumen del timbre = 0 (alto) a 7 (bajo).

Note que si elimina este código corto los botones volverán a su configuración predeterminada según el tipo de teléfono.

Configuración del tipo de teléfono

Para algunos teléfonos, el teléfono solo puede informar el tipo general al sistema pero no el modelo específico. Se recomienda que una vez conectados todos los teléfonos, configure correctamente los tipos de teléfonos en la configuración de IP Office.

- **Importante**
  Los tipos predeterminados no pueden cambiarse después de la instalación sin definir los valores predeterminados de la configuración. Por lo tanto, debe asegurarse de conectar el tipo de teléfono correcto a cada puerto. Si es necesario intercambiar teléfonos, use los procesos para intercambiar números de extensiones 187 en lugar de intercambiar el cableado.

1. Mediante el uso de IP Office Manager, reciba la configuración del sistema.
2. Seleccionar **Extensión**.
3. Seleccionando cada extensión por turno, compruebe en la ficha **Extn** que el campo **Tipo de dispositivo** muestre el valor correcto con el modelo del teléfono.

Tipo predeterminado	Modelos de teléfono posibles
T7100	T7100, M7100, M7100N, Unidad de audioconferencia.
T7208	T7208, M7208, M7208N.
M7310	T7406E, T7406, M7310, M7310N
M7310BLF	T7316, M7310BLF
M7324	M7324, M7324N

4. Guarde la configuración en el sistema de IP Office.

Capítulo 7.

Configuración básica mediante Manager

7. Configuración básica mediante Manager

La presente sección describe los cambios de configuración básicos requeridos para los sistemas IP Office que usen la aplicación IP Office Manager. La presente sección solo describe la configuración básica; la gama completa de configuraciones posibles a través de IP Office Manager se trata en el manual IP Office Manager 12.

Resumen

1. **Conexión de red** 99
   Utilice IP Office Manager para conectarse al sistema nuevo.
2. **Configuración inicial** 101
   El menú **Configuración inicial** se muestra la primera vez que IP Office Manager o IP Office Web Manager se conectan con un sistema nuevo.
3. **Configure el número de extensión** 103
   Vuelva a numerar todas las extensiones de usuario si es necesario.
4. **Deshabilitar cualquier troncal no utilizada** 104
   Deshabilitar el uso de troncales y canales de troncales no disponibles.
5. **Seleccionar la fuente de reloj para troncales digitales** 106
   La modificación de la troncal digital utilizada para proporcionar la señal de reloj al sistema IP Office para realizar la sincronización de llamadas.
6. **Ingreso de prefijos de troncales** 108
   En sistemas donde se utiliza un predijo para la marcación exterior, asegúrese de ingresar el mismo prefijo a los números entrantes para permitir la devolución de llamadas.
7. **Selección de modo de puerto DS16B/30B** 109
   Estos módulos pueden admitir teléfonos Avaya serie T y serie M al proporcionar puertos BST u otros teléfonos digitales Avaya al proporcionar puertos DS. La selección del tipo de puerto para el módulo completo se realiza mediante IP Office Manager.
8. **Cargando el archivo de licencia** 111
   Cargue el archivo de licencia que se proporciona para el sistema y controle el estado de la licencia para las licencias.

Configuración de seguridad básica

Luego de completar la configuración básica, debe seguir los procesos que se enumeran en el capítulo Seguridad del sistema 126.

7.1 Conexión de red

La sección siguiente describe en detalle la forma en que un sistema IP Office nuevo determina la dirección IP que debe utilizar.

Resolución de la dirección IP y el modo DHCP

Al encender una unidad de control IP Office nueva o devuelta a los valores predeterminados, la unidad envía una petición para la información de la dirección IP a un servidor DHCP. Esto ocurre con el cable LAN conectado o desconectado. El proceso a continuación se realiza en forma separada para el puerto LAN (LAN1 en la configuración) y el puerto WAN (LAN2 en la configuración) en la parte posterior de la unidad de control IP Office.

- El sistema crea una solicitud DHCP de la información de la dirección IP que debe utilizarse.
- Si el servidor DHCP responde en aproximadamente 10 segundos, la unidad de control vuelve en forma predeterminada a ser un cliente DHCP y utiliza la información de la dirección IP proporcionada por el servidor DHCP.
- Si no hay respuesta de un Servidor DHCP, la unidad de control vuelve en forma predeterminada a ser el cliente DHCP, pero asume la siguiente dirección predeterminada:
  - Puerto LAN (LAN1): 192.168.42.1/255.255.255.0.
  - Puerto WAN (LAN2): 192.168.43.1/255.255.255.0.
  - Tome nota que IP Office no comprueba si estas son direcciones válidas o disponibles en la red.
- Los sistemas que se ejecutan en modos estándar de IP Office se pueden configurar como un servidor DHCP. Pueden también configurarse para proporcionar DHCP solamente a los teléfonos Avaya IP y/o para acceder por medio de conexiones por marcación remotas. Las opciones de servidor DHCP no son compatibles con sistemas que funcionan en modos IP Office Basic Edition.
- Cuando una unidad de control IP500 V2 obtuvo una dirección IP y parámetros de configuración del modo DHCP, conservará esos parámetros aun cuando se haya reiniciado la unidad sin un archivo de configuración presente en la tarjeta SD del sistema. Para eliminar completamente la configuración existente de dirección IP y modo DHCP, debe devolver la configuración del sistema a los valores predeterminados 168.

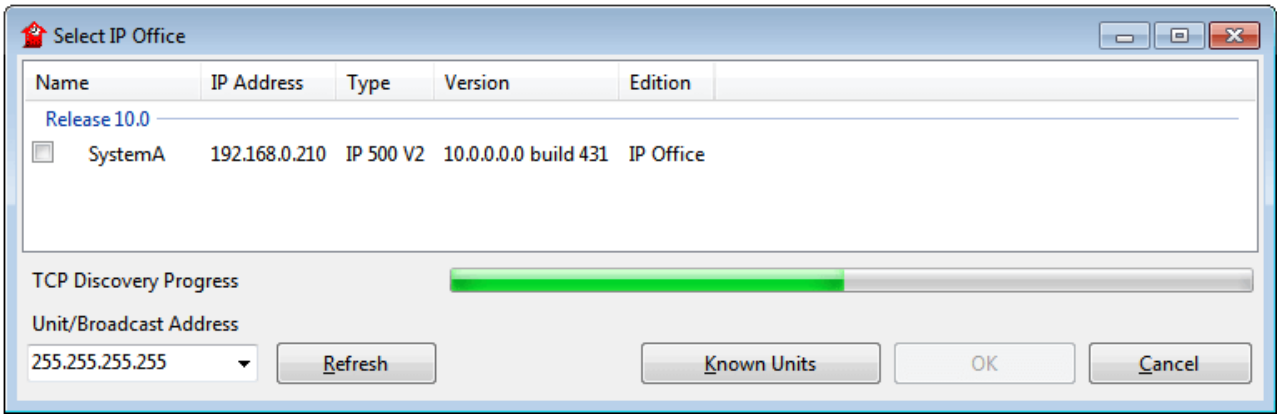
Conexión a la PC

Dependiendo de las condiciones aplicadas cuando se inició por primera vez la unidad de control de IP Office, puede conectarse una PC como sigue:

- **Si el sistema IP Office no está conectado a una red:**
  Conecte la PC directamente al IP Office. La PC debe estar configurada con una dirección válida en la misma red de los ajustes predeterminados del sistema IP Office descrito arriba.
- **Si el sistema IP Office está conectado a una red sin un servidor DHCP:**
  Conecte la PC directamente al IP Office. La PC debe estar configurada con una dirección válida en la misma red de los ajustes predeterminados del sistema IP Office descrito arriba.
- **Si el sistema IP Office está conectado a una red mediante un servidor DHCP:**
  Conecte la PC a la red. La PC debe estar configurada como cliente DHCP o con una dirección válida para la red.
- **Si el sistema IP Office utilizó una configuración generada previamente, haga lo siguiente:**
  Utilice las direcciones IP según lo establecido en la configuración. Asegúrese de que la PC se encuentre en la misma subred o en una red habilitada para enrutar a esa subred.

Para iniciar sesión en un sistema mediante IP Office Manager:

1. Seleccione **Inicio | Todos los programas | IP Office | Manager**.
   - Si la PC tiene instalado un software de firewall, puede recibir una notificación preguntando si desea permitir a este programa acceso a la red. Seleccione **Sí** o **Aceptar**.
2. Verifique la configuración predeterminada de la aplicación:
   a. Haga clic en **Archivo | Preferencias**.
   b. Si no planea administrar sistemas IP Office Basic Edition, seleccione **Modo estándar como predeterminado** y desmarque la opción **Establecer vista simplificada como predeterminada**.
   a. Haga clic en **Aceptar**.
3. Seleccione **Archivo | Abrir configuración** en la barra de menús.
4. Aparece la ventana **Seleccionar IP Office**. Después de algunos segundos, debe aparecer la unidad de control IP Office. El nombre predeterminado que se utiliza en una unidad de control IP Office recientemente instalada es su dirección MAC.



   - En caso que no se pueda encontrar el sistema requerido, puede modificar la dirección utilizada para la búsqueda. Ingrese o seleccione la dirección deseada en el campo **Dirección de la unidad/difusión** y luego haga clic en **Actualizar** para realizar una nueva búsqueda.
5. Haga clic en la casilla de verificación al lado del sistema y luego clic en **Aceptar**.
6. Aparecerá un cuadro con la solicitud de nombre y contraseña. Tanto el nombre como la contraseña predeterminados son ***Administrator***.
7. Ahora se le solicita que se desplace por el menú de configuración inicial. Consulte Configuración inicial 101.

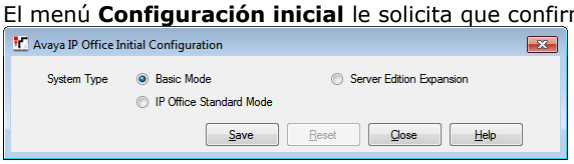
7.2 Configuración inicial

El menú de configuración inicial aparece la primera vez que IP Office Manager se conecta con un sistema nuevo o predeterminado.

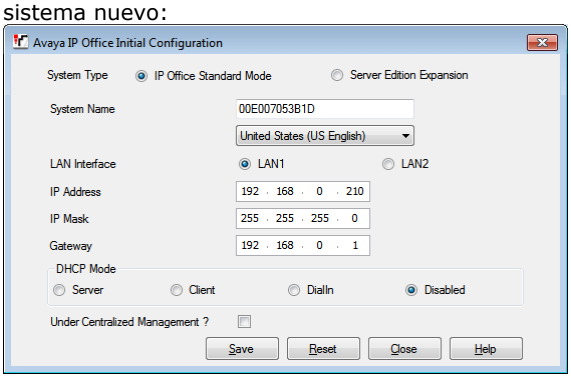
- El menú de configuración inicial puede volver a ejecutarse en cualquier momento seleccionando **Archivo | Configuración avanzada | Configuración inicial** en IP Office Manager o **Acciones | Comandos de servicio | Configuración inicial en** IP Office Web Manager. Tenga en cuenta que esto elimina la mayor parte de la configuración del sistema existente.

Para empezar la configuración inicial mediante IP Office Manager:

1. A través de IP Office Manager, conéctese al sistema 99.
2. Se le solicita que cambie las contraseñas predeterminadas.
   - **Contraseña de administrador**
     Esta contraseña se usa para acceder a la configuración de telefonía del sistema.
   - **Contraseña de administrador de seguridad**
     Esta contraseña se usa para acceder a la configuración de seguridad del sistema. Tenga en cuenta que, de manera predeterminada, la contraseña de administrador que se menciona arriba también puede utilizarse para la configuración de seguridad.
   - **Contraseña de sistema**
     Esta contraseña se usa para la actualización del sistema mediante IP Office Manager y también se puede usar para conectar System Monitor.
3. Introduzca las nuevas contraseñas y haga clic en **Aceptar**.
4. El menú **Configuración inicial** le solicita que confirme el modo de operación requerido para el sistema.



5. Para el **Tipo de sistema**, seleccione ***IP Office Standard Mode*** y haga clic en **Guardar**. Este modo cubre los sistemas IP Office Essential Edition y IP Office Preferred Edition.
6. El menú le solicita que establezca otras configuraciones. Es importante que verifique y establezca estas configuraciones correctamente ya que afectan a varias configuraciones predeterminadas que, luego, se aplicarán al sistema nuevo:



   - **Nombre del sistema:** Se utiliza como ayuda para identificar y acceder al sistema.
   - **Configuración regional:** Establece un rango de configuración predeterminada para que coincida con los requerimientos de telefonía de ese país. También establece el idioma predeterminado para el sistema y todos los usuarios.
   - **Configuración de la dirección IP:** Verifique que esta configuración, especialmente el **modo DHCP**, coincida con los requerimientos de la red del cliente. Alterne entre **LAN1** y **LAN2** para verificar la configuración de los puertos LAN y WAN respectivamente.
   - **En administración centralizada:** Esta configuración se utiliza para sistemas Branch en una red Avaya Aura. Consulte la documentación sobre instalación de Branch 12 por separado.
7. Haga clic en **Guardar**. La nueva configuración se abre en IP Office Manager. Actualmente, la configuración nueva no se ha guardado en el sistema. Elija una de las siguientes opciones:
   - **Continuar configuración básica:**
     Continúe la configuración básica utilizando las siguientes secciones de este capítulo y, luego, guarde la configuración cuando haya terminado.

- **Guardar y luego continuar la configuración básica:**
  Guarde la configuración 112 tal como se encuentra actualmente. Esto puede ocasionar que el sistema se reinicie para usar la nueva configuración; el menú de guardado le indicará si esta acción es necesaria. Luego de guardar la configuración y una vez que el sistema se haya reiniciado (en caso de que haya sido necesario) vuelva a cargar la configuración y continúe con la configuración básica.

8. Continúe con la configuración básica o haga clic en el icono guardar para guardar la configuración actualizada 112 y, luego, continúe.

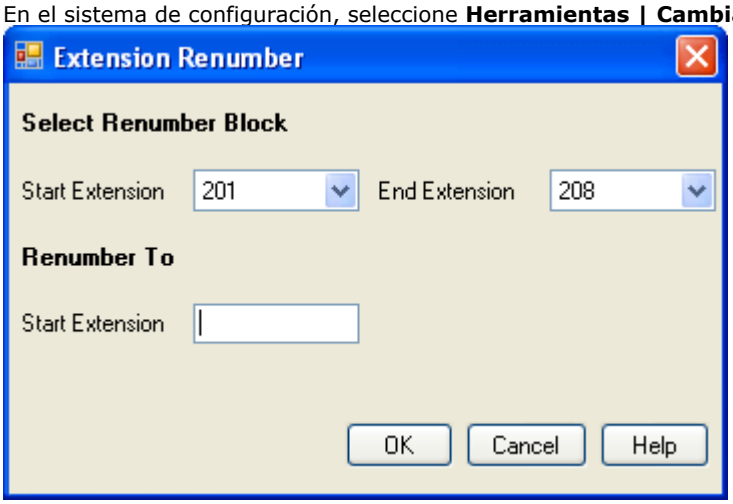
7.3 Numeración de las extensiones

Los sistemas modo estándar de IP Office pueden usar una combinación de números de extensión de hasta 15 caracteres. En forma predeterminada, los grupos de búsqueda y las extensiones están numeradas con tres dígitos empezando a partir de 200.

Para volver a enumerar todas las extensiones de usuarios mediante IP Office Manager:

IP Office Manager se puede usar para renumerar todas las extensiones del sistema. Esto actualizará también todas las referencias al número de extensión en otros campos de las configuración.

1. En el sistema de configuración, seleccione **Herramientas | Cambiar numeración de extensión**.



2. Seleccione el rango de extensiones de usuarios existentes al que le desea cambiar la numeración e introduzca el nuevo número de extensión inicial para dicho rango.
3. Haga clic en **Aceptar**.
4. Elija una de las siguientes opciones:
   - **Continuar configuración básica:**
     Continúe la configuración básica utilizando las siguientes secciones de este capítulo y, luego, guarde la configuración cuando haya terminado.
   - **Guardar y luego continuar la configuración básica:**
     Guarde la configuración 112 tal como se encuentra actualmente. Esto puede ocasionar que el sistema se reinicie para usar la nueva configuración; el menú de guardado le indicará si esta acción es necesaria. Luego de guardar la configuración y una vez que el sistema se haya reiniciado (en caso de que haya sido necesario) vuelva a cargar la configuración y continúe con la configuración básica.
5. Continúe con la configuración básica 104 o haga clic en el icono guardar para guardar la configuración actualizada 112 y, luego, continúe.

7.4 Deshabilitación de las troncales no utilizadas

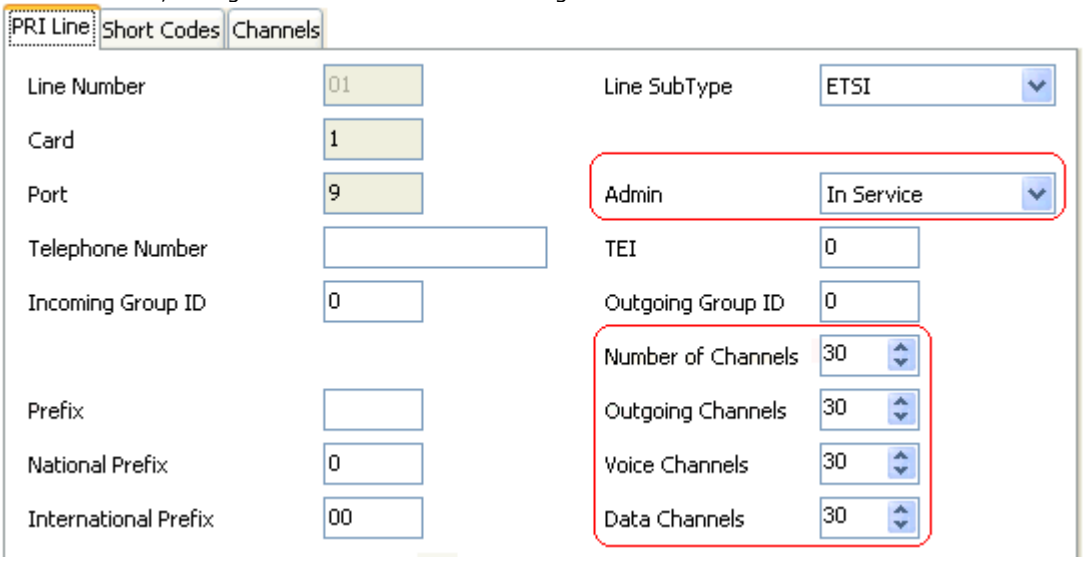
Cada tarjeta de troncal IP Office proporciona un número fijo de puertos de troncales con puertos de troncales digitales que soportan una cantidad fija de canales digitales. De forma predeterminada, la configuración de IP Office tiene entradas de configuración para todas las líneas troncales y canales posibles.

En aquellos casos donde la cantidad de troncales o canales de troncales en uso o con licencia es menor que la cantidad admitida por la tarjeta de troncales, es necesario inhabilitar las troncales y canales no utilizadas.

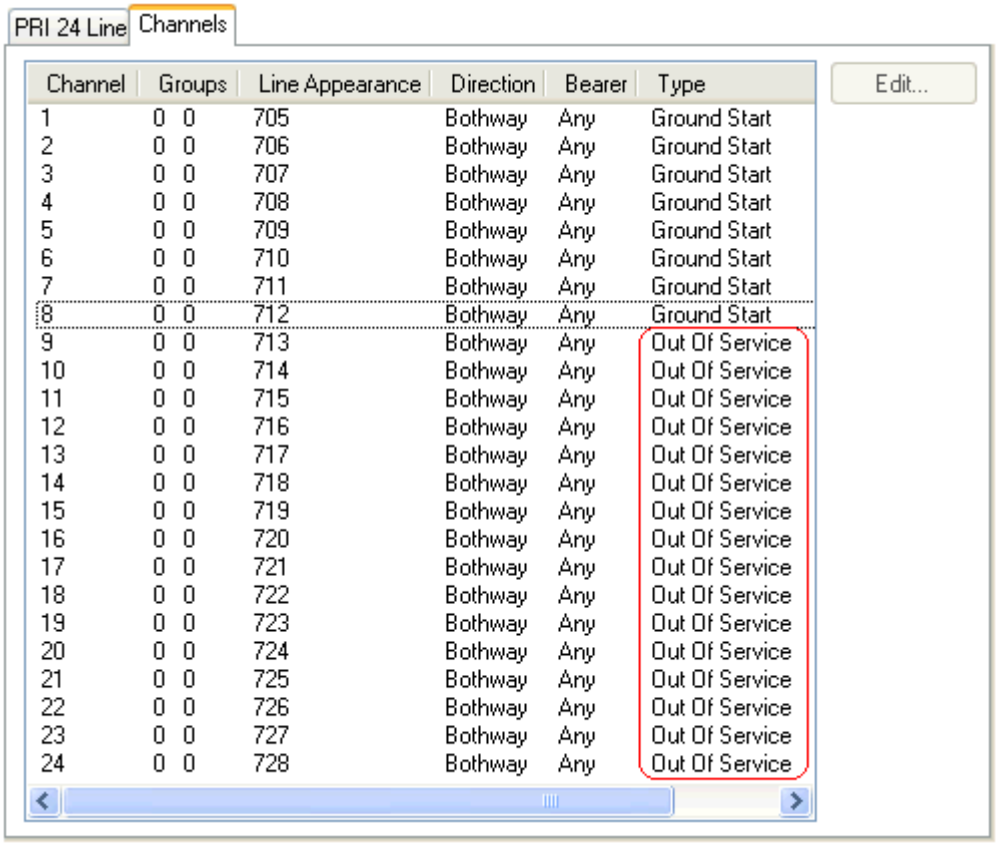
- ⚠ De no hacerlo, esto puedo ocasionar problemas con las llamadas salientes. Por ejemplo, en un sistema con una tarjeta de troncales ATM4 instalada pero con sólo dos troncales analógicas conectadas en realidad, de no inhabilitar las dos troncales restantes en la configuración de IP Office, esto ocasionará que fracase 50% de los intentos de llamada saliente. Esto se debe a que el sistema no puede detectar automáticamente el estado del servicio de troncales analógicas individuales.
    - Para modo Oficina En la versión 8.1 Feature Pack 1 y posteriores con cuatro tarjetas de troncales analógicas IP500 V2 y tarjetas combinadas ATM4 V2, el sistema puede detectar con troncales analógicas conectadas, de manera que puede tratar automáticamente puertos de troncales no conectados como fuera de servicio.
- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

Para deshabilitar troncales sin uso mediante IP Office Manager:

1. En la configuración de IP Office, seleccione Línea.
2. En cada línea, seleccione las líneas o canales que no están conectadas o en uso como fuera de servicio. La ubicación del ajuste relevante en este caso varía según el tipo de troncal.
    - **Troncales analógicas**
      Para inhabilitar la troncal entera, en el formulario principal configure la opción **Admin** en ***Fuera de servicio***.
    - **Troncales BRI, E1 PRI, S0 y QSIG**
      Para inhabilitar la troncal entera, en el formulario principal configure la opción **Admin** en ***Fuera de servicio***. De lo contrario, configure la cantidad de canales según la cantidad total de canales suscritos.



- **Troncales T1, T1 PRI y E1R2**
  Para inhabilitar la troncal entera, en el formulario principal configure la opción **Admin** en ***Fuera de servicio***. De lo contrario, seleccione la ficha Canales y configure los canales no utilizados como **Fuera de servicio**.



Channel	Groups	Line Appearance	Direction	Bearer	Type
1	0 0	705	Bothway	Any	Ground Start
2	0 0	706	Bothway	Any	Ground Start
3	0 0	707	Bothway	Any	Ground Start
4	0 0	708	Bothway	Any	Ground Start
5	0 0	709	Bothway	Any	Ground Start
6	0 0	710	Bothway	Any	Ground Start
7	0 0	711	Bothway	Any	Ground Start
8	0 0	712	Bothway	Any	Ground Start
9	0 0	713	Bothway	Any	Out Of Service
10	0 0	714	Bothway	Any	Out Of Service
11	0 0	715	Bothway	Any	Out Of Service
12	0 0	716	Bothway	Any	Out Of Service
13	0 0	717	Bothway	Any	Out Of Service
14	0 0	718	Bothway	Any	Out Of Service
15	0 0	719	Bothway	Any	Out Of Service
16	0 0	720	Bothway	Any	Out Of Service
17	0 0	721	Bothway	Any	Out Of Service
18	0 0	722	Bothway	Any	Out Of Service
19	0 0	723	Bothway	Any	Out Of Service
20	0 0	724	Bothway	Any	Out Of Service
21	0 0	725	Bothway	Any	Out Of Service
22	0 0	726	Bothway	Any	Out Of Service
23	0 0	727	Bothway	Any	Out Of Service
24	0 0	728	Bothway	Any	Out Of Service

  - Para T1, configure **Tipo** como ***Fuera de servicio***.
  - Para T1 PRI, configure el campo **Admin** en ***Fuera de servicio***.
  - En troncales E1R2, configure **Tipo de señalización de línea** como ***Fuera de servicio***.

3. Elija una de las siguientes opciones:
   - **Continuar configuración básica:**
     Continúe la configuración básica utilizando las siguientes secciones de este capítulo y, luego, guarde la configuración cuando haya terminado.
   - **Guardar y luego continuar la configuración básica:**
     Guarde la configuración 112 tal como se encuentra actualmente. Esto puede ocasionar que el sistema se reinicie para usar la nueva configuración; el menú de guardado le indicará si esta acción es necesaria. Luego de guardar la configuración y una vez que el sistema se haya reiniciado (en caso de que haya sido necesario) vuelva a cargar la configuración y continúe con la configuración básica.
4. Continúe con la configuración básica 106 o haga clic en el icono guardar para guardar la configuración actualizada 112 y, luego, continúe.

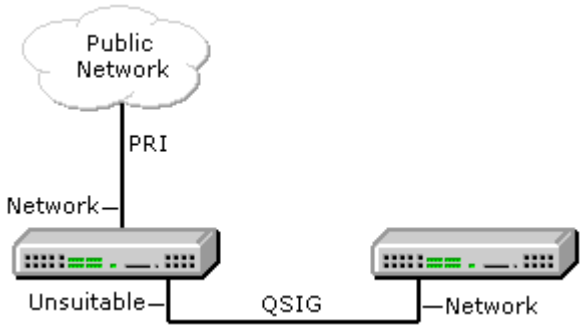
7.5 Configuración de la fuente de reloj para troncales digitales

Las troncales digitales requieren que el sistema de teléfono en cada extremo de la troncal comparta una señal de reloj para asegurar la sincronización de la señalización de llamada. El IP Office puede obtener y utilizar la señal de reloj de cualquiera de sus troncales digitales. Típicamente, se utiliza la señal de reloj proporcionada por una troncal digital en a central de comunicaciones de la oficina, ya que ésta es la fuente de reloj más precisa y confiable.

De no haber una fuente de reloj disponible, el sistema puede utilizar su propio reloj interno si es necesario. Sin embargo, se prefiere una fuente troncal externa. Para hacerlo, la configuración **Calidad del reloj** en cada línea de la configuración de IP Office contiene uno de los valores siguientes:

- ***Red***
  De estar disponible, se debe utilizar la señal de reloj proveniente de esta troncal como la fuente de reloj para la sincronización de llamadas. Si hay varias troncales con esta configuración, la troncal utilizada se determina en el orden de las ranuras 1 a 4 y, luego, por puerto en cada ranura.
- ***Reserva***
  De estar disponible, se debe utilizar la señal de reloj proveniente de esta troncal como la fuente de reloj en caso que ninguna de las troncales definidas como ***Red*** puedan proporcionar una fuente de reloj. Si hay varias troncales con esta configuración, la troncal utilizada se determina en el orden de las ranuras 1 a 4 y, luego, por puerto en cada ranura.
- ***Inadecuada***
  La fuente de reloj de esta troncal no se utilizará como la fuente de reloj.

En el ejemplo a continuación, el primer sistema IP Office es configurado para emplear la troncal de red pública como su fuente de reloj, ignorando la fuente de reloj posible proveniente de la troncal QSIG. El otro sistema IP Office emplea la señal de reloj recibida del primer IP Office en la troncal QSIG y su fuente de reloj correspondiente. Por tanto, ambos sistemas IP Office utilizan la misma fuente de reloj, proveniente de la red de comunicaciones pública.

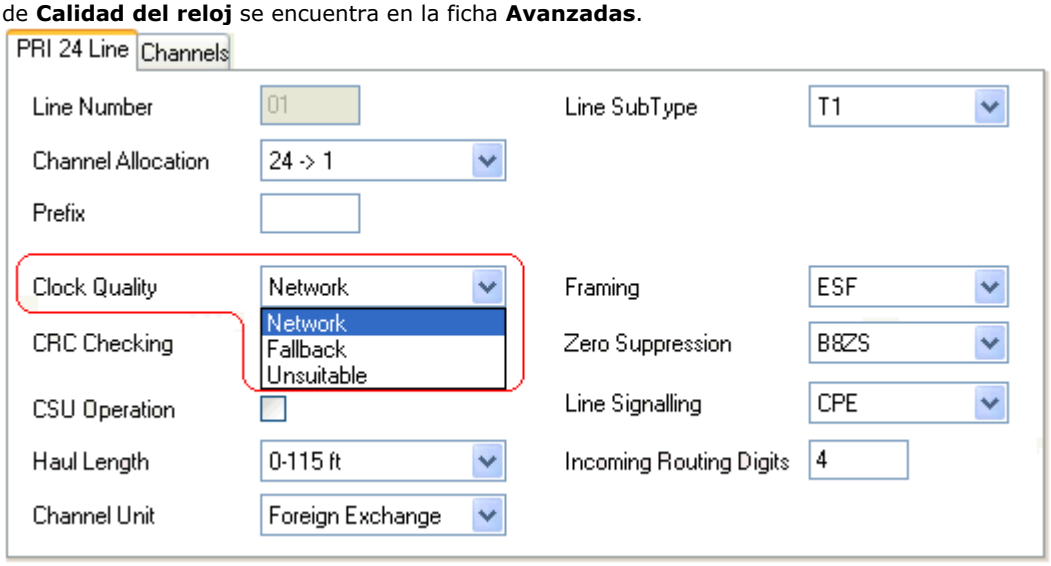


Visualización de la fuente de reloj actual

La fuente de reloj actual utilizada por el sistema IP Office aparece en la página **Recursos** dentro de System Status Application.

Para configurar la fuente de calidad del reloj de una troncal por medio de IP Office Manager:

1. En la configuración de IP Office, seleccione **Línea**.
2. En cada línea digital, seleccione la línea y en la ficha Línea seleccione la opción para que la troncal proporcione la fuente de reloj para la red, o bien para configurar la troncal como inadecuada. En troncales E1R2, la configuración de **Calidad del reloj** se encuentra en la ficha **Avanzadas**.



3. Asegúrese de que solamente una troncal esté configurada como ***Red***. De preferencia, ésta debería ser una troncal digital directa a la central de comunicaciones de la oficina.
4. Otra troncal puede configurarse como ***Reserva*** en caso de perder la conexión de troncal con la Red. De ser posible, ésta debería ser una troncal de un proveedor distinto, ya que esto disminuye las probabilidades de que ambas fuentes fallen al mismo tiempo.
5. Compruebe que todas las troncales digitales restantes estén configuradas como ***Inadecuado***.
6. Elija una de las siguientes opciones:
   - **Continuar configuración básica:**
     Continúe la configuración básica utilizando las siguientes secciones de este capítulo y, luego, guarde la configuración cuando haya terminado.
   - **Guardar y luego continuar la configuración básica:**
     Guarde la configuración 112 tal como se encuentra actualmente. Esto puede ocasionar que el sistema se reinicie para usar la nueva configuración; el menú de guardado le indicará si esta acción es necesaria. Luego de guardar la configuración y una vez que el sistema se haya reiniciado (en caso de que haya sido necesario) vuelva a cargar la configuración y continúe con la configuración básica.
7. Continúe con la configuración básica 108 o haga clic en el icono guardar para guardar la configuración actualizada 112 y, luego, continúe.

7.6 Configuración de los prefijos de troncales

De manera predeterminada, los sistemas con una tarjeta SD del sistema U-Law se devuelven a los valores predeterminados mediante un prefijo 9 para llamadas externas. Los sistemas se iniciaron con una tarjeta SD del sistema A-Law predeterminada a ningún prefijo (cualquier marcación que no coincida con un número interno se supone que es un número externo).

Cuando se ha implementado un prefijo para las llamadas salientes, debe agregarse este mismo prefijo a los ajustes de las troncales. Se utiliza entonces el prefijo troncal de la siguiente manera:

- **Llamadas entrantes**
  En las llamadas entrantes, el prefijo establecido de la troncal se agrega a cualquier Id. de persona que llama entrante que se recibe con la llamada y se almacena en el registro de llamadas de los teléfonos, etc. El prefijo debe tener un formato que permita que la Id. de persona que llama resultante pueda ser utilizada por las aplicaciones y teléfonos del sistema para realizar devoluciones de llamada. Por ejemplo, si el sistema se configura para que se requiera un 9 para indicar una llamada saliente, la troncal debe agregar un 9 a la Id. de la persona que llama entrante con el objetivo de que dicha Id. pueda utilizarse para realizar devoluciones de llamada.
- **Llamadas salientes**
  En las llamadas salientes, los códigos cortos utilizados para enrutar la llamada a una troncal deben quitar todos los prefijos de marcación externos (por ejemplo, 9) para que el número marcado desde el sistema a la troncal sea adecuado para el enrutado por parte del proveedor de la troncal.

Para usar prefijos troncales mediante IP Office Manager:

1. En la configuración de IP Office, seleccione Línea.
2. Ingrese el prefijo en cada línea. La ubicación de la configuración de prefijo varía según el tipo de troncal. Algunos tipos de troncales tienen un solo campo de prefijo. Otros tipos de troncales pueden tener campos de prefijos separados para llamadas nacionales, internacionales y de otro tipo.
3. Elija una de las siguientes opciones:
   - **Continuar configuración básica:**
     Continúe la configuración básica utilizando las siguientes secciones de este capítulo y, luego, guarde la configuración cuando haya terminado.
   - **Guardar y luego continuar la configuración básica:**
     Guarde la configuración 112 tal como se encuentra actualmente. Esto puede ocasionar que el sistema se reinicie para usar la nueva configuración; el menú de guardado le indicará si esta acción es necesaria. Luego de guardar la configuración y una vez que el sistema se haya reiniciado (en caso de que haya sido necesario) vuelva a cargar la configuración y continúe con la configuración básica.
4. Continúe con la configuración básica 109 o haga clic en el icono guardar para guardar la configuración actualizada 112 y, luego, continúe.

7.7 Selección de modo de puerto DS16B/30B

Cada módulo de expansión externo IP500 DS16B/DS30B y DS16B2/DS30B2 de un sistema puede admitir puertos telefónicos DS 286 o puertos telefónicos BST 285. Los módulos se devuelven de manera predeterminada a una operación de puerto de teléfono DS. El modo de cualquier módulo en particular se puede modificar a través de la configuración del sistema.

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.
- En los módulos DS16B/DS30B, el proceso de cargar el firmware adecuado para el modo seleccionado tarda hasta 10 minutos durante los cuales el módulo no está disponible. No aplicable a los módulos DS16B2/DS30B2.

Para cambiar el modo del puerto del módulo IP500 DS16B/30B:

1. En la configuración de IP Office, seleccione **Unidad de control**. Aparecen los módulos de expansión externos y la unidad de control.
2. Los módulos IP500 DS16B e IP500 DS30B aparecen como ***DIG ADPx16 RJ45*** y ***DIG ADPx30 RJ45***.
3. Seleccione uno de los módulos de expansión externos. En los detalles de la unidad, la lista desplegable **Modo de funcionamiento** se usa para seleccionar qué tipo de teléfonos admite el módulo. Seleccione el modo requerido.
   - Para puertos DS, seleccione ***DS: teléfonos serie 1400, 9500, 5400, 2400, T3, 440***.
   - Para puertos BST, seleccione ***BST: teléfonos serie T7000, M7000***.
4. Haga clic en **Aceptar**.
5. Continúe con la configuración básica 111 o haga clic en el icono guardar para guardar la configuración actualizada 112 y, luego, continúe.

7.8 Carga del archivo de licencia

El sistema IP Office requiere licencia para algunas funciones. Consulte Licencias 294. El archivo de licencia puede cargarse manualmente o cargarse previamente en la tarjeta SD del sistema 77.

¿Cómo se le agrega una licencia al sistema?

- Se carga al sistema un archivo XML que contiene el conjunto completo de licencias PLDS. El archivo de licencia es exclusivo para el número de serie de clave de la función de la tarjeta System SD instalada en el sistema.
    - La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.

Requerimientos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una licencia de sistema **Essential Edition** para la versión de IP Office específica que desea ejecutar.

Para cargar el archivo de licencia usando IP Office Manager, haga lo siguiente:

1. En la configuración del sistema, haga clic en **Licencia**.
2. El campo **Id. de host PLDS** muestra el número de serie de la tarjeta SD instalada en el sistema. Compruebe que este número coincida con el número para el que se emitieron las licencias.
    - La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.
3. Haga clic en **Agregar...** .
4. Para el tipo de licencia seleccione **PLDS** y haga clic en **Aceptar**.
5. Navegue hasta la ubicación del archivo XML que le proporcionaron que contiene las licencias. Seleccione el archivo y haga clic en **Abrir**.
6. Continúe con la configuración básica 112 o haga clic en el icono guardar para guardar la configuración actualizada 112 y, luego, continúe.

7.9 Guardado de la configuración

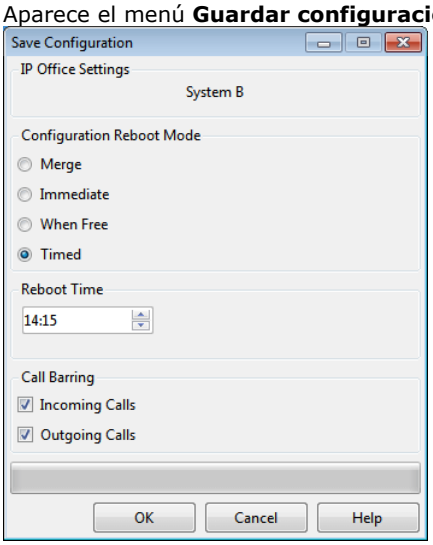
Una vez que haya finalizado la configuración básica, la nueva configuración debe guardarse nuevamente en el sistema. Es muy probable que esta acción requiera el reinicio del sistema.

Luego de guardar la configuración, vuelva a cargarla en IP Office Manager.

- Si modificó la configuración de la dirección IP, es posible que deba cambiar la configuración de su PC para volver a cargar la configuración.
- Luego de volver a cargar la configuración, todas las licencias deberían mostrarse como ***Válidas***.

Para guardar los cambios de configuración mediante IP Office Manager:

1. Haga clic en**Aceptar**para guardar todos los cambios del menú actual.
2. Haga clic en el icono .
3. Aparece el menú **Guardar configuración**.



- **Combinar**
  Este método se selecciona automáticamente si ninguno de los cambios de configuración realizados requiere un reinicio del sistema. Si este método se utiliza para una configuración que incluye cambios que si requieren un reinicio, dichos cambios no se aplican hasta que el sistema se reinicia de manera manual.
- **Inmediato**
  Este método guarda los nuevos cambios de configuración y, luego, reinicia el sistema. Se finalizan todas las llamadas actuales y los servicios en progreso. Este método se selecciona automáticamente si alguno de los cambios realizados hasta el momento requiere un reinicio antes de ser aplicados al sistema.
- **Permisos**
  Este método permite el uso del **Bloqueo de llamadas entrantes** y **Bloqueo de llamadas salientes**. Cuando los criterios para las opciones seleccionadas concuerdan, el sistema se reinicia.
- **Cronómetro (HH:MM)**
  Este método reinicia el sistema a la hora seleccionada. También se puede utilizar en conjunto con las opciones de bloqueo de llamada para reiniciar solo después del horario configurado cuando coincidan las opciones seleccionadas.
- **Bloqueo de llamadas entrantes**
  Se puede utilizar esta función junto con el método**Permisos** y el método de reinicio de **Cronómetro**. Cuando se lo selecciona, el sistema bloquea todas las llamadas entrantes. Sin embargo, permite que las llamadas existentes continúen hasta que finalicen.
- **Bloqueo de llamadas salientes**
  Se puede utilizar esta función junto con el método **Permisos** y el método de reinicio de **Cronómetro**. Cuando se lo selecciona, el sistema bloquea todas las llamadas salientes. Sin embargo, permite que las llamadas existentes continúen hasta que finalicen.
  - **ADVERTENCIA**
    Esta opción también bloquea la realización de llamadas de emergencia. Por lo tanto, siempre se la debe usar con precaución.

4. Seleccione las opciones requeridas y haga clic en **Aceptar**.

Configuración de seguridad básica

Luego de completar la configuración básica, debe seguir los procesos que se enumeran en el capítulo Seguridad del sistema 126.

Capítulo 8.

Configuración básica mediante IP Office Web Manager

8. Configuración básica mediante IP Office Web Manager

Esta sección aborda la configuración inicial básica de un sistema nuevo mediante IP Office Web Manager. El rango completo de configuración posible mediante IP Office Web Manager se cubre en el manual de IP Office Web Manager 12.

IP Office Web Manager no puede utilizarse actualmente para realizar los siguientes pasos de configuración básica. Si se requieren, utilice IP Office Manager en su lugar:

- **Cambio de numeración de extensión de usuario múltiple**.
- **Configuración del modo de operación de un módulo de expansión externo DS16B/30B**.

Resumen

1. **Conexión de red** 115
   Utilice IP Office Web Manager para conectarse al sistema nuevo.
2. **Configuración inicial** 117
   Se muestra el menú **Configuración inicial** la primera vez que IP Office Manager o IP Office Web Manager se conecta a un nuevo sistema.
3. **Carga del archivo de licencia** 119
   Cargue el archivo de licencia proporcionado por el sistema y verifique el estado de licencia de las licencias.
4. **Deshabilitar cualquier troncal no utilizada** 120
   Deshabilitar el uso de troncales y canales de troncales no disponibles.
5. **Seleccionar la fuente de reloj para troncales digitales** 121
   La modificación de la troncal digital utilizada para proporcionar la señal de reloj al sistema IP Office para realizar la sincronización de llamadas.
6. **Ingreso de prefijos de troncales** 123
   En sistemas donde se utiliza un predijo para la marcación exterior, asegúrese de ingresar el mismo prefijo a los números entrantes para permitir la devolución de llamadas.

Configuración de seguridad básica

Luego de completar la configuración básica, debe seguir los procesos que se enumeran en el capítulo Seguridad del sistema 126.

8.1 Conexión de red

La sección siguiente describe en detalle la forma en que un sistema IP Office nuevo determina la dirección IP que debe utilizar.

Resolución de la dirección IP y el modo DHCP

Al encender una unidad de control IP Office nueva o devuelta a los valores predeterminados, la unidad envía una petición para la información de la dirección IP a un servidor DHCP. Esto ocurre con el cable LAN conectado o desconectado. El proceso a continuación se realiza en forma separada para el puerto LAN (LAN1 en la configuración) y el puerto WAN (LAN2 en la configuración) en la parte posterior de la unidad de control IP Office.

- El sistema crea una solicitud DHCP de la información de la dirección IP que debe utilizarse.
- Si el servidor DHCP responde en aproximadamente 10 segundos, la unidad de control vuelve en forma predeterminada a ser un cliente DHCP y utiliza la información de la dirección IP proporcionada por el servidor DHCP.
- Si no hay respuesta de un Servidor DHCP, la unidad de control vuelve en forma predeterminada a ser el cliente DHCP, pero asume la siguiente dirección predeterminada:
  - Puerto LAN (LAN1): 192.168.42.1/255.255.255.0.
  - Puerto WAN (LAN2): 192.168.43.1/255.255.255.0.
  - Tome nota que IP Office no comprueba si estas son direcciones válidas o disponibles en la red.
- Los sistemas que se ejecutan en modos estándar de IP Office se pueden configurar como un servidor DHCP. Pueden también configurarse para proporcionar DHCP solamente a los teléfonos Avaya IP y/o para acceder por medio de conexiones por marcación remotas. Las opciones de servidor DHCP no son compatibles con sistemas que funcionan en modos IP Office Basic Edition.
- Cuando una unidad de control IP500 V2 obtuvo una dirección IP y parámetros de configuración del modo DHCP, conservará esos parámetros aun cuando se haya reiniciado la unidad sin un archivo de configuración presente en la tarjeta SD del sistema. Para eliminar completamente la configuración existente de dirección IP y modo DHCP, debe devolver la configuración del sistema a los valores predeterminados 168.

Conexión a la PC

Dependiendo de las condiciones aplicadas cuando se inició por primera vez la unidad de control de IP Office, puede conectarse una PC como sigue:

- **Si el sistema IP Office no está conectado a una red:**
  Conecte la PC directamente al IP Office. La PC debe estar configurada con una dirección válida en la misma red de los ajustes predeterminados del sistema IP Office descrito arriba.
- **Si el sistema IP Office está conectado a una red sin un servidor DHCP:**
  Conecte la PC directamente al IP Office. La PC debe estar configurada con una dirección válida en la misma red de los ajustes predeterminados del sistema IP Office descrito arriba.
- **Si el sistema IP Office está conectado a una red mediante un servidor DHCP:**
  Conecte la PC a la red. La PC debe estar configurada como cliente DHCP o con una dirección válida para la red.
- **Si el sistema IP Office utilizó una configuración generada previamente, haga lo siguiente:**
  Utilice las direcciones IP según lo establecido en la configuración. Asegúrese de que la PC se encuentre en la misma subred o en una red habilitada para enrutar a esa subred.

Avaya es compatible con los siguientes navegadores para IP Office Web Manager:

- **Microsoft Internet Explorer 10** y **11**.
- **Microsoft Edge**
- **Mozilla Firefox**
- **Google Chrome**
- **Safari**

Para iniciar sesión en un sistema mediante IP Office Web Manager

1. Introduzca la dirección IP del sistema IP Office. En el menú que aparece, haga clic en **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.

2. Aparece el menú para iniciar sesión en IP Office Web Manager.

3. Introduzca el nombre y la contraseña para la administración del sistema. Tanto el nombre como la contraseña predeterminados son ***Administrator***.

   - **Modo desconectado**
     Algunos cambios de configuración solo se pueden aplicar al sistema mediante un reinicio, por ejemplo, cambiar las configuraciones de línea. Para cambiar esas características necesita seleccionar el **Modo desconectado**. En ese modo, la parte superior de la ventana del navegador muestra un vínculo **Guardar en IP Office** que, cuando le hace clic, despliega un menú para reiniciar el sistema.

     - También puede cambiar a Modo desconectado después de iniciar sesión haciendo clic en y seleccionando **Modo desconectado**.

4. Haga clic en **Iniciar sesión**.

   a. Se le solicita que cambie todas las contraseñas predeterminadas.

   b. Para un sistema nuevo, aparece el menú de configuración inicial 101.

8.2 Configuración inicial

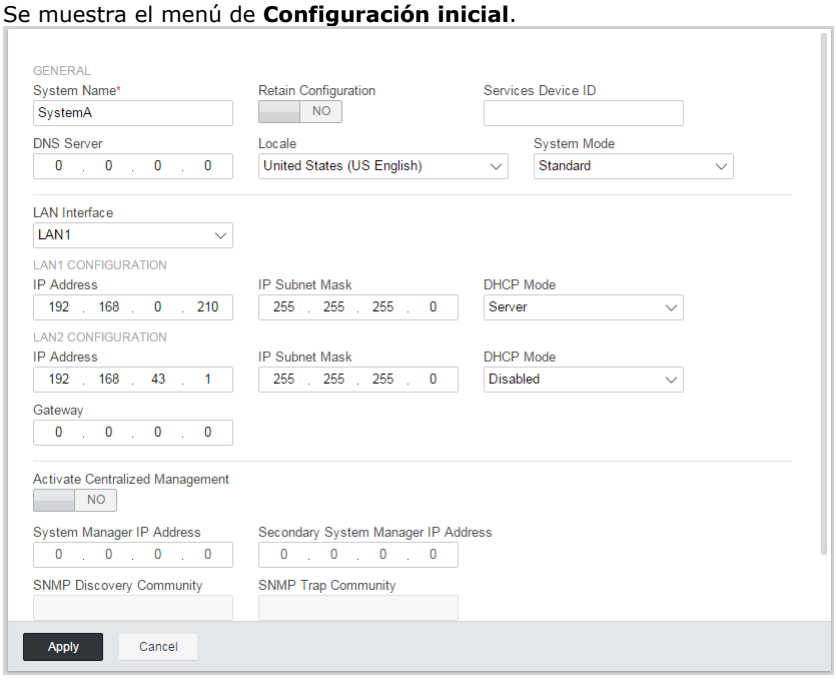
El menú de configuración inicial aparece la primera vez que IP Office Manager se conecta con un sistema nuevo o predeterminado.

- El menú de configuración inicial puede volver a ejecutarse en cualquier momento seleccionando **Archivo | Configuración avanzada | Configuración inicial** en IP Office Manager o **Acciones | Comandos de servicio | Configuración inicial en** IP Office Web Manager. Tenga en cuenta que esto elimina la mayor parte de la configuración del sistema existente.

Para comenzar la configuración inicial mediante IP Office Web Manager:

1. Conéctese al sistema utilizando un navegador 115. Tanto el nombre como la contraseña predeterminados son ***Administrator***.
2. Se le solicita que cambie las contraseñas predeterminadas.

   - **Contraseña de administrador**
     Esta contraseña se usa para acceder a la configuración de telefonía del sistema.
   - **Contraseña de administrador de seguridad**
     Esta contraseña se usa para acceder a la configuración de seguridad del sistema. Tenga en cuenta que, de manera predeterminada, la contraseña de administrador que se menciona arriba también puede utilizarse para la configuración de seguridad.
   - **Contraseña de sistema**
     Esta contraseña se usa para la actualización del sistema mediante IP Office Manager y también se puede usar para conectar System Monitor.
3. Ingrese las nuevas contraseñas y haga clic en **Guardar**.
4. Aparecerá un menú que le preguntará si desea permitir Google Analytics. Esta herramienta se utiliza para recolectar datos anónimos sobre el uso de Web Manager. La configuración puede cambiarse mediante el usuario de Web Manager luego de iniciar sesión.
5. Se muestra el menú de **Configuración inicial**.



6. Configure el **Modo de sistema** a **Estándar**.

7. Compruebe que la configuración coincida con la requerida por el sitio del cliente.
   - **Nombre del sistema:** Se utiliza como ayuda para identificar y acceder al sistema.
   - **Configuración regional:** Establece un rango de configuración predeterminada para que coincida con los requerimientos de telefonía de ese país. También establece el idioma predeterminado para el sistema y todos los usuarios.
   - **Configuración de la dirección IP:** Verifique que esta configuración, especialmente el **modo DHCP**, coincida con los requerimientos de la red del cliente. Alterne entre **LAN1** y **LAN2** para verificar la configuración de los puertos LAN y WAN respectivamente.
   - **En administración centralizada:** Esta configuración se utiliza para sistemas Branch en una red Avaya Aura. Consulte la documentación sobre instalación de Branch 12 por separado.
8. Haga clic en **Aplicar**. El sistema se reinicia usando las nuevas configuraciones. Después de que el sistema se reinicie, puede continuar con la configuración básica.
9. Vuelva a iniciar sesión en el sistema. Continúe con laCarga del archivo de licencia 119.

8.3 Carga del archivo de licencia

El sistema IP Office requiere licencia para algunas funciones. Consulte Licencias 294. El archivo de licencia puede cargarse manualmente o cargarse previamente en la tarjeta SD del sistema 77.

¿Cómo se le agrega una licencia al sistema?

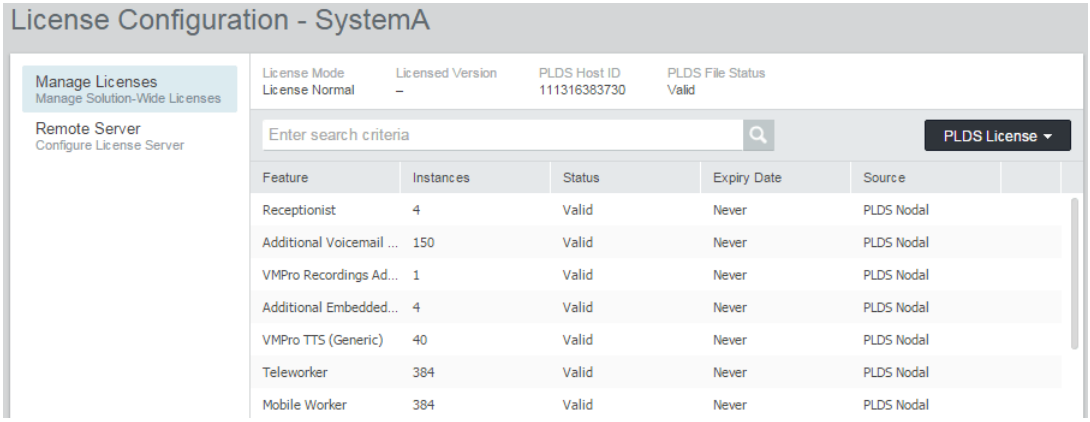
- Se carga al sistema un archivo XML que contiene el conjunto completo de licencias PLDS. El archivo de licencia es exclusivo para el número de serie de clave de la función de la tarjeta System SD instalada en el sistema.
    - La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.

Requerimientos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una licencia de sistema **Essential Edition** para la versión de IP Office específica que desea ejecutar.

Para cargar el archivo de licencia mediante IP Office Web Manager:

1. Mediante IP Office Web Manager 71, conéctese al sistema.
2. Seleccione **Configuración de sistema | Licencias**.
3. El campo **Id. de host PLDS** muestra el número de serie de la tarjeta SD instalada en el sistema. Compruebe que este número coincida con el número para el que se emitieron las licencias.
    - La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.
4. Haga clic en **Licencia PLDS**.
5. Seleccione **Enviar a IP Office** y haga clic en **Aceptar**.
6. Navegue hasta el archivo de licencia XML que tiene para el sistema y haga clic en**Aceptar**.
7. El archivo se carga al sistema y es leído. El menú debe enumerar las licencias y mostrar sus estados como **Válido**.



8. Vaya a Deshabilitación de las troncales no utilizadas 120.

8.4 Deshabilitación de las troncales no utilizadas

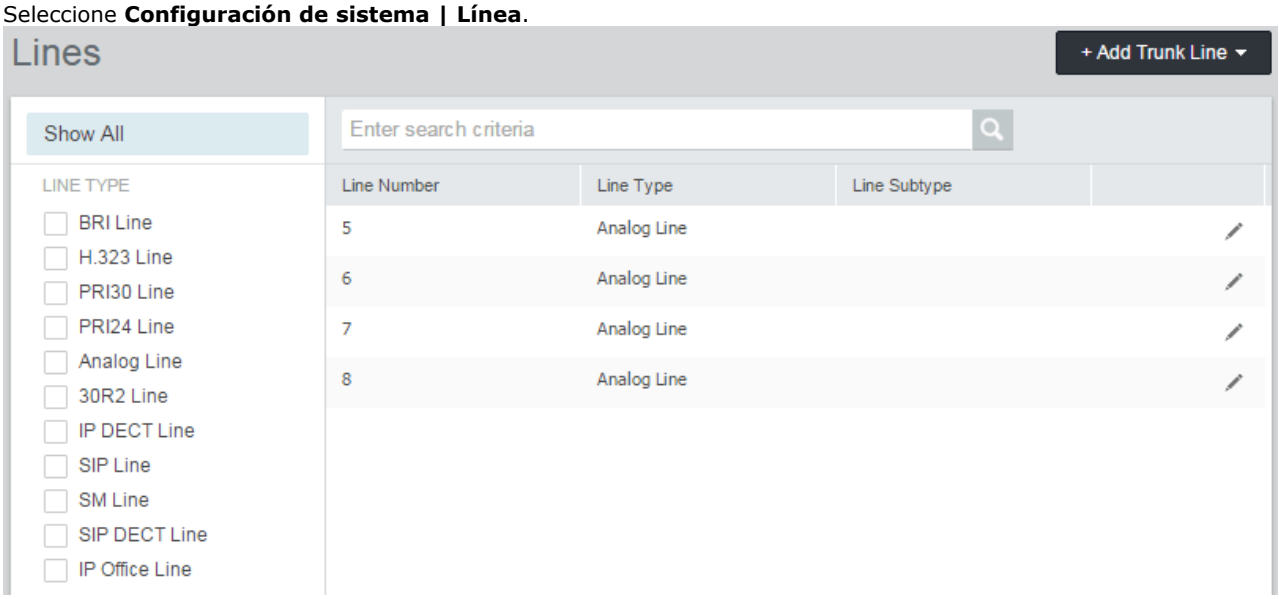
Cada tarjeta de troncal IP Office proporciona un número fijo de puertos de troncales con puertos de troncales digitales que soportan una cantidad fija de canales digitales. De forma predeterminada, la configuración de IP Office tiene entradas de configuración para todas las líneas troncales y canales posibles.

En aquellos casos donde la cantidad de troncales o canales de troncales en uso o con licencia es menor que la cantidad admitida por la tarjeta de troncales, es necesario inhabilitar las troncales y canales no utilizadas.

- ⚠ De no hacerlo, esto puedo ocasionar problemas con las llamadas salientes. Por ejemplo, en un sistema con una tarjeta de troncales ATM4 instalada pero con sólo dos troncales analógicas conectadas en realidad, de no inhabilitar las dos troncales restantes en la configuración de IP Office, esto ocasionará que fracase 50% de los intentos de llamada saliente. Esto se debe a que el sistema no puede detectar automáticamente el estado del servicio de troncales analógicas individuales.
  - Para modo Oficina En la versión 8.1 Feature Pack 1 y posteriores con cuatro tarjetas de troncales analógicas IP500 V2 y tarjetas combinadas ATM4 V2, el sistema puede detectar con troncales analógicas conectadas, de manera que puede tratar automáticamente puertos de troncales no conectados como fuera de servicio.
- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

Para deshabilitar troncales sin uso mediante IP Office Web Manager:

1. Mediante IP Office Web Manager 71, conéctese al sistema usando el **Modo desconectado**.
2. Seleccione **Configuración de sistema | Línea**.



3. Seleccione la troncal que necesita editar. Según el tipo de troncal, haga lo siguiente:
   - **Troncales analógicas**
     Para inhabilitar la troncal entera, en el formulario principal configure la opción **Admin** en ***Fuera de servicio***.
   - **Troncales BRI, E1 PRI, S0 y QSIG**
     Para inhabilitar la troncal entera, en el formulario principal configure la opción **Admin** en ***Fuera de servicio***. De lo contrario, configure la cantidad de canales según la cantidad total de canales suscritos.
   - **Troncales T1, T1 PRI y E1R2**
     Para inhabilitar la troncal entera, en el formulario principal configure la opción **Admin** en ***Fuera de servicio***. De lo contrario, seleccione la ficha Canales y configure los canales no utilizados como **Fuera de servicio**.
     - Para T1, configure **Tipo** como ***Fuera de servicio***.
     - Para T1 PRI, configure el campo **Admin** en ***Fuera de servicio***.
     - En troncales E1R2, configure **Tipo de señalización de línea** como ***Fuera de servicio***.
4. Vaya a Configuración de la fuente del reloj de la troncal digital. 121

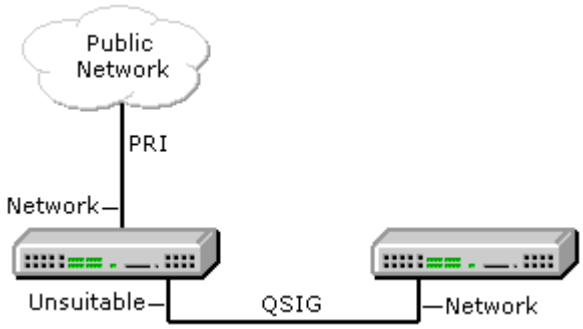
8.5 Configuración de la fuente de reloj para troncales digitales

Las troncales digitales requieren que el sistema de teléfono en cada extremo de la troncal comparta una señal de reloj para asegurar la sincronización de la señalización de llamada. El IP Office puede obtener y utilizar la señal de reloj de cualquiera de sus troncales digitales. Típicamente, se utiliza la señal de reloj proporcionada por una troncal digital en a central de comunicaciones de la oficina, ya que ésta es la fuente de reloj más precisa y confiable.

De no haber una fuente de reloj disponible, el sistema puede utilizar su propio reloj interno si es necesario. Sin embargo, se prefiere una fuente troncal externa. Para hacerlo, la configuración **Calidad del reloj** en cada línea de la configuración de IP Office contiene uno de los valores siguientes:

- ***Red***
  De estar disponible, se debe utilizar la señal de reloj proveniente de esta troncal como la fuente de reloj para la sincronización de llamadas. Si hay varias troncales con esta configuración, la troncal utilizada se determina en el orden de las ranuras 1 a 4 y, luego, por puerto en cada ranura.
- ***Reserva***
  De estar disponible, se debe utilizar la señal de reloj proveniente de esta troncal como la fuente de reloj en caso que ninguna de las troncales definidas como ***Red*** puedan proporcionar una fuente de reloj. Si hay varias troncales con esta configuración, la troncal utilizada se determina en el orden de las ranuras 1 a 4 y, luego, por puerto en cada ranura.
- ***Inadecuada***
  La fuente de reloj de esta troncal no se utilizará como la fuente de reloj.

En el ejemplo a continuación, el primer sistema IP Office es configurado para emplear la troncal de red pública como su fuente de reloj, ignorando la fuente de reloj posible proveniente de la troncal QSIG. El otro sistema IP Office emplea la señal de reloj recibida del primer IP Office en la troncal QSIG y su fuente de reloj correspondiente. Por tanto, ambos sistemas IP Office utilizan la misma fuente de reloj, proveniente de la red de comunicaciones pública.



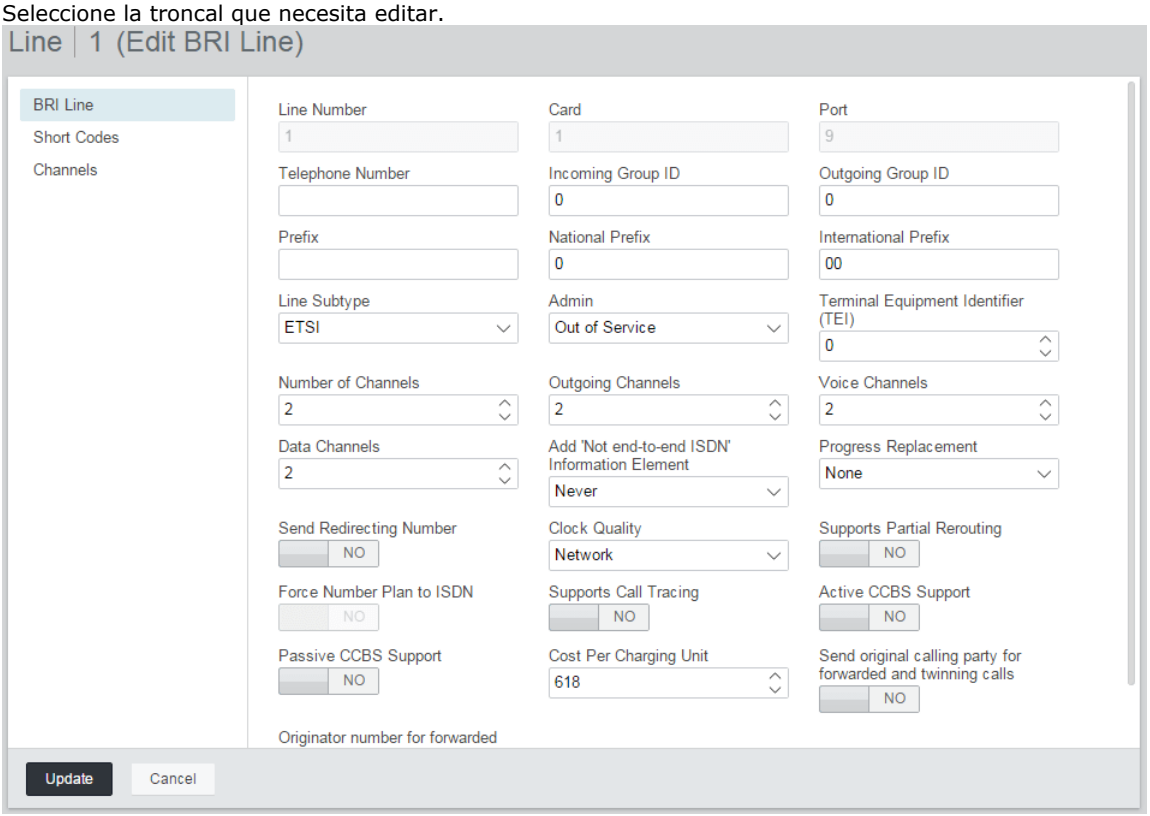
Visualización de la fuente de reloj actual

La fuente de reloj actual utilizada por el sistema IP Office aparece en la página **Recursos** dentro de System Status Application.

Para configurar la fuente de calidad del reloj de una troncal por medio de IP Office Web Manager:

1. Mediante IP Office Web Manager 71, conéctese al sistema usando el **Modo desconectado**.
2. Seleccione **Configuración de sistema | Línea**.

3. Seleccione la troncal que necesita editar.



4. Configure la **Calidad del reloj** en la configuración requerida y haga clic en **Actualizar**.
   - Asegúrese de que solamente una troncal esté configurada como ***Red***. De preferencia, ésta debería ser una troncal digital directa a la central de comunicaciones de la oficina.
   - Otra troncal puede configurarse como ***Reserva*** en caso de perder la conexión de troncal con la Red. De ser posible, ésta debería ser una troncal de un proveedor distinto, ya que esto disminuye las probabilidades de que ambas fuentes fallen al mismo tiempo.
   - Compruebe que las troncales digitales restantes estén configuradas como ***Inadecuado***.
5. Vaya a Configuración de los prefijos de troncales.

8.6 Configuración de los prefijos troncales

De manera predeterminada, los sistemas con una tarjeta SD del sistema U-Law se devuelven a los valores predeterminados mediante un prefijo 9 para llamadas externas. Los sistemas se iniciaron con una tarjeta SD del sistema A-Law predeterminada a ningún prefijo (cualquier marcación que no coincida con un número interno se supone que es un número externo).

Cuando se ha implementado un prefijo para las llamadas salientes, debe agregarse este mismo prefijo a los ajustes de las troncales. Se utiliza entonces el prefijo troncal de la siguiente manera:

- **Llamadas entrantes**
  En las llamadas entrantes, el prefijo establecido de la troncal se agrega a cualquier Id. de persona que llama entrante que se recibe con la llamada y se almacena en el registro de llamadas de los teléfonos, etc. El prefijo debe tener un formato que permita que la Id. de persona que llama resultante pueda ser utilizada por las aplicaciones y teléfonos del sistema para realizar devoluciones de llamada. Por ejemplo, si el sistema se configura para que se requiera un 9 para indicar una llamada saliente, la troncal debe agregar un 9 a la Id. de la persona que llama entrante con el objetivo de que dicha Id. pueda utilizarse para realizar devoluciones de llamada.
- **Llamadas salientes**
  En las llamadas salientes, los códigos cortos utilizados para enrutar la llamada a una troncal deben quitar todos los prefijos de marcación externos (por ejemplo, 9) para que el número marcado desde el sistema a la troncal sea adecuado para el enrutado por parte del proveedor de la troncal.

Configurar los prefijos troncales mediante IP Office Web Manager:

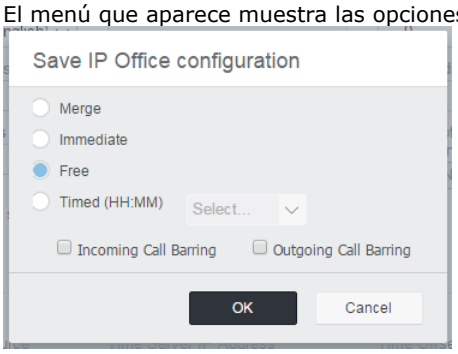
1. Mediante IP Office Web Manager 71, conéctese al sistema usando el **Modo desconectado**.
2. Seleccione **Configuración de sistema | Línea**.
3. Seleccione la troncal que necesita editar. La ubicación de la configuración **Prefijo** varía según el tipo de troncal. Algunos tipos de troncales tienen un solo campo de prefijo. Otros tipos de troncales pueden tener campos de prefijos separados para llamadas nacionales, internacionales y de otro tipo.
4. Guarde la configuración 124.

8.7 Guardado de la configuración

De manera predeterminada, IP Office Web Manager hace cambios en el momento en la configuración del sistema Sin embargo, si se usa en el modo desconectado, se necesita guardar los cambios en el sistema y reiniciar el sistema mediante el siguiente proceso.

Para guardar la configuración mediante IP Office Web Manager:

1. Haga clic en **Actualizar** para confirmar los cambios realizados en el menú actual.
2. En la parte superior del navegador, haga clic en**Guardar en IP Office**.
3. El menú que aparece muestra las opciones para guardar la configuración.



- **Combinar**
  Este método se selecciona automáticamente si ninguno de los cambios de configuración realizados requiere un reinicio del sistema. Si este método se utiliza para una configuración que incluye cambios que si requieren un reinicio, dichos cambios no se aplican hasta que el sistema se reinicia de manera manual.
- **Inmediato**
  Este método guarda los nuevos cambios de configuración y, luego, reinicia el sistema. Se finalizan todas las llamadas actuales y los servicios en progreso. Este método se selecciona automáticamente si alguno de los cambios realizados hasta el momento requiere un reinicio antes de ser aplicados al sistema.
- **Permisos**
  Este método permite el uso del **Bloqueo de llamadas entrantes** y **Bloqueo de llamadas salientes**. Cuando los criterios para las opciones seleccionadas concuerdan, el sistema se reinicia.
- **Cronómetro (HH:MM)**
  Este método reinicia el sistema a la hora seleccionada. También se puede utilizar en conjunto con las opciones de bloqueo de llamada para reiniciar solo después del horario configurado cuando coincidan las opciones seleccionadas.
- **Bloqueo de llamadas entrantes**
  Se puede utilizar esta función junto con el método**Permisos** y el método de reinicio de **Cronómetro**. Cuando se lo selecciona, el sistema bloquea todas las llamadas entrantes. Sin embargo, permite que las llamadas existentes continúen hasta que finalicen.
- **Bloqueo de llamadas salientes**
  Se puede utilizar esta función junto con el método **Permisos** y el método de reinicio de **Cronómetro**. Cuando se lo selecciona, el sistema bloquea todas las llamadas salientes. Sin embargo, permite que las llamadas existentes continúen hasta que finalicen.

  - **ADVERTENCIA**
    Esta opción también bloquea la realización de llamadas de emergencia. Por lo tanto, siempre se la debe usar con precaución.

4. Seleccione las opciones requeridas y haga clic en **Aceptar**.

Configuración de seguridad básica

Luego de completar la configuración básica, debe seguir los procesos que se enumeran en el capítulo Seguridad del sistema 126.

Capítulo 9.
Seguridad del sistema

9. Seguridad del sistema

El sistema IP Office y sus aplicaciones son compatibles con una gama de funciones que sirven para vincular este software con los usuarios de manera más segura. Los detalles completos de las opciones disponibles se describen en el **Manual de seguridad de la plataforma Avaya IP Office** 12 .

Esta sección sólo abarca algunos cambios básicos recomendados para contribuir a una mayor protección del nuevo sistema.

1. **Cambio de la configuración de seguridad predeterminada** 127
2. **Cambio de la contraseña de usuario remoto** 128
3. **Deshabilitación de la compatibilidad con líneas troncales SIP** 129
4. **Deshabilitación de la compatibilidad con teléfonos H.323** 129

Recomendaciones adicionales:

- Si la red en la que está conectado IP Office tiene acceso público externo a Internet, ese acceso debe controlarse por medio de un dispositivo de seguridad adicional como un firewall y, en el caso de VoIP, Session Border Controller (SBC).
- Si no se usa LAN2 (el puerto WAN), asegúrese de que no esté conectado a la red.

9.1 Cambio de la configuración de seguridad predeterminada

Este proceso cubre los cambios de seguridad mínimo necesarios para la ejecución del servicio IP Office en el servidor. Para obtener detalles completos de todas las configuraciones de seguridad de IP Office, consulte la ayuda de IP Office Manager.

Para establecer la configuración de seguridad inicial:

1. Inicie IP Office Manager.
2. Seleccione **Archivo | Opciones avanzadas | Configuración de seguridad**.
   - Si el **Menú Seleccionar IP Office** no aparece, haga clic en .
3. Seleccione el servidor y haga clic en **Aceptar**.
4. Ingrese el nombre de usuario y la contraseña del administrador.
5. En los sistemas con configuración de seguridad predeterminada, se muestra una serie de advertencias. Preste atención a cada advertencia y haga clic en **Aceptar**.
6. Seleccione y cambie las siguientes contraseñas:
   a. **Contraseña del sistema**
   IP Office Manager utiliza esta contraseña para actualizar el software del sistema. Haga clic en el botón **Cambiar** e ingrese una contraseña nueva. Haga clic en **Aceptar**.
   b. **Contraseña de correo de voz**
   El servidor de Voicemail Pro usa esta contraseña para conectarse con el sistema IP Office. Si se la establece, también es necesario establecer la misma contraseña en las preferencias del servidor de correo de voz usando el cliente Voicemail Pro.
   c. **Contraseña de monitor**
   La aplicación System Monitor usa esta contraseña para conectarse al sistema IP Office a través de UDP o TCP. Si no se establece, en su lugar se usa a **Contraseña del sistema** establecida más arriba.
7. La sección **Controles de aplicación** indica una serie de interfaces no seguras que usa el sistema. Anule la selección de las opciones que no requieren las aplicaciones de clientes planeadas. Al marcar o desmarcar los controles, la sección **Compatibilidad de aplicaciones** que se encuentra debajo comienza a reflejar el efecto del cambio.

Control de aplicación	Usado por	Notas
Servidor TFTP	System Monitor	Si se desactiva, además de desactivar las opciones TFTP que se encuentran debajo, el sistema no admite el componente de visualización de red de la aplicación System Monitor.
Lectura de directorio TFTP	IP DECT	Si se desactiva, DECT opera sin la función directorio de sistema.
Correo de voz TFTP	Voicemail Pro	Actívelo sólo si elsistema usa un servidor de correo de voz anterior a IP Office versión 9.1.
Código del programa	IP Office Manager	Se usa para hacer actualizaciones desde IP Office Manager, se recomienda desactivarlo si no es necesario.
DevLink	DevLink	
TAPI	TAPI/DevLink	Desactívelo excepto si el sitio cliente usará aplicaciones TAPI junto con IP Office.
Lectura de directorio HTTP	one-X Portal for IP Office	Actívela solamente si se usa one-X Portal for IP Office. Si se desactiva, one-X Portal for IP Office opera sin la función directorio personal.
Escritura de directorio HTTP	one-X Portal for IP Office	Actívela solamente si se usa one-X Portal for IP Office. Si se desactiva, one-X Portal for IP Office opera sin la función de actualización del directorio personal.

8. Haga clic en **Aceptar**.
9. Haga clic en **Usuarios del servicio**. De manera predeterminada, sólo los usuarios ***Administrator*** y ***EnhTcpaServer*** están habilitados.
   a. Seleccione ***EnhTcpaService***. Este servicio es utilizado por one-X Portal for IP Office. Si instalará one-X Portal for IP Office, recomendamos cambiar la contraseña sólo después de completar la instalación. Si no se instalará one-X Portal for IP Office:
      - Haga clic en el botón **Cambiar** e ingrese una contraseña nueva para el servicio.
      - Haga clic en **Estado de la cuenta** y seleccione ***Desactivado***.
      - Haga clic en **Aceptar**.

10.Haga clic en el icono para guardar los cambios de seguridad.

9.2 Cambio de contraseña de usuario remoto

La configuración de IP Office contiene a un usuario cuya contraseña se utiliza como la predeterminada para acceder por marcación remota a la red IP Office. Es recomendable cambiar la contraseña de este usuario.

Para cambiar la contraseña de usuario remoto:

1. Inicie IP Office Manager 68 y conéctese al sistema de IP Office.
2. Haga clic en **Usuarios** y en la lista de usuarios haga clic en **Remote Manager**.
3. En la ficha **Usuario** ingrese una nueva contraseña para el usuario y haga clic en **Aceptar**.
4. Haga clic en el icono para guardar la configuración actualizada en el sistema de IP Office.

9.3 Deshabilitación de la compatibilidad con líneas troncales SIP

El sistema IP Office admite líneas troncales SIP. Si estas no se requieren para la instalación del cliente, recomendamos deshabilitar la compatibilidad con líneas troncales SIP del sistema.

Para deshabilitar la compatibilidad con líneas troncales SIP:

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

1. Inicie IP Office Manager 68 y reciba la configuración del sistema IP Office.
2. Seleccione **Sistema**.
3. Seleccione **LAN1** y seleccione la ficha **VoIP**.
4. Verifique que la opción **Activar líneas troncales SIP** no esté seleccionada.
5. Repita el proceso para **LAN2**.
6. Haga clic en el icono guardar para almacenar la configuración actualizada en el sistema IP Office.

9.4 Deshabilitación de la compatibilidad con teléfonos H.323

IP Office es compatible con los teléfonos IP H.323 de forma predeterminada. Si estos no se requieren para la instalación del cliente, recomendamos deshabilitar la compatibilidad con teléfonos H.323 del sistema.

Para deshabilitar la compatibilidad con teléfonos H.323:

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

1. Inicie IP Office Manager 68 y reciba la configuración del sistema IP Office.
2. Seleccione **Sistema**.
3. Seleccione **LAN1** y seleccione la ficha **VoIP**.
4. Verifique que la opción **Activar Gatekeeper H323** no esté seleccionada.
5. Verifique que la opción **Habilitar extn. remota H323** no esté seleccionada.
6. Repita el proceso para **LAN2**.
7. Haga clic en el icono guardar para almacenar la configuración actualizada en el sistema IP Office.

Capítulo 10.
Ingreso

10. Ingreso

La integración es un proceso que le permite registrar un sistema IP500 V2 para soporte técnico y mantenimiento remoto de Avaya. El proceso de integración se logra usando la interfaz IP Office Web Manager.

Esta sección es un breve resumen de integración. Para obtener más detalles sobre la configuración y administración de los servicios SSL VPN, consulte la Guía de soluciones SSL VPN de Avaya IP Office. Puede descargar esta guía de http://support.avaya.com.

Pasos resumen

1. Iniciar sesión en IP Office Web Manager
2. **Integrar el sistema**
   Este proceso tiene 3 pasos principales:
   a. **Obtener un archivo de inventario**
      Debe exportar desde el sistema un archivo que contenga un inventario del equipo dentro del sistema. Este archivo es necesario para registrar el sistema para soporte técnico.
   b. **Registrar el sistema**
      Registre el sistema en el sitio web Global Registration Tool de Avaya y suba el archivo de inventario del sistema. Una vez que el sistema esté registrado, se entrega un archivo de integración para el sistema. Este archivo contiene los ajustes de configuración para el enlace de servicio SSL VPN.
   c. **Subir archivo de integración**
      Subir el archivo de integración al sistema. La información que contiene el archivo se utiliza para actualizar las configuración del sistema.

Cambios de configuración provocados por la integración

Cuando se sube un archivo de integración al sistema IP500 V2, puede realizar un número de cambios a la configuración del sistema. Es importante considerar estos potenciales cambios y asegurarse de que no sean reescritos o removidos.

Estos cambios son los siguientes. Aquellos marcados con * son opcionales y dependen de la configuración incluida en el archivo de integración por el proveedor de servicio.

- **Servicio SSL VPN**
  Se agrega un nuevo servicio SSL VPN a la sección de servicios de la configuración.
- **Alarmas SNMP***
  SNMP se puede configurar y 2 trampas de la alarma de SNMP se pueden agregar a la configuración. Considere que esto sobrescribirá cualquier configuración de SNMP existente si ya se ha configurado SNMP.
- **Códigos cortos***
  Se pueden agregar códigos cortos usando las acciones ***Establecer servicio nocturno de grupo de búsqueda*** y ***Borrar el servicio nocturno del grupo de búsqueda***. Estos se pueden utilizar para habilitar y deshabilitar el servicio SSL VPN.
- **Ruta IP***
  Se puede agregar a las rutas IP en la configuración una ruta IP estática para el servicio SSL VPN.
- **Certificado de seguridad**
  A la configuración de seguridad del sistema se les agrega un certificado de seguridad para el servicio SSL VPN.

10.1 Ingreso

1. Inicie sesión en IP Office Web Manager 71.

   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.

   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.

2. Haga clic en **Acciones** y seleccione **Integración**. Se mostrará el menú de integración.

   - **¿Está usando el hardware de la serie TAA?**
     Los sistemas adquiridos según las Normas federales de adquisición (FAR) de Estados Unidos (FAR) deben cumplir con los requisitos de Trade America Act (TAA). Para varios elementos del hardware de IP Office existen variantes TTA compatibles. Seleccione esta opción si el sistema IP Office incluye hardware TAA 310. Por lo general esto se indica cuando TAA aparece en la etiqueta en la parte posterior de la unidad de control del sistema.

3. Haga clic en **Obtener archivo de inventario** para descargar un archivo de inventario.xml para el sistema. Cuando registra el sistema IP Office para asistencia remota, el archivo de inventario se requiere como parte del registro y se carga en Global Registration Tool (GRT) de Avaya donde los datos de inventario se completan en la base de datos Avaya Customer Support (ACS).

4. Haga clic en **Registro de IP Office** para registrar el sistema en el sitio web de Global Registration Tool (GRT) de Avaya.

5. Cuando esté registrado, puede descargar un archivo de integración para el sistema desde el sitio web Global Registration Tool de Avaya. Este archivo contiene la configuración requerida para establecer una conexión VPN SSL entre el sistema IP Office y un servidor Avaya VPN Gateway (AVG).

6. Utilice la lista desplegable **Subir archivo de integración** sección para subir el archivo de integración al sistema.

Capítulo 11.

Administración de la tarjeta SD

11. Administración de la tarjeta SD

La unidad de control IP500 V2 tiene dos ranuras para tarjetas SD con la etiqueta **System SD** y **SD opcional** respectivamente. Se usan de la siguiente manera.

- **Tarjeta System SD**
  Debe haber una tarjeta System SD de Avaya instalada en esta ranura en todo momento. Que contiene copias del firmware y la configuración de IP Office, y que se utiliza como memoria no volátil de la unidad de control IP500 V2.
  - Cada tarjeta SD Avaya System tiene un número de serie exclusivo que se usa para generar y validar licencias.
  - La tarjeta también guarda los avisos necesarios para el funcionamiento del Embedded Voicemail y permite guardar mensajes de correo de voz incorporado.
  - Antes de un apagado o reinicio planeado del sistema IP Office, la configuración actual ejecutándose en la memoria RAM del sistema IP Office se copia a la carpeta **/primary** en la tarjeta System SD y en la memoria no volátil del sistema.
  - Después de un reinicio del sistema, la unidad de control IP500v2 carga el software dentro de la carpeta **/primary** en la unidad de control IP500 V2. En caso de no encontrar el software requerido o en caso que no sea válido, se utiliza una secuencia de opciones de respaldo; consulte la sección Inicio desde tarjetas SD 138 para obtener la información completa.
  - Después de un reinicio del sistema, la unidad de control IP500v2 carga el archivo de configuración (si lo hay) dentro de la carpeta **/primary** en la unidad de control IP500 V2. De no encontrar un archivo, el sistema lo buscará en su memoria interna no volátil. De no encontrar una copia del archivo, el sistema generará un archivo de configuración predeterminado. Consulte la sección Inicio desde tarjetas SD 138 para obtener la información completa.
  - Una vez al día (aproximadamente entre 00:00 y 00:30) el IP Office copia la configuración actual ejecutándose en RAM en la carpeta **/primary** de la tarjeta.
  - Los cambios a la configuración efectuados con IP Office Manager se guardan primero a la copia del archivo de configuración en la tarjeta, para después unificarse a la configuración que se ejecuta en la memoria RAM del sistema IP Office.
  - El bloqueo de escritura en las tarjetas dentro de una ranura de tarjetas System SD es ignorado.
- **Tarjeta SD Opcional**
  No es necesario que haya una tarjeta presente en esta ranura para la operación normal del IP Office. La ranura puede servir para realizar distintas acciones de mantenimiento.
  - Se puede insertar una tarjeta con software o configuración actualizada de IP Office para después transferir dichos archivos a la tarjeta System SD a fin de actualizar el sistema IP Office.
  - El contenido entero de la tarjeta System SD puede copiarse en la tarjeta SD opcional mientras se está ejecutando IP Office.
  - Se respeta el bloqueo de escritura en las tarjetas dentro de la ranura de tarjetas System SD.

⚠ **Extracción de la tarjeta**	Es necesario siempre apagar 153 las tarjetas antes de extraerlas cuando el sistema está en ejecución. Aunque las luces LED de la ranura de la tarjeta indican cuándo se están escribiendo datos en una tarjeta, la ausencia de parpadeos de la luz LED no es una medida de precaución suficiente. Apagar la tarjeta inhabilita el correo de voz incrustado y IP Office Web Manager. Si se extrae la tarjeta **System SD**, las funciones con licencias basadas en el número de serie de la tarjeta continúan operando por hasta dos horas.

Especificaciones de las tarjetas

Se pueden utilizar tarjetas de marcas distintas a Avaya dentro de la ranura **SD opcional** siempre y cuanto cumplan o superen el estándar siguiente:

- SDHC 4GB mínimo Clase 2+. Formato FAT32 con una sola partición. (las tarjetas SD Avaya IP Office son de 8 GB, las tarjetas anteriores eran de 4 GB.)

Carpetas de la tarjeta SD

La carpeta de la tarjeta **System SD /system** contiene las siguientes subcarpetas:

- **/primary**
  Contiene los archivos de firmware para la unidad de control de IP Office, los módulos de expansión externos y los teléfonos compatibles. Esta carpeta puede también contener archivos de música en espera y archivos de claves de licencias. Este es el conjunto principal de los archivos empleados por el sistema IP Office para el arranque. También contiene una copia almacenada de la configuración del sistema de IP Office.
- **/backup**
  Contiene una copia de la carpeta principal en algún punto previo. Con ayuda de IP Office Manager o SSA, puede invocar manualmente una copia de seguridad del contenido en la carpeta principal de archivos, o bien como parte de la actualización de software de IP Office con ayuda de IP Office Manager.
- **/backup_apl**
- **/lvmail**
  Contiene los avisos del sistema utilizados por el Embedded Voicemail. Observe que los mensajes del buzón de voz y los saludos se almacenan en una sub-carpeta dentro de la carpeta **/dynamic**.
    - La sub-carpeta **/AAG** se utiliza para guardar saludos del asistente automático de Embedded Voicemail.
- **/doc**
  Contiene la documentación relativa a instalación inicial del sistema.
- **/dynamic**
  Contiene los archivos utilizados por el sistema IP Office, los cuales son conservados durante un reinicio del sistema IP Office.
    - La sub-carpeta **/lvmail** se utiliza para almacenar mensajes de correo de voz de usuario y para grupos, grabaciones de nombres y anuncios. Sin importar la capacidad de la tarjeta, la capacidad de almacenamiento para el buzón de Embedded Voicemail estará limitada a 25 horas.
- **/temp**
  Contiene archivos temporales utilizados por el sistema IP Office, los cuales no son conservados durante un reinicio del sistema IP Office.
- **/ws**

La tarjeta **SD opcional** puede contener un conjunto de carpetas similar. Estas sirven como una copia de seguridad adicional, o bien pueden usarse como el origen para una actualización del contenido de la tarjeta System SD.

11.1 Inicio desde tarjetas SD

Cuando se enciende, la unidad de control IP500 V2 busca un archivo binario ip500v2.bin válido para cargar. Esto lo realiza usando la posible fuente a continuación en el orden que aparece, y saltando a la siguiente fuente si el archivo no está presente o no es válido.

1. Tarjeta System SD, carpeta ***/primary***.
2. La memoria propia, no volátil, de la unidad de control. Una vez que se ha instalado un sistema, emplea su memoria no volátil para conservar copias de la configuración y los archivos binarios de sistema que utiliza. Estos archivos pueden utilizarse para restaurar la operación durante un reinicio del sistema. Observe que aunque el sistema puede iniciarse dese la memoria no volátil, es necesario que la tarjeta System SD esté presente para el correcto funcionamiento del sistema.
3. Tarjeta System SD, carpeta ***/backup***.
4. Tarjeta SD Opcional, carpeta ***/primary***.
5. Tarjeta SD Opcional, carpeta ***/backup***.
6. De no encontrar un archivo, la unidad de control recurre a enviar solicitudes BOOTP a la red. IP Office Manager puede responder a la solicitud BOOTP. Consulte Eliminación del firmware operacional 203.

Una vez que se ha encontrado un archivo ip500v2.bin válido, la unidad de control de IP Office carga este firmware. La fuente desde donde se cargó el archivo binario de la unidad de control se utilizará en lo subsecuente para cargar los archivos posteriores.

Carga del archivo de configuración

Una vez instalados los archivos necesarios de firmware del sistema como se describe más arriba, la unidad de control IP500 V2 requiere un archivo de configuración:

- Si la unidad de control IP500 V2 fue iniciada utilizando archivos binarios desde una ubicación de tarjeta SD, buscará un archivo válido de configuración en la misma ubicación.
  - Si existe un archivo de configuración válido, se carga.
  - Si se encuentra un archivo de configuración existente que no es válido, se carga la copia de la configuración de la memoria no volátil si es que está presente; de lo contrario, adopta una configuración predeterminada.
  - Si no hay un archivo de configuración presente, utilice la copia en la memoria no volátil como se describe arriba a menos que el reinicio sea como resultado de un comando predeterminado del sistema.
- Si la unidad de control IP500 V2 fue iniciada utilizando archivos binarios desde su memoria no volátil, también cargará la copia de la configuración desde esa ubicación.
  - Indicará una alarma de inicio (vea abajo).
  - Intentará restaurar el archivo de firmware de la carpeta **/primary** en las tarjetas System SD desde a memoria no volátil.
  - No ocurre el proceso normal de reinicio para actualizar el firmware del módulo de expansión. Si se utiliza el comando **Archivo | Avanzadas | Actualización** sólo los módulos de expansión externos conectados físicamente en el sistema aparecerán para la actualización.

Operación después del inicio

Durante la operación normal, los archivos de configuración y binarios enviados a la tarjeta **/primary** carpeta mediante IP Office Manager también se escriben en la memoria no volátil.

Si el sistema se ha iniciado desde a memoria no volátil debido a un problema con la tarjeta SD, aún es posible actualizar el archivo ip500v2.bin con ayuda del asistente de actualizaciones IP Office.

Alarmas de inicio

El siguiente procedimiento corresponde si el sistema IP500 V2 se inicia usando un software diferente del guardado en la carpeta **/primary** de la tarjeta System SD.

- Aparecerá una alarma en System Status Application. También se generará una alarma si la tarjeta está en una ranura que no es compatible. Estas alarmas también pueden emitirse como alarmas SNMP, Syslog o de correo electrónico.
- IP Office Manager e menú **Seleccionar IP Office** hará aparecer un icono que indica si el sistema IP Office se ejecuta utilizando software distinto al contenido en la carpeta principal de la tarjeta System SD.
- Esta configuración puede visualizarse, pero es de sólo lectura. Si intenta enviar una configuración al sistema, obtendrá el mensaje de error ***Fallo al guardar datos de configuración. (Error interno)***.

Método alterno a la carpeta principal de la tarjeta System SD

Se puede forzar a la unidad de control a ignorar la carpeta ***/primary*** de la tarjeta System SD, así como su memoria no volátil durante el inicio. Puede lograr esto oprimiendo el botón **Aux** mientras realiza el encendido de la unidad de control.

Esta acción puede ser necesaria si, después de una actualización al sistema de IP Office, se decide que es necesario retroceder al firmware y la configuración de la copia de seguridad. El empleo del botón **Aux** debe restaurar la operación del sistema al utilizar los archivos de la carpeta ***/backup*** mientras el instalador a continuación restaura el contenido de la carpeta ***/primary*** a una versión anterior.

11.2 Creación de una tarjeta SD de IP Office

Los procesos a continuación aplican a las tarjetas SD de Avaya IP Office SD. También aplican a tarjetas SD que no son de Avaya para su uso en la ranura para la tarjeta SD opcional del sistema. En la ranura de SD del sistema sólo deben insertarse tarjetas SD del sistema Avaya.

La tarjeta debe tener el siguiente formato.

- SDHC 4GB mínimo Clase 2+. Formato FAT32 con una sola partición. (las tarjetas SD Avaya IP Office son de 8 GB, las tarjetas anteriores eran de 4 GB.)
- ⚠ **PRECAUCIÓN**
  Para dar formato a las tarjetas SD de Avaya, utilice únicamente los comandos de formato de IP Office Manager y System Status Application. Si se formatean las tarjetas con cualquier otro método, se elimina el número de serie usado para la licencia de IP Office desde la tarjeta.
- **ADVERTENCIA: Versión IP Office Manager**
  Este proceso utiliza archivos de software provistos por la versión instalada de IP Office Manager que está en uso. Debe asegurarse de que la versión de IP Office Manager que está en uso concuerde con la versión de software requerida.

Creación de una tarjeta en una PC local

Puede ejecutar estos procesos en una tarjeta SD insertada en un lector de tarjeta en la PC IP Office Manager. Puede después emplear esta tarjeta en la ranura de tarjeta SD del sistema de un nuevo sistema, o bien en la ranura para tarjeta SD opcional de un sistema existente para actualizar dicho sistema.

Formateo de una tarjeta SD

Las tarjetas Avaya SD sólo deben formatearse utilizando las opciones de formateo proporcionadas por las aplicaciones de IP Office. Este proceso normalmente no es necesario con las tarjetas Avaya SD, a menos que sospeche que la tarjeta ha recibido un formato incorrecto en otro momento.

- ⚠ **PRECAUCIÓN: Todos los archivos serán eliminados**
  Observe que este proceso elimina todos los archivos y carpetas existentes en la tarjeta. Una vez que se ha formateado una tarjeta, se pueden cargar a la tarjeta las carpetas y archivos requeridos para la operación de IP Office desde la PC IP Office Manager con ayuda del comando Recrear tarjeta SD de IP Office.

1. Inserte la tarjeta SD en la ranura del lector en la computadora IP Office Manager.
2. Mediante IP Office Manager, seleccione **Archivo | Avanzadas | Formatear tarjeta SD de IP Office**.
3. Seleccione **IP Office A-Law** o **IP Office U-Law**. Esta elección afecta solamente la etiqueta de la tarjeta visible al visualizar los detalles de la tarjeta. Esto no afecta el formato en sí. Seleccione la etiqueta que corresponda a los archivos que desea colocar en la tarjeta.
4. Navegue a la ubicación de la tarjeta y haga clic en **Aceptar**.
5. La barra de estado en la parte inferior de IP Office Manager mostrará el progreso del proceso de formateo.
6. Cuando se haya completado el formateo, puede usar el comando **Reproducir una tarjeta SD IP Office** para cargar las carpetas y archivos de IP Office en la tarjeta desde la PC IP Office Manager.

Reproducción de una tarjeta SD IP Office

Puede utilizar IP Office Manager para actualizar un grupo de archivos en una tarjeta System SD para que coincidan con los requeridos para la versión particular de IP Office. Esto se puede utilizar para actualizar la tarjeta desde un sistema existente o para preparar la tarjeta para un sistema nuevo.

IP Office Manager actualiza la tarjeta con los archivos del firmware binario para la unidad de control, los módulos de expansión externos y los teléfonos. También incluye los archivos de avisos para el funcionamiento del correo de voz integrado y la opción para los archivos de la aplicación web manager.

Se conservan los archivos existentes como la configuración de sistema, el archivo de licencia PLDS, los mensajes del correo de voz integrado y los saludos.

- Para usar la tarjeta en una ranura de tarjeta **System SD** de una unidad de control, debe ser una tarjeta System SD Avaya. La tarjeta debe tener el formato correcto (puede hacerlo mediante IP Office Manager), aunque no es necesario cambiar el formato de una tarjeta en funcionamiento antes de usar la recreación para actualizar el contenido de la tarjeta.
- El origen de los archivos copiados a la tarjeta SD son las subcarpetas en la carpeta ***\Memory Cards*** en el directorio de aplicaciones de Manager **Directorio de trabajo** (por lo general ***C:\Program Files(x86)\Avaya\IP Office\Manager***). Sin embargo, si se cambia el **Directorio de trabajo** a una ubicación sin un conjunto adecuado de subcarpetas ***\Memory Cards***, el conjunto de archivos requerido no se copiará en la tarjeta SD.
    - **ADVERTENCIA: Instalación de PCS14 y las unidades de control anteriores**
      PCS 310 Las unidades 14 o inferiores primero deben instalar la versión 8.1(65) (o posterior a 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1. Debe tomarse la precaución de comprobar que no se hagan llamadas antes de la actualización a la versión 10.0; de lo contrario, el sistema requerirá una licencia de actualización a 10.0 a pesar de que es "nuevo". El PCS de la unidad de control está impreso en la etiqueta que se encuentra en su parte posterior.

Configuración del nivel de software de sistema inicial

Cuando la unidad de control realiza la primera llamada, la versión de software en funcionamiento se graba de forma permanente en la unidad de control. Esto pasa a ser el nivel base de la unidad de control cuando se consideren los requerimientos del sistema para las licencias de actualización, etc. Por lo tanto, para un sistema nuevo, es importante que actualice la tarjeta System SD a la versión de software requerida antes de iniciar el sistema.

Determinar el nivel de software de la tarjeta System SD

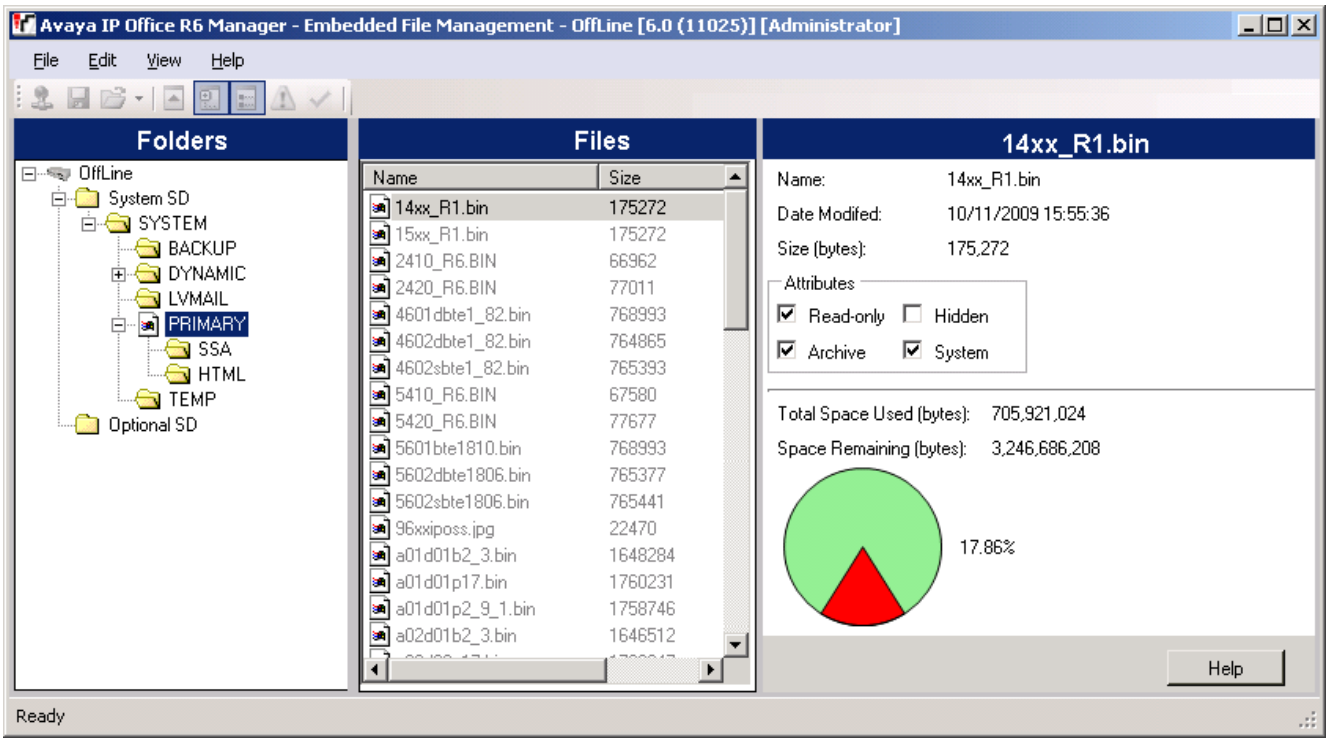
En la tarjeta SD, en la carpeta ***system/primary***, encuentre y abra el archivo ***filelist.txt***. La sección superior, al comienzo del archivo, termina con la versión del grupo de archivos que se copiaron anteriormente a la tarjeta. El resto del archivo detalla los archivos existentes.

Para actualizar/recrear una tarjeta System SD

1. Una vez iniciado, no interrumpa el proceso, por ejemplo, retirando la tarjeta SD. Este proceso toma alrededor de 20 minutos.
2. Inserte la tarjeta SD en la ranura del lector en la computadora IP Office Manager.
3. Mediante IP Office Manager, seleccione **Archivo | Avanzadas | Reproducir tarjeta SD de IP Office**.
4. Seleccione **IP Office A-Law** o **IP Office U-Law**. Esta selección afecta el modo de operación de los sistemas IP Office cuando sean devueltos a los ajustes predeterminados con esta tarjeta presente en la ranura de tarjetas **System SD**.
5. Navegue a la ubicación de la tarjeta y haga clic en **Aceptar**.
6. IP Office Manager indicará si desea incluir archivos IP Office Web Manager de Avaya como parte del proceso recreado. Esos archivos son necesarios si desea ejecutar IP Office Web Manager 71 para administrar el sistema IP Office en que se cargó la tarjeta o si desea utilizar integración 132.
7. IP Office Manager comenzará a crear carpetas en la tarjeta SD y a copiar a ellas los archivos requeridos. Este proceso toma alrededor de 20 minutos.
8. No extraiga la tarjeta SD durante este proceso. Espere hasta que IP Office Manager muestre un mensaje.

11.3 Visualización del contenido de la tarjeta

Con IP Office Manager, puede visualizar las carpetas y archivos en la tarjeta SD y en la tarjeta SD opcional. Puede entonces emplear varios comandos para cargar y descargar archivos desde y hacia las tarjetas.



1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Administración de archivos integrada**.
2. Seleccione el menú **Seleccionar IP Office** y seleccione el sistema IP Office.
3. Aparecerán los archivos contenidos en las tarjetas de memoria.

11.4 Creación de copia de seguridad en la carpeta de respaldo

Este proceso realiza una copia del contenido de la carpeta **/primary** en la tarjeta System SD y la almacena en la carpeta **/backup** carpeta en la misma tarjeta. Todos los archivos con nombres de archivo coincidentes se reemplazan. Este proceso toma alrededor de 6 minutos. Para conocer los métodos para restauración desde la **/backup** carpeta, consulte Restauración del sistema desde la carpeta de la copia de seguridad 145.

Estos procesos no realizan copias de seguridad de las indicaciones, los mensajes y los saludos que utilizan las operadoras automáticas y los buzones de voz del sistema. Se almacenan en las carpetas **/lvmail** y **/dynamic/lvmail** de la tarjeta.

11.4.1 Crear copia de seguridad en la carpeta de respaldo IP Office Manager

Para crear una copia de seguridad en la carpeta /respaldo mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Administración de archivos integrada**.
2. Seleccione el menú **Seleccionar IP Office** y seleccione el sistema IP Office.
3. Aparecerán los archivos contenidos en las tarjetas de memoria.
4. Seleccionar **Archivo | Archivos de respaldo del sistema**.
   - Se copiará el contenido de la carpeta **/primary** en la tarjeta System SD a la carpeta **/backup**. Este proceso toma alrededor de 6 minutos.

11.4.2 Crear copia de seguridad en la carpeta de respaldo mediante System Status Application

Para crear una copia de seguridad en la carpeta /respaldo mediante System Status Application

1. Inicie System Status 69 e ingrese al torrente del estado de IP Office.
2. En el panel de navegación, seleccione **Sistema**.
3. En la parte inferior de la pantalla, seleccione **Copia de seguridad de archivos del sistema**.
   - Se copiará el contenido de la carpeta **/primary** en la tarjeta System SD a la carpeta **/backup**. Este proceso toma alrededor de 6 minutos.

11.4.3 Crear copia de seguridad en la carpeta de respaldo mediante un teléfono del sistema

Este proceso lo puede utilizar un usuario configurado como usuario Teléfono del sistema empleando un teléfono serie 1400, 1600, 9500 o 9600 (con la excepción de los modelos XX01, XX02 y XX03). El **Código de inicio de sesión** se utiliza para restringir acceso a las funciones administrativas del sistema en el teléfono.

Para crear una copia de seguridad en la carpeta /respaldo mediante un teléfono del sistema

1. Seleccione **Funciones | Usuario Phone | Administración del sistema**.
2. Ingrese el código de su inicio de sesión de usuario IP Office.
3. Seleccione en el menú **Tarjeta de memoria**.
4. Seleccionar **Respaldo del sistema**.
   - Se copiará el contenido de la carpeta **/primary** en la tarjeta System SD a la carpeta **/backup**. Este proceso toma alrededor de 6 minutos.

11.4.4 Crear copia de seguridad en la carpeta de respaldo mediante IP Office Web Manager

Para crear una copia de seguridad en la carpeta /respaldo mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.

    a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.

    b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.

2. Haga clic en **Acciones** y seleccione **Respaldar**.

2. Como destino, seleccione ***En dispositivo***.

3. Haga clic en **Respaldar**.

11.5 Restauración del sistema desde la carpeta de respaldo

Puede copiar el contenido de la carpeta **/backup** en la tarjeta SD del sistema a la carpeta **/primary** carpeta en la misma tarjeta. Todos los archivos con nombres de archivo coincidentes se reemplazan. El sistema luego se reinicia mediante los archivos en la carpeta **/primary**.

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

11.5.1 Restauración del sistema desde la carpeta de respaldo mediante IP Office Manager

Para restaurar el sistema desde la carpeta /respaldo mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Administración de archivos integrada**.
2. Seleccione el menú **Seleccionar IP Office** y seleccione el sistema IP Office.
3. Aparecerán los archivos contenidos en las tarjetas de memoria.
4. Seleccionar **Archivo | Restaurar archivos del sistema**.
   - Se copiará el contenido de la carpeta **/backup** en la tarjeta SD de sistema se copia a la carpeta **/primary**. Este proceso toma alrededor de 6 minutos.
   - Cuando el proceso ha finalizado, el sistema se reinicia.

11.5.2 Restauración del sistema desde la carpeta de respaldo mediante System Status Application

Para restaurar el sistema desde la carpeta /respaldo mediante System Status Application

1. Inicie System Status 69 e ingrese al torrente del estado de IP Office.
2. En el panel de navegación, seleccione **Sistema**.
3. En la parte inferior de la pantalla, seleccione **Restaurar archivos del sistema**.
   - Se copiará el contenido de la carpeta **/backup** en la tarjeta SD de sistema se copia a la carpeta **/primary**. Este proceso toma alrededor de 6 minutos.
   - Cuando el proceso ha finalizado, el sistema se reinicia.

11.5.3 Restauración del sistema desde la carpeta de respaldo mediante un teléfono del sistema

Este proceso lo puede utilizar un usuario configurado como usuario Teléfono del sistema empleando un teléfono serie 1400, 1600, 9500 o 9600 (con la excepción de los modelos XX01, XX02 y XX03). El **Código de inicio de sesión** se utiliza para restringir acceso a las funciones administrativas del sistema en el teléfono.

Para restaurar el sistema desde la carpeta /respaldo mediante un teléfono del sistema

1. Seleccione **Funciones | Usuario Phone | Administración del sistema**.
2. Ingrese el código de su inicio de sesión de usuario IP Office.
3. Seleccione en el menú **Tarjeta de memoria**.
4. Seleccionar **Restaurar sistema**.
   - Se copiará el contenido de la carpeta **/backup** en la tarjeta SD de sistema se copia a la carpeta **/primary**. Este proceso toma alrededor de 6 minutos.
   - Cuando el proceso ha finalizado, el sistema se reinicia.

11.5.4 Restauración del sistema desde la carpeta de respaldo mediante IP Office Web Manager

Para restuarar el sistema desde la carpeta /respaldo mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.

    a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.

    b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.

2. Haga clic en **Acciones** y seleccione **Restaurar**.

2. Como destino, seleccione ***En dispositivo***.

3. Haga clic en **Restaurar**.

11.6 Creación de copia de seguridad en la tarjeta SD opcional

Este proceso copia todos los archivos en la tarjeta SD a la tarjeta SD opcional. Incluye las carpetas **/primary** y **/backup** y los archivos de Embedded Voicemail que incluyen archivos de mensajes. Esto sobrescribe todos los archivos y carpetas con nombres coincidentes en la tarjeta SD opcional.

Este procedimiento es un simple proceso de copiado. No se vuelven a copiar los archivos que ya están copiados y cambian durante el proceso. Es posible que cualquier otro archivo agregado mientras se ejecuta el proceso, por ejemplo, mensajes del correo de voz, no se copie.

Este proceso ocupa al menos 90 minutos y puede requerir un plazo mayor según la cantidad de datos que se van a copiar, por ejemplo, si el sistema IP Office utiliza el servicio de Embedded Voicemail para tomar mensajes.

11.6.1 Creación de copia de seguridad en la tarjeta opcional SD mediante IP Office Manager

Para crear una copia de seguridad de la tarjeta SD del sistema en la tarjeta SD opcional mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Administración de archivos integrada**.
2. Seleccione el menú **Seleccionar IP Office** y seleccione el sistema IP Office.
3. Aparecerán los archivos contenidos en las tarjetas de memoria.
4. Seleccionar **Archivo | Copiar tarjeta del sistema**.
   - Puede copiar el contenido de la tarjeta System SD a la tarjeta SD Opcional. Este proceso ocupa al menos 90 minutos, y puede llevar mucho tiempo más.

11.6.2 Creación de copia de seguridad en la tarjeta SD opcional mediante System Status Application

Para crear una copia de seguridad de la tarjeta SD del sistema en la tarjeta SD opcional mediante System Status Application

1. Inicie System Status 69 e ingrese al torrente del estado de IP Office.
2. En el panel de navegación, seleccione **Sistema**.
3. Seleccionar **Tarjetas de memoria**.
4. Seleccionar **System Card**.
5. En la parte inferior de la pantalla, seleccione **Copiar tarjeta del sistema**.
   - Puede copiar el contenido de la tarjeta System SD a la tarjeta SD Opcional. Este proceso ocupa al menos 90 minutos, y puede llevar mucho tiempo más.

11.6.3 Creación de copia de seguridad en la tarjeta SD opcional mediante IP Office Web Manager

Para crear una copia de seguridad de la tarjeta SD del sistema en la tarjeta SD opcional mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones**. Seleccione **Comandos de servicio** y seleccione **Copiar en SD opcional**.
3. Haga clic en **Aceptar**.

11.6.4 Creación de copia de seguridad en la tarjeta SD opcional mediante un teléfono del sistema

Este proceso lo puede utilizar un usuario configurado como usuario Teléfono del sistema empleando un teléfono serie 1400, 1600, 9500 o 9600 (con la excepción de los modelos XX01, XX02 y XX03). El **Código de inicio de sesión** se utiliza para restringir acceso a las funciones administrativas del sistema en el teléfono.

Para crear una copia de seguridad de la tarjeta SD del sistema en la tarjeta SD opcional mediante un teléfono del sistema

1. Seleccione **Funciones | Usuario Phone | Administración del sistema**.
2. Ingrese el código de su inicio de sesión de usuario IP Office.
3. Seleccione en el menú **Tarjeta de memoria**.
4. Seleccionar **Copiar**.
   - Puede copiar el contenido de la tarjeta System SD a la tarjeta SD Opcional. Este proceso ocupa al menos 90 minutos, y puede llevar mucho tiempo más.

11.7 Restauración de la configuración desde una tarjeta opcional

Los siguientes procesos crean una copia del archivo de configuración (***config.cfg***) y el archivo de licencias (***keys.txt***). Estos procesos toman unos pocos segundos.

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

11.7.1 Restauración del sistema desde la tarjeta SD opcional mediante IP Office Manager

Para copiar un archivo de configuración de la tarjeta SD opcional mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Administración de archivos integrada**.
2. Seleccione el menú **Seleccionar IP Office** y seleccione el sistema IP Office.
3. Aparecerán los archivos contenidos en las tarjetas de memoria.
4. Seleccionar **Archivo | Actualizar configuración**.
   - El archivo de configuración (***config.cfg***) y el archivo de licencias (***keys.txt***) dentro de la carpeta ***/primary*** en la tarjeta SD opcional a la carpeta se copian a la carpeta ***/primary*** en la tarjeta System SD. Este proceso toma alrededor de unos pocos segundos.
   - Una vez completado el proceso, se reiniciará el sistema IP Office.

11.7.2 Restauración del sistema desde la tarjeta SD opcional mediante un teléfono del sistema

Este proceso lo puede utilizar un usuario configurado como usuario Teléfono del sistema empleando un teléfono serie 1400, 1600, 9500 o 9600 (con la excepción de los modelos XX01, XX02 y XX03). El **Código de inicio de sesión** se utiliza para restringir acceso a las funciones administrativas del sistema en el teléfono.

Para copiar un archivo de configuración de la tarjeta SD opcional mediante un teléfono del sistema

1. Seleccione **Funciones | Usuario Phone | Administración del sistema**.
2. Ingrese el código de su inicio de sesión de usuario IP Office.
3. Seleccione en el menú **Tarjeta de memoria**.
4. Seleccionar **Actualizar configuración...**.
   - El archivo de configuración (***config.cfg***) y el archivo de licencias (***keys.txt***) dentro de la carpeta ***/primary*** en la tarjeta SD opcional a la carpeta se copian a la carpeta ***/primary*** en la tarjeta System SD. Este proceso toma alrededor de unos pocos segundos.
   - Una vez completado el proceso, se reiniciará el sistema IP Office.

11.8 Carga del software desde una tarjeta SD opcional

Estos procedimientos copian todos los archivos en la carpeta excepto el archivo de configuración (***config.cfg***) y el archivo de licencias (***keys.txt***). Estos procesos toman alrededor de 5 minutos. Estos procesos no recuperarán los avisos de Embedded Voicemail (consulte la sección Actualización del software de la tarjeta 152).

- **Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín Técnico de IP Office referente a la versión de software de IP Office que desea instalar. El boletín contiene información importante que puede haberse omitido en este manual. Puede encontrar los Boletines Técnicos de IP Office en el sitio Web de soporte técnico Avaya (*http://support.avaya.com*).

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

11.8.1 Carga del software desde la tarjeta SD opcional mediante IP Office Manager

Para copiar los archivos de software de la tarjeta SD opcional mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Administración de archivos integrada**.
2. Seleccione el menú **Seleccionar IP Office** y seleccione el sistema IP Office.
3. Aparecerán los archivos contenidos en las tarjetas de memoria.
4. Seleccionar **Archivo | Actualizar archivos binarios**.
   - Los archivos de software (todos los archivos de la carpeta excepto el archivo de configuración (***config.cfg***) y el archivo de licencias (***keys.txt***)) dentro de la carpeta ***/primary*** en la tarjeta SD opcional a la carpeta se copian a la carpeta ***/primary*** en la tarjeta System SD. Este proceso toma alrededor de 5 minutos.
   - Una vez completado el proceso, se reiniciará el sistema IP Office.

11.8.2 Carga del software desde la tarjeta SD opcional mediante un teléfono del sistema

Este proceso lo puede utilizar un usuario configurado como usuario Teléfono del sistema empleando un teléfono serie 1400, 1600, 9500 o 9600 (con la excepción de los modelos XX01, XX02 y XX03). El **Código de inicio de sesión** se utiliza para restringir acceso a las funciones administrativas del sistema en el teléfono.

Para copiar los archivos de software de la tarjeta SD opcional mediante un teléfono del sistema

1. Seleccione **Funciones | Usuario Phone | Administración del sistema**.
2. Ingrese el código de su inicio de sesión de usuario IP Office.
3. Seleccione en el menú **Tarjeta de memoria**.
4. Seleccionar **Actualizar binarios...**.
   - Los archivos de software (todos los archivos de la carpeta excepto el archivo de configuración (***config.cfg***) y el archivo de licencias (***keys.txt***)) dentro de la carpeta ***/primary*** en la tarjeta SD opcional a la carpeta se copian a la carpeta ***/primary*** en la tarjeta System SD. Este proceso toma alrededor de 5 minutos.
   - Una vez completado el proceso, se reiniciará el sistema IP Office.

11.9 Creación de una copia de seguridad en una PC

Este proceso copia la carpeta **/backup** de la tarjeta SD del sistema en una carpeta especificada en la PC con IP Office Web Manager. Este proceso toma aproximadamente 25 minutos.

Antes de usar este proceso, el contenido de la carpeta /Respaldo se puede actualizar con los archivos de la carpeta /principal en la misma tarjeta. Consulte la sección Creación de copia de seguridad en la carpeta de respaldo 143.

Para crear una copia de seguridad en una PC mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
    a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
    b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones** y seleccione **Respaldar**.
3. Como destino, seleccione ***Máquina cliente***.
4. Haga clic en **Configurar ruta**.
5. Seleccionar la ubicación para la copia de seguridad y hacer clic **Abrir**. Recomendamos que cree una carpeta nueva y luego seleccione esa carpeta.
6. Haga clic en **Iniciar respaldo**.
7. Espere hasta que aparezca un mensaje de copia de seguridad finalizada. Haga clic en **Cancelar** para cerrar el menú.

11.10 Restauración desde una PC

Este proceso restaura una copia de seguridad anterior, sobreescribiendo la carpeta /principal en la tarjeta SD del sistema.

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

Para restaurar el sistema desde una copia de seguridad de una PC mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
    a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
    b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones** y seleccione **Restaurar**.
3. Haga clic en **Restaurar desde** y seleccione ***Máquina cliente***.
4. Haga clic en **Aceptar**.
5. Haga clic en **Configurar ruta**.
6. Seleccione la carpeta que contiene la copia de seguridad anterior y haga clic en **Abrir**.
7. Haga clic en **Iniciar restauración**.
8. Espere hasta que aparezca un mensaje de restauración finalizada. Haga clic en **Cancelar** para cerrar el menú. El sistema se reinicia.

11.11 Actualización del software de la tarjeta

Además de utilizar el Asistente de actualización IP Office 180, las unidades de control IP500 V2 pueden actualizarse cargando el grupo de archivos de firmware requeridos en la tarjeta SD del sistema y reiniciando el sistema.

- **Boletines técnicos de IP Office**
  Debe obtener y leer el Boletín Técnico de IP Office referente a la versión de software de IP Office que desea instalar. El boletín contiene información importante que puede haberse omitido en este manual. Puede encontrar los Boletines Técnicos de IP Office en el sitio Web de soporte técnico Avaya (*http://support.avaya.com*).

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

Esto se puede hacer en varias formas.

Método	Descripción	Ubicación	Archivos de software	Avisos del Embedded Voicemail
Mediante IP Office Manager 182	Con ayuda de IP Office Manager, se compara el contenido en la tarjeta con los archivos que IP Office Manager tiene disponibles y se actualizan si es necesario.	**Local o remoto**	✓	✓
Actualización de la tarjeta System SD 183	Este método requiere apagar y extraer la tarjeta System SD de la unidad de control. Se actualiza el contenido de la tarjeta con ayuda de IP Office Manager.	**Local**	✓	✓
Actualización desde la tarjeta SD opcional. 184	Este método emplea una tarjeta SD cargada con la versión requerida del software IP Office. La tarjeta es insertada en la ranura de la tarjeta SD opcional y se copia su contenido a la tarjeta System SD.	**Local**	✓	–

11.12 Extracción y apagado de la tarjeta de memoria

Antes de extraer una tarjeta de memoria de un sistema IP Office en ejecución, es necesario apagar la tarjeta. La extracción de una tarjeta de memoria mientras el sistema está en ejecución puede ocasionar corrupción de los archivos. Los servicios de la tarjeta pueden reiniciarse ya sea reinsertando la tarjeta o con ayuda del comando Comando de inicio 155.

11.12.1 Apagado de una tarjeta mediante IP Office Manager

Para apagar una tarjeta de memoria mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Avanzado | Comandos de la tarjeta de memoria | Apagar** .
2. Con ayuda de la opción **Seleccionar IP Office** seleccione el sistema IP Office que contiene la tarjeta de memoria.
3. Haga clic en **Aceptar**.
   - En la parte posterior de la unidad de control, confirme que la luz LED correspondiente a la tarjeta de memoria está apagada.
   - Ahora puede extraer la tarjeta a fin de realizar las acciones de mantenimiento necesarias.

11.12.2 Apagado de una tarjeta mediante System Status Application

Para apagar una tarjeta de memoria mediante System Status Application

1. Inicie System Status 69 e ingrese al torrente del estado de IP Office.
2. En el panel de navegación, seleccione **Sistema**.
3. Seleccionar **Tarjetas de memoria**.
4. Seleccione ya sea **System Card** o bien **tarjeta opcional**.
5. En la parte inferior de la pantalla, seleccione **Cierre**.
   - En la parte posterior de la unidad de control, confirme que la luz LED correspondiente a la tarjeta de memoria está apagada.
   - Ahora puede extraer la tarjeta a fin de realizar las acciones de mantenimiento necesarias.

11.12.3 Apagado de una tarjeta mediante IP Office Web Manager

Para apagar una tarjeta mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones**. Seleccione **Comandos de servicio** y seleccione **Suspención de tarjeta de memoria**.
3. Seleccione la tarjeta que se detendrá y haga clic en **Aceptar**.

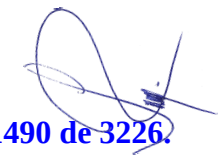
11.12.4 Apagado de una tarjeta mediante un teléfono del sistema

Este proceso lo puede utilizar un usuario configurado como usuario Teléfono del sistema empleando un teléfono serie 1400, 1600, 9500 o 9600 (con la excepción de los modelos XX01, XX02 y XX03). El **Código de inicio de sesión** se utiliza para restringir acceso a las funciones administrativas del sistema en el teléfono.

Para apagar una tarjeta que usa un teléfono del sistema

1. Seleccione **Funciones | Usuario Phone | Administración del sistema**.
2. Ingrese el código de su inicio de sesión de usuario IP Office.
3. Seleccione en el menú **Tarjeta de memoria**.
4. Seleccionar **Sistema** para la tarjeta System SD o bien **Opción** para la tarjeta SD opcional.
5. Seleccionar **Cierre**.
   - En la parte posterior de la unidad de control, confirme que la luz LED correspondiente a la tarjeta de memoria está apagada.
   - Ahora puede extraer la tarjeta a fin de realizar las acciones de mantenimiento necesarias.

Página 1489 de 3226.



11.13 Inicio de la tarjeta de memoria

Reinsertar una tarjeta de memoria en un sistema que ya está encendido reinicia automáticamente el funcionamiento de la tarjeta. Sin embargo, si la tarjeta se ha apagado 153 pero no se ha extraído, puede reiniciarse mediante IP Office Manager sin necesidad de un reinicio.

11.13.1 Inicio de una tarjeta mediante IP Office Manager

Para iniciar una tarjeta mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Avanzado | Comandos de la tarjeta de memoria | Inicio**.
2. Con ayuda de la opción **Seleccionar IP Office** seleccione el sistema IP Office que contiene la tarjeta de memoria.
3. Haga clic en **Aceptar**.

11.13.2 Inicio de una tarjeta mediante System Status Application

Para iniciar una tarjeta mediante System Status Application

1. Inicie System Status 69 e ingrese al torrente del estado de IP Office.
2. En el panel de navegación, seleccione **Sistema**.
3. Seleccionar **Tarjetas de memoria**.
4. Seleccione ya sea **System Card** o bien **tarjeta opcional**.
5. En la parte inferior de la pantalla, seleccione **Inicio**.

11.13.3 Inicio de una tarjeta mediante IP Office Web Manager

Para iniciar una tarjeta mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones**. Seleccione **Comandos de servicio** y seleccione **Inicio de tarjeta de memoria**.
3. Seleccione la tarjeta que se iniciará y haga clic en **Aceptar**.

11.13.4 Inicio de una tarjeta mediante un teléfono del sistema

Este proceso lo puede utilizar un usuario configurado como usuario Teléfono del sistema empleando un teléfono serie 1400, 1600, 9500 o 9600 (con la excepción de los modelos XX01, XX02 y XX03). El **Código de inicio de sesión** se utiliza para restringir acceso a las funciones administrativas del sistema en el teléfono.

Para iniciar una tarjeta mediante un teléfono del sistema

1. Seleccione **Funciones | Usuario Phone | Administración del sistema**.
2. Ingrese el código de su inicio de sesión de usuario IP Office.
3. Seleccione en el menú **Tarjeta de memoria**.
4. Seleccionar **Sistema** para la tarjeta System SD o bien **Opción** para la tarjeta SD opcional.
5. Seleccionar **Iniciar sistema**.

Capítulo 12.
Procesos adicionales

12. Procesos adicionales

Esta sección cubre diversos procesos de mantenimiento.

Procesos

- Cambio de un sistema IP Office Basic Edition al modo estándar 159
- Desactivación/Apagado de un sistema 161
- Reinicio de un sistema 163
- Modificación de los componentes 165
- Devolución de la configuración a valores predeterminados 168
- Devolver la seguridad a valores predeterminados 172
- Carga de un nuevo archivo de configuración 176
- Intercambio de usuarios de extensiones 187
- Acualización de sistemas 179
- Instalaciones telefónicas fuera del edificio 39
- Uso del puerto de salida externo 192
- Configuración del módulo So8 BRI 194
- Configuración SNMP 197
- Botón Restablecer 201
- Botón AUX 201
- Mantenimiento del puerto RS232 202
- Borrado del software principal 203
- Activación de IP Office Web Manager 206

Otros procesos

Los siguientes procesos adicionales de mantenimiento se abarcan en otras secciones de este documento:

- Creación de una tarjeta SD de IP Office 140
- Visualización de contenidos de tarjeta 142
- Creación de copia de seguridad de la configuración 143
- Restauración de la configuración 145
- Copiado en la tarjeta SD opcional 147
- Restauración desde la tarjeta SD opcional 149
- Extracción y apagado de la tarjeta de memoria 153
- Inicio de la tarjeta de memoria 155
- Integración 132
- Instalación de las aplicaciones de administración 64

12.1 Cambio de un sistema IP Office Basic Edition al modo estándar

El proceso a continuación cambiará el modo del sistema y lo dejará en su configuración predeterminada.

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

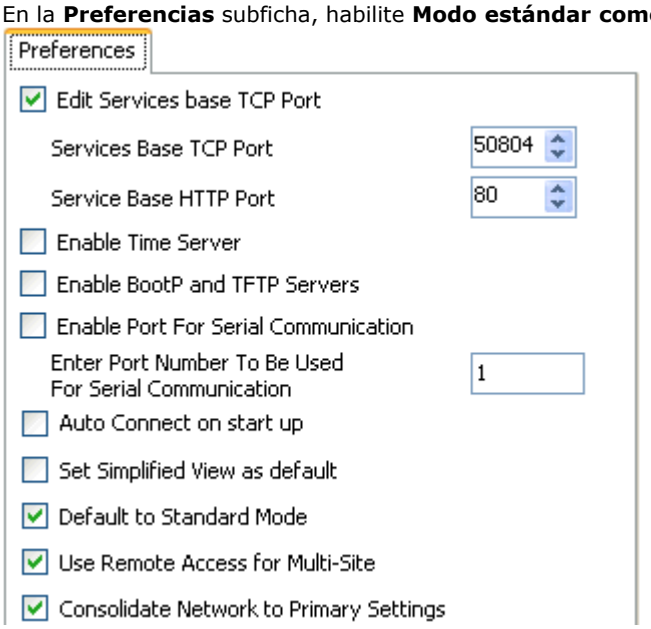
1. Use IP Office Manager para recibir la configuración del sistema 68.
2. Cuando se solicite, ingrese el nombre de usuario y contraseña del usuario de servicio.
3. La aplicación IP Office Manager pasará automáticamente a la vista simplificada ya que la configuración proviene de un sistema que funciona en modo IP Office Basic Edition.
4. Seleccione **Archivo | Avanzado | Pasar al modo standard (predeterminado)**.
5. La configuración cambia a una predeterminada para un sistema IP Office Essential Edition y IP Office Manager cambia a su modo de vista avanzada.
6. Este es un momento adecuado para comenzar la configuración inicial 98 antes de enviar la configuración de vuelta al sistema IP Office para reiniciar en IP Office Essential Edition.
   - Para ejecutar un sistema en modo IP Office Essential Edition o IP Office Preferred Edition su configuración debe incluir una licencia **Essential Edition**. Un sistema sin esta licencia no permitirá ninguna función telefónica hasta que se haya agregado la licencia.
7. Una vez que se ha reiniciado el sistema, use IP Office Manager para recibir nuevamente la configuración del sistema. El nombre de usuario y la contraseña para la configuración deben ser los predeterminados del modo IP Office versión estándar **Administrator** y **Administrator**.

12.2 Automatización del cambio a modo estándar

Si los únicos sistemas que instala son aquellos que usan modos estándar de IP Office, IP Office Manager se puede configurar para devolver automáticamente el sistema al modo estándar de IP Office.

- **ADVERTENCIA**
  El siguiente proceso requiere el reinicio del sistema IP Office a fin de que se apliquen los cambios introducidos. El reinicio finaliza todas las llamadas y servicios actuales.

1. En IP Office Manager, seleccione **Archivo | Preferencias**.
2. En la **Preferencias** subficha, habilite **Modo estándar como predeterminado**.



3. Con esta opción habilitada, cuando Manager recibe una configuración para un sistema nuevo o predeterminado IP Office Manager recibe el sistema que se ejecuta en IP Office Basic Edition, el cual se convertirá de manera automática en una configuración IP Office Essential Edition.
4. **Importante: Configuraciones de dirección IP predeterminadas para el servidor**
   La conversión establecerá el modo DHCP en ***Servidor*** y las direcciones LAN a sus direcciones predeterminadas de 192.168.42.1 y 192.168.43.1. Cómo usar IP Office Manager para cambiar estas configuraciones a los valores requeridos.
5. Este es un momento adecuado para comenzar la configuración inicial 98 antes de enviar la configuración de vuelta al sistema IP Office para reiniciar en IP Office Essential Edition.
   - Para ejecutar un sistema en modo IP Office Essential Edition o IP Office Preferred Edition su configuración debe incluir una licencia **Essential Edition**. Un sistema sin esta licencia no permitirá ninguna función telefónica hasta que se haya agregado la licencia.
6. Enviar la configuración de vuelta al sistema lo reinicia en modo IP Office Essential Edition.

12.3 Desactivación de un sistema

Los sistemas que funcionan con IP Office versión 6.0 deben apagarase a fin de realizar el mantenimiento en lugar de solo desactivarse. El apagado puede ser indefinido o por un período de tiempo establecido, después del cual el sistema IP Office se reiniciará automáticamente. Observe que las tarjetas de memoria de la unidad de control se pueden apagar 153 yreiniciar 155las tarjetas de memoria en forma separada del sistema.

Durante el proceso de apagado, la configuración actual en la memoria RAM de la unidad de control se copia a la memoria no volátil de la unidad de control. En los sistemas IP500 V2, esta memoria se encuentra en la tarjeta SD del sistema.

- **ADVERTENCIA**
  Siempre debe utilizar el proceso de cierre del sistema para apagarlo. Con tan sólo quitar el cable de corriente eléctrica apagar la entrada de energía podría causar la pérdida de datos de configuración.
  - Al apagarse el sistema, todas las llamadas de usuarios y los servicios en ejecución se interrumpirán de forma abrupta. Una vez que se haya apagado el sistema, este no se podrá usar para hacer o recibir ninguna llamada hasta que se reinicie.
  - El proceso de apagado toma alrededor de un minuto. Cuando apague un sistema con una Unified Communications Module instalada, el proceso puede tardar hasta tres minutos mientras la tarjeta cierra de forma segura todos los archivos abiertos y el sistema operativo.
- **Indicación de LED de apagado**
  Mientras el sistema permanezca apagado, las luces LED que se muestran en el sistema son las siguientes. No corte la energía del sistema ni quite ninguna tarjeta de memoria hasta que el sistema esté en este estado:
  - El LED1 en cada tarjeta base IP500 instalada comenzará a parpadear en rojo rápidamente, además del LED 9 si hay una tarjeta auxiliar de troncal instalada en la tarjeta base.
  - El LED del CPU LED en la parte posterior del sistema parpadeará en rojo rápidamente.
  - La tarjeta SD del sistema y los indicadores LED SD opcionales en la parte posterior del sistema se apagan.
- **Reinicio de un sistema**
  Para reiniciar un sistema cuando se ha apagado en forma indefinida, o bien para reiniciar un sistema antes de que el reinicio caduque, apague y vuelva a encender el suministro de energía del sistema.

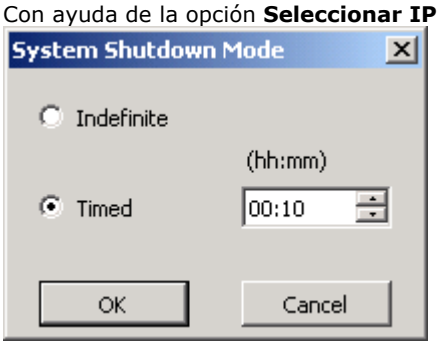
Opciones de proceso

1. **Apagado de un sistema mediante IP Office Manager** 161
2. **Apagado de un sistema mediante System Status Application** 162
3. **Apagado de un sistema mediante un teléfono del sistema** 162
4. **Apagado de un sistema mediante el botón AUX** 162
5. **Para actualizar un sistema mediante IP Office Web Manager** 162

12.3.1 Apagado de un sistema mediante IP Office Manager

Para apagar un sistema mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Cierre del sistema**.
2. Con ayuda de la opción **Seleccionar IP Office** aparecerá el menú **Modo de apagado del sistema**.



3. Seleccione el tipo de apagado que desea. Si elige **Indefinido**, el sistema sólo puede reiniciarse cuando se apague la energía del sistema y luego se vuelva a encender. Si elige un apagado **Programado**, el sistema IP Office se reiniciará una vez transcurrido el tiempo establecido.
4. Haga clic en **Aceptar**.
5. Espere hasta que todos los LED de la parte frontal del sistema parpadeen en rojo antes de realizar cualquier otra acción.

12.3.2 Apagado de un sistema mediante System Status Application

Para apagar un sistema mediante System Status Application

1. Inicie System Status 69 e ingrese al torrente del estado de IP Office.
2. En el panel de navegación, seleccione **Sistema**.
3. En la parte inferior de la pantalla, seleccione **Apagado del sistema**.
4. Seleccione el período de tiempo del apagado, o indefinido.
5. Haga clic en **Aceptar**.
6. Espere hasta que todos los LED de la parte frontal del sistema parpadeen en rojo antes de realizar cualquier otra acción.

12.3.3 Apagado de un sistema mediante un teléfono del sistema

Este proceso lo puede utilizar un usuario configurado como usuario Teléfono del sistema empleando un teléfono serie 1400, 1600, 9500 o 9600 (con la excepción de los modelos XX01, XX02 y XX03). El **Código de inicio de sesión** se utiliza para restringir acceso a las funciones administrativas del sistema en el teléfono.

A diferencia de IP Office Manager, un usuario de teléfono del sistema no puede elegir un apagado indefinido. Pueden establecer un período de apagado entre 5 minutos y 24 horas.

Para apagar un sistema que usa un teléfono del sistema

1. Seleccione **Funciones | Usuario Phone | Administración del sistema**.
2. Ingrese el código de su inicio de sesión de usuario IP Office.
3. Seleccione en el menú **Cierre del sistema**.
4. Seleccione el período de tiempo del apagado. Este lapso debe estar entre 5 minutos y 24 horas.
5. Oprima **Hecho** y luego presione **Confirm.** para comenzar el proceso de apagado.
6. Espere hasta que todos los LED de la parte frontal del sistema parpadeen en rojo antes de realizar cualquier otra acción.

12.3.4 Apagado de un sistema mediante el botón AUX

Este método es compatible con unidades de control IP500 V2.

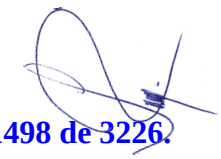
Para apagar un sistema mediante el botón AUX de IP500 V2

1. En la parte posterior de la unidad de control, mantenga presionado el botón **AUX** durante más de 5 segundos.
2. La unidad de control se apagará con el temporizador de reinicio configurado en 10 minutos.
3. Espere hasta que todos los LED de la parte frontal del sistema parpadeen en rojo antes de realizar cualquier otra acción.

12.3.5 Apagado de un sistema mediante IP Office Web Manager

Para apagar un sistema mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones**. Seleccione **Comandos de servicio** y luego presione **Cierre del sistema**.
3. Haga clic en **Aceptar**.
4. Espere hasta que todos los LED de la parte frontal del sistema parpadeen en rojo antes de realizar cualquier otra acción.



12.4 Reinicio de un sistema

Es posible que ocasionalmente sea necesario reiniciar el sistema. Por ejemplo, después de reinsertar una tarjeta SD del sistema con software de sistema actualizado. Eso se puede hacer mediante cualquiera de los siguientes procesos.

- **ADVERTENCIA**
  Siempre debe usarse uno de los siguientes métodos para reiniciar un sistema. Simplemente quitar y luego volver a aplicar alimentación al sistema puede causar la pérdida de datos y la operación inesperada del sistema.

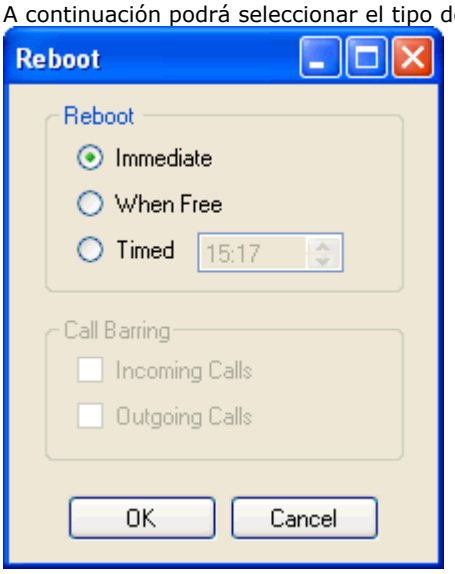
Opciones de proceso

1. **Reinicio de un sistema mediante IP Office Manager** 163
2. **Reinicio de un sistema mediante IP Office Web Manager** 164
3. **Reinicio de un sistema mediante el botón Restablecer** 164
4. **Reinicio de un sistema mediante un teléfono del sistema** 164

12.4.1 Reinicio de un sistema mediante IP Office Manager

Para reiniciar un sistema mediante IP Office Manager

1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Reiniciar**.
2. Utilice la lista desplegable **Seleccionar IP Office** para localizar y seleccionar el sistema IP Office. Ingrese un nombre de usuario y una contraseña válidos.
3. A continuación podrá seleccionar el tipo de reinicio deseado.



- **Reiniciar**
  Seleccione cuándo desea que ocurra el reinicio.
  - **Inmediatamente**
    Reinicie el sistema inmediatamente.
  - **Cuando esté libre**
    Reinicie el sistema cuando no hay llamadas en progreso. Este modo puede combinarse con las opciones de **Restricción de llamadas**.
  - **Programado**
    Igual que Reiniciar al liberar, pero el sistema espera una hora específica y luego espera a que no hayan llamadas en progreso. El horario es especificado con la opción **Hora de reinicio**. Este modo puede combinarse con las opciones de **Restricción de llamadas**.
- **Hora de reinicio**
  Este ajuste se utiliza cuando se selecciona el modo de reinicio **Programado**. Establece la hora para realizar el reinicio de IP Office. Si el horario es después de medianoche, se cancela la copia de seguridad rutinaria de todos los días del sistema IP Office.
- **Restricción de llamadas**
  Puede utilizar estos ajustes cuando se ha elegido el modo de reinicio Reiniciar al liberar. Y restringe el envío o recepción de nuevas llamadas.

4. Haga clic en **Aceptar**.

12.4.2 Reinicio de un sistema mediante IP Office Web Manager

Para reiniciar un sistema mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
    a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
    b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones**. Seleccione **Comandos de servicio** y luego presione **Reiniciar**.
3. Seleccione cuándo desea que ocurra el reinicio.
    - **Inmediatamente**
      Reinicie el sistema inmediatamente.
    - **Gratuita**
      Reinicie el sistema cuando no hay llamadas en progreso.
    - **Programado**
      Reinicie el sistema en el momento establecido.
4. Haga clic en **Aceptar**.

12.4.3 Reinicio de un sistema mediante el botón Restablecer

Para reiniciar un sistema mediante el botón Restablecer

Use este proceso para reiniciar el sistema cuando esté libre. Una vez invocado, el sistema bloquea cualquier llamada nueva entrante o saliente hasta después del reinicio.

1. En la parte posterior de la unidad de control, mantenga presionado el botón **Restablecer** button for between 5 to 10 seconds until the **CPU** cambie a anaranjado fijo.
2. Cuando oprime el botón **CPU** LED cambia a anaranjado fijo, suelte el botón.
    - Si se ha configurado el **CPU** LED cambió a anaranjado intermitente o bien rojo, mantenga el botón presionado hasta el **CPU** LED cambia a verde intermitente. Luego suelte el botón y reintente el proceso una vez que el LED de la CPU ha vuelto a verde fijo.
3. Espere a que finalice el reinicio antes de realizar cualquier otra acción.

12.4.4 Apagado de un sistema mediante un teléfono del sistema

Esta función no se admite en teléfonos de sistema para un sistema que se ejecuta en el modo estándar de IP Office.

12.5 Modificación de los componentes

Excepto por las tarjetas de memoria (consulte la sección Extracción de la tarjeta de memoria 153), las tarjetas y módulos de expansión externos sólo deben extraerse y agregarse a un sistema de IP Office cuando el sistema está apagado 161.

En las secciones siguientes, el término componente puede referirse a una tarjeta conectada al IP Office o a un módulo de expansión externo.

Observe que en el caso de los puertos de extensión, existe una entrada de extensión y una entrada de usuario en la configuración de IP Office, en forma predeterminada. Las entradas de extensión pueden ser eliminadas sin eliminar la entrada de usuario correspondiente. Esto permite conservar los ajustes de usuario y su asociación con una extensión distinta al modificar el número **Extensión de base** de la extensión para coincidir con la **ID de extensión del usuario**.

Procesos

- **Reemplazo de un componente por otro igual** 166
- **Reemplazo de un componente de mayor capacidad** 166
- **Reemplazo de un componente de menor capacidad** 166
- **Inserción de un componente nuevo** 166
- **Eliminación permanente de un componente** 167
- **Reemplazo por un tipo diferente de componente** 167

12.5.1 Reemplazo de un componente por otro igual

En caso de reemplazar un componente por otro del mismo tipo, no es necesario realizar cambios a la configuración.

Para realizar un reemplazo de un componente por otro igual

1. Apague el sistema 161.
2. Desactive la alimentación del sistema.
3. Extraiga la tarjeta o el módulo de expansión externo. Observe que la ranura de tarjeta o el puerto de extensión utilizado para el reemplazo debe quedar instalado en la misma posición.
4. Instale el reemplazo con ayuda del procedimiento apropiado para el componente correspondiente (Ajuste de las tarjetas IP500 80, Integración de módulos de expansión externos 88).
5. Reinicie el sistema de IP Office.

12.5.2 Reemplazo por equipos de mayor capacidad

En caso de reemplazar un componente por otro del mismo tipo pero con mayor capacidad, IP Office creará automáticamente las entradas de configuración para las nuevas troncales o extensiones/usuarios durante el reinicio.

Para reemplazar un componente por uno del mismo tipo pero de mayor capacidad

1. Apague el sistema 161.
2. Desactive la alimentación del sistema.
3. Extraiga la tarjeta o el módulo de expansión externo. Observe que la ranura de tarjeta o el puerto de extensión utilizado para el reemplazo debe quedar instalado en la misma posición.
4. Instale el reemplazo con ayuda del procedimiento apropiado para el componente correspondiente (Ajuste de las tarjetas IP500 80, Integración de módulos de expansión externos 88).
5. Reinicie el sistema de IP Office.
6. Utilice IP Office Manager para configurar las nuevas troncales o extensiones/usuarios.

12.5.3 Reemplazo por equipos de menor capacidad

En caso de reemplazar un componente por otro del mismo tipo pero con menor capacidad, debería editar la configuración de IP Office después de reiniciarlo para eliminar las entradas redundantes.

Para reemplazar un componente por uno del mismo tipo, pero de menor capacidad

1. Apague el sistema 161.
2. Desactive la alimentación del sistema.
3. Extraiga la tarjeta o el módulo de expansión externo. Observe que la ranura de tarjeta o el puerto de extensión utilizado para el reemplazo debe quedar instalado en la misma posición.
4. Instale el reemplazo con ayuda del procedimiento apropiado para el componente correspondiente (Ajuste de las tarjetas IP500 80, Integración de módulos de expansión externos 88).
5. Reinicie el sistema de IP Office.
6. Con ayuda de IP Office Manager, elimine las troncales o extensiones/usuarios que ya no están admitidos por el nuevo componente instalado.

12.5.4 Inserción de un componente nuevo

En caso de estar agregando un componente nuevo en una ranura o puerto disponible, IP Office creará automáticamente las entradas de configuración para las nuevas troncales o extensiones/usuarios durante el reinicio.

Para agregar un nuevo componente

1. Apague el sistema 161.
2. Desactive la alimentación del sistema.
3. Instale el reemplazo con ayuda del procedimiento apropiado para el componente correspondiente (Ajuste de las tarjetas IP500 80, Integración de módulos de expansión externos 88).
4. Reinicie el sistema de IP Office.
5. Utilice IP Office Manager para configurar las nuevas troncales o extensiones/usuarios.

12.5.5 Extracción permanente

En caso de estar eliminando el componente en forma permanente, deberá editar la configuración para eliminar entradas de troncales o extensiones/usuarios redundantes.

Para eliminar un componente de manera permanente

1. Apague el sistema 161.
2. Desactive la alimentación del sistema.
3. Extraiga la tarjeta o el módulo de expansión externo.
4. Reinicie el sistema de IP Office.
5. Con ayuda de IP Office Manager, elimine las troncales o extensiones/usuarios en la configuración que corresponden al componente eliminado.
6. En el menú **Unidad de control** de la configuración elimine la entrada del componente que ya no está presente en el sistema.

12.5.6 Reemplazo por un tipo diferente

En caso de reemplazar un componente con otro de distinto tipo, el proceso debe dividirse en dos etapas.

1. Primero, extraiga el componente existentes con ayuda del procedimiento para Extracción permanente 167 y ajuste la configuración y reinicie el equipo.
2. A continuación, instale el nuevo componente con ayuda del procedimiento para Inserción de un componente nuevo 166 proceso.

12.6 Devolver la configuración a valores predeterminados

Los siguientes procesos borran la configuración contenida en la memoria de la unidad de control. Esto incluye tanto la configuración actual empleada en la memoria RAM como la copia de seguridad de la configuración, almacenada en la memoria no volátil. A continuación, el sistema se reinicia con una configuración predeterminada.

Este proceso debe realizarse desde una PC con dirección de IP fija, directamente conectada a la unidad de control con el sistema desconectado de la red. Después de este proceso, la dirección IP predeterminada de la unidad de control será 192.168.42.1.

- **Sistemas de modo estándar**
  Para la versión 7.0 de IP Office y superiores, los sistemas IP500 V2 que usan tarjetas SD de sistema **IP Office A-Law** o **IP Office U-Law** Las tarjetas SD del sistema cambian de manera predeterminada a modo IP Office Basic Edition. Al cargar la configuración cambia IP Office Manager a su vista simplificada. Para cambiar el sistema de vuelta a operación en modo estándar IP Office, consulte Cambio del sistema al modo estándar 101.

Opciones de proceso

1. **Devolver la configuración a valores predeterminados mediante IP Office Manager** 168
2. **Devolver la configuración a valores predeterminados mediante IP Office Web Manager** 168
3. **Devolver la configuración a valores predeterminados mediante el botón Restablecer** 169
4. **Devolver la configuración a valores predeterminados mediante un teléfono del sistema** 171
5. **Devolver la configuración a valores predeterminados mediante depuración** 170
6. **Devolver la configuración a valores predeterminados mediante carga por reinicio** 171

12.6.1 Devolver la configuración a valores predeterminados mediante IP Office Manager

Lea y observe las advertencias respecto de la devolución de la configuración 168 antes de usar este proceso.

Para borrar la configuración mediante IP Office Manager

1. Inicie IP Office Manager.
2. Seleccionar **Archivo | Avanzado | Borrar configuración (predeterminado)**.
3. Seleccione el sistema que se devolverá a los valores predeterminados y haga clic **Aceptar**.
4. Ingrese un nombre de administración y una contraseña, y haga clic en **Aceptar**.

12.6.2 Devolver la configuración a valores predeterminados mediante IP Office Web Manager

Lea y observe las advertencias respecto de la devolución de la configuración 168 antes de usar este proceso.

Para devolver la configuración a valores predeterminados mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones**. Seleccione **Comandos de servicio** y luego presione **Borrar configuración**.
3. Haga clic en **Aceptar**.
4. Espere hasta que el sistema se haya reiniciado antes de volver a iniciar sesión.

12.6.3 Devolver la configuración a valores predeterminados mediante el botón Restablecer

Lea y observe las advertencias respecto de la devolución de la configuración 168 antes de usar este proceso.

Para devolver la configuración a sus valores predeterminados mediante el botón Restablecer

1. En la parte posterior de la unidad de control, mantenga presionado el botón **Restablecer** entre 10 a 30 segundos hasta que el led **CPU** cambie a anaranjado intermitente.
2. Cuando oprime el botón **CPU** LED cambia a anaranjado intermitente, suelte el botón.
   - Si se ha configurado el **CPU** LED cambió a rojo, mantenga el botón presionado hasta el **CPU** LED cambia a verde intermitente. Luego suelte el botón y reintente el proceso una vez que el LED de la CPU ha vuelto a verde fijo.
3. Espere a que finalice el reinicio antes de realizar cualquier otra acción.

12.6.4 Devolver la configuración a valores predeterminados mediante depuración

Lea y observe las advertencias respecto de la devolución de la configuración [168] antes de usar este proceso.

- **ADVERTENCIA**
  El puerto RS232 solo debe utilizarse si es absolutamente necesario y solo si las acciones no pueden completarse mediante IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer un máximo esfuerzo para asegurar que existe una copia de respaldo de la configuración del sistema.

Para borrar la configuración mediante depuración:

Este proceso elimina los ajustes de configuración de IP Office sin modificar los ajustes de seguridad. Es un procedimiento más sencillo que el método de carga por reinicio.

1. Compruebe que cuenta con una copia de seguridad de la configuración de IP Office antes de realizar esta acción. Si no es posible descargar una copia de la configuración con ayuda de IP Office Manager, verifique en el directorio de aplicaciones de IP Office Manager en busca de configuraciones descargadas anteriormente.
   a. Utilice IP Office Manager para descargar una copia actualizada de la configuración. De no ser posible, verifique la carpeta de aplicaciones IP Office Manager en busca de una copia anterior de la configuración.
   b. Mediante IP Office Manager, seleccione **Archivo | Abrir configuración**.
   c. Con ayuda de la opción **Menú Seleccionar IP Office**localice y seleccione el sistema IP Office. Haga clic en **Aceptar**.
   d. Ingrese el nombre y contraseña de una cuenta de usuario de servicio para este sistema IP Office. Haga clic en **Aceptar**. IP Office Manager recibirá y visualizará la configuración del sistema IP Office.
      - Si no lo ha hecho aún, esta acción crea una entrada BOOTP en IP Office Manager para el sistema IP Office.
      - Esta acción también confirma que existe una comunicación entre la PC IP Office Manager e IP Office antes de continuar con el proceso.
   e. Seleccione **Archivo | Guardar configuración como...** y guarde una copia del archivo de configuración en la PC.
2. Conecte el cable serial entre la PC y el puerto DTE RS232 en la unidad de control IP Office.
   a. Inicie el programa de terminales en su PC. Compruebe que ha sido configurada por como aparece en la Configuración del puerto DTE RS232 [293]. En una sesión de HyperTerminal, la configuración actual aparece resumida en la base de la pantalla.
   b. Ingrese **AT** (sensible a mayúsculas). La unidad de control debe responder ***Aceptar***.
   c. Ingrese **AT-DEBUG**. La unidad de control responderá con la hora, la fecha, y un aviso ***Hello>*** para demostrar que está lista para aceptar comandos.
3. Para eliminar la configuración actual de la memoria RAM, ingrese **eraseconfig**. La línea de comando ***Hello>*** aparecerá de nuevo al completar la acción.
4. Para eliminar la configuración de respaldo almacenada en la memoria Flash no volátil, ingrese **erasenvconfig**. La línea de comando ***Hello>*** aparecerá de nuevo al completar la acción.
5. Para reiniciar el sistema IP Office ingrese **reboot**. IP Office se reiniciará con una configuración predeterminada.
6. Cierre sesión en el programa de terminal.
7. Puede usar ahora IP Office Manager para modificar y cargar un archivo de configuración anterior, o bien recibir y editar la configuración actual predeterminada de la unidad de control.

12.6.5 Devolver la configuración a valores predeterminados mediante un teléfono del sistema

Este proceso no lo admiten los teléfonos del sistema para un sistema que se ejecuta en el modo estándar de IP Office.

12.6.6 Devolver la configuración a valores predeterminados mediante carga por reinicio

Lea y observe las advertencias respecto de la devolución de la configuración 168 antes de usar este proceso.

- **ADVERTENCIA**
  El puerto RS232 solo debe utilizarse si es absolutamente necesario y solo si las acciones no pueden completarse mediante IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer un máximo esfuerzo para asegurar que existe una copia de respaldo de la configuración del sistema.

Para borrar la configuración y la configuración de seguridad mediante la carga por reinicio

Este proceso también devuelve a los valores predeterminados la configuración de seguridad de IP Office.

1. Compruebe que cuenta con una copia de seguridad de la configuración de IP Office antes de realizar esta acción. Si no es posible descargar una copia de la configuración con ayuda de IP Office Manager, verifique en el directorio de aplicaciones de IP Office Manager en busca de configuraciones descargadas anteriormente.
   a. Utilice IP Office Manager para descargar una copia actualizada de la configuración. De no ser posible, verifique la carpeta de aplicaciones IP Office Manager en busca de una copia anterior de la configuración.
   b. Mediante IP Office Manager, seleccione **Archivo | Abrir configuración**.
   c. Con ayuda de la opción **Menú Seleccionar IP Office**localice y seleccione el sistema IP Office. Haga clic en **Aceptar**.
   d. Ingrese el nombre y contraseña de una cuenta de usuario de servicio para este sistema IP Office. Haga clic en **Aceptar**. IP Office Manager recibirá y visualizará la configuración del sistema IP Office.
      - Si no lo ha hecho aún, esta acción crea una entrada BOOTP en IP Office Manager para el sistema IP Office.
      - Esta acción también confirma que existe una comunicación entre la PC IP Office Manager e IP Office antes de continuar con el proceso.
   e. Seleccione **Archivo | Guardar configuración como...** y guarde una copia del archivo de configuración en la PC.
2. Conecte el cable serial entre la PC y el puerto DTE RS232 en la unidad de control IP Office.
   a. Inicie el programa de terminales en su PC. Compruebe que ha sido configurada por como aparece en la Configuración del puerto DTE RS232 293. En una sesión de HyperTerminal, la configuración actual aparece resumida en la base de la pantalla.
   b. Disponga las ventanas de programa de forma que el programa Terminal y el Registro TFTP de IP Office Manager sean visibles al mismo tiempo.
   c. Desconecte la energía de la unidad de control IP Office.
   d. Encienda la unidad de control y oprima la tecla de escape cada segundo hasta que aparezca un mensaje de Loader. Vea más abajo un ejemplo.

      ```
      P12 Loader 2.4
      CPU Revision 0x0900
      ```

   e. Ingrese **AT** (sensible a mayúsculas). La unidad de control debe responder ***OK***.
   f. De no recibir la respuesta OK, compruebe los ajustes de su programa de terminal y repita el proceso anterior.
3. Realice el proceso de eliminación.
   - Para eliminar el registro de alarmas, ingrese ***AT-X1***.
   - Para eliminar la configuración actual, ingrese ***AT-X2***. Una respuesta típica es ***Eliminar Sector 2 (NV Config)*** seguido de ***Aceptar***. Ingrese ***AT-X3***. Una respuesta típica es ***Eliminación Sector (Config)*** seguido por una serie de respuestas ***Aceptar***.
4. Apague la energía de la unidad de control y luego enciéndala de nuevo. En el programa de terminal, verá varios mensajes conforme la unidad de control realiza distintas tareas de inicio.
5. Cierre sesión en el programa de terminal.
6. Puede usar ahora IP Office Manager para modificar y cargar un archivo de configuración anterior, o bien recibir y editar la configuración actual predeterminada de la unidad de control.

12.7 Definición de la configuración de seguridad predeterminada

Si es necesario, los ajustes de seguridad para el acceso al sistema se pueden devolver a los valores predeterminados. Esto incluye restaurar todas las cuentas de usuario de servicio de seguridad, incluidas aquellas que fueron usadas por aplicaciones IP Office. Por lo tanto, es posible que tales aplicaciones se deban reconfigurar para usar las cuentas de usuario de servicio o contraseñas de cuenta nuevas.

Restaurar la configuración inicial de la seguridad del sistema no afecta las contraseñas de los usuarios, los códigos del correo de voz ni los códigos de inicio de sesión. Sin embargo, las características de seguridad incluyen reglas para las contraseñas de usuario permitidas. Por lo tanto, al respetar la seguridad predeterminada es posible que se indique que algunas contraseñas de usuario existentes son erróneas.

Si se respeta la seguridad predeterminada, también se debe respetar el asesoramiento del capítulo Protección del sistema 126. Para obtener más información sobre los ajustes de seguridad predeterminados para un sistema, consulte la documentación IP Office Manager.

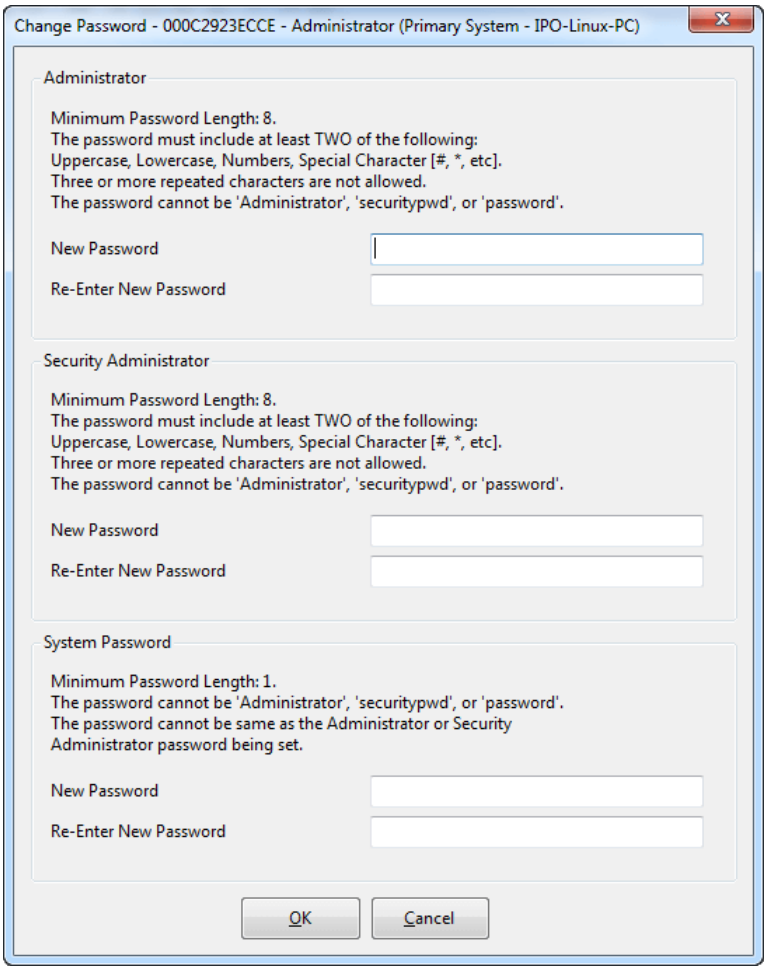
- **ADVERTENCIA: Interrupción de servicio**
  Aunque cuando se vuelven las configuraciones de seguridad a los valores predeterminados no se requiere reiniciar el sistema, esto puede causar la interrupción del servicio durante varios minutos mientras que el sistema genera un certificado de seguridad nuevo.

Opciones de proceso

1. **Devolver la configuración de seguridad a valores predeterminados mediante IP Office Manager** 173
2. **Devolver la configuración a valores predeterminados mediante IP Office Web Manager** 173
3. **Devolver la configuración de seguridad a valores predeterminados mediante el puerto RS232** 174
4. **Devolver la configuración de seguridad a valores predeterminados mediante carga por reinicio** 175

Inicio de sesión después de devolver la configuración de seguridad predeterminada:

Cuando IP Office Manager se conecta a un sistema con la configuración de seguridad predeterminada, le avisa que modifique las contraseñas predeterminadas. Esto también es aplicable si una de las contraseñas se devuelve al valor predeterminado.



12.7.1 Devolver la seguridad a valores predeterminados mediante IP Office Manager

Lea y observe las advertencias sobre cómo devolver la seguridad a valores predeterminados 172 antes de usar este proceso.

- **ADVERTENCIA: Interrupción de servicio**
  Aunque cuando se vuelven las configuraciones de seguridad a los valores predeterminados no se requiere reiniciar el sistema, esto puede causar la interrupción del servicio durante varios minutos mientras que el sistema genera un certificado de seguridad nuevo.

Para devolver la configuración de seguridad a los valores predeterminados mediante IP Office Manager

1. Inicie IP Office Manager.
2. Seleccionar **Archivo | Opciones avanzadas | Borrar configuración de seguridad (predeterminada)**.
3. Seleccione el sistema del menú y haga clic **Aceptar**.
4. Ingrese el nombre y la contraseña para acceder a la configuración de seguridad.
5. IP Office Manager indica cuándo se ha restaurado la configuración de seguridad.

12.7.2 Devolver la seguridad a valores predeterminados mediante IP Office Web Manager

Lea y observe las advertencias sobre cómo devolver la seguridad a valores predeterminados 172 antes de usar este proceso.

- **ADVERTENCIA: Interrupción de servicio**
  Aunque cuando se vuelven las configuraciones de seguridad a los valores predeterminados no se requiere reiniciar el sistema, esto puede causar la interrupción del servicio durante varios minutos mientras que el sistema genera un certificado de seguridad nuevo.

Para devolver la configuración de seguridad de un sistema mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones**. Seleccione **Comandos de servicio** y luego presione **Borrar ajustes de seguridad**.
3. Haga clic en **Aceptar**.

12.7.3 Devolver la seguridad a valores predeterminados mediante el puerto RS232

Lea y observe las advertencias sobre cómo devolver la seguridad a valores predeterminados [172] antes de usar este proceso.

- **ADVERTENCIA: Interrupción de servicio**
  Aunque cuando se vuelven las configuraciones de seguridad a los valores predeterminados no se requiere reiniciar el sistema, esto puede causar la interrupción del servicio durante varios minutos mientras que el sistema genera un certificado de seguridad nuevo.
- **ADVERTENCIA**
  El puerto RS232 solo debe utilizarse si es absolutamente necesario y solo si las acciones no pueden completarse mediante IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer un máximo esfuerzo para asegurar que existe una copia de respaldo de la configuración del sistema.

Para devolver la configuración de seguridad a los valores predeterminados a través de DTE

Este proceso define como predeterminados los ajustes de seguridad de IP Office sin modificar los ajustes de configuración.

1. Conecte el cable serial entre la PC y el puerto DTE en la unidad de control IP Office.
2. Inicie el programa de terminales en su PC. Compruebe que ha sido configurada por como aparece en la sección Configuración del puerto DTE [293]. En una sesión de HyperTerminal, la configuración actual aparece resumida en la base de la pantalla.
3. Ingrese **AT** (sensible a mayúsculas). La unidad de control debe responder ***Aceptar***.
4. Ingrese **AT-SECURITYRESETALL**.
5. Recibirá un aviso para confirmar la dirección MAC de la unidad de control antes de continuar. Ingrese la dirección.
6. Después de aproximadamente un minuto, la unidad de control responderá ***Aceptar*** una vez finalizada esta acción.
7. Cierre sesión en el programa de terminal.
8. Puede usar IP Office Manager ahora para recibir y editar los nuevos configuración de seguridad predeterminados de la unidad de control.

12.7.4 Devolver la seguridad a valores predeterminados mediante carga por reinicio

Lea y observe las advertencias sobre cómo devolver la seguridad a valores predeterminados 172 antes de usar este proceso.

- **ADVERTENCIA: Interrupción de servicio**
  Aunque cuando se vuelven las configuraciones de seguridad a los valores predeterminados no se requiere reiniciar el sistema, esto puede causar la interrupción del servicio durante varios minutos mientras que el sistema genera un certificado de seguridad nuevo.
- **ADVERTENCIA**
  El puerto RS232 solo debe utilizarse si es absolutamente necesario y solo si las acciones no pueden completarse mediante IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer un máximo esfuerzo para asegurar que existe una copia de respaldo de la configuración del sistema.

Para devolver la configuración de seguridad de un sistema a través de carga por reinicio

Este proceso devuelve los ajustes de seguridad y de configuración a las opciones predeterminadas.

1. Compruebe que cuenta con una copia de seguridad de la configuración de IP Office antes de realizar esta acción. Si no es posible descargar una copia de la configuración con ayuda de IP Office Manager, verifique en el directorio de aplicaciones de IP Office Manager en busca de configuraciones descargadas anteriormente.
   a. Utilice IP Office Manager para descargar una copia actualizada de la configuración. De no ser posible, verifique la carpeta de aplicaciones IP Office Manager en busca de una copia anterior de la configuración.
   b. Mediante IP Office Manager, seleccione **Archivo | Abrir configuración**.
   c. Con ayuda de la opción **Menú Seleccionar IP Office**localice y seleccione el sistema IP Office. Haga clic en **Aceptar**.
   d. Ingrese el nombre y contraseña de una cuenta de usuario de servicio para este sistema IP Office. Haga clic en **Aceptar**. IP Office Manager recibirá y visualizará la configuración del sistema IP Office.
      - Si no lo ha hecho aún, esta acción crea una entrada BOOTP en IP Office Manager para el sistema IP Office.
      - Esta acción también confirma que existe una comunicación entre la PC IP Office Manager e IP Office antes de continuar con el proceso.
   e. Seleccione **Archivo | Guardar configuración como...** y guarde una copia del archivo de configuración en la PC.
2. Conecte el cable serial entre la PC y el puerto DTE RS232 en la unidad de control IP Office.
   a. Inicie el programa de terminales en su PC. Compruebe que ha sido configurada por como aparece en la Configuración del puerto DTE RS232 293. En una sesión de HyperTerminal, la configuración actual aparece resumida en la base de la pantalla.
   b. Disponga las ventanas de programa de forma que el programa Terminal y el Registro TFTP de IP Office Manager sean visibles al mismo tiempo.
   c. Desconecte la energía de la unidad de control IP Office.
   d. Encienda la unidad de control y oprima la tecla de escape cada segundo hasta que aparezca un mensaje de Loader. Vea más abajo un ejemplo.

      ```
      P12 Loader 2.4
      CPU Revision 0x0900
      ```

   e. Ingrese **AT** (sensible a mayúsculas). La unidad de control debe responder ***OK***.
   f. De no recibir la respuesta OK, compruebe los ajustes de su programa de terminal y repita el proceso anterior.
3. Para eliminar la configuración actual en la memoria RAM, ingrese **AT-X3**. Una respuesta típica es ***Eliminación Sector (Config)*** seguido por una serie de respuestas ***Aceptar***.
4. Para eliminar la copia de seguridad de la configuración almacenada en la memoria no volátil, ingrese **AT-X2**. Una respuesta típica es ***Eliminar Sector 2 (NV Config)*** seguido de ***Aceptar***. IP Office 403 solamente: Si ejecuta una unidad de control IP Office 403, ingrese también **AT-X4**.
5. Apague la energía de la unidad de control y luego enciéndala de nuevo. En el programa de terminal, verá varios mensajes conforme la unidad de control realiza distintas tareas de inicio.
6. Cierre sesión en el programa de terminal.
7. Puede usar ahora IP Office Manager para modificar y cargar un archivo de configuración anterior, o bien recibir y editar la configuración actual predeterminada de la unidad de control.

12.8 Carga de una configuración

La configuración existente de un sistema se puede reemplazar por una configuración nueva que se haya preparado por separado.

- La configuración creada debe coincidir con el equipo físico del sistema IP Office donde está cargada la configuración. De lo contrario, el sistema IP Office puede reiniciarse y experimentar otras dificultades.

Opciones de proceso

1. **Creación de un archivo de configuración sin conexión** 177
2. **Carga de una configuración mediante IP Office Manager** 178
3. **Carga de una configuración mediante IP Office Web Manager** 178
4. **Carga de un archivo de configuración en una tarjeta SD del sistema** 178

12.8.1 Creación de un archivo de configuración sin conexión

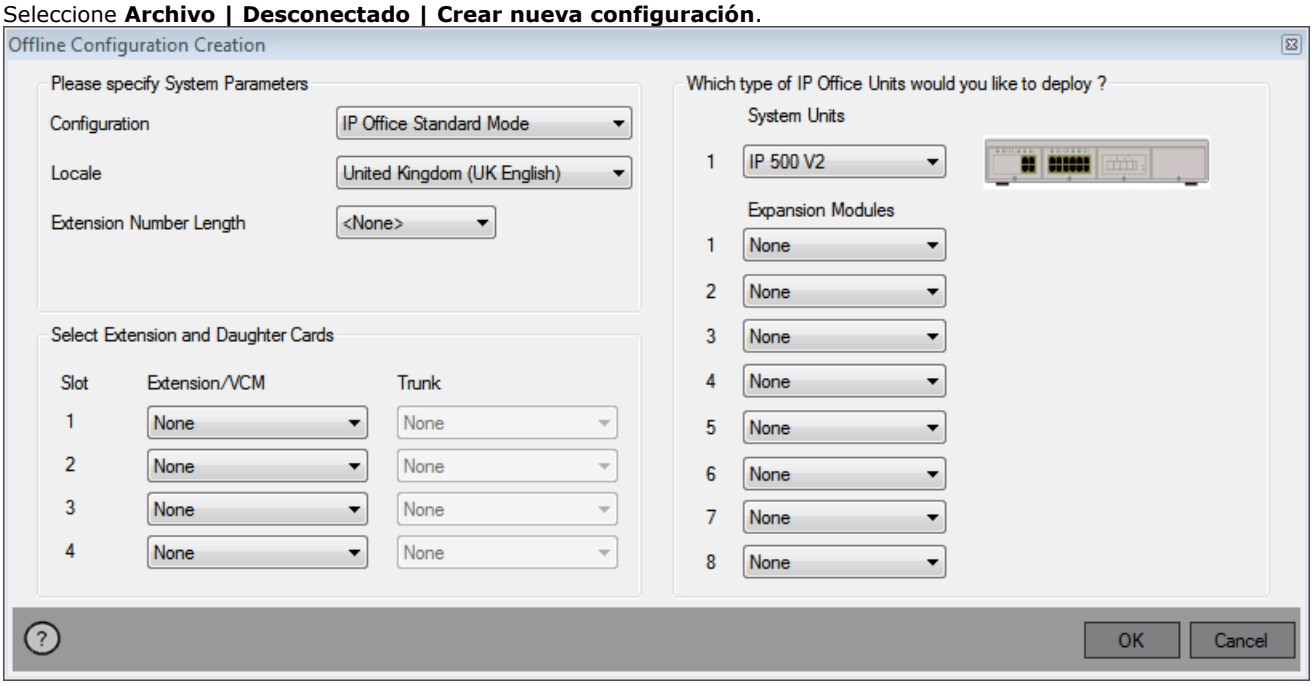
IP Office Manager se puede utilizar para crear una nueva configuración sin necesidad de conectarse a un sistema IP Office. Puede especificar durante el proceso la ubicación del sistema, el tipo de tarjetas de troncales que utiliza y el tipo de unidad de control y módulos de expansión que incluye.

Esto permite crear una configuración antes de instalar el sistema. El archivo de configuración se puede colocar en la tarjeta System SD antes de instalarla en el sistema. De lo contrario, la configuración puede cargarse en el sistema después de realizar la instalación inicial del sistema.

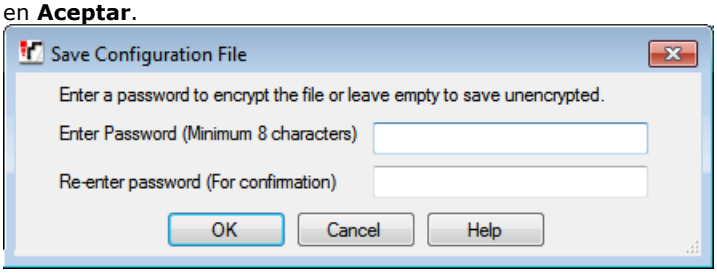
- La configuración creada debe coincidir con el equipo físico del sistema IP Office donde está cargada la configuración. De lo contrario, el sistema IP Office puede reiniciarse y experimentar otras dificultades.

Para crear un archivo de configuración sin conexión

1. Inicie IP Office Manager sin ninguna configuración cargada en IP Office Manager
2. Seleccione **Archivo | Desconectado | Crear nueva configuración**.



3. Seleccione el tipo de configuración que desea crear. El equipo y los ajustes se restringen a los compatibles en el modo seleccionado.
4. Cuando haya terminado el proceso, haga clic en **Aceptar**.
5. IP Office Manager creará y cargará la configuración.
6. Edite la configuración para adaptarse a los requerimientos del cliente. Esto puede incluir importar información desde archivos CSV preparados previamente.
    - Tenga en cuenta que ya que esta configuración se está realizando sin conexión, y sin licencias, puede configurar características que podrían convertirse en no compatibles una vez que la configuración se cargue en el sistema con conexión.
7. Cuando haya completado el proceso, seleccione **Archivo | Guardar configuración como**.
8. Cuando se le indique que ingrese una contraseña para encriptar el archivo, deje los campos en blanco y haga clic en **Aceptar**.



12.8.2 Carga de una configuración mediante IP Office Manager

Este proceso reemplazará la configuración existente.

- La configuración creada debe coincidir con el equipo físico del sistema IP Office donde está cargada la configuración. De lo contrario, el sistema IP Office puede reiniciarse y experimentar otras dificultades.

Para cargar una configuración sin conexión mediante IP Office Manager

1. Inicie IP Office Manager.
2. Seleccionar **Archivo | Desconectado | Abrir archivo...**.
3. Seleccione el archivo de configuración y haga clic en **Abrir**.
4. Compruebe que los ajustes de configuración son los esperados y realice cualquier ajuste de ser necesario.
5. Seleccionar **Archivo | Desconectado | Enviar configuración...**.
6. Seleccione el sistema y haga clic en **Aceptar**.
7. Ingrese un nombre de administración y una contraseña, y haga clic en **Aceptar**.
8. Seleccione cuándo debe cargarse la nueva configuración. No seleccione la opción **Combinar**.
9. Haga clic en **Aceptar**.

12.8.3 Carga de una configuración mediante IP Office Web Manager

Este proceso reemplazará la configuración existente.

- La configuración creada debe coincidir con el equipo físico del sistema IP Office donde está cargada la configuración. De lo contrario, el sistema IP Office puede reiniciarse y experimentar otras dificultades.

Para cargar una configuración sin conexión mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Haga clic en **Acciones**. Seleccione **Comandos de servicio** y luego presione **Cargar configuración**. Haga clic en **Supervisión** y seleccione **Cargar configuración**.
3. Haga clic en **Navegación** y seleccione el archivo de configuración.
4. Haga clic en **Cargar**.
5. Haga clic en **Aceptar**.
6. Reinicie el sistema para que la nueva configuración se aplique por completo. Consulte la sección Reinicio de un sistema 163.

12.8.4 Carga de una configuración en una tarjeta SD del sistema

Este proceso reemplazará la configuración existente.

- La configuración creada debe coincidir con el equipo físico del sistema IP Office donde está cargada la configuración. De lo contrario, el sistema IP Office puede reiniciarse y experimentar otras dificultades.

Para cargar una configuración directamente en una tarjeta SD del sistema

1. Cambie el nombre del archivo de configuración sin conexión a *config.cfg*.
2. Apague y extraiga la tarjeta SD del sistema. Consulte la sección Extracción y apagado de la tarjeta de memoria 153.
3. Inserte la tarjeta SD en la PC y muestre el contenido de la tarjeta.
4. Abra la carpeta /sistema/principal y reemplace el archivo config.cfg existente por el archivo nuevo.
5. Reinserte la tarjeta SD del sistema en el sistema.
6. Reinicie el sistema. Consulte la sección Reinicio de un sistema 163.

12.9 Acualización de sistemas

Hay varios métodos por los cuales el sistema se puede actualizar a una nueva versión de software principal de IP Office.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecuten versiones anteriores a 8.1(65) antes deben actualizarse a IP Office versión 8.1(65) (o posterior a 8.1) o cualquier versión de IP Office 9.0 y luego actualizarla a IP Office versión 9.1 o posterior. Para las versiones anteriores no se requiere una actualización intermedia si el sistema se sigue actualizando.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 10.0:**
  IP Office versión 10 y versiones posteriores solo son compatibles con licencias PLDS. Para actualizar un sistema que está usando licencias ADI, esas licencias se deben migrar primero a PLDS.

  - Para migrar de licencia debe obtener un archivo de licencia de migración mediante IP Office Manager (**Herramientas | Migración de licencia**) y, luego, enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra todas las licencias virtuales que posea para que el sistema emita una equivalencia de las licencias PLDS pero ahora asociadas a la clave de función. Actualice el sistema solo cuando ya haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que si continúa con la migración de licencia, Avaya borrará todos los registros de la posesión de licencias ADI que posee para esa clave de función.

- **ADVERTENCIA: Requisitos de actualización de licencia**
  En un sistema nuevo, al hacer la primera llamada el nivel de software en ejecución se escribe en la memoria permanente de la unidad de control. Cualquier actualización subsiguiente a una versión más nueva requiere la adición de la licencia **Essential Edition** para la versión de destino. Los sistemas actualizados sin dicha licencia muestran *"Sin licencia disponible"* en algunos teléfonos y no se permite ninguna función de telefonía.

- **Nota: Sistemas Server Edition**
  Las unidades de control IP500 V2 que se configuran como sistemas IP500 V2 Expansion sistema reciben licencias y actualizaciones a través de los menús de administración web de Server Edition. Consulte la documentación de Server Edition.

⚠ ADVERTENCIAS

- **Compruebe los Boletines técnicos de IP Office**
  Verifique el último Boletín Técnico de IP Office referente a la versión de software de IP Office antes de continuar con el procedimiento. Puede que contenga información relacionada con cambios ocurridos después de completar este documento. Los boletines técnicos están disponibles en http://support.avaya.com.

  - **IP Office Web Manager**
    Para agregar IP Office Web Manager se necesitan cambios en la configuración de seguridad de los sistemas. Para los nuevos sistemas, estos cambios se realizan automáticamente. Sin embargo, para un sistema que se está actualizando, los cambios solo se pueden realizar si se establece la configuración de seguridad predeterminada del sistema. Consulte la sección Activación de IP Office Web Manager 206 para los pasos adicionales que se deberían realizar antes de actualizar a IP Office versión 8.0 o posterior.

- **Otras aplicaciones IP Office**
  La actualización del software principal de una unidad de control IP Office requerirá que se realicen actualizaciones del software asociado. Los niveles de software de aplicación compatibles con la versión principal de IP Office se detallan en el Boletín técnico de IP Office para la versión.

Opciones de proceso

1. **Actualización mediante el asistente de actualización de IP Office Manager** 180
   Este proceso actualiza el sistema o los sistemas mediante los archivos firmware instalados con la aplicación IP Office Manager.
2. **Actualizar de manera remota los archivos de la tarjeta SD del sistema mediante IP Office Manager** 182
   Este proceso actualiza los archivos de la tarjeta SD del sistema de manera remota mediante IP Office Manager. El sistema necesita entonces reiniciarse para usar los nuevos archivos.
3. **Actualización de una tarjeta SD del sistema mediante la PC IP Office Manager** 183
   Una PC con IP Office Manager se puede usar para actualizar directamente los archivos en una tarjeta SD. Esa tarjeta luego se puede insertar en el sistema y este se reinicia.
4. **Actualización mediante una tarjeta SD opcional** 184
   Este procso actualiza el sistema al usar IP Office Manager para crear una tarjeta SD cargada con los archivos instalados con la aplicación IP Office Manager.
5. **Actualización mediante IP Office Web Manager** 185
   Este proceso actualiza el sistema mediante un conjunto de archivo firmware proporcionados con este fin. No requiere IP Office Manager.

12.9.1 Actualizar mediante el asistente de actualización

El asistente de actualización es parte de IP Office Manager. Puede usarse para actualizar los diversos sistemas al mismo tiempo.

- **ADVERTENCIA: Versión IP Office Manager**
  Este proceso utiliza archivos de software provistos por la versión instalada de IP Office Manager que está en uso. Debe asegurarse de que la versión de IP Office Manager que está en uso concuerde con la versión de software requerida.
- **Múltiples copias de Manager**
  Si hay más de una copia de IP Office Manager en ejecución, es posible que IP Office solicite archivos BIN a una instancia de IP Office Manager distinta de la que inició el proceso de actualización. Asegúrese de que sólo una copia de IP Office Manager esté en ejecución durante la actualización de un sistema IP Office.
- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecuten versiones anteriores a 8.1(65) antes deben actualizarse a IP Office versión 8.1(65) (o posterior a 8.1) o cualquier versión de IP Office 9.0 y luego actualizarla a IP Office versión 9.1 o posterior. Para las versiones anteriores no se requiere una actualización intermedia si el sistema se sigue actualizando.
- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 10.0:**
  IP Office versión 10 y versiones posteriores solo son compatibles con licencias PLDS. Para actualizar un sistema que está usando licencias ADI, esas licencias se deben migrar primero a PLDS.
  - Para migrar de licencia debe obtener un archivo de licencia de migración mediante IP Office Manager (**Herramientas | Migración de licencia**) y, luego, enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra todas las licencias virtuales que posea para que el sistema emita una equivalencia de las licencias PLDS pero ahora asociadas a la clave de función. Actualice el sistema solo cuando ya haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que si continúa con la migración de licencia, Avaya borrará todos los registros de la posesión de licencias ADI que posee para esa clave de función.

Para actualizar sistemas que usan el asistente de actualización

1. Compruebe que cuenta con una copia de seguridad de la configuración de IP Office antes de realizar esta acción. Si no es posible descargar una copia de la configuración con ayuda de IP Office Manager, verifique en el directorio de aplicaciones de IP Office Manager en busca de configuraciones descargadas anteriormente.
   a. Utilice IP Office Manager para descargar una copia actualizada de la configuración. De no ser posible, verifique la carpeta de aplicaciones IP Office Manager en busca de una copia anterior de la configuración.
   b. Mediante IP Office Manager, seleccione **Archivo | Abrir configuración**.
   c. Con ayuda de la opción **Menú Seleccionar IP Office**localice y seleccione el sistema IP Office. Haga clic en **Aceptar**.
   d. Ingrese el nombre y contraseña de una cuenta de usuario de servicio para este sistema IP Office. Haga clic en **Aceptar**. IP Office Manager recibirá y visualizará la configuración del sistema IP Office.
      - Si no lo ha hecho aún, esta acción crea una entrada BOOTP en IP Office Manager para el sistema IP Office.
      - Esta acción también confirma que existe una comunicación entre la PC IP Office Manager e IP Office antes de continuar con el proceso.
   e. Seleccione **Archivo | Guardar configuración como...** y guarde una copia del archivo de configuración en la PC.
2. Seleccione **Archivo | Avanzadas | Actualización**. Se inicia el Asistente de actualizaciones, el cual busca a la unidad de IP Office con ayuda de la dirección **Unidad/difusión**. Ajuste la dirección y haga clic en **Actualizar** si no aparecen las unidades de control esperadas. Aparece la versión actual del archivo BIN de cada IP Office dentro de la memoria de cada unidad de control. Esto es independientemente de si el archivo .bin está actualmente en uso por otro módulo en el sistema.
3. La columna **Versión** indica la versión actual del software instalado. La columna **Disponible** indica la versión del software que IP Office Manager tiene disponible. En caso que la versión disponible sea superior, se selecciona automáticamente la casilla de verificación al lado de esta fila.
   - Si alguno de los módulos tiene una versión de software anterior a la versión 2.1 es necesario realizar una actualización con la casilla de verificación **Validar** sin seleccionar. De ser éste el caso, continúe solamente con el proceso de actualización utilizando una PC con dirección IP fija en el mismo dominio LAN y segmento LAN que la unidad del sistema de IP Office y actualice solamente el sistema con versión anterior a 2.1.
   - En caso que sea realizar una actualización en múltiples etapas, utilice los siguientes pasos adicionales para seleccionar el software interino apropiado:
     - Haga clic derecho sobre el asistente de actualizaciones y haga clic en **Seleccionar directorio**. Localice y seleccione el directorio que contiene el archivo bin para el nivel de software intermedio.
     - El asistente de actualización debe mostrar una lista de as unidades de control que tienen disponible una actualización de software.

- Actualizar a niveles particulares del software IP Office 10.0 o posterior requiere la licencia Essential Edition apropiada para la versión. Las columnas **Con licencia** y **Se requiere licencia** indican las licencias que posee y las licencias que necesita para el software que está ejecutando el sistema actualmente.

4. Seleccione la casilla de verificación de cada módulo que desee actualizar.
5. Están disponibles las siguientes opciones adicionales:
   - **Archivos de respaldo del sistema**
     Si selecciona esta opción, antes de la actualización al nuevo software, los archivo actuales en la carpeta **/primary** en la tarjeta System SD se copian a la carpeta **/backup**. Si el espacio de la tarjeta SD es insuficiente para esta acción, IP Office Manager muestra la advertencia *"No hay espacio suficiente en la tarjeta SD"*.
   - **Cargar los archivos de sistema**
     Si selecciona esta opción, se realiza una copia del conjunto completo de archivos de software de IP Office Manager a la carpeta **/primary** en la tarjeta System SD. Además del software de la unidad de control y del módulo, incluye archivos de software de teléfono y los archivos utilizados para IP Office Web Manager. Los archivos de firmware de los teléfonos IP Avaya se cargan en primer lugar y, al terminar, si la opción **Reiniciar teléfonos IP** a continuación también está seleccionada, se reinician los teléfonos Avaya IP. Luego, el sistema continúa cargando cualquier otro archivo. Si el espacio de la tarjeta SD es insuficiente para esta acción, IP Office Manager muestra la advertencia *"No hay espacio suficiente en la tarjeta SD"*.
   - **Reiniciar teléfonos IP**
     Esta opción está disponible si la opción anterior, **Cargar archivos de sistema**, también está seleccionada. Si se selecciona esta opción, una vez que el sistema se ha reiniciado y ha cargado los archivos de firmware del teléfono, se reinician los teléfonos IP. Esto hace que los teléfonos vuelvan a cargar los archivos de configuración y que vuelvan a verificar si el firmware cargado actualmente coincide con el que está actualmente disponible a través del servidor de archivos configurado (de manera predeterminada, el sistema IP Office). Si se selecciona esta opción, después del reinicio del sistema, los teléfonos muestran el mensaje *"Actualizando desde el sistema"* hasta que el sistema los reinicie, después de que cargar los archivos de firmware de los teléfonos.
6. Seleccione **Actualizar**. Se le solicitará la contraseña de sistema para cada sistema. Ingrese la contraseña y haga clic en **Aceptar**. Los siguientes pasos dependen de las opciones de actualización seleccionadas. No cancele ni cierre la aplicación del asistente de actualizaciones mientras el proceso está funcionando.
   - **Espacio insuficiente en la tarjeta SD**
     Este mensaje aparece si la tarjeta SD del sistema tiene espacio insuficiente. Para continuar con una actualización confiable, la tarjeta SD debe actualizarse de manera local 183.
   - **Actualización validada**
     Si ha utilizado la opción **Validar** tomará lugar una serie de acciones como sigue;
     a. El asistente de actualización comprueba la cantidad de memoria RAM disponible en la unidad de control para almacenar temporalmente los nuevos archivos BIN. Si no hay memoria suficiente disponible, recibirá una notificación preguntando si desea continuar con una actualización sin conexión o cancelar la actualización.
        - Si elige sin conexión el IP Office se reinicia en modo fuera de línea. Es posible que necesite usar la opción **Actualizar** en Upgrade Wizard para volver a establecer la conexión después del reinicio. Puede intentar validar de nuevo la actualización para comprobar la cantidad de memoria RAM disponible para transferir los archivos BIN. Si la memoria disponible es aún insuficiente, se ofrece la opción para hacer una actualización sin validar o para cancelar.

     b. Los archivos bin necesarios son transferidos al sistema y almacenados en la memoria temporal.

     c. Si se han seleccionado, se ejecutan las acciones respaldar archivos de sistema y subir archivos de sistema.

     d. Una vez que se han transferido todos los archivos, el asistente de actualización le preguntará si acepta continuar con el proceso de actualización. Seleccione **Sí** para continuar. La unidad de control se reinicia y se actualiza en primer lugar. Luego procede con la actualización de los módulos de expansión externos.
   - **Actualización sin validar**
     Debe evitarse este método de actualización a menos que sea absolutamente necesario. Solo se requiere para sistemas IP Office con software previo a la versión 2.1 y sólo debe realizarse desde una PC IP Office Manager con dirección de IP fija que opere en el mismo segmento y sub-red LAN que el sistema IP Office. Durante la actualización, las unidades y los módulos borran su contenido actual y luego solicitan el nuevo archivo de software a IP Office Manager.
7. Después de la actualización, compruebe que el asistente de actualización muestre que se han actualizado las unidades y módulos seleccionados. Es posible que necesite seleccionar **Actualizar** para actualizar la información en la pantalla del asistente de actualización.
8. Repita el proceso conforme sea necesario.

12.9.2 Actualización remota de la tarjeta SD del sistema mediante Manager

Este proceso copiará todos los archivos de sistema que no están presentes en la tarjeta SD del sistema y aquellos archivos que tengan una versión distinta de aquellos que ya estén presentes en la tarjeta. Esto incluye los archivos de software IP Office y los archivos de instrucciones de Embedded Voicemail.

- **ADVERTENCIA: Versión IP Office Manager**
  Este proceso utiliza archivos de software provistos por la versión instalada de IP Office Manager que está en uso. Debe asegurarse de que la versión de IP Office Manager que está en uso concuerde con la versión de software requerida.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecuten versiones anteriores a 8.1(65) antes deben actualizarse a IP Office versión 8.1(65) (o posterior a 8.1) o cualquier versión de IP Office 9.0 y luego actualizarla a IP Office versión 9.1 o posterior. Para las versiones anteriores no se requiere una actualización intermedia si el sistema se sigue actualizando.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 10.0:**
  IP Office versión 10 y versiones posteriores solo son compatibles con licencias PLDS. Para actualizar un sistema que está usando licencias ADI, esas licencias se deben migrar primero a PLDS.

  - Para migrar de licencia debe obtener un archivo de licencia de migración mediante IP Office Manager (**Herramientas | Migración de licencia**) y, luego, enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra todas las licencias virtuales que posea para que el sistema emita una equivalencia de las licencias PLDS pero ahora asociadas a la clave de función. Actualice el sistema solo cuando ya haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que si continúa con la migración de licencia, Avaya borrará todos los registros de la posesión de licencias ADI que posee para esa clave de función.

Para actualizar un sistema que usa el administrador de archivos incrustado

1. Mediante IP Office Manager, seleccione **Archivo | Opciones avanzadas | Administración de archivos integrada**.
2. Seleccione el menú **Seleccionar IP Office** y seleccione el sistema IP Office.
3. Aparecerán los archivos contenidos en las tarjetas de memoria.
4. Seleccionar **Archivo | Archivos de respaldo del sistema**. Se copiará el contenido de la carpeta **/primary** en la tarjeta System SD a la carpeta **/backup**. Este proceso toma alrededor de 6 minutos.
5. Seleccione **Archivo | Cargar archivos de sistema**. Los archivos de sistema que contiene IP Office Manager serán subidos a la carpeta **/primary** en la tarjeta System SD. Esto incluye los archivos de software IP Office y los archivos de instrucciones de Embedded Voicemail. Dependiendo de los archivos que necesitan actualización, este proceso puede tomar hasta 40 minutos.

12.9.3 Actualización local de la tarjeta SD del sistema mediante Manager

Si tiene acceso físico a la unidad de control IP500 V2, puede seguir el procedimiento que se indica a continuación. Este método puede utilizarse en combinación con un reinicio programado, lo que permite que la actualización de la tarjeta se realice durante el horario normal de operaciones, seguido por el reinicio fuera del horario normal de operaciones.

Si la tarjeta se utiliza para Embedded Voicemail, este servicio no estará disponible mientras la tarjeta permanezca apagada. Las funciones con licencia continuarán funcionando hasta por dos horas mientras la tarjeta está apagada.

- **ADVERTENCIA: Versión IP Office Manager**
  Este proceso utiliza archivos de software provistos por la versión instalada de IP Office Manager que está en uso. Debe asegurarse de que la versión de IP Office Manager que está en uso concuerde con la versión de software requerida.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecuten versiones anteriores a 8.1(65) antes deben actualizarse a IP Office versión 8.1(65) (o posterior a 8.1) o cualquier versión de IP Office 9.0 y luego actualizarla a IP Office versión 9.1 o posterior. Para las versiones anteriores no se requiere una actualización intermedia si el sistema se sigue actualizando.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 10.0:**
  IP Office versión 10 y versiones posteriores solo son compatibles con licencias PLDS. Para actualizar un sistema que está usando licencias ADI, esas licencias se deben migrar primero a PLDS.

  - Para migrar de licencia debe obtener un archivo de licencia de migración mediante IP Office Manager (**Herramientas | Migración de licencia**) y, luego, enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra todas las licencias virtuales que posea para que el sistema emita una equivalencia de las licencias PLDS pero ahora asociadas a la clave de función. Actualice el sistema solo cuando ya haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que si continúa con la migración de licencia, Avaya borrará todos los registros de la posesión de licencias ADI que posee para esa clave de función.

Para actualizar una tarjeta SD del sistema mediante una PC

1. Apague la tarjeta de memoria System SD 153 y extráigala de la unidad de control.
2. Repita el proceso para reproducir una tarjeta SD 140. Este proceso sobrescribirá los archivos de software en la tarjeta con los archivos disponibles para IP Office Manager. Este proceso toma alrededor de 20 minutos.
   - El proceso no afecta ningún archivo de configuración actual, avisos y mensajes del Correo de voz integrado, ni archivos de datos SMDR temporales.
   - El proceso no elimina ningún archivo de licencia PLDS actual. Se necesita restaurar el archivo luego de recrear la tarjeta SD.
3. Cuando ha terminado el proceso de reproducción, reinserte la tarjeta en la ranura **System SD**.
4. Mediante IP Office Manager, seleccione **Archivo | Avanzadas | Reiniciar**.
5. En el menú **Seleccionar IP Office**, seleccione el sistema IP500 V2 y haga clic en **Aceptar**.
6. Seleccione el tipo de reinicio que desea realizar y haga clic en **Aceptar**.
7. Al reiniciar el sistema, durante el proceso cargará los archivos de software en la carpeta principal de la tarjeta System SD.

12.9.4 Actualización mediante una tarjeta SD opcional

La PC con IP Office Manager se puede usar para cargar el conjunto completo de archivos de operación en una tarjeta SD. Esto incluye el firmware para el sistema principal, los archivos firmware del teléfono y los archivos para el correo de voz incrustado. Si la tarjeta contiene archivos de configuración, mensajes y avisos, tales archivos no se borran con este proceso.

- **ADVERTENCIA: Versión IP Office Manager**
  Este proceso utiliza archivos de software provistos por la versión instalada de IP Office Manager que está en uso. Debe asegurarse de que la versión de IP Office Manager que está en uso concuerde con la versión de software requerida.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecuten versiones anteriores a 8.1(65) antes deben actualizarse a IP Office versión 8.1(65) (o posterior a 8.1) o cualquier versión de IP Office 9.0 y luego actualizarla a IP Office versión 9.1 o posterior. Para las versiones anteriores no se requiere una actualización intermedia si el sistema se sigue actualizando.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 10.0:**
  IP Office versión 10 y versiones posteriores solo son compatibles con licencias PLDS. Para actualizar un sistema que está usando licencias ADI, esas licencias se deben migrar primero a PLDS.

  - Para migrar de licencia debe obtener un archivo de licencia de migración mediante IP Office Manager (**Herramientas | Migración de licencia**) y, luego, enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra todas las licencias virtuales que posea para que el sistema emita una equivalencia de las licencias PLDS pero ahora asociadas a la clave de función. Actualice el sistema solo cuando ya haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que si continúa con la migración de licencia, Avaya borrará todos los registros de la posesión de licencias ADI que posee para esa clave de función.

Actualice al actualizar una tarjeta SD opcional

1. Apague la tarjeta SD opcional y extráigala. Consulte la sección Extracción y apagado de la tarjeta de memoria 153.
2. Repita el proceso para reproducir una tarjeta SD 140. Este proceso sobrescribirá los archivos de software en la tarjeta con los archivos disponibles para IP Office Manager. Este proceso toma alrededor de 20 minutos.
3. Reinserte la tarjeta en la ranura para tarjeta SD opcional.
4. Copie todos los archivos de la tarjeta SD opcional a la tarjeta SD del sistema. Consulte la sección Carga del software desde una tarjeta SD opcional 150.
5. Reinicie el sistema. Consulte la sección Reinicio de un sistema 163.

12.9.5 Actualización mediante IP Office Web Manager

Avaya puede dejar disponibles paquetes de actualización para su uso con IP Office Web Manager. Una vez desempaquetado en una PC local, se puede usar el proceso a continuación para actualizar el sistema.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 9.1:**
  Los sistemas existentes que ejecuten versiones anteriores a 8.1(65) antes deben actualizarse a IP Office versión 8.1(65) (o posterior a 8.1) o cualquier versión de IP Office 9.0 y luego actualizarla a IP Office versión 9.1 o posterior. Para las versiones anteriores no se requiere una actualización intermedia si el sistema se sigue actualizando.

- **ADVERTENCIA: Actualización de los sistemas anteriores a la versión 10.0:**
  IP Office versión 10 y versiones posteriores solo son compatibles con licencias PLDS. Para actualizar un sistema que está usando licencias ADI, esas licencias se deben migrar primero a PLDS.

  - Para migrar de licencia debe obtener un archivo de licencia de migración mediante IP Office Manager (**Herramientas | Migración de licencia**) y, luego, enviar ese archivo a Avaya. Tenga en cuenta que este proceso también migra todas las licencias virtuales que posea para que el sistema emita una equivalencia de las licencias PLDS pero ahora asociadas a la clave de función. Actualice el sistema solo cuando ya haya obtenido el archivo de licencia PLDS de reemplazo para el sistema. Tenga en cuenta que si continúa con la migración de licencia, Avaya borrará todos los registros de la posesión de licencias ADI que posee para esa clave de función.

Para actualizar un sistema mediante IP Office Web Manager

1. Inicie sesión en IP Office Web Manager 71.
   a. Ingrese la dirección IP del sistema en el navegador. Seleccione **IP Office Web Manager**. De manera alternativa, ingrese *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Ingrese un nombre de usuario de administración y una contraseña, y haga clic en **Iniciar sesión**.
2. Desempaque los archivos de actualización en una ubicación en su PC cliente.
3. Haga clic en **Acciones** y seleccione **Actualización**.
4. Haga clic en **Configurar ruta**.
5. Seleccione la carpeta que contiene los archivos desempaquetados y haga clic en **Abrir**.
6. Haga clic en **Iniciar actualización**.

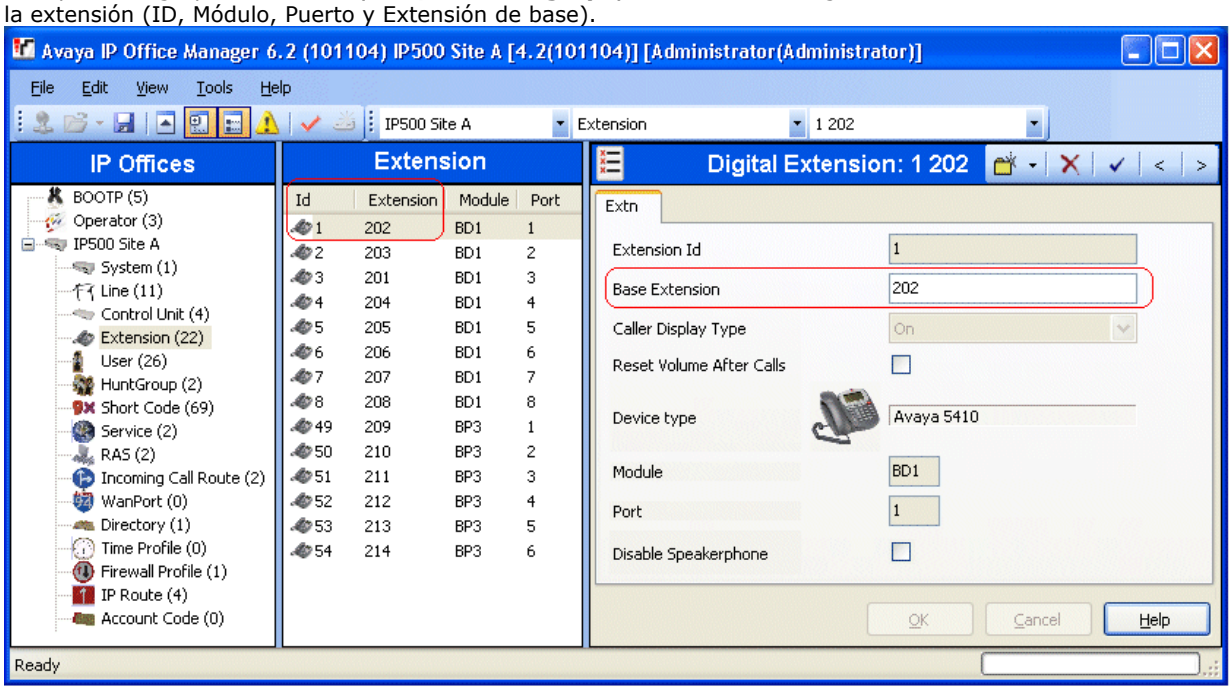
12.10 Intercambio de usuarios de extensiones

Aunque el ejemplo a continuación muestra a dos usuarios intercambiando sus extensiones, puede emplearse este método para intercambiar múltiples usuarios en la configuración y aplicar los intercambios después de una sola fusión de los cambios de la configuración.

Intercambio de usuarios de extensiones

En este ejemplo, el Usuario A (202) y el Usuario B (203) desean intercambiar extensiones.

1. Cargue la configuración de IP Office y seleccione **Extensión**.
2. Localice la extensión con la **Extensión de base** con valor ***202***, es decir, la que coincide con el número de extensión del Usuario A.
   - Si el panel de grupo está visible (**Ver | Panel de grupo**) en IP Office Manager, este mostrará los detalles de la extensión (ID, Módulo, Puerto y Extensión de base).

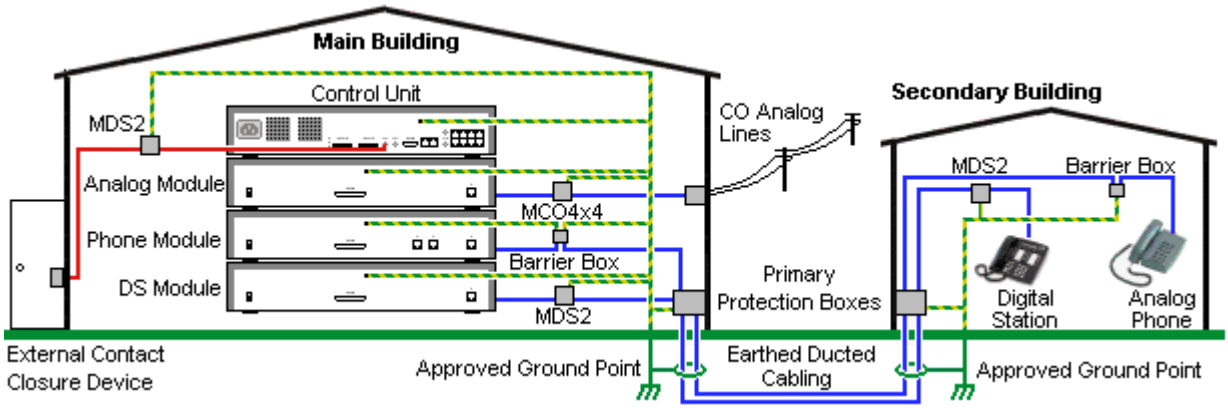


3. Seleccione esta extensión y cambie el valor **Extensión de base** a ***203***, es decir, para coincidir con el número de extensión del Usuario B. Si IP Office Manager está configurado para validar las ediciones, le advertirá que este cambio entra en conflicto con la configuración de Extensión de base existente para otra extensión. Ignore esta advertencia en este momento. Haga clic en **Aceptar**.
4. Localice la otra extensión con **Extensión de base** con valor ***203***, es decir, la que coincide con el número de extensión del Usuario B.
5. Seleccione esta extensión y cambie el valor **Extensión de base** a ***202***, es decir, para que coincida con el número de extensión del Usuario A. Si el panel de error está visible (**Ver | Panel de errores**), las advertencias sobre los conflictos entre extensiones deberán desaparecer ahora. Haga clic en **Aceptar**.
6. Guarde la configuración en el sistema de IP Office.
7. Desde cada extensión, marque el código corto de cierre de sesión establecido en el sistema IP Office. El valor predeterminado es ****36***.
   - Si alguno de los usuarios está configurado para **Inicio de sesión forzado**, tendrán que completar el proceso de inicio de sesión desde la nueva extensión con ayuda del Código de inicio de sesión.

12.11 Instalaciones telefónicas fuera del edificio

Los siguientes son los únicos escenarios contemplados en los cuales las extensiones cableadas y dispositivos fuera del edificio principal pueden conectarse al sistema IP Office. En estos escenarios, debe equiparse asimismo protección adicional bajo la forma de puesta a tierra de protección y protectores contra picos.

- **⚠ PRECAUCIÓN**
  La instalación de protección adicional no elimina el riesgo de daños. Simplemente disminuye la probabilidad de que ocurran daños.



- Deben mantenerse separados los cables de distintos tipos, por ejemplos líneas de troncales, extensiones telefónicas, conexiones de tierra y energía.
- Todo el cableado entre edificios deben quedar encerrado dentro de ductos aterrizados. En forma ideal, estos ductos deben colocarse bajo tierra.
- Debe equiparse una caja de protección primaria en el punto donde los cables penetran al edificio. Esta protección debe ser de tipo de tres puntos (positivo, negativo y tierra). Típicamente, se trata de una protección de tubo de gas proporcionada por la compañía telefónica local. El cable de tierra debe ser lo suficientemente grueso para manejar todas las líneas afectadas por un choque indirecto al mismo tiempo.

Tipo de conexión	Tipo de dispositivo de protección	Requisito
Extensiones de teléfonos analógicos Módulo de expansión externos Phone (únicamente puertos POT 291 o TELÉFONO 291).	**Caja de protección IP Office** 190 Sólo admite una conexión. Máximo 16 con cualquier módulo de expansión.	• La conexión del módulo de expansión externo al teléfono debe ser por vía de un protector contra picos en cada extremo en el punto de protección principal de cada edificio. • Los módulos de expansión externos IP Office, la unidad de control y los dispositivos IROB deben estar conectados al punto de conexión de tierra de protección en su propio edificio. • La conexión entre edificios debe realizarse con ductos aterrizados, preferiblemente bajo tierra. El cable no debe estar expuesto al exterior en ningún punto.
Únicamente extensiones telefónicas DS Phone	**ITW Linx MDS2** 189 Es compatible con hasta 4 conexiones. Este dispositivo era llamado anteriormente Avaya 146E.	
Extensiones de teléfono BST	Ninguno	No admitida actualmente.
Troncales analógicas	**ITW Linx MCO4x4** 189 Admite hasta 4 líneas de dos hilos. Este dispositivo era llamado anteriormente Avaya 146C.	En las instalaciones en la República de Sudáfrica, es un requisito equipar las troncales analógicas con protección contra picos. En otras localidades donde se considera que el riesgo de rayos es alto, se recomienda adoptar protección adicional de las troncales analógicas entrantes.
Interruptor de salida externo	**ITW Linx MDS2** 189 Es compatible con hasta 4 conexiones. Este dispositivo era llamado anteriormente Avaya 146E.	Las conexiones de un puerto Ext O/P de IP Office hacia un dispositivo de relevadores externo debe hacerse mediante un protector contra picos. Cuando se utiliza el MDS2 en el puerto Ext O/P, utilice solo la Línea 1 y los conectores del Equipo 1. No utilice la Línea 2 ni los conectores del Equipo 2.

El rango de dispositivos towerMAX se encuentra en el sitio de ITWLinx (http://www.itwlinx.com).

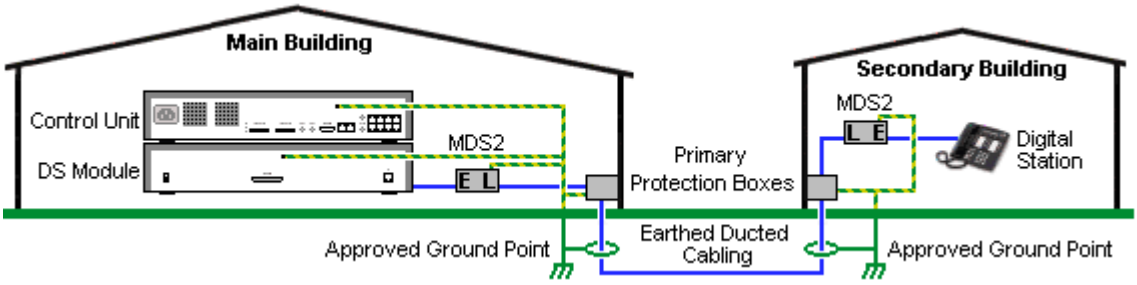
12.11.1 Teléfonos DS

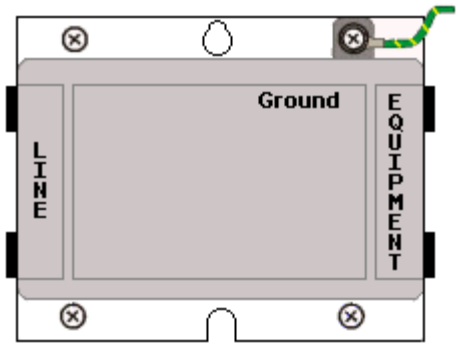
Cuando se requieren extensiones de teléfono digital en otro edificio, es necesario utilizar el equipo de producción adicional IROB. En teléfonos conectados a los puertos DS de IP Office, el dispositivo compatible proporcionado por ITWLinx es un módulo towerMAX DS/2. Este dispositivo IROB era llamado anteriormente 146E IROB de Avaya.

- **ADVERTENCIA**
  Este dispositivo no es compatible con conexiones de puerto BST, es decir, con teléfonos serie 4100, serie T, serie 7400 y serie M.

El dispositivo de protección debe instalarse conforme a las instrucciones proporcionadas con el aparato. Los puntos de tierra en la unidad de control IP Office y los módulos de expansión externos deben conectarse a un punto de tierra de protección con ayuda de un cable 18AWG con recubrimiento verde y amarillo.

Típicamente, los dos puertos 2 RJ45 EQUIPO del IROB están conectados directamente a los dos puertos 2 RJ45 LÍNEA. Esto permite el cableado estructurado RJ45 existente, utilizando los pins 4 y 5 sin necesidad de volver a tender el cableado para hasta dos conexiones DS. Sin embargo, cada uno de estos puertos puede utilizarse para conectar una segunda extensión mediante los pins 3 y 6.

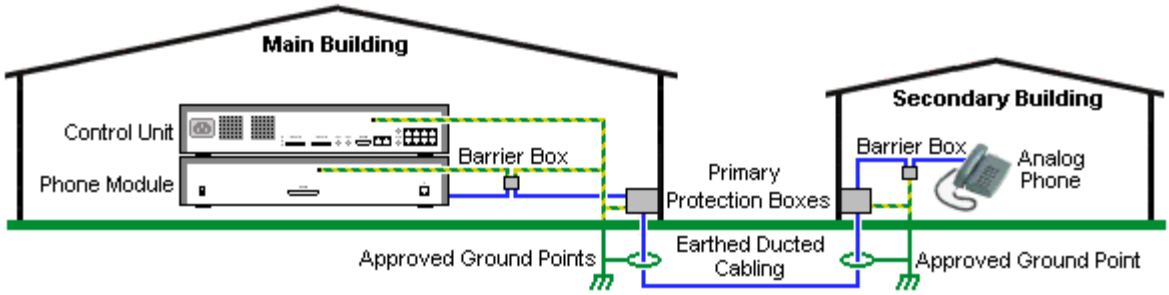


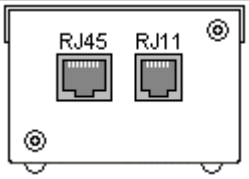
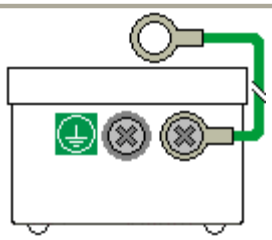
LÍNEA		Señal		EQUIPO	
RJ45 8 1	1	No se utiliza.		1	RJ45 8 1
	2	No se utiliza.		2	
	3	Negativo II (opcional)		3	
	4	Negativo I		4	
	5	Positivo I		5	
	6	Positivo II (Opcional)		6	
	7	No se utiliza.		7	
	8	No se utiliza.		8	

12.11.2 Caja de protección para teléfonos analógicos

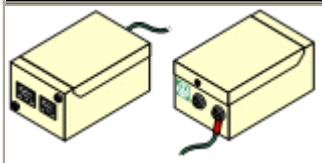
Cuando se requieren extensiones analógicas de teléfono en otro edificio, es necesario utilizar equipo de protección adicional, es decir las cajas de protección para teléfono de IP office, así como conexiones de tierra de protección.

- ⚠ **PRECAUCIÓN**
  Los puertos TELÉFONO (POT) en la parte delantera de las unidades de control no deben utilizarse para extensiones externas al edificio principal.
- Deben utilizarse las cajas de protección específicas y correctas para IP Office. Estos módulos han sido diseñados específicamente para los voltajes de señal utilizados por el sistema de IP Office:
  - Debe usarse solamente la caja de protección para teléfono IP Office con los módulos Phone V1.
  - Debe usarse solamente la caja de protección para teléfono IP Office V2 con los módulos Phone V2.
  - No debe utilizarse ningún otro tipo de cajas de protección para teléfonos analógicos.
- En casos donde se requiera instalar más de tres cajas de protección en un edificio, deben instalarse en un bastidor con ayuda de un kit de montaje para Caja de protección 191.
- Puede utilizarse un máximo de 16 cajas de protección con cualquier módulo Phone.
- La caja de protección para el teléfono no se conecta al capacitor de timbre de llamada en los módulos Phone V1.



Edificio principal	Cajas de protección	Edificio secundario
• **RJ11** Conecte al puerto TELÉFONO (POT) en el módulo Phone con ayuda del cable incluido con la caja de protección. • **RJ45** Conecte la caja de protección para el edificio secundario con ayuda de una protección primaria en ambas edificaciones.		• **RJ11** Conecte al teléfono analógico. No incluye cable. • **RJ45** Del edificio principal, con conexión por protección primaria en ambos edificios.
• **Tornillo central** Conecte a la puesta a tierra de protección del edificio principal (o a la terminal de tierra en el kit de montaje de bastidor de la caja de protección). Utilice un cable 18AWG (mínimo) con recubrimiento verde y amarillo. • **Tornillo del lado derecho** Conecte al punto de tierra en el módulo Phone con ayuda del cable de tierra incluido con la caja de protección.		• **Tornillo central** Conecte a la puesta a tierra de protección del edificio principal. Utilice un cable 18AWG (mínimo) con recubrimiento verde y amarillo. • **Tornillo del lado derecho** No utilizado.

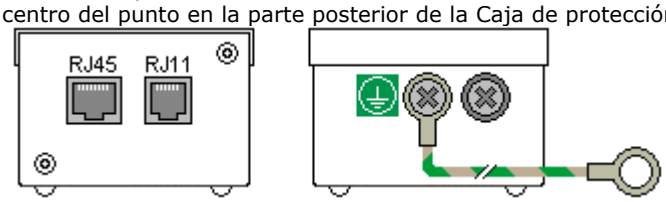
1. Los siguientes cables deben mantenerse separados, es decir, no deben enrutarse dentro del mismo haz:
   - Terminales de tierra de la caja de protección a los módulos Phone.
   - Cables internos, por ejemplo las terminales de extensión que van directamente a los módulos Phone.
   - Los cables del teléfono externo que van directamente a las cajas de protección.

Cajas de protección IP Office		Código SAP
	**Caja de protección para teléfono (81V)** Utilice con módulo Phone V1. Incluye un cable de RJ45 a RJ11 y una terminal para conexión a tierra funcional.	700293897
	Caja de protección para teléfono V2 (101V) Utilice con módulo Phone V2. Incluye un cable de RJ45 a RJ11 y una terminal para conexión a tierra funcional.	700385495
	Kit de montaje en bastidor con cajas de protección	700293905

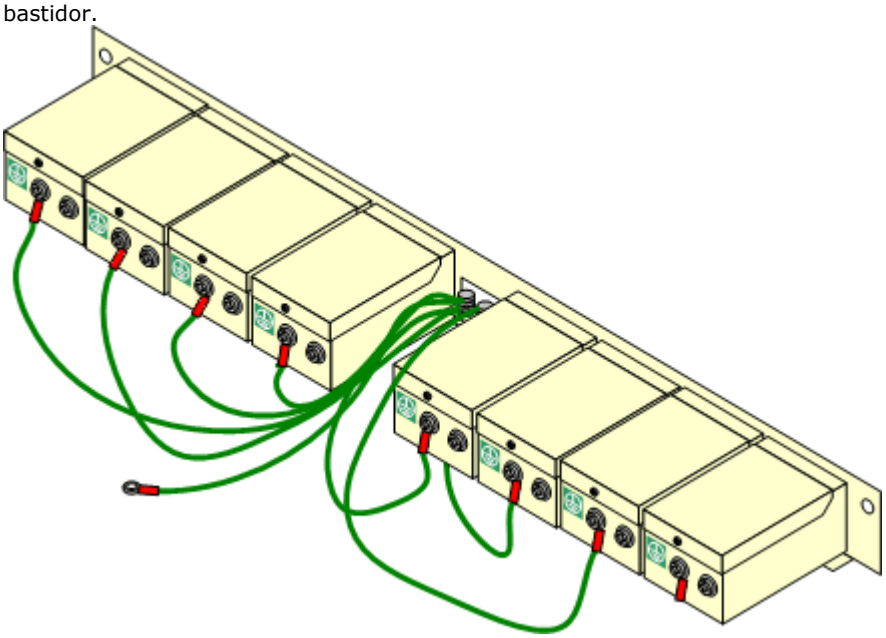
12.11.3 Cajas de protección para montaje en bastidor

En casos donde se requiera instalar más de tres cajas de protección, éstas deben instalarse en un bastidor. El kit de montaje en bastidor para cajas de protección (código SAP 700293905) admite hasta ocho cajas de protección para teléfono.

1. Desatornille los dos tornillos dispuestos en diagonal en la parte delantera de las cajas de protección y utilice los mismos tornillos para sujetar la caja de protección a la tira de montaje del bastidor.
2. Cada caja de bastidor es suministrada con un cable verde sólido conectado al tornillo de tierra funcional. Desconecte y deseche este cable. Conecte un cable de tierra verde/amarillo al tornillo de protección de tierra en el centro del punto en la parte posterior de la Caja de protección.



3. La tira de montaje del bastidor contiene pilares de tierra roscados M4. Conecte el otro extremo del cable de tierra de la caja de protección con ayuda de roldanas y tuercas M4 al pilar de tierra de ese lado de la tira de montaje del bastidor.



4. Con ayuda de un cable 14AWG con recubrimiento verde y amarillo, conecte uno de los pilares de tierra a la tierra de protección del edificio.
5. Con ayuda de un cable 14AWG con recubrimiento verde y amarillo, conecte el otro pilar de tierra al módulo Phone.
6. Compruebe que los siguientes cables no están enrutados dentro del mismo haz:
   - Terminales de tierra de la caja de protección al módulo Phone.
   - Cables internos, por ejemplo los cables que van directamente al módulo Phone.
   - Los cables del teléfono externo que van directamente a las cajas de protección.

12.12 Uso del puerto de salida externo

Todas las unidades de control de IP Office están equipadas con un puerto EXT O/P. El puerto está marcado como EXT O/P y se localiza en la parte trasera de la unidad de control, a un lado del enchufe de entrada de la unidad de suministro de energía.

Este puerto puede usarse para controlar hasta dos dispositivos externos, tales como interruptores de relevador de entrada de puerta. La aplicación habitual para estos interruptores es activar los relevadores en sistemas de entrada por puertas. Sin embargo, siempre y cuando se cumplan los criterios para los límites máximos de corriente, voltaje y protección si es necesario, se pueden usar los interruptores para otras aplicaciones.

Los conmutadores pueden cerrarse, abrirse o pulsarse (cerrarse durante 5 segundos y luego abrirse). Esto se puede hacer de diferente formas:

- Utilizando los códigos cortos de IP Office Manager
- A través de la opción **Apertura de puerta** en IP Office SoftConsole.
- A través de la acción **Abrir puerta** en Voicemail Pro.

Códigos cortos predeterminados
Los siguientes son los códigos cortos predeterminados en la configuración de IP Office para operar el interruptor de salida externo. Se utilizan las funciones de código corto Relevador encendido (cerrado), Relevador apagado (abierto) y Pulso relevador.

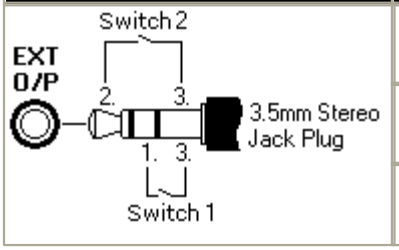
Estado	Interruptor 1	Interruptor 2
Cerrado	*39	*42
Abierto	*40	*43
Pulso	*41	*44

12.12.1 Conexión de puerto

Estos puertos se hallan en la parte posterior de las unidades de control de IP Office. Se utilizan para la conexión con relevadores conmutadores externos. El puerto utiliza una clavija estéreo de 3.5 mm estándar para la conexión.

El sistema IP Office puede abrir (alta resistencia), cerrar (baja resistencia) o pulsar (cerrar por cinco segundos y luego abrir) los dos interruptores en el puerto. Cada interruptor puede operarse separadamente. Estos interruptores están diseñados para activar relevadores externos en sistemas como sistemas de apertura de puertas.

- **PRECAUCIÓN:**
  En instalaciones donde este puerto está conectado a un dispositivo externo al edificio, la conexión debe realizarse mediante un protector de pico MDS2 y debe haber una conexión con línea a tierra para protección en la unidad de control de IP Office. Cuando se utiliza el MDS2 en el puerto Ext O/P, utilice solo la Línea 1 y los conectores del Equipo 1. No utilice la Línea 2 ni los conectores del Equipo 2.

EXT O/P	Pin	Descripción
	1	Interruptor 1.
	2	Interruptor 2.
	3	0 Volts (Tierra/Chasís)

- Capacidad del interruptor: 0,7A.
- Voltaje máximo: 55V d.c.
- Resistencia efectiva: 0.7 ohms.
- Corriente de corto circuito: 1A.
- Capacidad de corriente de circuito inverso: 1.4A.
- Compruebe que los pins 1 y 2 llevan siempre un voltaje positivo con respecto al pin 3.

Los módulos sellados pre-construidos con frecuencia están equipados con clavijas de audio estéreo de 3.5 mm. Puede ser necesario emplear un multímetro para determinar las conexiones de cableado en una clavija disponible. Por lo general el cable de prueba es el 3 (común a ambos relevadores).

12.13 Módulo BRI So8

12.13.1 Ejemplo 1: Terminal ISDN

En este ejemplo, las llamadas DID 123456 son enrutadas hacia el primer puerto del módulo de expansión So8. Este puerto ha sido configurado como Grupo de línea ID 701.

1. **Configurar enrutamiento de una llamada entrante**
   El destino es un código corto que dirige la llamada hacia la ID de grupo de línea que contiene las líneas So. La **Capacidad de portadora** ha sido configurada como ***Cualquiera***, a fin de admitir datos y voz por esta ruta.
   - **ID de grupo de línea:** 0
   - **Número entrante:** 123456
   - **Destino:** 123456
   - **Capacidad de portadora:** Cualquiera
2. **Crear un código corto de sistema**
   Este es un destino utilizado en la Ruta de llamadas entrantes.
   - **Código corto:** 123456
   - **Número de teléfono:** 123456
   - **ID de grupo de línea:** 701
   - **Función:** Marcar
3. Envíe la configuración a la unidad de control.

Cualquier llamada entrante al sistema principal en DID 123456 será pasada directamente al primer puerto.

Si desea asignar los DID de su recurso particular a puertos individuales para evitar los cargos de red cuando marque entre ellos, intente variaciones de lo siguiente:

1. Tiene rangos DID, por ejemplo: 7325551000 a 7325551099. Desea asignar 7325551000-19 al puerto 1 y 7325551020-20 al puerto 2, etc.
2. Configurar Ruta de llamadas entrantes:
   El símbolo # se utiliza a continuación en vez de "n" para evitar problemas con "Main". El signo menos significa que el número es procesado desde la izquierda y por lo tanto esperará a tener el número completo.
   - ID de grupo de línea: 701
   - Número entrante: -100x
   - Destino: #
3. Repita para el ID de grupo de línea 702 etc.
4. Cree códigos cortos, por ejemplo:
   - Código corto: 100x
   - Número de teléfono: .
   - ID de grupo de línea: 701
   - Función: Marcar

Las llamadas S0 marcadas sin el código de área se manejan localmente sin cargos de red. Las llamadas con códigos de área se procesarán mediante la red.

12.13.2 Ejemplo 2: Conferencia de video

En este ejemplo, las llamadas son enrutadas a un módulo Polycom Viewstation conectado a un puerto S0 en el sistema IP Office.

Se utilizaron los siguientes ajustes en cuatro canales de datos entrantes de una línea PRI:

- Número de línea: 5
- Asignación de canales: 23 -> 1
- Tipo de interruptor: 5ESS
- Subtipo de línea: PRI
- Proveedor: AT&T
- Canales: 1-4
- Grupo de línea entrante: 95
- Grupo de línea saliente: 95
- Dirección: Ambos sentidos
- Portadora: Datos
- Servicio: Accunet (esto es importante)
- Admin: En servicio

Para enrutar una llamada de video entrante en las líneas PRI configuradas anteriormente hacia un módulo SO8, es necesario lo siguiente:

1. Crear un código de marcación corto con el puerto SO como su Grupo de línea destino. En este ejemplo, se utilizó el siguiente:
   - Código corto: 1500
   - Número: .
   - Función: Marcar
   - Grupo de línea: 601 (el número del puerto SO8)
2. Crear un Enrutamiento de llamada entrante que enrute las llamadas apropiadas hacia ese código corto. En este ejemplo, se utilizó el siguiente:
   - Grupo de línea: 95 (identifica las llamadas que utilizan las líneas PRI configuradas anteriormente)
   - Destino: 1500 (el código corto creado arriba)
   - Portadora: Cualquiera

Para permitir que el dispositivo de video en el puerto S0 realice llamadas salientes a las líneas PRI, es también necesario un código corto.

1. En este ejemplo, se utilizó el siguiente:

- Código: 91N;
- Número: N
- Función: Marcar
- Grupo de línea: 95

Ajustes del módulo Polycom Video
Los módulos Polycom empleados en el ejemplo anterior fueron los módulos Viewstation 128, Viewstation 256 y Viewstation MP.

El módulo Polycom debe tener un software compatible con "ETSI ISDN Estándar" (ISDN Europeo) y tener el ajuste de protocolo ISDN Switch en "Standard ETSI Euro-ISDN".

Los siguientes ajustes fueron utilizados durante las pruebas:

Características	**Admin/Software y Hardware/Software**
• Polycom View Station 512 MP. • Interfaz NTSC UIS. • View Station PVS 1419.	• Software: 7.0.1. • Interfaz de red: Interfaz S/T. • Versión ISDN: IEUS v18:a00320
Configuración Admin/General	**Admin/Video Red/ISDN Video Red**
• País: EUA • Idioma: Inglés (EUA) • Respuesta automática: Sí • Permitir marcar: Sí • Permitir configuración de usuario: Sí • Tiempo máximo en llamada: 480.	• Código de país: 1 • Código de área: 732 • Número A: en blanco • Número B: en blanco • Protocolo ISDN Switch: Standard ETSI Euro-ISDN.
Configuración de usuario	**Admin/Video Network/IMUX**
• Respuesta automática: Sí • PIP: Auto • Control a distancia de la cámara: Sí • Modo MP: Auto	• Números: en blanco • SPID: en blanco • Calidad de audio: 168KB/s • Marcación avanzada: Canales de marcación en paralelo
Información del sistema	**Admin/Software y Hardware/Hardware**
• Versión: 7.0.1 • Modelo: VS: 512	• Cámara: NTSC • Interfaz Video Comm: ISDN_Quad_BRI • Tipo de interfaz de red: Interfaz S/T.
Red Admin/Video	**Admin/Video Network/Call Preference**
• Configuración de puntos múltiples: Auto	• Llamadas de video ISDN (H:320): Sí

12.14 SNMP

SNMP (Protocolo simple de administración de red) es un protocolo de red estándar que permite monitoread y administrar dispositivos de datos en toda la red. Puede integrarse un agente SNMP a los dispositivos de red, como enrutadores y concentradores. Puede entonces utilizarse una aplicación de administrador SNMP como CastleRock o HP OpenView para establecer comunicación con estos dispositivos.

Las versiones IP Office 2.0 y posteriores son compatibles con comunicaciones SNMP. Esta comunicación puede ser:

- **Encuestas:**
  Algunas aplicaciones SNMP (llamadas "administradores") envían mensajes de encuesta a la red. Después registran las respuestas enviadas por dispositivos compatibles SNMP (llamados "agentes"). Esto permite a la aplicación crear un mapa de red y levantar una alarma cuando no responden dispositivos que estaban presentes anteriormente.
  - La mayoría de las aplicaciones de administrador SNMP pueden realizar encuestas simples de dirección IP para localizar dispositivos no compatibles con SNMP. Sin embargo, este método de encuestas no identificar el tipo de dispositivo y otros datos.
  - Las encuestas SNMP incluyen detalles sobre el dispositivo que envía la respuesta. Por ejemplo, la respuesta de una unidad de control IP Office incluye el tipo de unidad de control, nivel de software, información de la tabla de enrutamiento, tiempo de funcionamiento, etc.
- **Trampas:**
  El agente SNMP de un dispositivo puede enviar detalles sobre un evento al administrador SNMP cuando ocurren ciertos eventos. Esto se conoce como una "trampa" SNMP. Éstas aparecen en el registro de eventos del administrador SNMP. La mayoría de los administradores SNMP pueden configurarse para enviar alertas adicionales en respuesta a trampas particulares.
- **Administración:**
  Algunos agentes SNMP admiten administración de dispositivos y cambios de configuración mediante la interfaz del administrador SNMP. IP Office no soporta esta función.

La operación de SNMP con IP Office ha sido sometida a prueba con Castle Rock SNMPc-EE 5.1.6c y HP OpenView Network Node Manager 6.41.

La información disponible vía SNMP

Como se describió anteriormente, la información SNMP puede ser encuestada por la aplicación SNMP o recibida como resultado de una trampa SNMP enviada por IP Office.

Aunque no es posible editar los archivos ***.mib*** es posible leerlo con un editor de texto, y contiene descripciones de todos los múltiples objetos de información que pueden encuestarse o enviarse y la información que contiene cada objeto. Para una lista de los archivos ***.mib*** consulte Instalación de los archivos MIB de IP Office 198. Los objetos ***NOTIFICATION-TYPE*** son los que se utilizan para las trampas SNMP 200, los otros tipos de objetos son aquellos que pueden ser encuestados 200.

12.14.1 Instalación de los archivos MIB de IP Office

A fin de permitir la comunicación completa entre un agente SNMP y un gerente SNMP, este último debe cargar los archivos MIB (Base de Información de Administración) específicos para el dispositivo agente SNMP, así como de las funciones compatibles. Estos archivos MIB contienen detalles de la información que puede proporcionar el agente y las trampas que puede enviar. Puede encontrar más detalles sobre las estructura de los archivos MIB de IP Office, los grupos MIB dentro de estos archivos, y trampas para eventos, en la sección "Manual de instalación de IP Office".

Los archivos MIB para la operación de IP Office están incluidos en el DVD IP Office dentro de la carpeta ***\AdminCD\smnp_mibs***. Los archivos reales requeridos y el método de carga dependen de la aplicación de administrador SNMP que esté utilizando. Los detalles siguientes cubren las dos aplicaciones de administrador SNMP que se han sometido a prueba.

HP Open View Network Node Manager

1. Copie los siguientes archivos MIB a la carpeta de aplicaciones MIB.

	Archivo MIB	Origen
a.	rfc2737-entity-mib.mib	snmp_mibs\standard folder en el OpenView Install CD.
b.	avayagen-mib.mib	\AdminCD\snmp_mibs\IPOffice en el DVD Admin de IP Office.
c.	ipo-prod-mib.mib	\AdminCD\snmp_mibs\IPOffice en el DVD Admin de IP Office.
d.	ipo-mib.mib	\AdminCD\snmp_mibs\IPOffice en el DVD Admin de IP Office.
e.	inet-address-mib.mib	\AdminCD\snmp_mibs\Standard en el DVD Admin de IP Office.
f.	rfc2213-integrated-services-mib.mib	\AdminCD\snmp_mibs\Standard en el DVD Admin de IP Office.
g.	diffserv-dscp-tc.mib	\AdminCD\snmp_mibs\Standard en el DVD Admin de IP Office.
h.	diffserv-mib-hpov.mib	\AdminCD\snmp_mibs\Standard en el DVD Admin de IP Office.
i.	ipo-phones-mib.mib	\AdminCD\snmp_mibs\IPOffice en el DVD Admin de IP Office.

2. Inicie la consola de OpenView Network Node Manager.
3. Seleccione Opciones, luego Cargar/Descargar de archivos MIB: SNMP.
4. Seleccione Cargar y seleccione todos los archivos MIB enumerados arriba..
5. Seleccione Compilar.

CastleRock SNMPc 5.1.6c y versiones anteriores

1. Copie los siguientes archivos MIB a la carpeta de aplicaciones MIB, por lo general C:\Program Files\SNMPc Network Manager\mibfiles.

	Archivo MIB	Origen
a.	ENTITY-MIB	\AdminCD\snmp_mibs\Standard en el DVD Admin IP Office.
b.	AVAYAGEN-MIB.mib	\AdminCD\snmp_mibs\IPOffice en el DVD Admin IP Office.
c.	IPO-PROD-MIB.mib	\AdminCD\snmp_mibs\IPOffice en el DVD Admin IP Office.
d.	IPO-MIB.mib	\AdminCD\snmp_mibs\IPOffice en el DVD Admin IP Office.
e.	INET-ADDRESS-MIB.mib	\AdminCD\snmp_mibs\Standard en el DVD Admin IP Office.
f.	INTEGRATED-SERVICES-MIB	\AdminCD\snmp_mibs\Standard en el DVD Admin IP Office.
g.	DIFFSERV-DSCP-TC.mib	\AdminCD\snmp_mibs\Standard en el DVD Admin IP Office.
h.	DIFFSERV-MIB.mib	\AdminCD\snmp_mibs\Standard en el DVD Admin IP Office.
i.	IPO-PHONES-MIB.mib	\AdminCD\snmp_mibs\IPOffice en el DVD Admin IP Office.

2. En SMNPc, seleccione Config | Base de datos MIB.
3. Seleccione Agregar y seleccione los archivos MIB enumerados arriba en el orden que aparecen.

CastleRock SNMPc V5.0.1

Las instrucciones de instalación de MIB mencionadas anteriormente son válidas para CastleRock SNMPc V5.0.8 y versiones posteriores. En V5.0.1 de CastleRock SNMPc, es necesario seguir este procedimiento:

1. Copie todos los archivos MIB IP Office y archivos MIB estándar del DVD de aplicaciones del administrador de IP Office al directorio mibfiles de SNMPc.
2. Desde el directorio mibfiles de SNMPc, abra los archivos STANDARD.mib y SNMPv2-SMI.mib con el Bloc de notas.
3. En el archivo SNMPv2-SMI.mib, encuentre la definición de zeroDotZero y cópiela al portapapeles.
4. En el archivo STANDARD.MIB, encuentre la sección SNMPv2-SMI y pegue la definición de zeroDotZero del portapapeles antes del final de esta sección (justo antes del enunciado END).
5. Guarde el archivo STANDARD.MIB modificado.
6. Agregue el archivo MIB SNMP-FRAMEWORK-MIB.mib a la base de datos MIB con ayuda de las instrucciones proporcionadas en la guía de instalación de IP Office.
7. Agregue los archivos MIB listados en las instrucciones proporcionadas en la guía de instalación de IP Office, en el orden correcto.
8. Compile los archivos MIB listos para usarse.

La razón para lo anterior es: El archivo IPO-PHONES-MIB.mib depende del archivo DIFFSERV-MIB.mib para obtener la definición de la convención textual de IndexInteger. El archivo DIFFSERV-MIB necesita la definición de la convención textual zeroDotZero, la cual se define normalmente en el archivo SNMPv2-SMI.mib. Sin embargo, la inclusión de SNMPv2-SMI.mib en el archivo MIB tiene como resultado errores debido conflictos ocurridos con definiciones internas en SNMPc y la sección SNMPv2-SMI dentro del archivo STANDARD.mib. Por lo tanto, para resolver este problema, es necesario colocar la definición requerida para zeroDotZero dentro de la sección SNMPv2-SMI en el archivo STANDARD. mib de SNMPc.

12.14.2 Habilitación de SNMP y soporte para encuestas

A fin que la unidad de control de IP Office pueda ser descubierta y encuestada por un administrador SNMP, su agente SNMP debe estar habilitado y colocado en la misma comunidad de lectura que el administrador SNMP.

1. En IP Office Manager, reciba la configuración de la unidad de control.
2. Haga doble clic en **Sistema** desde el panel del árbol de configuración y seleccione la ficha SNMP.
3. Seleccione la casilla **SNMP habilitado**.
4. En Puerto SNMP, ingrese el número del puerto UDP utilizado por el agente SNMP para escuchar y responder al tráfico SNMP. El valor predeterminado normal es 161.
5. En **Comunidad (Sólo lectura)**, ingrese la comunidad a la cual pertenece el dispositivo para el acceso de lectura. Este nombre de comunidad debe ser el mismo que el empleado por la aplicación del administrador SNMP cuando envía peticiones al dispositivo. Se utiliza frecuentemente una comunidad pública para establecer la comunicación y luego se modifica (en ambos extremos del agente y administrador SNMP) por razones de seguridad.
6. Haga clic en **Aceptar**.
7. Envíe la configuración de vuelta al sistema de IP Office y reinicie.
8. Después del reinicio de la unidad IP Office, el administrador SNMP debe poder encontrar la unidad de control.
9. La respuesta de la unidad de control incluye detalles sobre el tipo de unidad de control y el nivel actual del software nuclear.

12.14.3 Habilitación de envío de trampas SNMP

En IP Office Manager, reciba la configuración de la unidad de control.

1. Haga doble clic en **Sistema** desde el árbol de configuración y seleccione la solapa **Eventos del sistema**.
2. Asegúrese de que esté seleccionada la opción **SNMP habilitado** y seleccione los demás ajustes necesarios en la sección Configuración de agente SNMP.
3. Haga clic en la ficha Alarmas.
4. Haga clic en **Agregar...** y seleccione **Captura** como nuevo tipo de alarma. Puede agregar hasta 2 capturas SNMP, cada una con un destino y una configuración de alarma diferentes.
   - **Dirección del servidor**
     Ingrese la dirección IP o el nombre de dominio completo de la PC que ejecuta la aplicación de administración SNMP.
   - **Puerto**
     Ingrese el Puerto al cual deben enviarse los mensajes de trampas. Este es el puerto UDP al cual el sistema IP Office envía los mensajes de trampa SNMP. El valor predeterminado es 162.
   - **Comunidad**
     Configure la Comunidad que utilizarán el agente y el administrador SNMP. Se utiliza frecuentemente una comunidad pública para establecer la comunicación y luego se modifica (en ambos extremos del agente y administrador SNMP) por razones de seguridad.
   - **Formato**
     De manera predeterminada, se usa IP Office. SMGR sólo se usa si el sistema se administra a través de Avaya SMGR.
   - **Nivel mínimo de seguridad**
     Configure la severidad de alarma o niveles superiores para las alarmas que deben enviarse.
5. Seleccione los **Eventos** que deben enviarse.
6. Haga clic en **Aceptar**.
7. Envíe la configuración de vuelta al sistema de IP Office y reinicie.

12.15 Botón Restaurar

Las unidades de control IP500 V2 tienen un botón **Restaurar**. Al oprimir este botón mientras se inicia la unidad de control, el inicio de la unidad se pausa hasta liberar el botón. El efecto de oprimir el botón durante la operación normal dependerá de cuánto tiempo oprime el botón, y es indicado por el estado de la luz LED del CPU.

Duración oprimido (segundos)	LED del CPU	Acción	Resumen
0 a 5.	**Desactivado**	**Ninguno**	Ninguno.
5 a 10.	**Anaranjado**	**Reiniciar al liberar**	Reiniciar cuando se libere, con bloqueo de llamadas entrantes/salientes. Se recomienda reiniciar el sistema con el botón restaurar durante Audit Trail.
10 a 30.	**Parpadeando en anaranjado**	**Borrar configuración**	Elimina la configuración, el registro de alarmas y el registro de auditoría. Reinicio inmediato sin esperar a que terminen las llamadas activas. Consulte la sección Eliminación de la configuración 168 para obtener la información completa.
30 a 40.	**Rojo**	**Eliminar todo.**	Elimina la configuración, el registro de alarmas y el software nuclear. Consulte la sección Eliminación del software operacional 203 para obtener la información completa.
Más de 40.	**Verde parpadeando**	**Ninguno**	Ninguno.

12.16 Botón AUX

Las unidades de control IP500 V2 cuentan con un botón AUX. Este botón puede utilizarse para lo siguiente.

- Al oprimir este botón mientras la unidad de control se está reiniciando, ésta omitirá el reinicio 138 desde la carpeta ***/primary*** en la tarjeta System SD.
- Si lo oprime por más de cinco segundos mientras el sistema está en ejecución, la unidad de control se apagará durante 10 minutos.

12.17 Mantenimiento del puerto RS232

Normalmente no se utiliza el puerto RS232 en la parte posterior de las unidades de control durante la configuración de un sistema IP Office. Sin embargo, el puerto puede usarse para diversos procesos de mantenimiento.

- ⚠ **ADVERTENCIA**
  El puerto RS232 solo debe utilizarse si es absolutamente necesario y solo si las acciones no pueden completarse mediante IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer un máximo esfuerzo para asegurar que existe una copia de respaldo de la configuración del sistema.

Procesos de mantenimiento del puerto RS232

1. **Conexión y configuración del cable del puerto RS232** 293
2. **Devolver la configuración a valores predeterminados mediante depuración** 170
3. **Devolver la configuración a valores predeterminados mediante carga por reinicio** 171
4. **Devolver la seguridad a valores predeterminados mediante el puerto RS232** 174
5. **Devolver la configuración a valores predeterminados mediante carga por reinicio** 175
6. **Borrado del software principal mediante depuración** 204
7. **Borrado del software principal mediante carga por reinicio** 205

12.18 Borrado del software principal

Cuando se elimina el firmware cargado por la unidad de control, esta comienza a enviar solicitudes BOOTP para recibir archivos de firmware de reemplazo. IP Office Manager puede actuar como servidor BOOTP y responder a la petición de la unidad de control con un archivo apropiado de los instalados en IP Office Manager.

A diferencia de otras unidades de control, al borrar el firmware cargado por una unidad de control IP500 V2, la unidad buscará un firmware sustituto en sus tarjetas SD antes de enviar una solicitud BOOTP a la aplicación IP Office Manager.

- ⚠ No realice los siguientes procedimientos a menos que sea absolutamente necesario. El software de IP Office normalmente puede se actualizan mediante IP Office Manager 179.
- ⚠ Este procedimiento borra el software operativo. Antes de intentar este procedimiento, debe conocer las direcciones MAC e IP del sistema, además de contar con una copia de seguridad de su configuración y con el archivo .bin correcto para el tipo de unidad de control y el nivel del software.
- ⚠ Este proceso no funciona en la presencia de firewalls que bloqueen TFTP y/o BOOTP.

Los procedimientos siguientes debes realizarse desde una PC con dirección de IP fija, directamente conectada a la unidad de control de IP Office con el sistema IP Office desconectado de la red. Durante el proceso, la dirección IP de la unidad de control puede volver a un valor predeterminado dentro del rango entre 192.168.42.1 y 192.168.42.10. Si esto ocurre, puede ser necesario corregir la entrada de BOOTP en IP Office Manager para corresponder con la dirección utilizada por el sistema.

Opciones de proceso

1. **Borrado del software principal mediante el botón Restablecer** 203
   Observe que este modo también cambia la configuración a valores predeterminados.
2. **Borrado del software principal mediante depuración** 204
3. **Borrado del software principal mediante la carga por reinicio** 205

12.18.1 Borrado del software principal mediante el botón Restablecer

Lea la nota y las advertencias respecto de la borrado del software principal 203 antes de usar este proceso. Además, lea y observe las advertencias respecto de la devolución de la configuración 168 antes de usar este proceso.

Para borrar el software principal y la configuración mediante el botón Restablecer

Use este proceso para reiniciar el sistema cuando esté libre. Una vez invocado, el sistema bloquea cualquier llamada nueva entrante o saliente hasta después del reinicio.

1. Ejecute IP Office Manager.
   - En las entradas **BOOTP**, compruebe que exista una entrada que coincida con la dirección MAC, la dirección IP y el archivo .bin empleado por el sistema. Normalmente se crea una entrada en forma automática cuando se ha cargado una configuración para el sistema IP Office. .
     - De no existir una entrada, cree una manualmente. Puede encontrar los primeros dos detalles en los ajustes de la Unidad de control en el archivo de configuración. A continuación, cierre y reinicie IP Office Manager.
   - En **Archivo | Preferencias** compruebe que IP Office Manager esté configurado en 255.255.255.255. Verifique también que la opción **Habilitar servidor BootP** esté seleccionada.
   - Seleccione **Ver | TFTPLog**.
   - Compruebe que el archivo .bin requerido está presente en el directorio de trabajo de Manager.
2. En la parte posterior de la unidad de control, mantenga presionado el botón **Restablecer** entre 30 a 40 segundos hasta que el led **CPU** cambie a rojo.
3. Cuando oprime el botón **CPU** LED cambia a rojo, suelte el botón.
4. El sistema borra su software actual y envía una petición BootP a la red para solicitar nuevo software.

12.18.2 Borrado del software principal mediante depuración

Lea la nota y las advertencias respecto de la borrado del software principal 203 antes de usar este proceso.

- **ADVERTENCIA**
  El puerto RS232 solo debe utilizarse si es absolutamente necesario y solo si las acciones no pueden completarse mediante IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer un máximo esfuerzo para asegurar que existe una copia de respaldo de la configuración del sistema.

Para borrar el software principal mediante depuración

1. Ejecute IP Office Manager.
   - En las entradas **BOOTP**, compruebe que exista una entrada que coincida con la dirección MAC, la dirección IP y el archivo .bin empleado por el sistema. Normalmente se crea una entrada en forma automática cuando se ha cargado una configuración para el sistema IP Office. .
     - De no existir una entrada, cree una manualmente. Puede encontrar los primeros dos detalles en los ajustes de la Unidad de control en el archivo de configuración. A continuación, cierre y reinicie IP Office Manager.
   - En **Archivo | Preferencias** compruebe que IP Office Manager esté configurado en 255.255.255.255. Verifique también que la opción **Habilitar servidor BootP** esté seleccionada.
   - Seleccione **Ver | TFTPLog**.
   - Compruebe que el archivo .bin requerido está presente en el directorio de trabajo de Manager.
2. Conecte el cable serial entre la PC y el puerto DTE RS232 en la unidad de control IP Office.
   a. Inicie el programa de terminales en su PC. Compruebe que ha sido configurada por como aparece en la Configuración del puerto DTE RS232 293. En una sesión de HyperTerminal, la configuración actual aparece resumida en la base de la pantalla.
   b. Ingrese **AT** (sensible a mayúsculas). La unidad de control debe responder ***Aceptar***.
   c. Ingrese **AT-DEBUG**. La unidad de control responderá con la hora, la fecha, y un aviso ***Hello>*** para demostrar que está lista para aceptar comandos.
3. Para eliminar la configuración actual en la memoria RAM, ingrese **actualizar**.
4. La unidad IP Office eliminará el software actual, para luego enviar una petición BootP a la red para solicitar nuevo software. IP Office Manager responderá al comenzar la transferencia del software vía TFTP.

12.18.3 Borrado del software principal mediante la carga por reinicio

Lea la nota y las advertencias respecto de borrado del software principal 203 antes de usar este proceso.

- **ADVERTENCIA**
  El puerto RS232 solo debe utilizarse si es absolutamente necesario y solo si las acciones no pueden completarse mediante IP Office Manager o IP Office Web Manager. En todos los casos, debe hacer un máximo esfuerzo para asegurar que existe una copia de respaldo de la configuración del sistema.

Para borrar el software principal mediante carga por reinicio

1. Ejecute IP Office Manager.
   - En las entradas **BOOTP**, compruebe que exista una entrada que coincida con la dirección MAC, la dirección IP y el archivo .bin empleado por el sistema. Normalmente se crea una entrada en forma automática cuando se ha cargado una configuración para el sistema IP Office. .
     - De no existir una entrada, cree una manualmente. Puede encontrar los primeros dos detalles en los ajustes de la Unidad de control en el archivo de configuración. A continuación, cierre y reinicie IP Office Manager.
   - En **Archivo | Preferencias** compruebe que IP Office Manager esté configurado en 255.255.255.255. Verifique también que la opción **Habilitar servidor BootP** esté seleccionada.
   - Seleccione **Ver | TFTPLog**.
   - Compruebe que el archivo .bin requerido está presente en el directorio de trabajo de Manager.
2. Conecte el cable serial entre la PC y el puerto DTE RS232 en la unidad de control IP Office.
   a. Inicie el programa de terminales en su PC. Compruebe que ha sido configurada por como aparece en la Configuración del puerto DTE RS232 293. En una sesión de HyperTerminal, la configuración actual aparece resumida en la base de la pantalla.
   b. Disponga las ventanas de programa de forma que el programa Terminal y el Registro TFTP de IP Office Manager sean visibles al mismo tiempo.
   c. Desconecte la energía de la unidad de control IP Office.
   d. Encienda la unidad de control y oprima la tecla de escape cada segundo hasta que aparezca un mensaje de Loader. Vea más abajo un ejemplo.

      ```
      P12 Loader 2.4
      CPU Revision 0x0900
      ```

   e. Ingrese **AT** (sensible a mayúsculas). La unidad de control debe responder ***OK***.
   f. De no recibir la respuesta OK, compruebe los ajustes de su programa de terminal y repita el proceso anterior.
3. Ingrese **AT-X**. La unidad de control debe responder **Eliminar sectores múltiples**.
4. La unidad de control solicitará a continuación el archivo .bin necesario. En las unidades de control IP500 V2, el archivo se buscará en la tarjeta SD del sistema. En otras unidades de control, proviene de IP Office Manager y aparece en el registro TFTP.
5. En caso que no parezcan estar ocurriendo las transferencias de archivo, compruebe que la dirección IP que aparece en el registro TFTP coincide con la entrada en BOOTP. Modifique la entrada BOOTP si es necesario.
6. El sistema se reiniciará cuando haya terminado.

12.19 Activación de IP Office Web Manager

El acceso a IP Office Web Manager se hace por medio de la dirección IP del sistema y luego se selecciona el enlace ***IP Office Web Manager***. Para poder utilizar IP Office Web Manager, se debe cumplir una serie de criterios según se indica a continuación. La mayoría de estos, se aplica automáticamente a un nuevo sistema instalado con IP Office versión 8.0 o superior. Sin embargo, para sistemas que se están actualizando a IP Office versión 8.0 o superior, es posible que se necesite realizar pasos de actualización adicionales.

Activación de IP Office Web Manager

1. Los archivos IP Office Web Manager deben estar presentes en la tarjeta SD del sistema. Esto se puede hacer de distintas maneras:
   - Seleccionando incluir dichos archivos cuando se lo soliciten mientras se recrea la tarjeta SD de IP Office 140 mediante IP Office Manager.
   - Seleccionando **Cargar archivos del sistema** cuando se actualiza el sistema mediante IP Office Manager.
2. La seguridad del sistema IP Office debe permitir el funcionamiento de IP Office Web Manager:
   - Esto se realiza automáticamente para cualquier nuevo sistema instalado con software IP Office versión 8.0 o posterior.
   - Esto se realiza automáticamente para cualquier sistema existente con una versión de IP Office anterior a 8.0 durante la actualización, si el sistema se configura para usar la contraseña predeterminada de versiones anteriores a IP Office 8.0.
   - Para cualquier sistema actualizado a IP Office versión 8.0 sin primero volver a establecer la contraseña predeterminada, puede:
     - Mediante IP Office Manager:
       1. Si no lo ha hecho, seleccione **Ver | Vista avanzada**.
       2. Seleccionar **Archivo | Opciones avanzadas | Borrar configuración de seguridad (predeterminada)**.
       3. En el menú **Seleccionar IP Office**, seleccione el sistema requerido y haga clic en **Aceptar**.
       4. Introduzca el nombre de usuario **Administrator** y la contraseña de la cuenta.
       5. IP Office Manager confirmará si la acción se realizó correctamente o no.
     - Establezca la configuración de seguridad del sistema mediante un cable DTE RS232 172.

Capítulo 13.
Componentes del sistema

13. Componentes del sistema

Esta sección contempla los componentes individuales que pueden encontrarse en la instalación de un sistema IP Office.

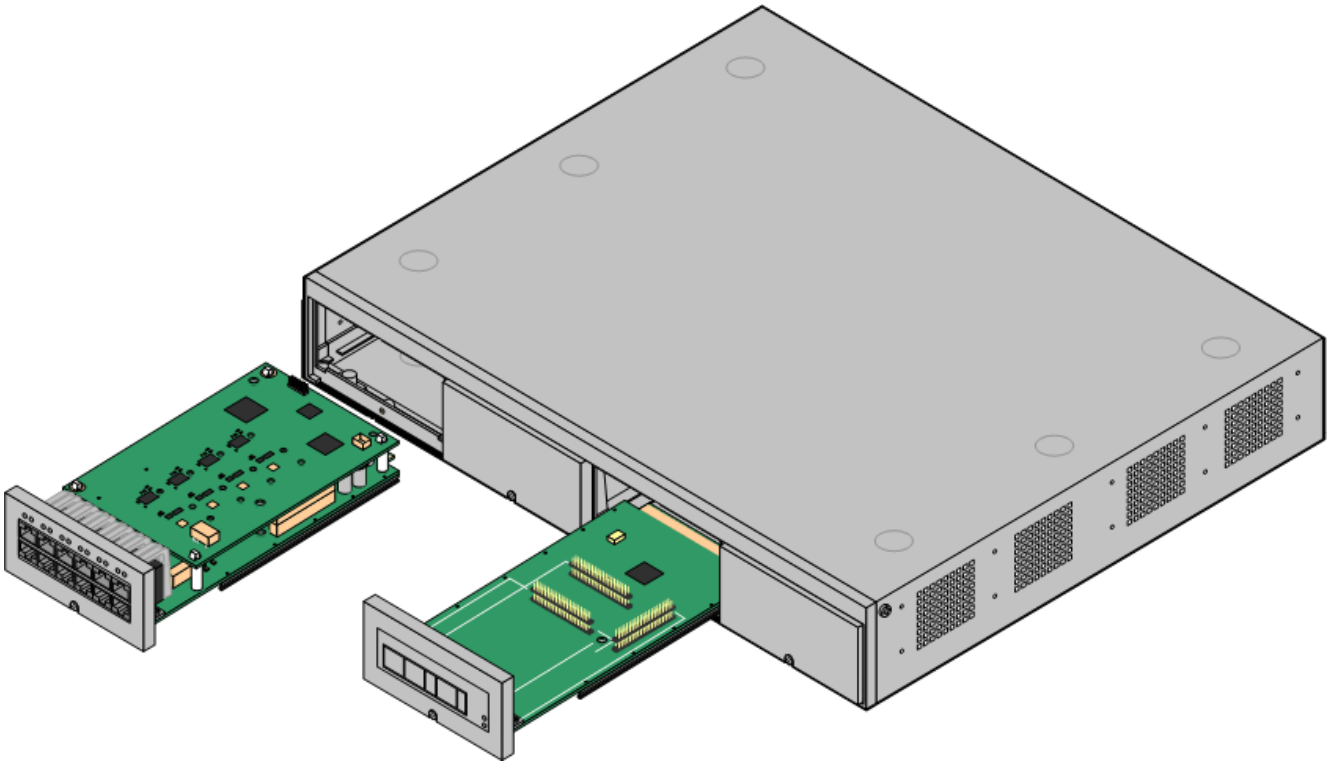
- **Unidad de control IP500 V2** 209
- **Tarjetas System SD** 212
- **Tarjetas base IP500** 213
- **Tarjetas auxiliares de troncales IP500** 231
- **Módulos de expansión externos IP500** 238
- **Kits de montaje** 261
- **Teléfonos** 262
- **Complementos del teléfono** 263
- **Aplicaciones** 264
- **Puertos físicos** 279
- **Licencias** 294

Se incluye información adicional de:

- **Compatibilidad con hardware y software** 302
- **Niveles de PCS de hardware** 310
- **Hardware de TAA** 310

13.1 Unidad de control IP500 V2

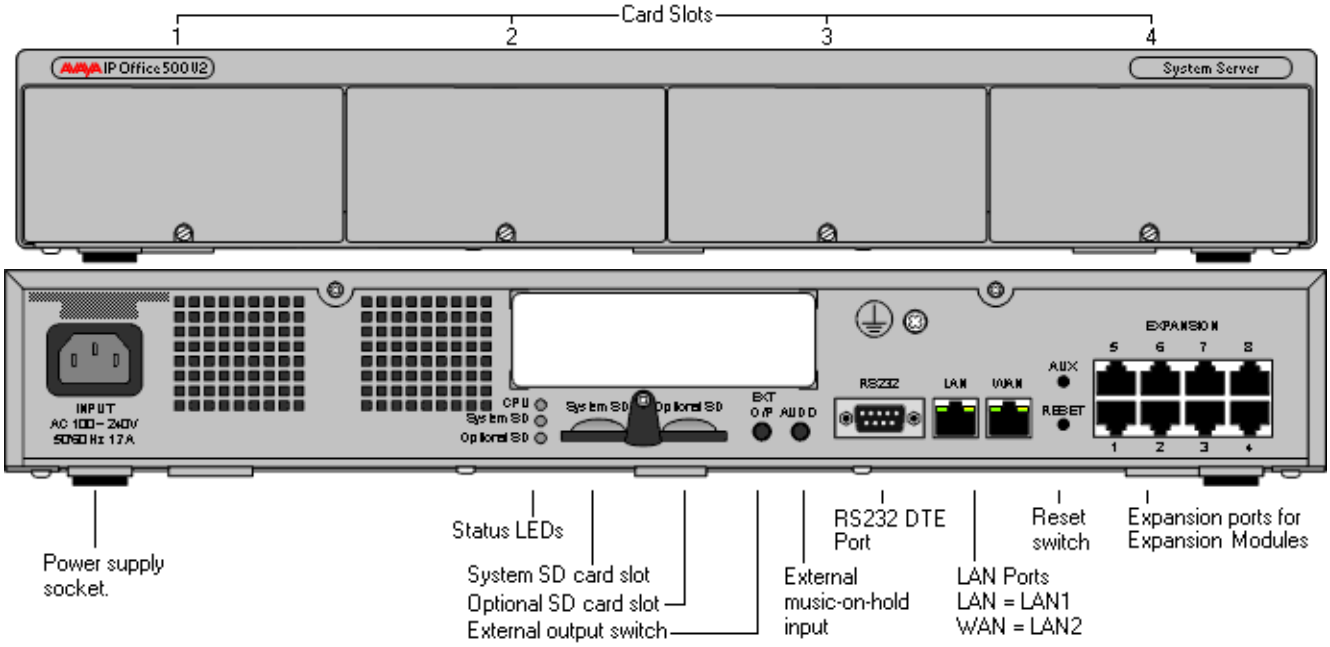
Las ranuras están numeradas de 1 al 4, de izquierda a derecha. Se pueden usar en cualquier orden. Sin embargo, en caso de exceder la capacidad del tipo de tarjeta en particular, la tarjeta en la ranura de la extrema derecha será desactivada. La unidad no debe utilizarse con ranuras al descubierto.



- Avaya IP Office IP 500 V2 también es conocido como "Unidad de control IPO IP500 V2", "IP Office IP 500 v2", "IPO IP500 v2", "IP 500 V2", "IP500 V2", "Conjunto de unidad de sistema IPO 500v2" o "IP Office 500 v2". A lo largo de este documento se usa el término IP500 V2.

Función	Capacidad
Extensiones máximas	Hasta 384 extensiones en modos estándar de IP Office.
Grupos en conferencia	128 como estándar, pero máximo 64 en cualquier conferencia individual. Se aplica la supresión de silencio a las conferencias con más de 10 participantes.
Tarjetas de troncales	Cuatro tarjetas auxiliares de líneas troncales IP500.
Canales de compresión de voz	Hasta 148 canales usando VCM IP500 y tarjetas combinadas IP500.
Canales de correo de voz	El sistema permite utilizar un máximo de 40 canales para sesiones de conexión de Voicemail Pro/ TAPI WAV (con sujeción a las licencias disponibles). Hasta 6 canales para Embedded Voicemail (dos predeterminados, los canales adicionales requieren licencias).
Localidades	Compatibles en todas las localidades de IP Office 45.
Nivel de software	IP Office Essential Edition: Mínimo 6.0. IP Office Basic Edition - modo PARTNER®: Mínimo 6.0. IP Office Basic Edition - modo Norstar: Mínimo 6.1. IP Office Basic Edition: Mínimo 7.0. Archivo Bin = ip500v2.bin.
Suministro de energía	Unidad interna de suministro de energía
Montaje	Instalación independiente, montada en bastidor (requiere kit de montaje en bastidor IPO IP500) o montada en pared (requiere kit de montaje en pared IPO IP500).
Dimensiones	Ancho: 445mm/17,5". Profundidad: 365mm/14,4". Altura: 73mm/2.9"/2U. Distancia de seguridad: 90mm a todos los costados, 220m hacia el frente.
Memoria	Tamaño máximo de archivo de configuración: 2.048KB.

Nombre		Descripción	País	Código SAP
Unidades de control IP500 V2	**Unidad de control IPO IP500 V2**	Unidad de control IP Office 500 V2		700476005
	IPO IP500 V2 CNTRL UNIT TAA	- Trade Agreements Act 310 variante que cumple con los requisitos.		700501510
Tarjeta de memoria SD Avaya	**IPO IP500 V2 SYS SD CARD AL**	Tarjeta SD de IP500 V2 A-Law		700479702
	IPO IP500 V2 SYS SD CARD MUL	Tarjeta SD de IP500 V2 U-Law		700479710
Cable de energía aterrizado IEC60320 C13	**IPO - PWR LEAD (EARTHED) EU CEE7/7**	CEE7/7	Europa	700289762
	IPO - PWR LEAD (EARTHED) UK	BS1363	Reino Unido	700289747
	IPO - PWR LEAD (EARTHER) US	NEMA5-15P	América	700289770
Kits de montaje	**IPO IP500 WALL MNTG KIT V3**	IPO IP500 WALL MNTG KIT V3		700503160
Otros	**Kit de placa de cierre IP500**	Kit de placa de cierre IP500		700429194



Puertos	Descripción
AUDIO 282	Enchufe estéreo de 3.5. Se utiliza para la entrada de la fuente externa de música de espera.
Aux 138	• Al oprimir este botón mientras la unidad de control se está reiniciando, ésta omitirá el reinicio 138 desde la carpeta ***/primary*** en la tarjeta System SD. • Si lo oprime por más de cinco segundos mientras el sistema está en ejecución, la unidad de control se apagará durante 10 minutos.
CPU	Indica el estado de la unidad de control. • **Alternado verde/rojo** = Iniciando sistema. • **Verde encendida** = Está bien. • **Roja encendida** = No hay software. • **Parpadeando en Rojo** = Error/Apagado.
EXPANSIÓN 288	Enchufe RJ45. Utilizado para dirigir las conexiones a los módulos de expansión externos con ayuda del cable de interconexión para expansiones incluido con el módulo de expansión.
EXT O/P 192	Enchufe estéreo de 3.5. Se utiliza para operar el interruptor de sistemas de relevadores, como controles de entrada por puerta. El puerto contiene dos interruptores independientes, controlados por el sistema de IP Office.
ENTRADA 34	Puerto de entrada de la corriente AC.
LAN 289	Enchufe RJ45. Este puerto es un puerto cruzado MDI de 10/100Mbps dobles y auto-sensibles. Junto con el puerto WAN, forma una interruptor Ethernet capa 3 administrada.
Optional SD 136	Utilizada para la tarjeta SD opcional. La luz LED se utiliza en el mismo modo que para System SD *(ver abajo)*.
RESTAURAR 201	Este interruptor se utiliza para reiniciar IP Office, borrando opcionalmente la configuración la configuración y/o el software nuclear durante el proceso. Consulte la sección Botón Restaurar 201.
RS232 293	Enchufe para conector tipo D de 9 vías. Utilizado para operaciones de mantenimiento del sistema.
System SD 136	Utilizada para la tarjeta System SD. La luz LED se utiliza como sigue: • **Apagado** = Apagado de la tarjeta. • **Verde encendido** = tarjeta presente. • **Verde parpadeando** = Tarjeta en uso. • **Anaranjado estable** = Reinicio inminente. • **Rojo parpadeando** = Tarjeta iniciándose o apagándose. • **Rojo parpadeando rápido** = tarjeta llena • **Rojo estable** = Falla de tarjeta/tipo incorrecto.
WAN 289	Enchufe RJ45. Este puerto es un puerto cruzado MDI de 10/100Mbps dobles y auto-sensibles. Junto con el puerto WAN, forma un interruptor Ethernet capa 3 administrada. Este puerto no es compatible en sistemas que funcionan en IP Office Basic Edition - modo PARTNER®, IP Office Basic Edition - modo Norstar o IP Office Basic Editions.
⏚	Se utiliza para la conexión con la puesta a tierra de protección o funcional 90. Se recomienda el uso de una conexión de tierra para todos los sistemas, y puede ser un requerimiento de ley en algunas localidades.

13.2 Tarjetas SD del sistema IP500 V2

Este tipo de tarjeta se usa con las unidades de control IP500 V2 y es obligatoria. La tarjeta se usa para otorgar licencias al sistema y también para el correo de voz integrado si se la requiere. También contiene los archivos del firmware que cargan el sistema y los teléfonos cuando se instala el sistema.

La unidad de control debe estar equipada con una de estas llaves de funciones, incluso si no se está utilizando una licencia.

- La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.

- De forma predeterminada, la tarjeta puede utilizarse para 2 puertos de Embedded Voicemail. Se pueden habilitar puertos adicionales con un máximo de 6 mediante la inserción de licencias 294. La capacidad de mensajes y saludos del buzón de correo de voz admite dos conexiones simultáneas y quince horas de almacenamiento. Esto puede incrementarse a seis canales mediante la adición de licencias, cada uno de los cuales permite dos canales adicionales y cinco horas de almacenamiento adicionales.

- ⚠ **PRECAUCIÓN**
  Solo debe aplicarse formato a estas tarjetas mediante IP Office Manager o System Status Application. Sólo deben retirarse las tarjetas del sistema después de haber apagado la tarjeta 153 o apagado el sistema. 161.

Candado de la Clave de funciones	Código SAP
IPO IP500 V2 SYS SD CARD A-LAW	700479702
IPO IP500 V2 SYS SD CARD MU-LAW	700479710

  - **Tarjeta SD de IP Office U-Law**
    Un sistema equipado con este tipo de tarjeta operará en modo predeterminado en telefonía U-Law y en Sistema clave IP Office Basic Edition . Diseñado para localidades en Norteamérica.

  - **Tarjeta SD de IP Office A-Law**
    Un sistema equipado con este tipo de tarjeta operará en modo predeterminado en telefonía A-Law y en sistema PBX IP Office Basic Edition . Diseñado para localidades fuera de Norteamérica.

Embedded Voicemail

La tarjeta SD del sistema puede usarse para proporcionar Embedded Voicemail para el sistema. Sin la licencia, el Embedded Voicemail provisto por el sistema admite dos conexiones simultáneas y 15 horas de almacenamiento. Este puede expandirse a hasta 6 canales mediante la adición de licencias 294, donde cada una de las cuales tiene dos canales adicionales y cinco horas de almacenamiento adicionales.

Para obtener detalles sobre la configuración de la aplicación de Embedded Voicemail, consulte el manual de instalación de esta aplicación. Las tarjetas vienen precargadas con los siguientes idiomas:

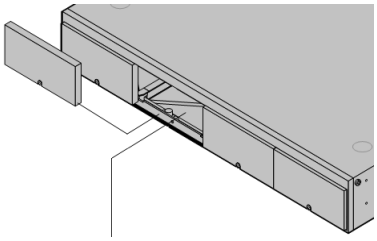
- **Árabe**, **cantonés**, **danés**, **holandés**, **inglés (Reino Unido)**, **inglés (EE. UU.)**, **finlandés**, **francés**, **francés (Canadá)**, **alemán**, **hebreo**, **italiano**, **japonés**, **coreano**, **mandarín**, **noruego**, **polaco**, **portugués**, **portugués (Brasil)**, **ruso**, **español**, **español (Argentina)**, **español (América Latina)**, **español (México)**, **sueco**, **turco**.

Codificación PCM

- **A-Law o Mu-Law**
  PCM (Modulación por pulsos codificados) es un método para codificar voz como datos. En telefonía se utilizan ampliamente dos métodos de codificación, A-law y Mu-law (también llamado U-law). Por lo general, Mu-law se utiliza en Norteamérica y en algunas otras ubicaciones, en tanto que A-law se utiliza en el resto del mundo. Además de configurar la codificación PCM correcta para la región, la configuración A-Law o Mu-Law de un sistema IP Office al iniciarlo originalmente afecta un amplio rango de ajustes predeterminados relacionados con la configuración de líneas y otros valores.

  - En los sistemas IP500 V2, la codificación predeterminada se establece por el tipo de tarjeta SD de sistema instalada cuando el sistema se inicia por primera vez.

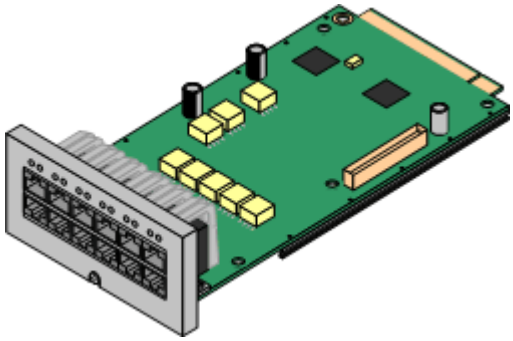
13.3 Tarjetas base IP500



La unidad de control de IP500 V2 tiene 4 ranuras para la inserción de las tarjetas base de IP500. Las ranuras están numeradas de 1 al 4, de izquierda a derecha. Por lo general se les puede utilizar en el orden que sea sin embargo, en caso de exceder la capacidad del tipo de tarjeta en particular, la tarjeta en la ranura de la extrema derecha será desactivada.

Cada tarjeta base incluye un panel delantero integrado con los puertos para las conexiones de cable. Típicamente los primeros ocho puertos de la izquierda se utilizan para conectar dispositivos de extensiones. Los cuatro puertos a la izquierda se utilizan para conectar troncales cuando se ha conectado una tarjeta auxiliar de troncales 27 a la tarjeta base.

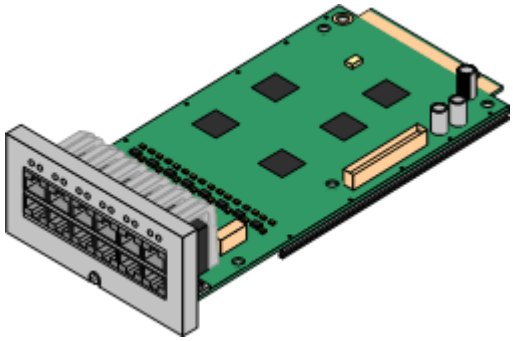
Tarjeta base de estación digital IP500 224



Esta tarjeta proporciona ocho puertos 8 DS (estación digital) para la conexión de teléfonos digitales Avaya.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500 27 que utiliza los puertos de la tarjeta base para realizar conexiones de troncales.
- **Máximo:** 3 tarjetas por unidad de control.
  - Las conexiones para teléfonos 4100, 7400, serie M y serie T utiliza la tarjeta IP500 TCM8 Digital Station.

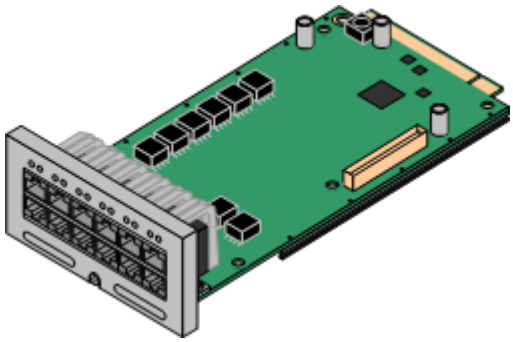
Tarjeta base de teléfono analógico IP500 217



La tarjeta esta disponible en dos variantes, proporcionando ya sea 2 u 8 puertos de teléfono analógico.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500 27 que utiliza los puertos de la tarjeta base para realizar conexiones de troncales.
- **Máximo:** Cuatro por unidad de control.
  - Los puertos de troncales analógicas no incluyen un capacitor de timbre. En sitios donde existe este requerimiento, debe realizarse la conexión mediante un enchufe Maestro que contenga capacitores de timbre.
  - Si está equipada una tarjeta auxiliar de troncales analógicas IP500, durante los cortes de energía el puerto 8 se conecta al puerto de troncales analógicas 12.

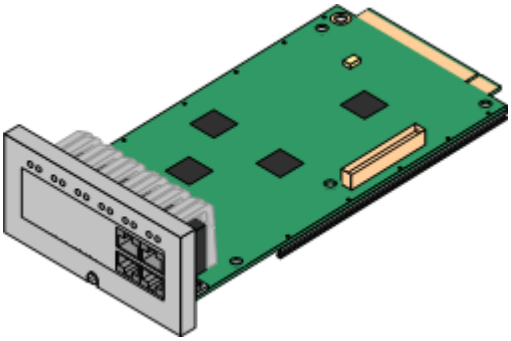
Tarjeta de estación digital TCM8 IP500 228



Esta tarjeta proporciona ocho puertos BST (estación digital) para la conexión de los teléfonos Avaya 4100, 7400, serie M y serie T.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500 27 que utiliza los puertos de la tarjeta base para realizar conexiones de troncales.
- **Máximo:** 4 por unidad de control por unidad de control IP500 V2.

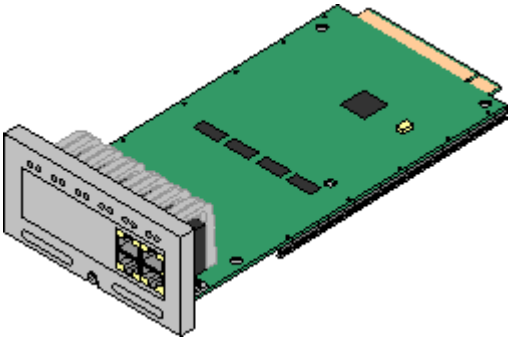
Tarjeta base de VCM IP500



Esta tarjeta está disponible en variantes que soportan 32 o 64 canales de compresión de voz para el uso con llamadas VoIP.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500 que utiliza los puertos de la tarjeta base para realizar conexiones de troncales.
- **Máximo:** Dos por unidad de control

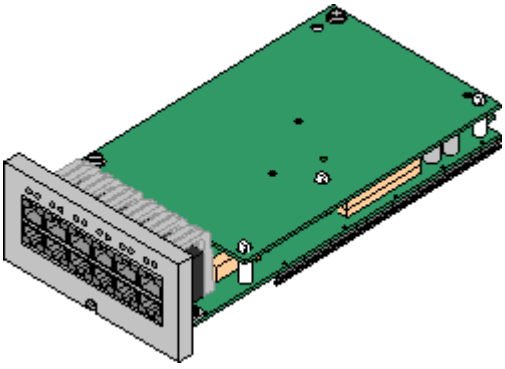
Tarjeta base de expansión de cuatro puertos IP500



Esta tarjeta agrega cuatro puertos de expansión adicionales a los módulos de expansión externos. La tarjeta trae incluidos cuatro cables de interconexión amarillos de 2m.

- Esta tarjeta no admite ninguna tarjeta auxiliar de troncales IP500.
- **Máximo:** 1 por unidad de control (solamente en la ranura 4 del lado derecho).
- **Módulos de expansión compatibles:** Los siguientes módulos de expansión externos son compatibles:
  - Módulo de troncales analógicas IP500
  - Módulo BRI So8 IP500
  - Módulo de estación digital IP500
  - Módulo de estación digital A IP500
  - Módulo de estación digital B IP500
  - Módulo Phone IP500

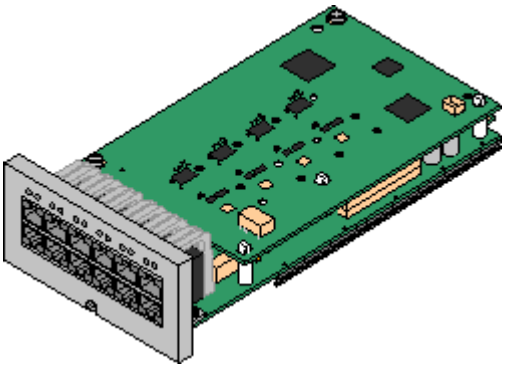
Tarjeta combinada BRI IP500



Esta tarjeta proporciona seis puertos de estación digital (1-6), dos puertos de extensiones analógicas (7-8) y dos puertos de troncales BRI (9-10, cuatro canales). La tarjeta también ofrece 10 canales de compresión de voz.

- **Máximo:** 2 tarjetas combinadas por unidad de control IP500 V2, sin importar el tipo.
  - Las tarjetas combinadas IP500 están equipadas previamente con una tarjeta auxiliar de troncales que no se puede extraer ni cambiar por otra tarjeta auxiliar de troncales de otro tipo o capacidad.
  - Los sistemas IP Office Basic Edition - modo Norstar y IP Office Basic Edition están limitados a un máximo de 12 canales BRI que usan tarjetas combinadas BRI o tarjetas auxiliares troncales BRI.

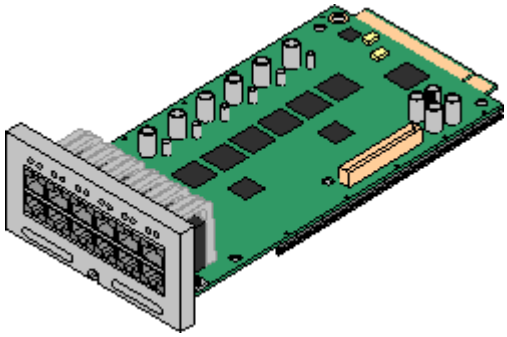
Tarjeta combinada ATM IP500/Tarjeta combinada ATM IP500 V2



Esta tarjeta proporciona seis puertos de estación digital (1-6), dos puertos de extensiones analógicas (7-8) y dos puertos de troncales analógicas (9-12). La tarjeta también ofrece 10 canales de compresión de voz.

- **Máximo:** 2 tarjetas combinadas por unidad de control IP500 V2, sin importar el tipo.
  - Las tarjetas combinadas IP500 están equipadas previamente con una tarjeta auxiliar de troncales que no se puede extraer ni cambiar por otra tarjeta auxiliar de troncales de otro tipo o capacidad.
  - Los puertos de troncales analógicas no incluyen un capacitor de timbre. En sitios donde existe este requerimiento, debe realizarse la conexión mediante un enchufe Maestro que contenga capacitores de timbre.
  - Durante cortes de energía, el puerto 8 del teléfono se conecta al puerto para troncales analógicas 12.

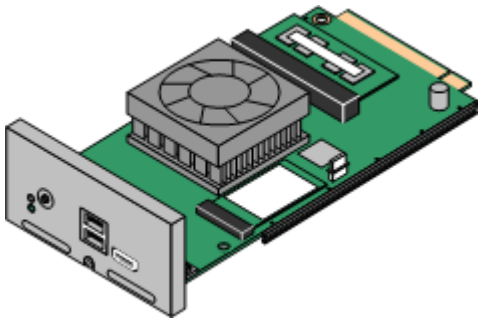
Tarjeta base ETR6 IP500 226



Esta tarjeta solo es compatible en una unidad de control IP500 V2 que funciona en IP Office Basic Edition - modo PARTNER® o IP Office Basic Edition. Proporciona seis puertos ETR para la conexión de teléfonos ETR. También se proporcionan dos puertos de extensiones analógicas para su uso de emergencia con la tarjeta de troncales analógicas.

- La tarjeta puede equiparse con una tarjeta auxiliar de troncales IP500, la cual utiliza los puertos de la tarjeta base para la conexión de troncales..
- **Máximo:** 3 por unidad de control IP500 V2.
- Los puertos de troncales analógicas no incluyen un capacitor de timbre. En sitios donde existe este requerimiento, debe realizarse la conexión mediante un enchufe Maestro que contenga capacitores de timbre.
- Si está equipada una tarjeta auxiliar de troncales IP500, durante los cortes de energía los puertos 7 y 8 se conectan al puerto de troncales analógicas 12. Sin embargo, durante la operación normal los puertos analógicos 7 y 8 no son utilizables.

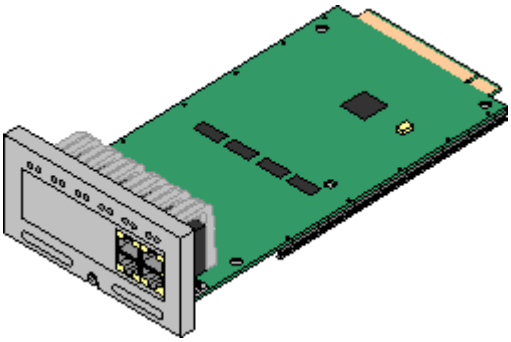
Unified Communications Module 223



Esta tarjeta funciona como un servidor Linux incorporado para las aplicaciones one-X Portal for IP Office y/o Voicemail Pro.

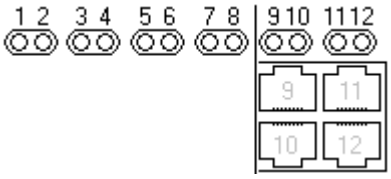
13.3.1 Tarjeta de expansión de cuatro puertos

Esta tarjeta se usa para agregar 4 puertos de expansión adicionales a la unidad de control.



- **Compatibilidad**
  Proporciona cuatro puertos de expansión 288 adicionales para la conexión con módulos de expansión externos.
- **Módulos de expansión compatibles:** Los siguientes módulos de expansión externos son compatibles:
  - Módulo de troncales analógicas IP500
  - Módulo BRI So8 IP500
  - Módulo de estación digital IP500
  - Módulo de estación digital A IP500
  - Módulo de estación digital B IP500
  - Módulo Phone IP500
- **Máximo por unidad de control:** 1 - Solamente en la ranura 4 del lado derecho.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✗.
- **Modos de IP Office:** No compatibles en modos IP Office Basic Edition.

- Cada módulo de expansión externo incluye un cable de interconexión para expansiones azul de 1 metro (3'3"). Este cable sedebe usar cuando se conecte a puertos de expansión en la parte trasera de una unidad de control.
- Al realizar la conexión con los puertos de expansión de una tarjeta IP500 4-Port Expansion card, puede utilizar el cable de interconexión para expansiones amarillo de dos metros (6'6") en vez del cable azul estándar. La tarjeta de expansión de 4 puertos IP500 contiene cuatro cables amarillos.



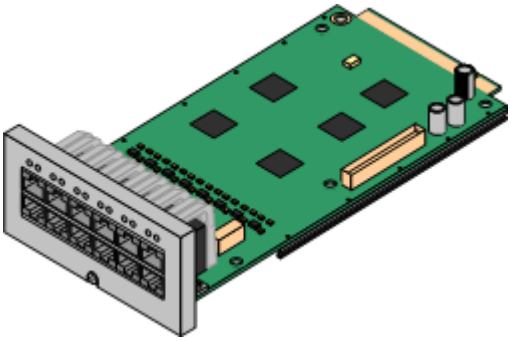
- Las luces LED 1 a 8 se utilizan para los puertos de expansión en la parte trasera de la unidad de control. Las luces LED 9 a 12 se utilizan para los puertos de expansión propios de la tarjeta.

Verde	**Encendido**	Módulo de expansión presente.
Rojo	**Parpadeando**	Iniciando sistema.
Rojo	**Encendido**	Error.
Anaranjado	**Parpadeo regular**	La tarjeta base está bien.

Nombre	Descripción	Código SAP
IPO IP500 EXP CARD 4PT	Incluye cuatro cables amarillos de interconexión de 2 metros.	700472889
IPO EXP CABLE RJ45/RJ45 2M YELLOW	Para uso exclusivo con la tarjeta 4-Port Expansion.	700472871

13.3.2 Teléfono analógico

Esta tarjeta se usa para agregar puertos de teléfono analógicos a la unidad de control. La tarjeta está disponible en dos variantes, proporcionando ya sea 2 u 8 puertos de teléfono analógico.



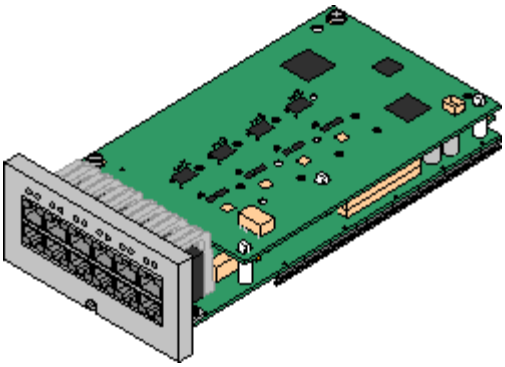
- **Compatibilidad**
  Proporciona ya sea ocho o dos puertos telefónicos analógicos 282 dependiendo de la variante de tarjeta.
- **Máximo por unidad de control:** 4.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✓ 1.
- **Modos de IP Office:** Compatible en todos los modos.

Tipo de puerto	Puertos	Funciones
Teléfono analógico	**1 a 8**	• Compatible con los modos DTMFA, DTMFC, DTMFD, FSK y UK20 de señal ICLID. • REN 2 (1 para dispositivo de timbrado externo). • Corriente con teléfono descolgado: 25 mA • Voltaje del negativo: 40 V. • Los puertos no incluyen un capacitor de timbre, ya que están diseñados para su uso en la conexión con teléfonos analógicos de dos hilos. Para conectar con teléfonos analógicos de cuatro hilos, la conexión debe efectuarse con un enchufe maestro y capacitores de timbre. • Si está equipada una tarjeta de troncales analógicas para Phone 8, en caso de ocurrir un corte de energía el puerto 8 se conecta al puerto de troncales analógicas 12. **Luces LED puerto** • Las extensiones de teléfono analógico no utilizan ninguna luz LED para indicar su estado. • Se utiliza la luz LED1 asimismo para indicar el estado de la tarjeta base: • **Rojo encendido** = Error/no compatible. • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
Puertos de tarjeta opcional de troncales	**9 a 12**	La tarjeta puede equiparse con una tarjeta troncal auxiliar de cualquier tipo. La tarjeta auxiliar de troncales utiliza entonces los puertos 9 a 12 en la tarjeta base para realizar las conexiones de troncales. **Luces LED puerto** El uso de indicadores LED depende del tipo de tarjeta auxiliar instalada en la tarjeta base: • Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar: • **Rojo encendido** = Error • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema. **Tarjeta analógica** • **Verde encendida** = V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde parpadeando** = Línea en uso. **Tarjeta PRI** • **Apagado** = No troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso. • **Rojo/verde parpadeando rápido** (puerto 9) o **Verde parpadeando rápido** (puerto 10) = señal de indicación de alarma (AIS) desde el extremo remoto de la troncal. • **Rojo con parpadeo verde** (puerto 9) o **Parpadeo verde** (puerto 10) = Puerto en modo de bucle de retroceso (configurado con IP Office System Monitor). **Tarjeta BRI** • **Apagado** = No hay una troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso.

Nombre	Descripción	Código SAP
IPO 500 Extn Card Phone 2	IP Office 500 Extension Card Phone 2	700431778
IPO 500 Extn Card Phone 8	IP Office 500 Extension Card Phone 8	700417231

13.3.3 Tarjeta combinada ATM

Estas tarjetas se utilizan para agregar una combinación de puertos a una unidad de control IP500 V2. No es compatible con unidades de control IP500. La versión más reciente de tarjeta combinada ATM IP500 ATM V2 solo es compatible con IP Office versión 8.1 Feature Pack 1 y posteriores.



- **Proporciona**
  - 10 canales de compresión de voz. Compatible con códecs G.711, G729a y G.723 con función de cancelación de eco de 64 ms. G.722 es compatible con la versión 8.0 y posteriores de IP Office.
  - 6 puertos de estación digital para teléfonos digitales Avaya DS 41 compatibles (excepto la serie 3800).
  - 2 puertos de extensión analógica.
  - 4 puertos de troncales analógicas:
    Dependiendo de la versión de la tarjeta combinada, V1 o V2, la tarjeta auxiliar de troncal analógica equivale a una Tarjeta para troncales analógicas IP500 4 233 V1 o V2 respectivamente.
- Durante cortes de energía, el puerto 8 del teléfono se conecta al puerto para troncales analógicas 12.
- **Máximo por unidad de control:** 2 tarjetas combinadas de cualquier tipo por unidad de control IP500 V2.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✓ 1.
  - Las tarjetas combinadas IP500 están equipadas previamente con una tarjeta auxiliar de troncales que no se puede extraer ni cambiar por otra tarjeta auxiliar de troncales de otro tipo o capacidad.
- **Modos de IP Office:** Compatible en todos los modos.
- **Nivel de software de IP Office:** 6.0+.
  Esto depende de la versión de la tarjeta, de la siguiente manera:
  - **V1:** 6.0+. Las nuevas tarjetas PCS04 incorporadas solo son compatibles con sistemas que ejecutan IP Office versión 6.1 (20), 7.0(12), 8.0 y posteriores. Consulte el Consejo técnico de Avaya IP Office 237.
  - **V2:** IP Office versión 8.1 Feature Pack 1 o posteriores.

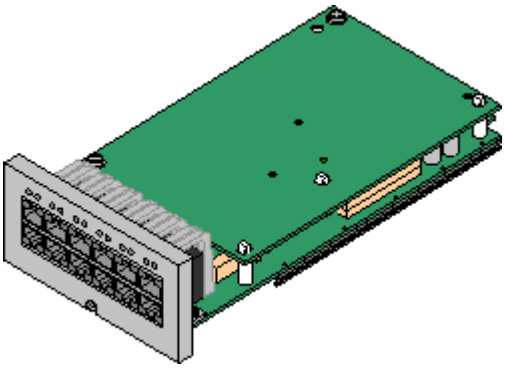
Tipo de puerto	Puertos	Funciones
Estación digital	**1 a 6**	Proporciona puertos DS 286 para teléfonos digitales Avaya DS 41 compatibles (excepto la serie 3800). **indicadores LED** • **Destello verde** = Teléfono detectado. • **Verde encendida** = Teléfono activo. • Se utiliza la luz LED1 asimismo para indicar el estado de la tarjeta base: • **Rojo encendido** = Error/no compatible. • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
Teléfono analógico	**7 a 8**	• Compatible con los modos DTMFA, DTMFC, DTMFD, FSK y UK20 de señal ICLID. • REN 2 (1 para dispositivo de timbrado externo). • Corriente con teléfono descolgado: 25 mA • Voltaje del negativo: 40 V. • Los puertos no incluyen un capacitor de timbre, ya que están diseñados para su uso en la conexión con teléfonos analógicos de dos hilos. Para conectar con teléfonos analógicos de cuatro hilos, la conexión debe efectuarse con un enchufe maestro y capacitores de timbre. • Durante cortes de energía, el puerto de extensión 8 se conecta al puerto 12 de troncales analógicas. • Las extensiones de teléfono analógico no utilizan ninguna luz LED para indicar su estado.
Troncal analógica	**9 a 12**	• Detección de tonos DTMF, ICLID y ocupado. • Protección para sobrevoltaje y contra descargas eléctricas (rayo) (igual puede requerir equipos de protección adicionales 39).

Tipo de puerto	Puertos	Funciones
		• Marcación DTMF y LD (desconexión de bucle). • Cancelación de eco. **indicadores LED** • **Verde encendida** = V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde parpadeando** = Línea en uso. • Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar: • **Rojo encendido** = Error • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.

Nombre	Descripción	Código SAP
IPO IP500 V2 COMB CARD ATM4	IPO IP500 V2 COMBINATION CARD ATM4	700476013
IPO IP500 V2 COMB CARD ATM4 TAA	- Trade Agreements Act 310 variante que cumple con los requisitos.	700501513
IPO IP500 V2 COMB CARD ATM4 V2	IPO IP500 V2 COMBINATION CARD ATM4 V2	700504556

13.3.4 Tarjeta combinada BRI

Esta tarjeta permite agregar una combinación de puertos a una unidad de control IP500 V2.



- **Proporciona**
  - 10 canales de compresión de voz. Compatible con códecs G.711, G729a y G.723 con función de cancelación de eco de 64 ms. G.722 es compatible con la versión 8.0 y posteriores de IP Office.
  - 6 puertos de estación digital para teléfonos digitales Avaya DS 41 compatibles (excepto la serie 3800).
  - 2 puertos de extensión analógica.
  - 2 puertos de troncales BRI (4 canales BRI).
- **Máximo por unidad de control:** 2 tarjetas combinadas de cualquier tipo.
  - Los sistemas IP Office Basic Edition - modo Norstar y IP Office Basic Edition están limitados a un máximo de 12 canales BRI que usan tarjetas combinadas BRI o tarjetas auxiliares troncales BRI.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✓ 1.
  - Las tarjetas combinadas IP500 están equipadas previamente con una tarjeta auxiliar de troncales que no se puede extraer ni cambiar por otra tarjeta auxiliar de troncales de otro tipo o capacidad.
- **Modos de IP Office:** No compatible en modo IP Office Basic Edition - modo PARTNER®.

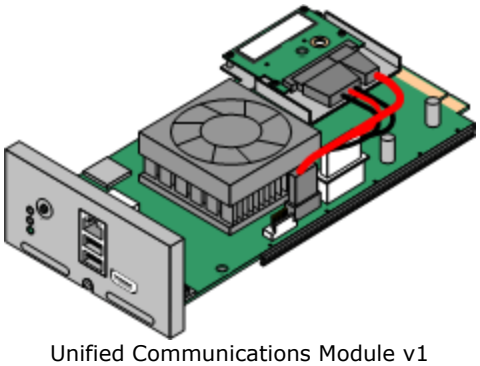
Tipo de puerto	Puertos	Funciones
Estación digital	**1 a 6**	Proporciona puertos DS 286 para teléfonos digitales Avaya DS 41 compatibles (excepto la serie 3800). **indicadores LED** • **Destello verde** = Teléfono detectado. • **Verde encendida** = Teléfono activo. • Se utiliza la luz LED1 asimismo para indicar el estado de la tarjeta base: • **Rojo encendido** = Error/no compatible. • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
Teléfono analógico	**7 a 8**	• Compatible con los modos DTMFA, DTMFC, DTMFD, FSK y UK20 de señal ICLID. • REN 2 (1 para dispositivo de timbrado externo). • Corriente con teléfono descolgado: 25 mA • Voltaje del negativo: 40 V. • Los puertos no incluyen un capacitor de timbre, ya que están diseñados para su uso en la conexión con teléfonos analógicos de dos hilos. Para conectar con teléfonos analógicos de cuatro hilos, la conexión debe efectuarse con un enchufe maestro y capacitores de timbre. • Las extensiones de teléfono analógico no utilizan ninguna luz LED para indicar su estado.
Troncal BRI	**9 a 10**	• Cada puerto de troncales soporta 2B+D canales. • El protocolo de tasa básica ETSI o AusTS013 configurado en toda la configuración IP Office. **indicadores LED** • **Apagado** = No hay una troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso. • Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar: • **Rojo encendido** = Error • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
No utilizado	**11 a 12**	–

Nombre	Descripción	Código SAP
TARJETA COMBINADA BRI PARA IPO IP500 V2	TARJETA COMBINADA BRI PARA IPO IP500 V2	700476021

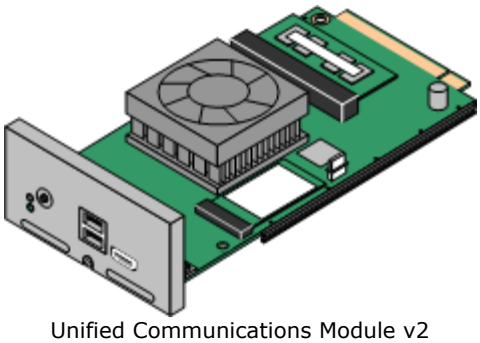
13.3.5 Unified Communications Module

Esta tarjeta es un servidor integrado que permite que las aplicaciones de IP Office basadas en Linux se ejecuten dentro de la unidad de control de IP Office y que no precisen PC independientes. La dirección IP del servidor se establece durante su configuración inicial y posteriormente puede modificarse accediendo al servidor a través del navegador web.

Existen dos tipos de tarjeta. La Unified Communications Module v2 es compatible con IP Office versión 9.1 y posteriores. La Unified Communications Module v1 es compatible con IP Office versión 8.0 con Service Pack Q1 2012 o posteriores. Aunque son físicamente diferentes, los dos tipos de tarjetas son actualmente compatibles con las mismas aplicaciones y capacidades de aplicaciones. Sin embargo, la v2 no otorga una licencia Preferred Edition implícita y no se entrega con el software instalado previamente.



Unified Communications Module v1



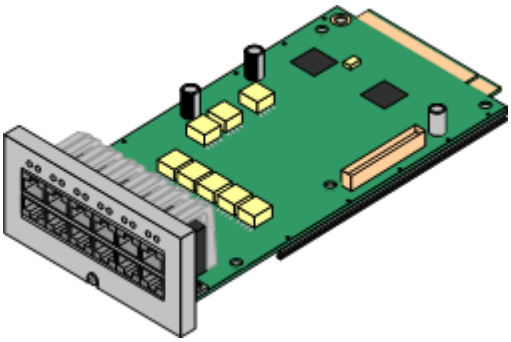
Unified Communications Module v2

- **Compatible con**
  Voicemail Pro o aplicaciones one-X Portal for IP Office.
  - **Usuarios de IP Office:** Hasta 200 usuarios cuando se ejecutan Voicemail Pro y one-X Portal for IP Office. Más de 200 usuarios cuando solo se ejecuta Voicemail Pro.
  - **Usuarios de one-X Portal for IP Office simultáneos:** 50.
  - **Máximo de puertos de correo de voz:** Hasta 20 puertos cuando se ejecutan Voicemail Pro y one-X Portal for IP Office. Hasta 40 puertos cuando solo se ejecuta Voicemail Pro.
  - **Small Community Network:** 6 sistemas como máximo.
- **Licencias**
  Con ambos tipos de tarjeta, se requiere una licencia **Essential Edition** como requisito previo. El servidor de correo de voz también necesita que el sistema cuente con una licencia **Preferred Edition**.
  - En versiones anteriores a los sistemas IP Office 10, Unified Communications Module v1 le concede al sistema host la licencia Preferred Edition virtual que necesita para Voicemail Pro. Esto ya no se aplica a la versión 10 de IP Office ni a las posteriores. Los sistemas IP Office existentes que se actualicen a la versión 10 de IP Office deben utilizar el proceso de migración de licencia de IP Office para conservar la licencia existente.
- **Máximo por unidad de control:** 1 tarjetas por unidad de control.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✗
- **Modos de IP Office:** No compatibles en modos IP Office Basic Edition.
- **ADVERTENCIA:**
  La tarjeta Unified Communications Module v1 se suministra con una cubierta plástica extraíble ubicada sobre los puertos externos (LAN, USB y HDMI) en la placa frontal de la tarjeta. Esta cubierta siempre debe estar en su lugar durante el funcionamiento normal de la tarjeta. Solo debe extraerla temporalmente durante tareas de mantenimiento que requieren acceso a los puertos y debe volver a colocarla una vez que finalice el mantenimiento.
- **ADVERTENCIA: La tarjeta se mantiene caliente después del apagado del sistema**
  Al extraer una Unified Communications Module de un sistema, se debe tener cuidado de no tocar el disipador de calor del módulo. El disipador de calor permanece caliente durante un largo tiempo después de que se apaga el sistema.

Nombre	Descripción	Código SAP
IPO UC MODULE	IP Office Unified Communications Module v1	700501442
IPO UC MODULE V2	IP Office Unified Communications Module v2	700507449

13.3.6 Estación digital

Esta tarjeta permite agregar puertos de extensión para estaciones digitales (DS) a una unidad de control IP500 e IP500 V2. Proporciona ocho puertos de extensión DS RJ45, para su uso con teléfonos digitales Avaya DS compatibles 41. Se proporcionan cuatro puertos RJ45 para las conexiones de troncales cuando la tarjeta está equipada con una tarjeta auxiliar de troncales IP500.



- **Compatibilidad**
  Incluye 8 puertos DS 286 para teléfonos digitales Avaya DS 41 (excepto la serie 3800).
- **Máximo por unidad de control:** 3 tarjetas por unidad de control.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✓ 1.
- **Modos de IP Office:** Compatible en todos los modos.

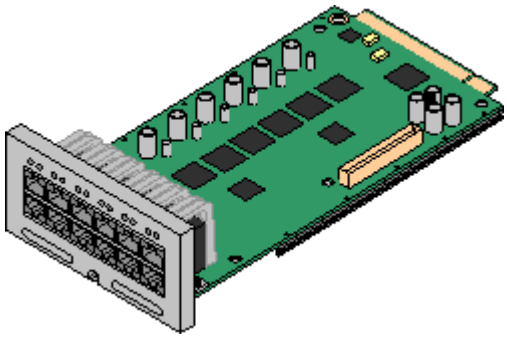
Tipo de puerto	Puertos	Funciones
Estación digital	**1 a 8**	Proporciona puertos DS 286 para teléfonos digitales Avaya DS 41 compatibles (excepto la serie 3800). **indicadores LED** • **Destello verde** = Teléfono detectado. • **Verde encendida** = Teléfono activo. • Se utiliza la luz LED1 asimismo para indicar el estado de la tarjeta base: • **Rojo encendido** = Error/no compatible. • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
Puertos de tarjeta opcional de troncales	**9 a 12**	La tarjeta puede equiparse con una tarjeta troncal auxiliar de cualquier tipo. La tarjeta auxiliar de troncales utiliza entonces los puertos 9 a 12 en la tarjeta base para realizar las conexiones de troncales. **Luces LED puerto** El uso de indicadores LED depende del tipo de tarjeta auxiliar instalada en la tarjeta base: • Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar: • **Rojo encendido** = Error • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema. **Tarjeta analógica** • **Verde encendida** = V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde parpadeando** = Línea en uso. **Tarjeta PRI** • **Apagado** = No troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso. • **Rojo/verde parpadeando rápido** (puerto 9) o **Verde parpadeando rápido** (puerto 10) = señal de indicación de alarma (AIS) desde el extremo remoto de la troncal. • **Rojo con parpadeo verde** (puerto 9) o **Parpadeo verde** (puerto 10) = Puerto en modo de bucle de retroceso (configurado con IP Office System Monitor). **Tarjeta BRI** • **Apagado** = No hay una troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso.

Nombre	Descripción	Código SAP
IPO 500 Extn Card Dgtl Sta 8	IP Office 500 Extension Card Digital Station 8	700417330

IPO IP500 EXTN CARD DGTL STA 8 TAA	- Trade Agreements Act variante que cumple con los requisitos.	700501512

13.3.7 Tarjeta ETR6

Esta tarjeta se usa para agregar 6 puertos de extensión de teléfono ETR 41 a una unidad de control IP500 V2. También incluye dos puertos de extensión analógica para usar en caso de emergencias solamente si la tarjeta está equipada con una tarjeta auxiliar de líneas troncales analógica. Se proporcionan 4 puertos RJ45 (9 a 12) adicionales para las conexiones de troncales cuando la tarjeta está equipada con una tarjeta auxiliar de troncales IP500.



- **Compatible con teléfonos** ETR 41 y analógicos. Cada teléfono ETR puede utilizarse con un teléfono ETR o analógico. El soporte de teléfonos ETR 34D está limitado a un máximo de dos por tarjeta ETR6, cuatro en total.
  - La compaginación en equipos de compaginación externos no se admite a través de puertos ETR6. No se admite a través de puertos POT.
  - Los únicos teléfonos analógicos probados por Avaya para IP500 V2 son los Avaya Serie 6200. Si se usan otros teléfonos analógicos, es responsabilidad del cliente asegurarse de que dichos teléfonos funcionen correctamente.
- **Máximo por unidad de control:** 3.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✓ 1. No compatible con la tarjeta auxiliar de líneas troncales BRI IP500.
- **Modos de IP Office:** Solo se admite en los modos IP Office Basic Edition - modo PARTNER® o IP Office Basic Edition (U-Law) con configuración regional de América del Norte.

Tipo de puerto	Puertos	Funciones

ETR	**1 a 6**	• REN 1.
		• Marcación DTMF únicamente.
		• Indicación de mensaje en espera 51V escalonado.
		• ICLID modo Bellcore 202.
		Indicadores LED
		• Los puertos ETR no utilizan ninguna luz LED para indicar su estado.
		• Se utiliza la luz LED1 asimismo para indicar el estado de la tarjeta base:
		  • **Rojo encendido** = Error/no compatible.
		  • **Rojo parpadeando lentamente** = Iniciando sistema.
		  • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien.
		  • **Rojo parpadeando rápido** = Apagado del sistema.

EF	**7 a 8**	• Si está equipada una tarjeta auxiliar de troncales IP500, ambos puertos se conectan al puerto de troncales analógicas 12 en caso de ocurrir un corte de energía. • Compatible con los modos DTMFA, DTMFC, DTMFD, FSK y UK20 de señal ICLID. • REN 2 (1 para dispositivo de timbrado externo). • Corriente con teléfono descolgado: 25 mA • Voltaje del negativo: 40 V. • Los puertos no incluyen un capacitor de timbre, ya que están diseñados para su uso en la conexión con teléfonos analógicos de dos hilos. Para conectar con teléfonos analógicos de cuatro hilos, la conexión debe efectuarse con un enchufe maestro y capacitores de timbre. • Las extensiones de teléfono analógico no utilizan ninguna luz LED para indicar su estado.

Puerto de troncales opcionales	**9 a 12**	Depende del tipo de tarjeta auxiliar de troncales equipada. El ETR6 puede equiparse ya sea con una tarjeta Troncal analógica 233, o bien con una tarjeta de troncales PRI 236.
		Indicadores LED
		El uso de indicadores LED depende del tipo de tarjeta auxiliar instalada en la tarjeta base:
		• Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar:
		  • **Rojo encendido** = Error
		  • **Rojo parpadeando lentamente** = Iniciando sistema.
		  • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien.
		  • **Rojo parpadeando rápido** = Apagado del sistema.
		Tarjeta analógica
		• **Verde encendida** = V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva.
		• **Verde parpadeando** = Línea en uso.
		Tarjeta PRI
		• **Apagado** = No troncal presente.
		• **Verde encendida** = Troncal presente.
		• **Verde parpadeando** = Troncal en uso.

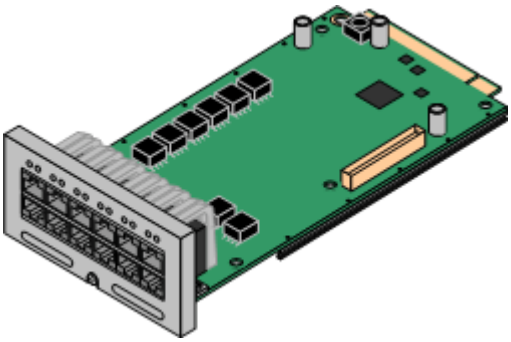
Página1562 de 3226.

		• **Rojo/verde parpadeando rápido** (puerto 9) o **Verde parpadeando rápido** (puerto 10) = señal de indicación de alarma (AIS) desde el extremo remoto de la troncal. • **Rojo con parpadeo verde** (puerto 9) o **Parpadeo verde** (puerto 10) = Puerto en modo de bucle de retroceso (configurado con IP Office System Monitor).

Nombre	Descripción	Código SAP
TARJETA DE EXTENSIÓN IPO IP500 V2 ETR6	TARJETA DE EXTENSIÓN IPO IP500 V2 ETR6	700476039

13.3.8 Estación digital TCM8

Esta tarjeta se usa para agregar puertos de extensión BST RJ45 a una unidad de control IP500 V2. Proporciona ocho puertos de extensión RJ45 para teléfonos digitales Avaya BST compatibles 41. Se proporcionan cuatro puertos RJ45 para las conexiones de troncales cuando la tarjeta está equipada con una tarjeta auxiliar de troncales IP500.



- **Compatibilidad**
  Proporciona ocho puertos BST para estaciones digitales compatibles de las series 4100, 7400, M y T.
- **Máximo por unidad de control:** 4.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✓ 1.
- **Modos de IP Office:** Compatible en todos los modos.

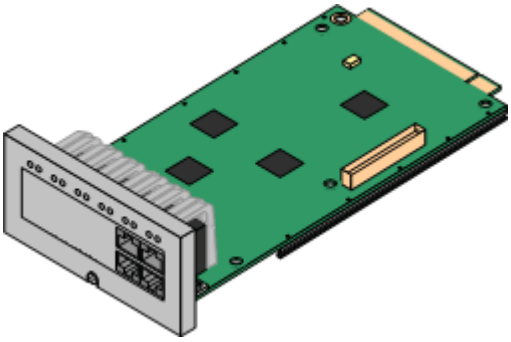
Tipo de puerto	Puertos	Funciones
BST	**1 a 8**	**indicadores LED** • **Verde encendida** = Teléfono detectado. • Se utiliza la luz LED1 asimismo para indicar el estado de la tarjeta base: • **Rojo encendido** = Error/no compatible. • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
Puertos de tarjeta opcional de troncales	**9 a 12**	La tarjeta puede equiparse con una tarjeta troncal auxiliar de cualquier tipo. La tarjeta auxiliar de troncales utiliza entonces los puertos 9 a 12 en la tarjeta base para realizar las conexiones de troncales. **indicadores LED** El uso de indicadores LED depende del tipo de tarjeta auxiliar instalada en la tarjeta base: • Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar: • **Rojo encendido** = Error • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema. **Tarjeta analógica** • **Verde encendida** = V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde parpadeando** = Línea en uso. **Tarjeta PRI** • **Apagado** = No troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso. • **Rojo/verde parpadeando rápido** (puerto 9) o **Verde parpadeando rápido** (puerto 10) = señal de indicación de alarma (AIS) desde el extremo remoto de la troncal. • **Rojo con parpadeo verde** (puerto 9) o **Parpadeo verde** (puerto 10) = Puerto en modo de bucle de retroceso (configurado con IP Office System Monitor). **Tarjeta BRI** • **Apagado** = No hay una troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso.

Nombre	Descripción	Código SAP
IPO 500 TCM 8 Extn Card Assy	IP Office 500 TCM 8	700500758

13.3.9 VCM

Este tipo de tarjeta se usa para agregar canales de compresión de voz a la unidad de control. Estos canales se utilizan para llamadas VoIP, lo que incluye extensiones IP y/o troncales IP. Las unidades de control IP500 V2 admiten hasta 148 canales de compresión de voz mediante tarjetas VCM IP500 y tarjetas combinadas IP500 219.

Las tarjetas están disponibles en variantes de 32 canales y 64 canales. Todas las variantes de tarjetas tienen 4 puertos RJ45 que se utilizan para conexiones de líneas troncales cuando una tarjeta auxiliar de troncales IP500 231.



- **Compatibilidad**
  Códecs G.711, G.729a y G.723 con cancelación de eco de 64ms. La cantidad máxima de canales en uso simultáneamente en la tarjeta base VCM IP500 VCM depende del códec utilizado. La siguiente tabla supone que todas las llamadas que emplean el VCM utilizan el mismo códec.
  - G.722 es compatible en la versión 8.0 IP Office y superiores en sistemas con una tarjeta de compresión de voz IP500 o una tarjeta combinada IP500.

Códec	IP500 VCM 32 IP500 VCM 32 V2	IP500 VCM 64 IP500 VCM 64 V2
G.711	32	64
G.729a	30	60
G.723	22	44
G.722	30	60

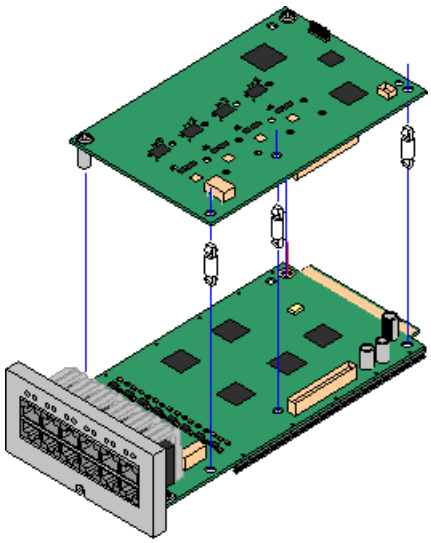
- **Máximo por unidad de control:** 2.
- **Compatibilidad con tarjetas de líneas troncales IP500:** ✓ 1.
- **Modos de IP Office:** No compatibles en modos IP Office Basic Edition.

Tipo de puerto	Puertos	Funciones
Ausente	**1 a 8**	Ausente. **indicadores LED** • Las luces LED 1 a 8 no están etiquetadas. Se utilizan para indicar la utilización del canal de compresión de voz. Cada luz LED encendida representa un uso de 12.5% de la capacidad del canal de compresión de voz (capacidad total de la tarjeta, en vez de capacidad de la licencia). • Se utiliza la luz LED1 asimismo para indicar el estado de la tarjeta base: • **Rojo encendido** = Error/no compatible. • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema.
Puertos de tarjeta opcional de troncales	**9 a 12**	La tarjeta puede equiparse con una tarjeta troncal auxiliar de cualquier tipo. La tarjeta auxiliar de troncales utiliza entonces los puertos 9 a 12 en la tarjeta base para realizar las conexiones de troncales. **indicadores LED** El uso de indicadores LED depende del tipo de tarjeta auxiliar instalada en la tarjeta base: • Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar: • **Rojo encendido** = Error • **Rojo parpadeando lentamente** = Iniciando sistema. • **Rojo parpadeando cada cinco segundos** = La tarjeta está bien. • **Rojo parpadeando rápido** = Apagado del sistema. **Tarjeta analógica** • **Verde encendida** = V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva. • **Verde parpadeando** = Línea en uso. **Tarjeta PRI** • **Apagado** = No troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso. • **Rojo/verde parpadeando rápido** (puerto 9) o **Verde parpadeando rápido** (puerto 10) = señal de indicación de alarma (AIS) desde el extremo remoto de la troncal.

Tipo de puerto	Puertos	Funciones	
			• **Rojo con parpadeo verde** (puerto 9) o **Parpadeo verde** (puerto 10) = Puerto en modo de bucle de retroceso (configurado con IP Office System Monitor).
		Tarjeta BRI	• **Apagado** = No hay una troncal presente. • **Verde encendida** = Troncal presente. • **Verde parpadeando** = Troncal en uso.

	Nombre	Descripción	Código SAP
Módulos de compresión de voz IP500	**IPO IP500 MC VCM 32**	IP Office 500 Media Módulo de codificación de voz de tarjeta de medios 32	700417389
	IPO IP500 VCM 32 TAA	- Trade Agreements Act 310 variante que cumple con los requisitos.	700501518
	IPO IP500 MC VCM 64	IP Office 500 Media Módulo de codificación de voz de tarjeta de medios 64	700417397
Módulos de compresión de voz IP500 V2	**IPO IP500 MC VCM 32 V2**	Módulo de codificación de voz 32 V2 Tarjeta de medios IP500	700504031
	IPO IP500 VCM 32 TAA V2	- Trade Agreements Act 310 variante que cumple con los requisitos.	700504033
	IPO IP500 MC VCM 64 V2	Módulo de codificación de voz 64 V2 Tarjeta de medios IP500	700504032

13.4 Tarjetas auxiliares de troncales IP500

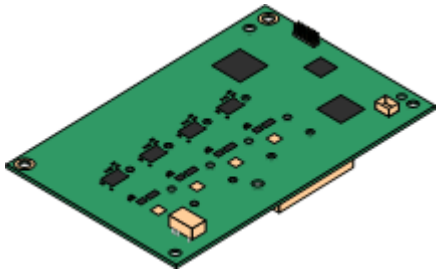


Muchos tarjetas base IP500 24 pueden equiparse con tarjetas auxiliares de troncales IP500 para admitir la conexión de troncales a la tarjeta base.

Cada tarjeta auxiliar está equipada con los pilares de soporte requeridos para su instalación, así como una tarjeta para identificar la presencia de la tarjeta auxiliar en la parte de adelante de la tarjeta base después de la instalación.

- Las tarjetas combinadas IP500 están pre-equipadas con una tarjeta auxiliar de troncales que no puede ser extraída ni cambiada por otro tipo de tarjeta auxiliar de troncales.

Tarjeta de troncales analógicas IP500/Tarjeta de troncales analógicas IP500 V2 233

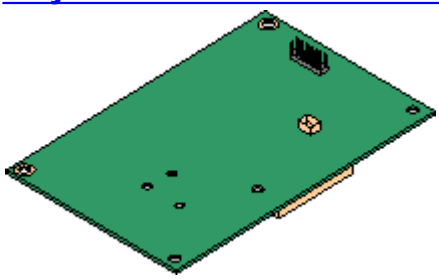


Estas tarjetas permiten que la tarjeta base admita cuatro troncales analógicas de inicio por bucle.

  - Los puertos de troncales analógicas no incluyen un capacitor de timbre. En sitios donde existe este requerimiento, debe realizarse la conexión mediante un enchufe Maestro que contenga capacitores de timbre.
  - Si está instalada la tarjeta base con puertos de teléfono analógico, durante un corte de energía el puerto de teléfono 8 se conecta al puerto de las troncales analógicas 12.

- **Máximo:** 4 tarjetas por unidad de control. La tarjeta de troncales analógicas IP500 V2 solo se admite en el IP500 V2.

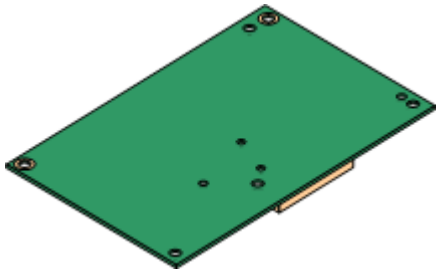
Tarjeta de troncales PRI-U IP500 236



Esta tarjeta permite que la tarjeta base admita dos conexiones con troncales PRI. La tarjeta está disponible en variantes de puerto individual o dual. La tarjeta puede configurarse para troncales E1 PRI, T1 de hurto de bits, T1 PRI o E1R2 PRI. También está disponible una variante T1(J) para uso en Japón.

- **Máximo:** Cuatro por unidad de control.
- El sistema IP Office admite 8 canales B sin licencia en cada puerto PRI-U IP500 instalado. Los canales B adicionales, hasta donde lo permiten la capacidad de los puertos instalados y el modo PRI seleccionado, requieren que se agreguen licencias tipo **IP500 Universal PRI (Canales adicionales)** 296 a la configuración. Estos canales adicionales consumen licencias con base en los canales adicionales que sean configurados como en servicio, desde el puerto 9 de la ranura 1 en adelante. Los canales D no son afectados por las licencias.

Tarjeta de enlace BRI de IP500 235



Esta tarjeta permite que la tarjeta base admita hasta cuatro conexiones de troncales BRI, con cada troncal suministrando canales digitales 2B+D. Esta tarjeta está disponible en variantes de 2 puertos (4 canales) y 4 puertos (8 canales).

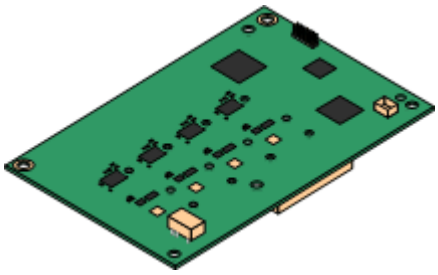
- **Máximo:** 4 tarjetas por unidad de control.
- **Conexión S-Bus**: La tarjeta puede ser alternada del modo de troncales To al modo So. Este modo requiere de resistores de terminación adicionales y de un cable de interconexión cruzada ISDN, consulte la sección Puerto BRI (So) 283.

- Los sistemas IP Office Basic Edition - modo Norstar y IP Office Basic Edition están limitados a un máximo de 12 canales BRI que usan tarjetas combinadas BRI o tarjetas auxiliares troncales BRI.

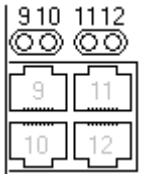
13.4.1 Tarjeta de troncales analógicas

Estas tarjetas se pueden agregar a una tarjeta base IP500 para suministrar esa tarjeta con compatibilidad para cuatro troncales analógicas de inicio por bucle. La versión más reciente de tarjeta de trocales analógicas IP500 V2 solo es compatible con sistemas IP500 V2 que ejecutan IP Office versión 8.1 Feature Pack 1 y posteriores.

Esta tarjeta puede colocarse en cualquier tarjeta base IP500 no combinada, excepto la tarjeta de expansión de cuatro puertos IP500 y Unified Communications Module.



- **Puertos/Canales**
  Cuatro puertos de troncales analógicas de arranque por bucle. Conexiones vía la tarjeta base IP500 anfitriona.
  - Detección de tonos DTMF, ICLID y ocupado.
  - Protección para sobrevoltaje y contra descargas eléctricas (rayo) (igual puede requerir equipos de protección adicionales 39).
  - Marcación DTMF y LD (desconexión de bucle).
  - Cancelación de eco.
- **Cancelación de eco**
  La cancelación de eco que admite la tarjeta varía dependiendo del tipo de tarjeta.
  - **V1:** La cancelación de eco se puede seleccionar manualmente en ***8***, ***16***, ***32***, ***64*** o ***128*** milisegundos o ***Desactivado***. El valor predeterminado es 16 milisegundos.
  - **V2:** La cancelación de eco se puede seleccionar manualmente en ***Activado*** o ***Desactivado***. El valor predeterminado es ***Activado***. La tarjeta de troncales analógicas IP500 V2 también admite reducción de eco configurado en ***Activado*** de manera predeterminada.
- **Indicación de estado de servicio/estado de la línea**
  - **V1:** No se admite la detección de estado de línea individual para líneas inactivas. Por lo tanto, los indicadores LED y System Status Application de la tarjeta sencillamente indican que la tarjeta está instalada y cuándo se está usando la línea.
  - **V2:** No se admite la detección automática de estado de línea para líneas inactivas. Los indicadores LED y System Status Application de la tarjeta indican que la línea individual está conectada e inactiva o se está usando.
- **Coincidencia de impedancia**
  - **V1:** Para esta tarjeta, solo se puede utilizar la coincidencia de impedancia manual y solo en regiones seleccionadas.
  - **V2:** Esta tarjeta admite coincidencia de impedancia automática en el inicio del sistema y este modo está activado en forma predeterminada. Puede usar la coincidencia de impedancia manual o no usarla, según la necesidad. La coincidencia de impedancia se admite en todas las configuraciones regionales.
- **Detección de actividad de voz (VAD)**
  Compatible con tarjetas ATM4U-V2 sólo en IP Office versión 9.1 y superior. Si se activa, habilita la compatibilidad de funciones de las líneas troncales analógicas que requieren indicación de progreso de llamada, por ejemplo, el uso de mobile twinning. Esta función no está habilitada de manera predeterminada.
- **Puertos para cortes de energía**
  Sin importar del tipo de tarjeta IP500 anfitriona, durante los cortos de energía los pins 4 y 5 del puerto 12 se conecta a los pins 7 y 8. Además, cuando se instala en una tarjeta base de 8 puertos para teléfonos analógicos IP500, durante los cortes de energía, el puerto de extensión 8 se conecta al puerto de troncales analógicas 12.
- **Licencia:** No se requieren licencias.
- **Máximo por unidad de control:** 4.
- **Nivel de software de IP Office:**
  Esto depende de la versión de la tarjeta, de la siguiente manera:
  - **V1:** 4.0+.
    Las nuevas tarjetas PCS10 integradas solo son compatibles con sistemas que ejecutan IP Office versión 6.1(20), 7.0(12), 8.0 y posteriores. Consulte el Consejo técnico de Avaya IP Office 237.
  - **V2:** 8.1 Feature Pack 1+



Puertos de la tarjeta auxiliar (9-12)
Las luces LED para los puertos 9 a 12 de la tarjeta IP500 se utilizan como sigue:

- **Verde encendida** = V1: Tarjeta instalada. V2: Línea conectada al puerto pero inactiva.
- **Verde parpadeando** = Línea en uso.

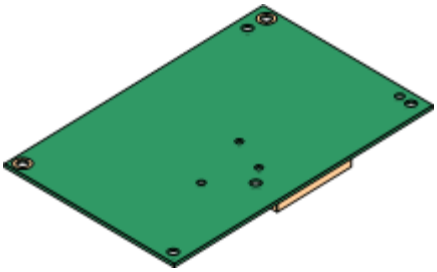
- Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar:
  - **Rojo encendido** = Error
  - **Rojo parpadeando lentamente** = Iniciando sistema.
  - **Rojo parpadeando cada cinco segundos** = La tarjeta está bien.
  - **Rojo parpadeando rápido** = Apagado del sistema.

Nombre	Descripción	Código SAP
IPO 500 Trnk Anlg 4 Uni	IP Office 500 Trunk Card Analog 4 Universal	700417405
Tarjeta de troncales analógicas IPO IP500 4 V2	Tarjeta de troncales analógicas IP Office 500 4 Universal V2	700503164

13.4.2 Tarjetas de líneas troncales BRI

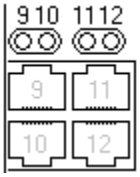
Esta tarjeta puede agregarse a una tarjeta base IP500 para proporcionar a la tarjeta soporte para troncales BRI (To) 284. La tarjeta está disponible en variantes que proporcionan ocho canales (cuatro troncales físicas) o cuatro canales (dos troncales físicas).

Esta tarjeta puede colocarse en cualquier tarjeta base IP500 no combinada, excepto la tarjeta de expansión de cuatro puertos IP500 y Unified Communications Module.



- **Puertos/Canales**
  2 o 4 puertos de troncales BRI. Conexiones vía los puertos 9 a 12 de la tarjeta base IP500 anfitriona.
- Cada puerto de troncales soporta 2B+D canales.
- El protocolo de tasa básica ETSI o AusTS013 configurado en toda la configuración IP Office.
- **Licencia:** No se requieren licencias.
- **Máximo por unidad de control:** 4.
- **Nivel de software de IP Office:** 4.0+.
- **Conexión S-Bus:** En sistemas IP Office 4.2+, esta tarjeta puede alternar al modo de troncales To 284 al modo So 283. Este modo requiere de resistores de terminación adicionales y de un cable de interconexión cruzada ISDN, consulte la sección Puerto BRI (So) 283.
- Esta tarjeta está aprobada para el uso en los siguientes países:

Brasil.	Nueva Zelanda.
China.	Rusia.
India.	Sudáfrica.
Argentina.	Emiratos Árabes Unidos (EAU).
Australia.	Unión europea (UE).



Puertos tarjeta auxiliar (9-12)
Las luces LED para los puertos 9 a 12 de la tarjeta base IP500 se utilizan como sigue:

- **Apagado** = No hay una troncal presente.
- **Verde encendida** = Troncal presente.
- **Verde parpadeando** = Troncal en uso.

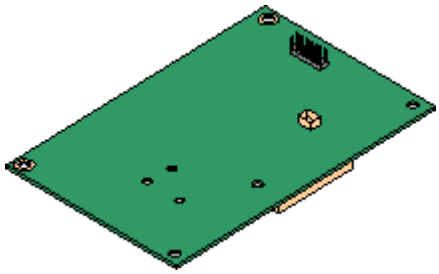
- Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar:
  - **Rojo encendido** = Error
  - **Rojo parpadeando lentamente** = Iniciando sistema.
  - **Rojo parpadeando cada cinco segundos** = La tarjeta está bien.
  - **Rojo parpadeando rápido** = Apagado del sistema.

Nombre	Descripción	Código SAP
Troncal IPO 500 BRI 4 Uni	Tarjeta de troncales analógicas de acceso básico 4 Universal IP500	700417413
TRONCAL IPO IP500 BRI 4 UNI TAA	- Trade Agreements Act 310 variante que cumple con los requisitos.	700501515
Troncal IPO 500 BRI 8 Uni	Tarjeta de troncales analógicas de acceso básico 8 Universal IP500	700417421
IP0 IP500 BRI S0 CONVTR CBL	Cable convertidor IP500 BRI So	700458649

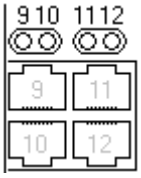
13.4.3 Tarjetas de troncales PRI

Esta tarjeta puede agregarse a una tarjeta base IP500 para proporcionar a la tarjeta soporte para troncales PRI. La tarjeta está disponible en variantes de puerto individual o dual.

Esta tarjeta puede colocarse en cualquier tarjeta base IP500 no combinada, excepto la tarjeta de expansión de cuatro puertos IP500 y Unified Communications Module.



- **Puertos/Canales**
  1 o 2 Troncales PRI 292. Cada puerto admite los siguientes tipos de línea PRI. En tarjetas de puerto dual, ambos puertos deben ser del mismo tipo de línea. Puede modificar la selección de tipo de línea con ayuda de IP Office Manager. Las opciones disponibles dependerán del modo de operación y localidad del sistema IP Office.
    - E1 PRI (30B+D canales por puerto).
    - E1R2 PRI (30B canales por puerto).
    - T1 hurto de bits (24B canales por puerto) o T1 PRI (23B+D canales por puerto).
    - También está disponible una variante T1(J) para uso en Japón (Feature Pack 9.1 y posterior).
  - Puede seleccionar el modo deseado con IP Office Manager haciendo clic derecho sobre el icono de la línea y seleccionando **Cambiar tipo de línea de tarjeta PRI universal** ; luego seleccione el tipo de línea deseado.
  - La conexión de las troncales físicas es vía los puertos 9 a 10 de la tarjeta base IP500 anfitriona.
  - Los puertos 11 y 12 pueden servir como puntos de prueba para conectar equipos de prueba y monitoreo para el puerto adyacente.
- **Licencias**
  El sistema IP Office admite 8 canales B sin licencia en cada puerto PRI-U IP500 instalado. Los canales B adicionales, hasta donde lo permiten la capacidad de los puertos instalados y el modo PRI seleccionado, requieren que se agreguen licencias tipo **IP500 Universal PRI (Canales adicionales)** a la configuración. Estos canales adicionales consumen licencias con base en los canales adicionales que sean configurados como en servicio, desde el puerto 9 de la ranura 1 en adelante. Los canales D no son afectados por las licencias.
- **Máximo por unidad de control:** 4 por unidad de control en modos estándar de IP Office. Solo 1 tarjeta de un solo puerto en otros modos.
- **Nivel de software:** 4.1+.



Puertos tarjeta auxiliar (9-12)
Las luces LED para los puertos 9 a 12 de la tarjeta base IP500 se utilizan como sigue:

- **Apagado** = No troncal presente.
- **Verde encendida** = Troncal presente.
- **Verde parpadeando** = Troncal en uso.
- **Rojo/verde parpadeando rápido** (puerto 9) o **Verde parpadeando rápido** (puerto 10) = señal de indicación de alarma (AIS) desde el extremo remoto de la troncal.
- **Rojo con parpadeo verde** (puerto 9) o **Parpadeo verde** (puerto 10) = Puerto en modo de bucle de retroceso (configurado con IP Office System Monitor).

- Se utiliza la luz LED 9 asimismo para indicar el estado de la tarjeta auxiliar:
  - **Rojo encendido** = Error
  - **Rojo parpadeando lentamente** = Iniciando sistema.
  - **Rojo parpadeando cada cinco segundos** = La tarjeta está bien.
  - **Rojo parpadeando rápido** = Apagado del sistema.

Nombre	Descripción	Código SAP
IPO 500 TRNK PRI UNVRSL SNGL	IP Office 500 Trunk Card Primary Rate 1 Universal	700417439
TRONCAL IPO IP500 PRI UNVRSL SNGL TAA	- Trade Agreements Act 310 variante que cumple con los requisitos.	700501514

IPO 500 TRNK PRI UNIVRSL DUAL	IP Office 500 Trunk Card Primary Rate 2 Universal	700417462
TRONCAL IPO IP500 PRI UNVSL DUAL TAA	- Trade Agreements Act 310 variante que cumple con los requisitos.	700501517
IPO IP500 TARJETA troncal T1(J) PRI DUAL JAPÓN	Tarjeta de interfaz T1(J) dual	700509377

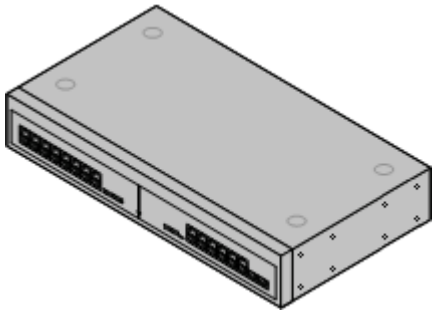
13.5 Módulos de expansión externos IP500

Los siguientes módulos de expansión externos IP500 son compatibles con la versión 10.1 de IP Office. Cada módulo utiliza una unidad de suministro de energía 33 externa, incluida con el módulo. El cable de energía 34 específico de la localidad para el PSU debe solicitarse por separado.

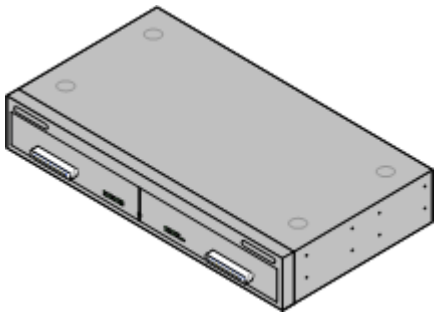
El módulo externo se puede apilar sobre la unidad de control. También se puede montar en la pared o en un rack con uno de los kits de montaje de IP Office 261.

- Los sistemas que funcionan en modos estándar de IP Office admiten ocho módulos de expansión externos o 12 si la unidad de control se instala con una tarjeta base de expansión de cuatro puertos IP500.

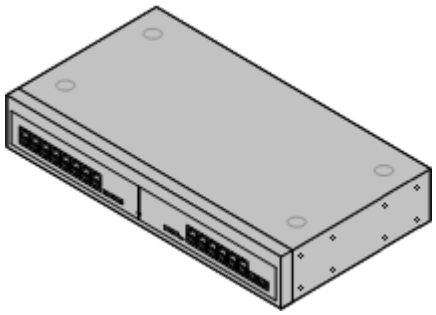
- **Módulos de estación digital IP500** 245
  Según la variante, ofrecen 16 o 30 puertos RJ45 DS 286 adicionales para teléfonos digitales Avaya DS 41 compatibles.



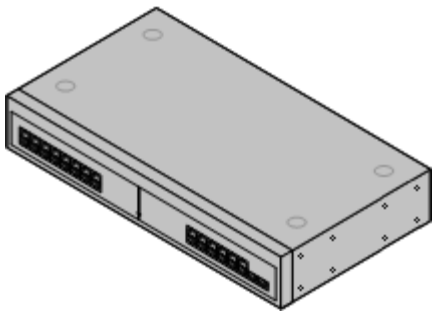
- **Módulos de Estación Digital A IP500** 247
  Según la variante, ofrecen puertos RJ21 para conectar 16 o 30 teléfonos digitales Avaya BST 41 adicionales. Compatibilidad solo en IP500 V2.



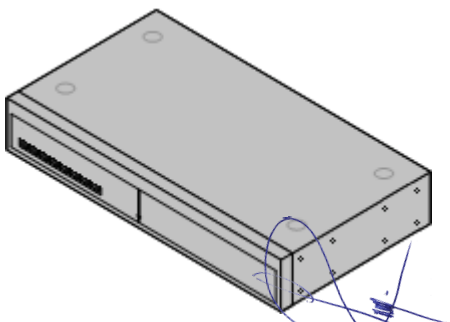
- **Módulos de estación digital B/B2 IP500** 250
  Según la variante, ofrecen 16 o 30 puertos RJ45 adicionales. Estos se pueden usar como puertos DS 286 para teléfonos digitales Avaya DS compatibles 41 o bien puertos BST 285 para teléfonos digitales Avaya BST compatibles 41. Sin embargo, el módulo sólo admite un tipo de puerto en cualquier momento. Para IP Office versión 10.1, los módulos DS16B/DS30B han sido reemplazados por los modelos DS16B2/DS30B2.



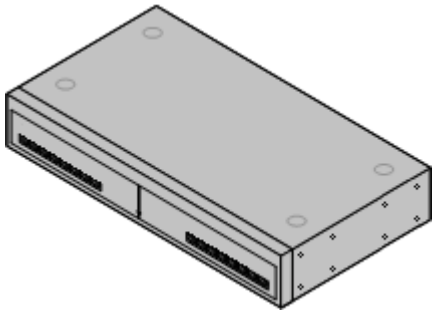
- **Módulos teléfono IP500** 252
  Según la variante, ofrecen 16 o 30 puertos TELÉFONO 291 para conectar teléfonos analógicos.



- **Módulo BRI So8 IP500** 243
  Proporciona ocho puertos BRI-So 283 para conectar dispositivos ISDN. Esta unidad no está diseñada para admitir troncales BRI.



- **Módulo de troncales analógicas IP500** 240
  Proporciona 16 puertos ANALÓGICOS 282 adicionales para conectar troncales analógicas. Es compatible con troncales de arranque por bucle y de arranque por tierra.
  - El uso con troncales de inicio por tierra requieren que el módulo de troncales y la unidad de control de IP Office estén conectados a tierra.
- En IP Office Basic Edition - modo PARTNER®, IP Office Basic Edition - modo Norstar y IP Office Basic Editions, solo se admite un módulo de troncales analógicas.



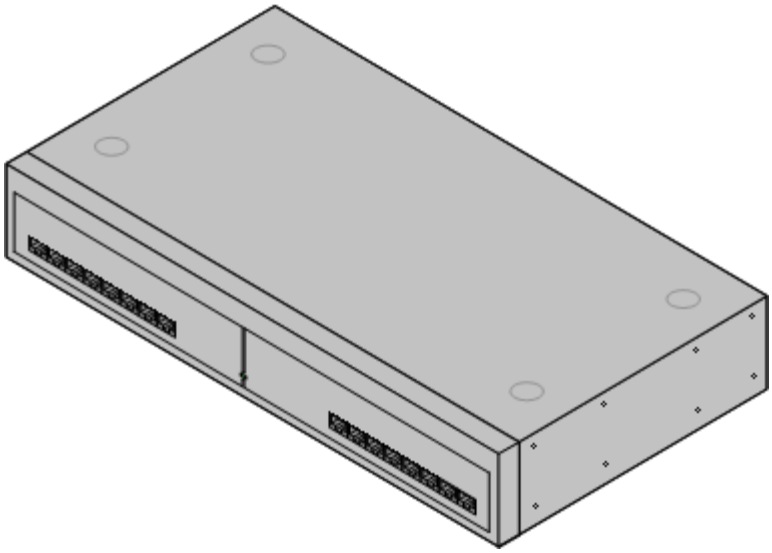
13.5.1 Troncal analógica de 16 líneas

El módulo de Troncales analógicas IP500 se utiliza asimismo para agregar 16 troncales análogas adicionales a un sistema IP Office. El módulo es compatible con troncales de arranque por bucle y, con una conexión a tierra adecuada, con troncales de arranque por tierra.

- En IP Office Basic Edition - modo PARTNER®, IP Office Basic Edition - modo Norstar y IP Office Basic Editions, solo se admite un módulo de troncales analógicas.

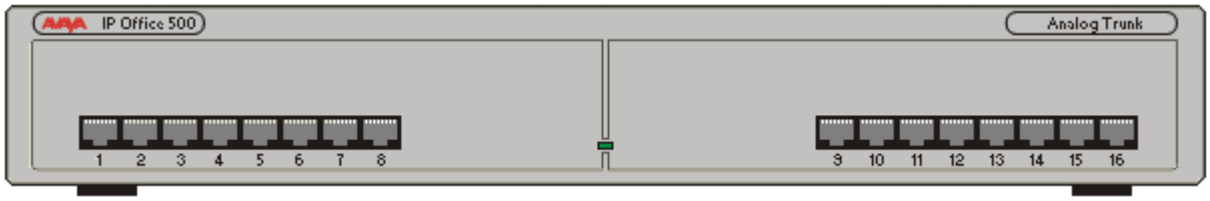
  - ⚠ **ADVERTENCIA**
    En todas las instalaciones de IP Office, cualquier módulo o unidad de control que utilice conexiones de troncales analógicas debe estar conectado a una puesta a tierra funcional 38.

  - ⚠ **PRECAUCIÓN**
    En áreas con alto riesgo de descargas eléctricas, todos los módulos que utilicen conexiones de troncales analógicas deben estar conectadas a una puesta a tierra de protección 38 y a equipos de protección contra picos 39.



Función	Detalles
Localidades	Este módulo está disponible solamente en localidades de América del Norte.
Nivel de software	Nivel mínimo de software nuclear IP Office 1.0 Archivo Bin = naatm16.bin.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	El módulo está equipado con una unidad externa de suministro de energía de 2 pines y 40W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe del módulo DC I/P. Se requiere un cable de energía IEC60320 C7 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en la pared o sobre un soporte mediante IPO IP500 RACK MNTG KIT V3 26.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71mm/2.8"/2U.
Peso	Sin caja: 2.9Kg/6.6lbs. En caja: 4.2Kg/9.4lbs.

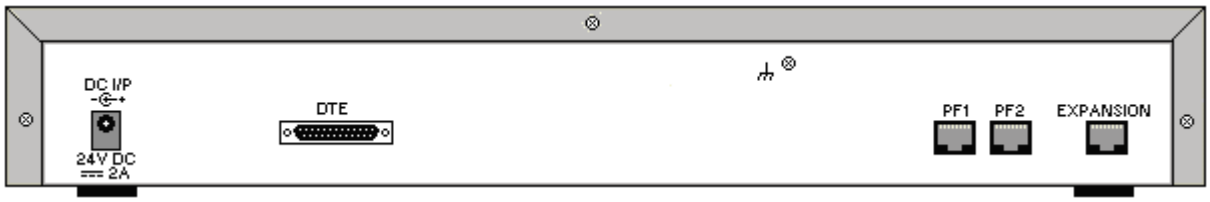
Parte delantera del módulo



Luces LED puerto	Ninguno

Indicador LED en el centro del módulo	El indicador LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **Rojo parpadeando** = Módulo iniciándose/Cargando firmware. • **Luz roja encendida** = Error. • **Luz verde encendida** = El módulo está bien.

Parte trasera del módulo



Puertos	Descripción
ANALÓGICO 282	Enchufe RJ45. Se utiliza para conectar troncales analógicas. Se pueden configurar los puertos para troncales de arranque por bucle o por tierra, mediante la configuración de IP Office. En caso de ocurrir un corte de energía, los puertos Analógico 1 y 2 se conectan directamente a los puertos de extensión analógica PF1 y PF2 respectivamente. De estar presentes, los teléfonos conectados deben etiquetarse claramente como dispositivos para casos de corte de energía. Esto es sólo compatible con las troncales analógicas de arranque por bucle.
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía Avaya de 40 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C7 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
DTE 293	Enchufe para conector tipo D de 25 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
PF 290	Enchufe RJ45. Puertos de extensiones analógicas para cortes de energía. Consulte la sección Analógico arriba.
	Punto de la puesta a tierra. Se utiliza para la conexión con puesta a tierra funcional 38 de ser necesario. En módulos anteriores, donde no está presente este tornillo, debe utilizarse en su lugar el tornillo superior central de la cubierta. • IMPORTANTE En todas las instalaciones de IP Office, cualquier módulo o unidad de control que utilice conexiones de troncales analógicas debe estar conectado a una puesta a tierra funcional 38. • ⚠ PRECAUCIÓN En áreas con alto riesgo de descargas eléctricas, todos los módulos o unidades de control que utilicen conexiones de troncales analógicas deben estar conectadas a una puesta a tierra de protección 38 y a equipos de protección contra picos 39.

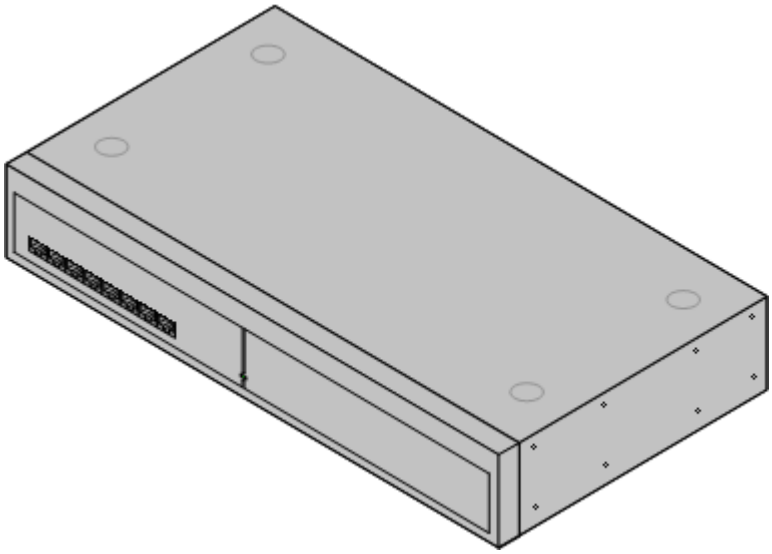
Códigos de piezas y equipos relacionados

Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Artículo	Variante	País	Código SAP
IPO IP500 EXP MOD ANLG TRNK 16	**América**	América	700449473
IPO IP500 EXP MOD ANLG TRNK 16 TAA	- Trade Agreements Act 310 variante que cumple con los requisitos.	América	700501511
Cable de energía IEC60320 C7	**NEMA1-15**	América	700213390
Kit de montaje	**IPO IP500 WALL MNTG KIT V3**	Todos	700503160

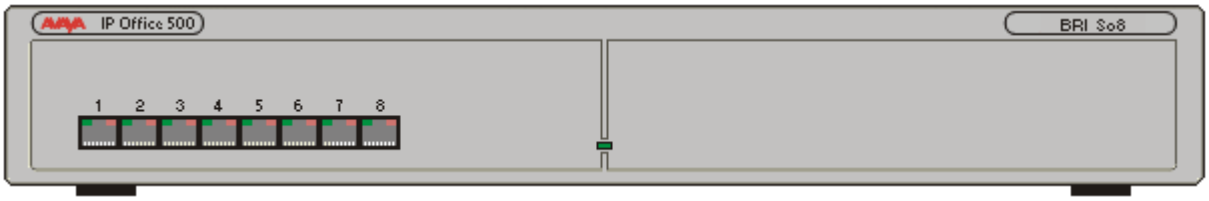
13.5.2 BRI So8

El módulo So8 se utiliza para agregar puertos de interfaz ETSI BRI S0 a los sistemas IP Office. Estos puertos pueden utilizarse para conectar dispositivos ISDN.



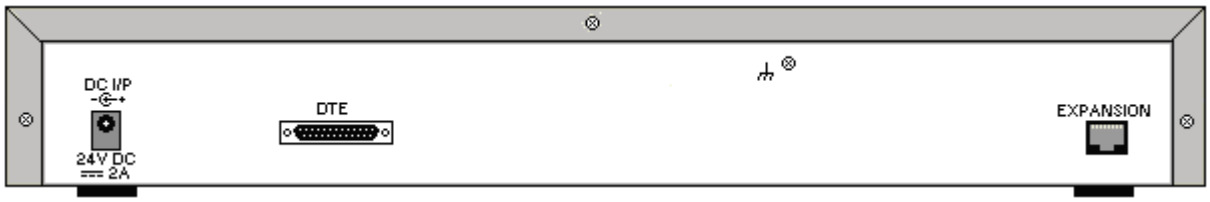
Función	Detalles
Localidades	Compatibles en todas las localidades de IP Office 45.
Nivel de software	Nivel mínimo de software nuclear IP Office 1.0 Archivo Bin = nas0-16.bin.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	La unidad está equipada con una unidad externa de suministro de externo con puesta en tierra de 3 pines y 60W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe DC I/P de la unidad. Existe el cable específico a la localidad IEC60320 C13 33 para la PSU externa, pero no viene incluido con la unidad.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en la pared o sobre un soporte mediante IPO IP500 RACK MNTG KIT V3 26.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71mm/2.8"/2U.
Peso	Sin caja: 2.8Kg/6.3lbs. En caja: 4.1Kg/9.2lbs.

Parte delantera del módulo



Luces LED puerto	• **Verde encendida** = Conectado. • **Destello verde** = Actividad.
Indicador LED en el centro del módulo	El indicador LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **Rojo parpadeando** = Módulo iniciándose/Cargando firmware. • **Luz roja encendida** = Error. • **Luz verde encendida** = El módulo está bien.

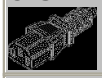
Parte trasera del módulo



Puertos	Descripción
BRI 283	Enchufe RJ45. Se utiliza para conectar dispositivos de terminal ISDN. Nota: Estos puertos aparecen como líneas en la configuración de IP Office. Sin embargo, no pueden utilizarse la conexión con líneas BRI externas.
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía Avaya de 60 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
DTE 293	Enchufe para conector tipo D de 25 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
⏚	Punto de la puesta a tierra funcional. Se utiliza para la conexión con la puesta a tierra de protección o funcional 38 de ser necesario. En módulos anteriores, donde no está presente este tornillo, debe utilizarse en su lugar el tornillo superior central de la cubierta.

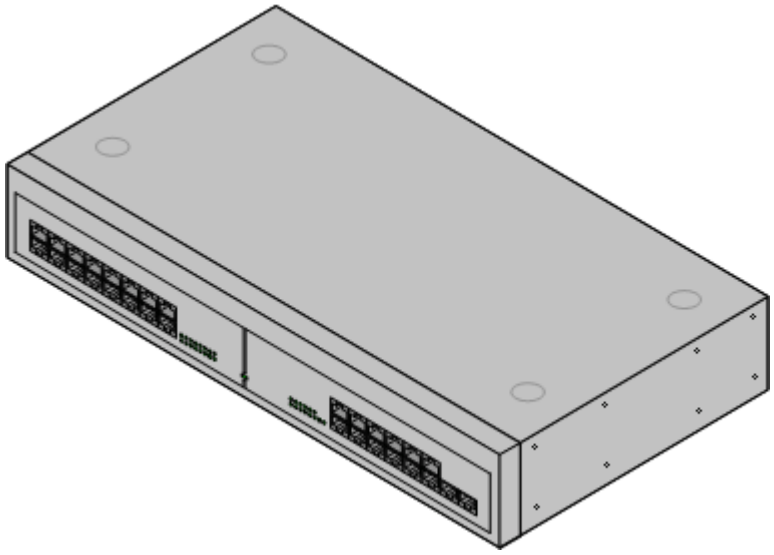
Códigos de piezas y equipos relacionados

Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Artículo	Variante	País	Código SAP
IPO 500 BRI So8		Todos	700449515
Cable de energía IEC60320 C13 	**CEE7/7**	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	América	700289770
Kit de montaje	**IPO IP500 WALL MNTG KIT V3**	Todos	700503160

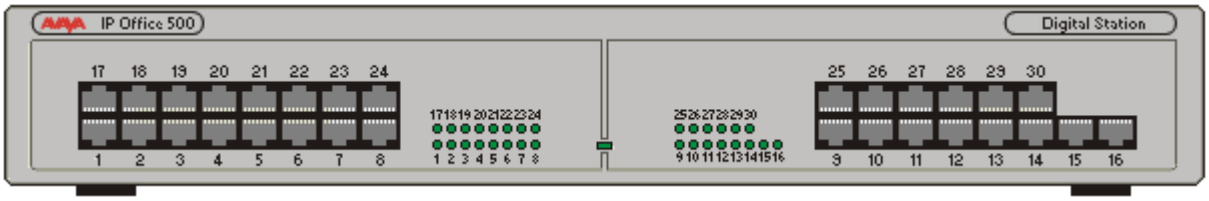
13.5.3 DS16/30

Los módulos IPO 500 Digital Station permiten agregar puertos DS 286 adicionales a un sistema IP Office para admitir teléfonos digitales Avaya DS 41. El módulo está disponible con variantes para 16 y 30 puertos, conocidas respectivamente como IP500 DS16 e IP500 DS30. Estos módulos también se conocen como módulos IP500 DS V2. Estos módulos han sido reemplazados por IP500 DS16B/30B 250.



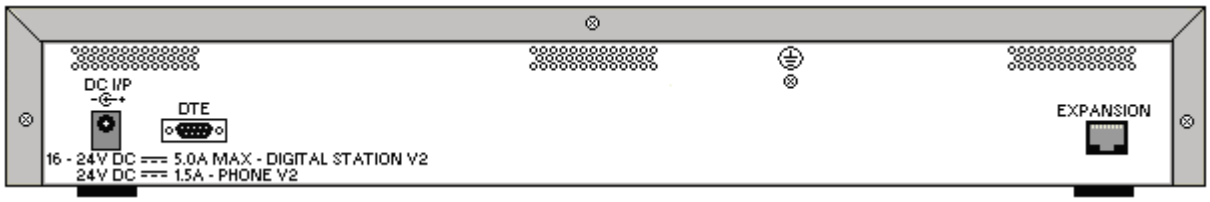
Función	Detalles
Localidades	Compatibles en todas las localidades de IP Office 45.
Nivel de software	Nivel mínimo de software nuclear IP Office Versión 2.1(31) Archivo Bin = nadcpV2.bin.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	El módulo está equipado con un módulo de suministro de energía externo con puesta en tierra de 3 pines y 60W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe del módulo DC I/P. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en la pared o sobre un soporte mediante IPO IP500 RACK MNTG KIT V3 261.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8".
Peso	Sin caja: 3.5Kg/7.8lbs. En caja: 4.8Kg/10.8lbs. (basada en DS30)

Parte delantera del módulo



Luces LED puerto	• **Destello verde** = Teléfono detectado. • **Verde encendida** = Teléfono activo.
Indicador LED en el centro del módulo	El indicador LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **Rojo parpadeando** = Módulo iniciándose/Cargando firmware. • **Luz roja encendida** = Error. • **Luz verde encendida** = El módulo está bien.

Parte trasera del módulo



Puerto	Descripción
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía aterrizada de 3 pines y 60 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
DS 286	Enchufe RJ45. Puerto de Estación digital. Se utiliza para la conexión con teléfonos DS compatibles con IP Office 41. Cuando se conecta a una extensión fuera del edificio 39, esta conexión debe efectuarse con dispositivos de protección IROB adicionales a la protección principal del edificio. El módulo debe asimismo conectarse a una conexión de tierra de protección.
DTE 293	Enchufe para conector tipo D de 9 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
⏚	Punto de la puesta a tierra de protección. Se requiere el uso de la conexión a tierra para protección en todas las instalaciones, consulte la sección Puesta a tierra 90. Cuando el módulo se conecta a extensiones analógicas en otro edificio, se requiere emplear una caja protectora IP Office Phone Barrier Box V2 (101V) en ambos extremos; consulte la sección Protección contra rayos/Conexiones fuera del edificio 39.

Códigos de piezas y equipos relacionados

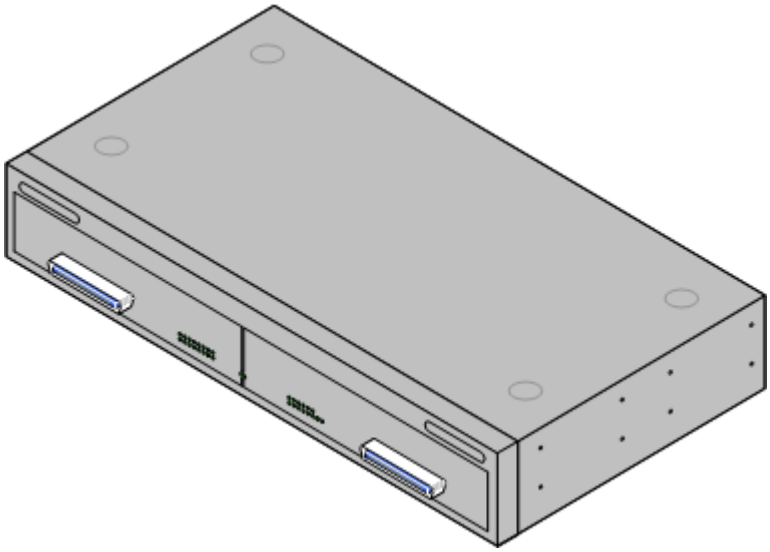
Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Artículo	Variante	País	Código SAP
IPO IP500 EXP MOD DGTL STA 16	**16 puertos**	Todos	700449499
IPO IP500 EXP MOD DGTL STA 16 TAA	- Trade Agreements Act 310 variante que cumple con los requisitos.		–
IPO IP500 EXP MOD DGTL STA 30	**30 puertos**		700426216
Cable de energía IEC60320 C13	**CEE7/7**	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	América	700289770
Kit de montaje	**IPO IP500 WALL MNTG KIT V3**	Todos	700503160

13.5.4 DS16A/30A

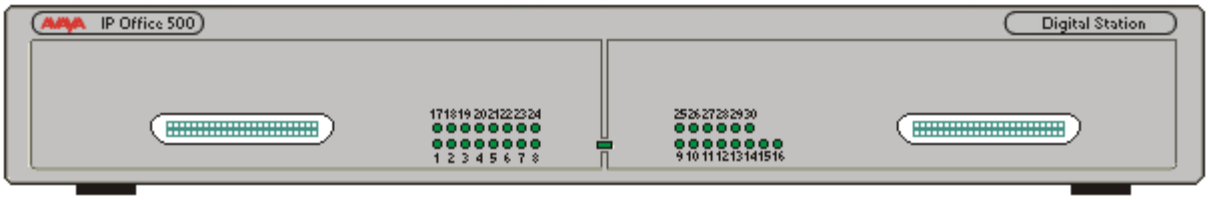
Estos módulos se pueden usar para agregar puertos BST 285 en los teléfonos digitales compatibles Avaya BST 41. El módulo está disponible con variantes para 16 y 30 puertos, conocidas respectivamente como IP500 DS16A e IP500 DS30A.

Los módulos usan conectores RJ21; 1 en la versión de 16 puertos, 2 en la de 30 puertos. En el caso de conexiones BST que usan el puerto RJ45, use los módulos IP500 DS16B/30B 250.



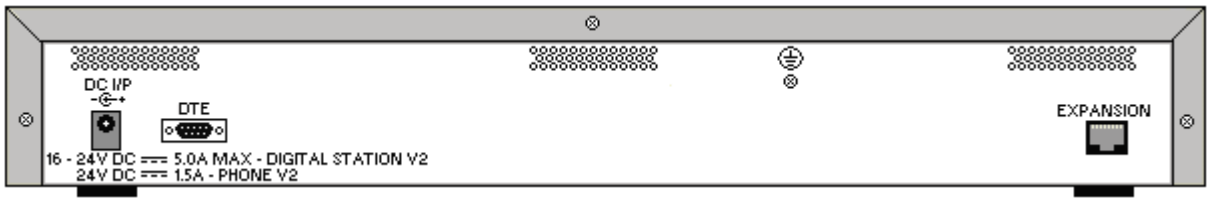
Función	Detalles
Localidades	Compatibles en todas las localidades de IP Office 45.
Nivel de software	Como mínimo IP Office versión 7.0 (sólo BST). Archivo Bin = nadcpaV1.bin.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	El módulo está equipado con un módulo de suministro de energía externo con puesta en tierra de 3 pines y 60W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe del módulo DC I/P. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en la pared o sobre un soporte mediante IPO IP500 RACK MNTG KIT V3 261.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8".
Peso	Sin caja: 3.5Kg/7.8lbs. En caja: 4.8Kg/10.8lbs. (Basado en DS30A RJ21)

Parte delantera del módulo



Luces LED puerto	• **Verde encendida** = Teléfono detectado.
Indicador LED en el centro del módulo	El indicador LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **Rojo parpadeando** = Módulo iniciándose/Cargando firmware. • **Luz roja encendida** = Error. • **Luz verde encendida** = El módulo está bien. • **Verde parpadeando** = Módulo iniciándose/Cargando firmware (solo el módulo IP500 DS16A/30A).

Parte trasera del módulo



Puertos	Descripción
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía aterrizada de 3 pines y 60 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
RJ21 285	En el caso de la versión 7.0 de IP Office, los módulos son compatibles solo con teléfonos que requieren puertos BST 285.
DTE 293	Enchufe para conector tipo D de 9 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
⏚	Punto de la puesta a tierra de protección. Se requiere el uso de la conexión a tierra para protección en todas las instalaciones, consulte la sección Puesta a tierra 90. Cuando el módulo se conecta a extensiones analógicas en otro edificio, se requiere emplear una caja protectora IP Office Phone Barrier Box V2 (101V) en ambos extremos; consulte la sección Protección contra rayos/Conexiones fuera del edificio 39.

Códigos de piezas y equipos relacionados

Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Artículo	Variante	País	Código SAP
IPO 500 Digital Station 16A RJ21 UNIT ASSY	**RJ21**	Todos	700500699
IPO 500 Digital Station 30A RJ21 UNIT ASSY	**RJ21**		700500698
Cable de energía IEC60320 C13	**CEE7/7**	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	Norteamérica	700289770
Kit de montaje	**IPO IP500 WALL MNTG KIT V3**	Todos	700503160

Pinout del cable RJ21

Se utiliza el siguiente pinout para los puertos RJ21.

Primer conector RJ21

Puerto		Pin	Cable
1	Positivo	26	Blanco/Azul
	Negativo	1	Azul/Blanco
2	Positivo	27	Blanco/Anaranjado
	Negativo	2	Anaranjado/Blanco
3	Positivo	28	Blanco/Verde
	Negativo	3	Verde/Blanco
4	Positivo	29	Blanco/Café
	Negativo	4	Café/Blanco
5	Positivo	30	Blanco/Gris
	Negativo	5	Gris/Blanco
6	Positivo	31	Rojo/Azul
	Negativo	6	Azul/Rojo
7	Positivo	32	Rojo/Anaranjado
	Negativo	7	Anaranjado/Rojo
8	Positivo	33	Rojo/Verde
	Negativo	8	Verde/Rojo
9	Positivo	34	Rojo/Café
	Negativo	9	Café/Rojo
10	Positivo	35	Rojo/Gris
	Negativo	10	Gris/Rojo
11	Positivo	36	Negro/Azul
	Negativo	11	Azul/Negro
12	Positivo	37	Negro/Anaranjado
	Negativo	12	Anaranjado/Negro
13	Positivo	38	Negro/Verde
	Negativo	13	Verde/Negro
14	Positivo	39	Negro/Café
	Negativo	14	Café/Negro
15	Positivo	40	Negro/Gris
	Negativo	15	Gris/Negro
16	Positivo	41	Amarillo/Azul
	Negativo	16	Azul/Amarillo
No utilizado		42	Amarillo/Anaranjado
		17	Anaranjado/Amarillo
		43	Violeta/Gris
		08	Gris/Violeta

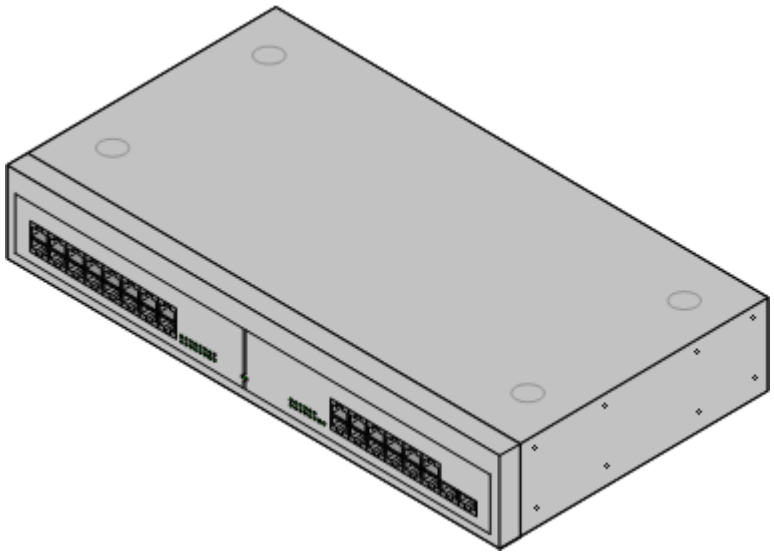
Segundo conector RJ21

Puerto		Pin	Cable
17	Positivo	26	Blanco/Azul
	Negativo	1	Azul/Blanco
18	Positivo	27	Blanco/Anaranjado
	Negativo	2	Anaranjado/Blanco
19	Positivo	28	Blanco/Verde
	Negativo	3	Verde/Blanco
20	Positivo	29	Blanco/Café
	Negativo	4	Café/Blanco
21	Positivo	30	Blanco/Gris
	Negativo	5	Gris/Blanco
22	Positivo	31	Rojo/Azul
	Negativo	6	Azul/Rojo
23	Positivo	32	Rojo/Anaranjado
	Negativo	7	Anaranjado/Rojo
24	Positivo	33	Rojo/Verde
	Negativo	8	Verde/Rojo
25	Positivo	34	Rojo/Café
	Negativo	9	Café/Rojo
26	Positivo	35	Rojo/Gris
	Negativo	10	Gris/Rojo
27	Positivo	36	Negro/Azul
	Negativo	11	Azul/Negro
28	Positivo	37	Negro/Anaranjado
	Negativo	12	Anaranjado/Negro
29	Positivo	38	Negro/Verde
	Negativo	13	Verde/Negro
30	Positivo	39	Negro/Café
	Negativo	14	Café/Negro
No utilizado		40	Negro/Gris
		15	Gris/Negro
		41	Amarillo/Azul
		16	Azul/Amarillo
		42	Amarillo/Anaranjado
		17	Anaranjado/Amarillo
		43	Violeta/Gris
		08	Gris/Violeta

13.5.5 DS16B/30B, DS16B2/30B2

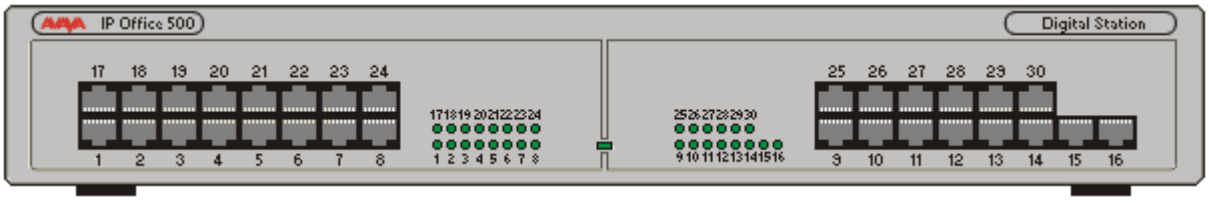
Este tipo de módulo se puede usar para agregar puertos RJ45 adicionales para teléfonos digitales. A través de la configuración del sistema, cada módulo se configura en modo DS 286 para admitir teléfonos digitales Avaya DS 41 o bien puertos modo BST 285 para los teléfonos digitales Avaya BST 41 (puertos DS sólo en las unidades de control IP500). Consulte la sección Selección de modo de puerto DS16B2/30B2 109.

Los módulos están disponibles con variantes para 16 y 30 puertos, conocidas respectivamente como IP500 DS16B e IP500 DS30B. DS16B y DS30B han sido reemplazados por los modelos DS16B2 y DS30B2, que ofrecen la misma funcionalidad.



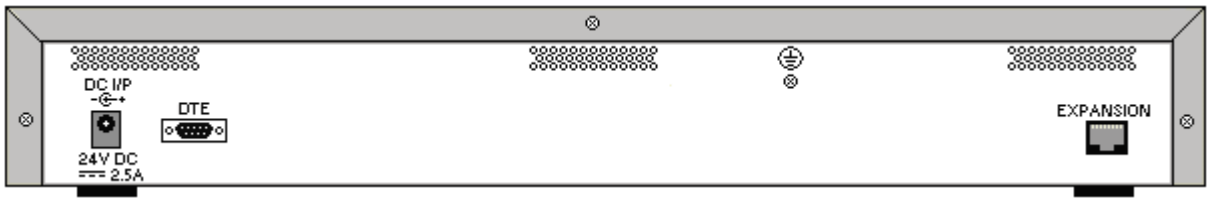
Función	Detalles
Localidades	Compatibles en todas las localidades de IP Office 45.
Nivel de software	• **DS16B/DS30B:**IP Office versión 9.0. IP500 (solo DS) e IP500 V2 (DS o TCM). Para IP Office versión 8.1 (Service Pack 9 y posteriores), estos módulos solamente admiten puertos DS. • **DS16B2/DS30B2:** IP Office versión 10.1.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	El módulo está equipado con un módulo de suministro de energía externo con puesta en tierra de 3 pines y 60W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe del módulo DC I/P. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en la pared o sobre un soporte mediante IPO IP500 RACK MNTG KIT V3 26.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8".
Peso	Sin caja: 3.5Kg/7.8lbs. En caja: 4.8Kg/10.8lbs. (basada en DS30)

Parte delantera del módulo



Luces LED puerto	• **Destello verde** = Teléfono detectado. • **Verde encendida** = Teléfono activo.
Indicador LED en el centro del módulo	El indicador LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **Rojo parpadeando** = Módulo iniciándose/Cargando firmware. • **Luz roja encendida** = Error. • **Luz verde encendida** = El módulo está bien.

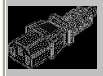
Parte trasera del módulo



Puerto	Descripción
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía aterrizada de 3 pines y 60 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
DS 286	Enchufe RJ45. Puerto de Estación digital. Se utiliza para la conexión con teléfonos DS compatibles con IP Office 41. Cuando se conecta a una extensión fuera del edificio 39, esta conexión debe efectuarse con dispositivos de protección IROB adicionales a la protección principal del edificio. El módulo debe asimismo conectarse a una conexión de tierra de protección.
DTE 293	Enchufe para conector tipo D de 9 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
⏚	Punto de la puesta a tierra de protección. Se requiere el uso de la conexión a tierra para protección en todas las instalaciones, consulte la sección Puesta a tierra 90. Cuando el módulo se conecta a extensiones analógicas en otro edificio, se requiere emplear una caja protectora IP Office Phone Barrier Box V2 (101V) en ambos extremos; consulte la sección Protección contra rayos/Conexiones fuera del edificio 39.

Códigos de piezas y equipos relacionados

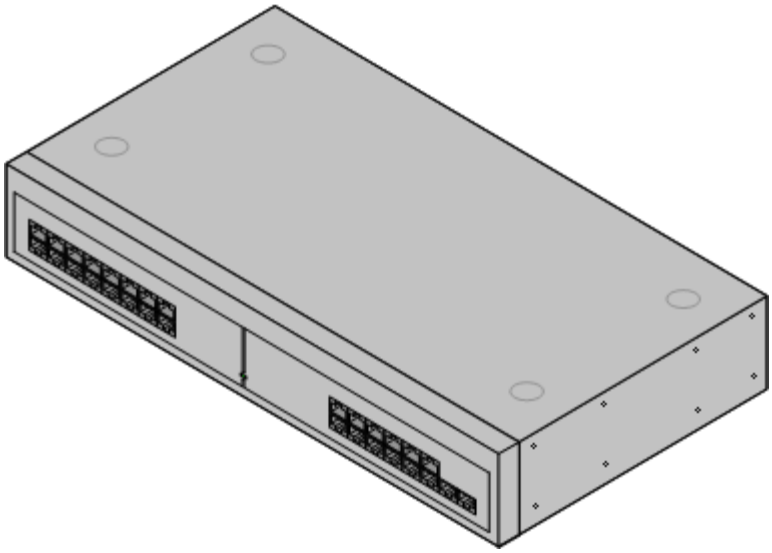
Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Artículo	Variante	País	Código SAP
IPO IP500 MÓD. EXP. DS16B DGTL ST	**16 puertos**	Todos	700501585
IPO IP500 MÓD. EXP. DS30B DGTL ST	**30 puertos**	Todos	700501586
IPO IP500 MÓD. EXP. DS16B2 DGTL ST	**16 puertos**	Todos	700511093
IPO IP500 MOD. EXP. DS30B2 DGTL ST	**30 puertos**	Todos	700511094
Cable de energía IEC60320 C13	**CEE7/7**	Europa	700289762
	**BS1363**	Reino Unido	700289747
	NEMA5-15P	América	700289770
Kit de montaje	**IPO IP500 WALL MNTG KIT V3**	Todos	700503160

13.5.6 Teléfono 16/30

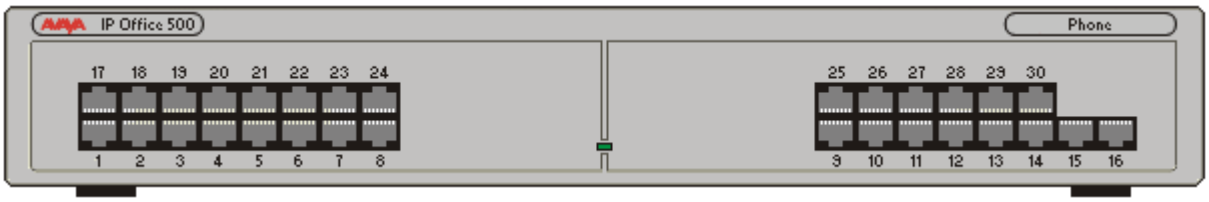
Los módulos Phone IP500 pueden equiparse para agregar puertos adicionales TELÉFONO a los sistemas IP Office.

El módulo está disponible con variantes para 16 y 30 puertos, conocidas respectivamente como IP500 Phone 16 y IP500 Phone 30.



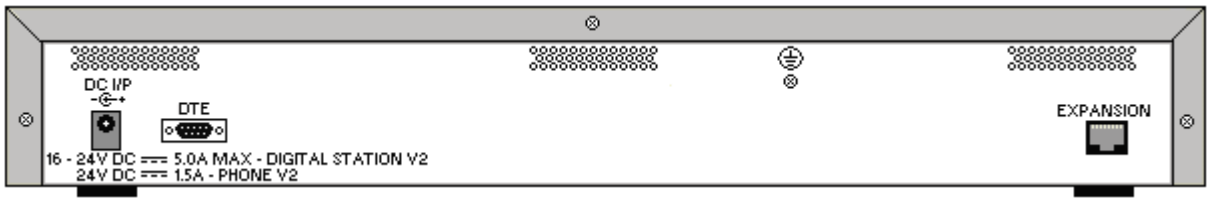
Función	Detalles
Localidades	Compatibles en todas las localidades de IP Office 45.
Nivel de software	Nivel mínimo de software nuclear IP Office Versión 2.1(36) .Archivo Bin = dvpots.bin.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	El módulo está equipado con una unidad externa de suministro de energía aterrizada de 3 pins y 60W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe del módulo DC I/P. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en la pared o sobre un soporte mediante IPO IP500 RACK MNTG KIT V3 261.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71 mm/2,8".
Peso	Sin caja: 3.1Kg/6.94lbs. En caja: 4.4Kg/9.7lbs. (Con base en Phone 30 V2).

Parte delantera del módulo



Indicador LED en el centro del módulo	El indicador LED central en todos los módulos de expansión externos se usa para indicar el estado general del módulo de la siguiente manera: • **Rojo parpadeando** = Módulo iniciándose/Cargando firmware. • **Luz roja encendida** = Error. • **Luz verde encendida** = El módulo está bien. • **Verde parpadeando** = Módulo iniciándose/Cargando firmware (solo el módulo IP500 DS16A/30A).

Parte trasera del módulo



Puertos	Descripción
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía aterrizada de 3 pines y 60 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
DTE 293	Enchufe para conector tipo D de 9 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
TELÉFONO 291	Enchufe RJ45. Se utiliza para conectar teléfonos analógicas. Se utiliza para conectar teléfonos analógicos de dos hilos. Para conectar con teléfonos analógicos de cuatro hilos, la conexión debe efectuarse con un enchufe maestro y capacitores de timbre. Cuando se conecta a una extensión fuera del edificio 39, la conexión debe equiparse con Cajas de protección IP Office 190 adicionales a la protección principal del edificio. El módulo debe asimismo conectarse a una conexión de tierra de protección.
⏚	Punto de la puesta a tierra de protección. Se requiere el uso de la conexión a tierra para protección en todas las instalaciones, consulte la sección Puesta a tierra 38. Cuando el módulo se conecta a extensiones analógicas en otro edificio, se requiere emplear una caja protectora IP Office Phone Barrier Box V2 (101V) en ambos extremos; consulte la sección Protección contra rayos/Conexiones fuera del edificio 39.

Códigos de piezas y equipos relacionados

Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

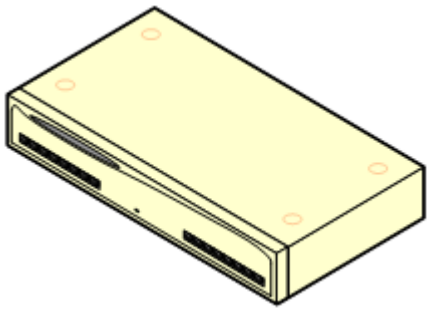
Artículo	Variante	País	Código SAP
IPO IP500 EXP MOD PHONE 16	**16 puertos**	Todos	700449507
IPO IP500 EXP MOD PHONE 30	**30 puertos**	Todos	700426224
Cable de energía IEC60320 C13	**CEE7/7**	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	América	700289770
Kit de montaje	**IPO IP500 WALL MNTG KIT V3**	Todos	700503160
IPO PHONE BARRIER BOX (101V) RHS		Todos	700385495

13.6 Módulos de expansión IP400

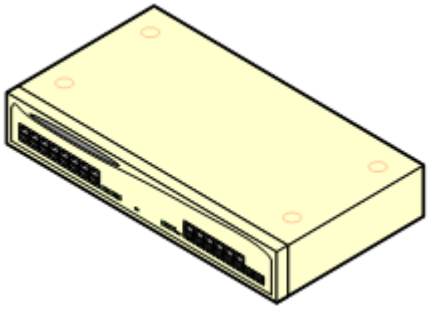
Los siguientes módulos de expansión externos IP400 son compatibles con la versión 10.1 de IP Office y pueden utilizarse con unidades de control IP500 V2. Cada módulo utiliza una unidad de suministro de energía 33 externa, incluida con el módulo. El cable de energía 34 específico de la localidad para el PSU debe solicitarse por separado.

Si se van a instalar en bastidor, estas unidades deben instalarse con el kit de montaje en bastidor IP400. Si se van a instalar en bastidor, estas unidades deben instalarse con el kit de montaje en bastidor IPO IP500. Estas unidades no pueden montarse en pared.

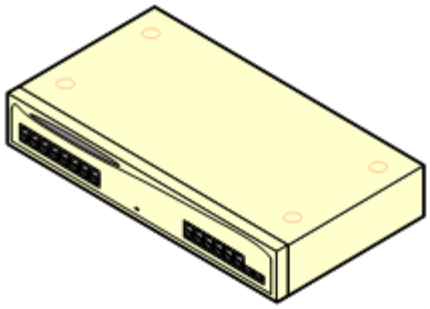
- **Módulo de troncales analógicas IP400 (ATM16)** 255
  Proporciona 16 puertos ANALÓGICOS 282 adicionales para conectar troncales analógicas. Es compatible con troncales de arranque por bucle y de arranque por tierra.
  - Disponible en múltiples variantes para distintas localidades.
  - El uso con troncales de inicio por tierra requieren que el módulo de troncales y la unidad de control de IP Office estén conectados a tierra.



- **Módulo de estación digital V2 IP400** 257
  Dependiendo de la variante, proporciona entre 16 y 30 puertos DS 286 adicionales para teléfonos digitales Avaya compatibles. 41. Esta versión reemplaza el módulo de estación digital anterior.



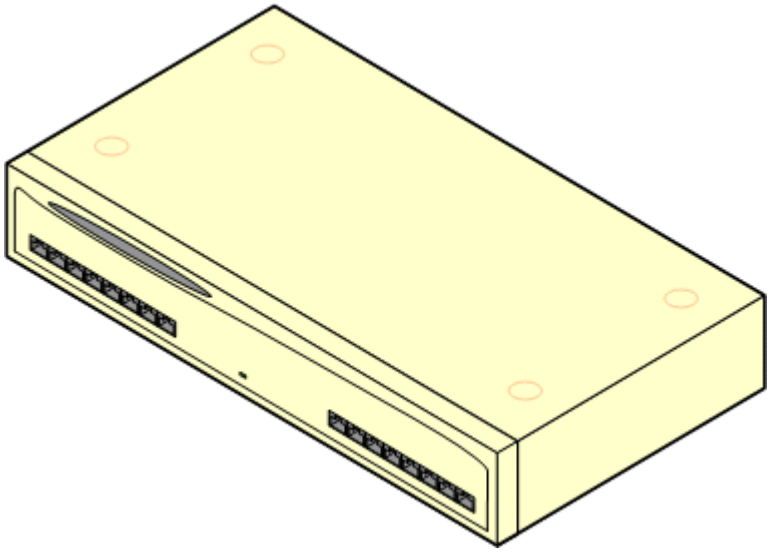
- **Módulo Phone V2 IP400** 259
  Dependiendo de la variante, proporciona entre 8, 16 y 30 puertos TELÉFONO 291 adicionales para teléfonos analógicos. Esta versión reemplaza el módulo Phone anterior. En IP Office 3.1, el módulo Phone V2 admite un mayor rango de opciones de indicación de mensaje en espera (MWI) que los módulos Phone V1.



13.6.1 Troncal analógica de 16 líneas

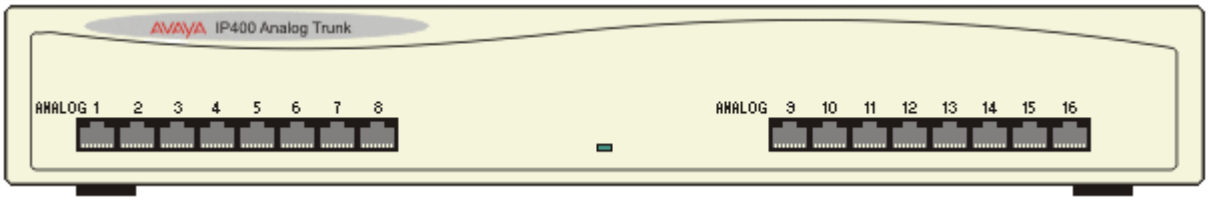
El módulo de Troncales analógicas IP400 (también conocido como ATM16) se utiliza para agregar 16 troncales análogas adicionales a un sistema IP Office. El módulo es compatible con troncales de arranque por bucle y, con una conexión a tierra adecuada, con troncales de arranque por tierra.

- **ADVERTENCIA**
  En todas las instalaciones de IP Office, cualquier módulo o unidad de control que utilice conexiones de troncales analógicas debe estar conectado a una puesta a tierra funcional 38.
- **PRECAUCIÓN**
  Dentro de la República de Sudáfrica y en áreas con alto riesgo de descargas eléctricas, todos los módulos o unidades de control que utilicen conexiones de troncales analógicas deben estar conectadas a una puesta a tierra de protección 38 y a un equipo de protección contra picos 39.

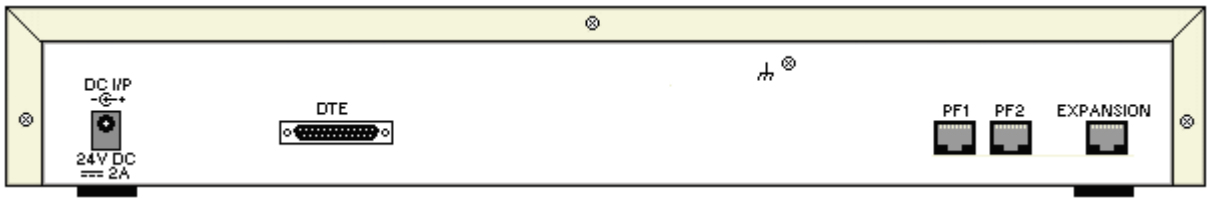


Función	Detalles
Localidades	Están disponibles variantes específicas para distintas localidades de IP Office locales, vea abajo.
Nivel de software	Nivel mínimo de software nuclear IP Office 1.0 Archivo Bin = naatm16.bin.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	El módulo está equipado con una unidad externa de suministro de energía de 2 pines y 40W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe del módulo DC I/P. Se requiere un cable de energía IEC60320 C7 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en bastidor sobre un sistema de bastidor de 19" con ayuda del Kit opcional de montaje en bastidor IP400.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71mm/2.8"/2U.
Peso	Sin caja: 2.9Kg/6.6lbs. En caja: 4.2Kg/9.4lbs.

Parte delantera del módulo



Parte trasera del módulo



Puertos	Descripción
ANALÓGICO 282	Enchufe RJ45. Se utiliza para conectar troncales analógicas. Se pueden configurar los puertos para troncales de arranque por bucle o por tierra, mediante la configuración de IP Office. En caso de ocurrir un corte de energía, los puertos Analógico 1 y 2 se conectan directamente a los puertos de extensión analógica PF1 y PF2 respectivamente. De estar presentes, los teléfonos conectados deben etiquetarse claramente como dispositivos para casos de corte de energía. Esto es sólo compatible con las troncales analógicas de arranque por bucle.
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía Avaya de 40 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C7 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
DTE 293	Enchufe para conector tipo D de 25 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
PF 290	Enchufe RJ45. Puertos de extensiones analógicas para cortes de energía. Consulte la sección Analógico arriba.
	Punto de la puesta a tierra. Se utiliza para la conexión con puesta a tierra funcional 38 de ser necesario. En módulos anteriores, donde no está presente este tornillo, debe utilizarse en su lugar el tornillo superior central de la cubierta. • IMPORTANTE En todas las instalaciones de IP Office, cualquier módulo o unidad de control que utilice conexiones de troncales analógicas debe estar conectado a una puesta a tierra funcional 38. • ⚠ PRECAUCIÓN Dentro de la República de Sudáfrica y en áreas con alto riesgo de descargas eléctricas, todos los módulos o unidades de control que utilicen conexiones de troncales analógicas deben estar conectadas a una puesta a tierra de protección 38 y a un equipos de protección contra picos 39.

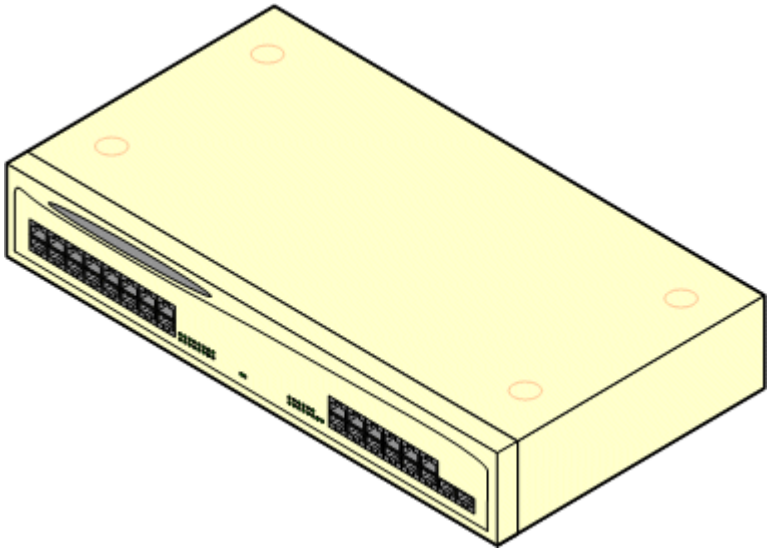
Códigos de piezas y equipos relacionados

Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Artículo	Variante	País	Código SAP
Troncal analógica de 16 líneas IP400	América	América	700211360
	Europa	Europa	700241680
	Nueva Zelanda	Nueva Zelanda	700241698
Cable de energía IEC60320 C7	CEE7/16	Europa	700213382
	BS1363	Reino Unido	700213374
	NEMA1-15	América	700213390
	Corea	Corea	700254519
Kit de montaje en bastidor IP400		Todos	700210800

13.6.2 Estación digital V2

La Estación Digital IP400 V2 (también conocida como DS V2) se utiliza para agregar puertos DS adicionales a un sistema IP Office. La DS V2 está disponible con variantes para 16 y 30 puertos, conocidas respectivamente como DS16 V2 y DS30 V2.

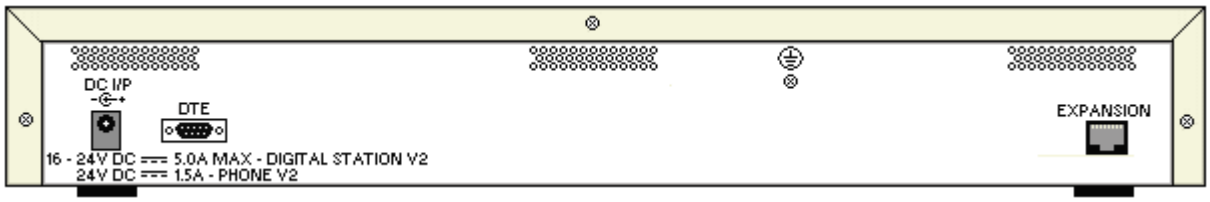


La DS V2 reemplaza a la Estación Digital IP400 original, conocida actualmente como DS V1. La versión del módulo está indicada en las etiquetas ubicadas en la base y en la parte posterior del módulo.

Función	Detalles
Localidades	Compatibles en todas las localidades de IP Office 45.
Nivel de software	Nivel mínimo de software nuclear IP Office Versión 2.1(31) Archivo Bin = nadcpV2.bin.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	El módulo está equipado con un módulo de suministro de energía externo con puesta en tierra de 3 pines y 60W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe del módulo DC I/P. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en bastidor sobre un sistema de bastidor de 19" con ayuda del Kit opcional de montaje en bastidor IP400.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71mm/2.8"/2U.
Peso	Sin caja: 3.5Kg/7.8lbs. En caja: 4.8Kg/10.8lbs. (Con base en DS30 V2)

Parte delantera del módulo

Parte trasera del módulo



Puertos	Descripción
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía aterrizada de 3 pines y 60 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
DS 286	Enchufe RJ45. Puerto de Estación digital. Se utiliza para la conexión con teléfonos DS compatibles con IP Office 41. Cuando se conecta a una extensión fuera del edificio 39, esta conexión debe efectuarse con dispositivos de protección IROB adicionales a la protección principal del edificio. El módulo debe asimismo conectarse a una conexión de tierra de protección.
DTE 293	Enchufe para conector tipo D de 9 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
⏚	Punto de la puesta a tierra de protección. Se requiere el uso de la conexión a tierra para protección en todas las instalaciones, consulte la sección Puesta a tierra 38. Cuando el módulo se conecta a extensiones analógicas en otro edificio, se requiere emplear una caja protectora IP Office Phone Barrier Box V2 (101V) en ambos extremos; consulte la sección Protección contra rayos/Conexiones fuera del edificio 39.

Códigos de piezas y equipos relacionados

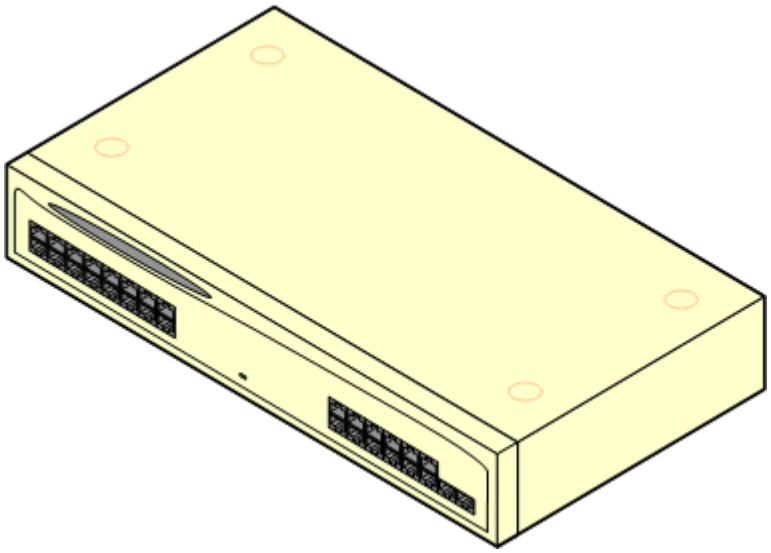
Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Artículo	Variante	País	Código SAP
Estación digital IP400 V2	16 puertos	Todos	700359839
	30 puertos		700359847
Cable de energía IEC60320 C13	CEE7/7	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	América	700289770
Kit de montaje en bastidor IP400		Todos	700210800

13.6.3 Teléfono V2

El módulo Phone IP400 V2 (también conocido como módulo Phone V2) se utiliza para agregar puertos TELÉFONO adicionales a un sistema IP Office. Los puertos TELÉFONO se utilizan para teléfonos analógicos.

El módulo Phone V2 está disponible con variantes para 8, 16 y 30 puertos, conocidas respectivamente como Phone 8, Phone 16 y Phone 30.

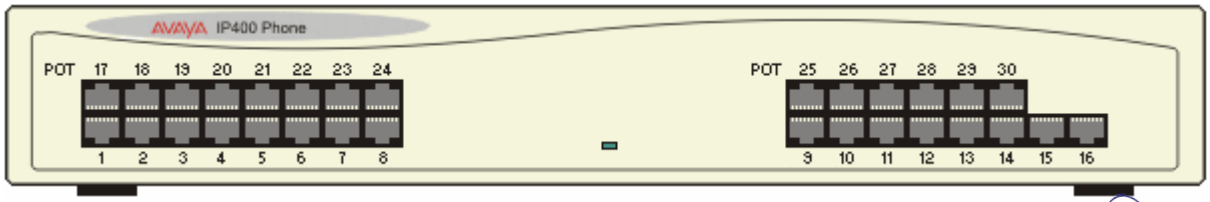


El módulo Phone V2 reemplaza el módulo Phone IP400 original, conocido actualmente como Phone V1. La versión del módulo está indicada en las etiquetas ubicadas en la base y en la parte posterior del módulo. Los cambios principales son:

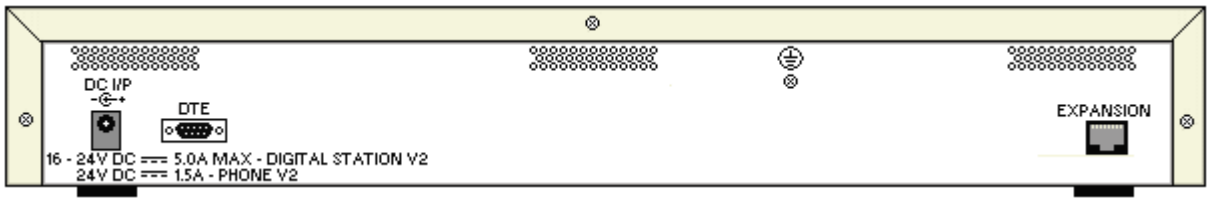
- El módulo Phone V2 emplea una unidad externa de suministro de externo con puesta en tierra de 3 pines y 60W.
- Con IP Office 3.1, el indicador de mensaje en espera (MWI) de cada puerto puede configurarse para ***Ninguno***, ***Activado***, ***51V escalonado***, ***81V***, ***Inversión de línea A*** o bien ***Inversión de línea B***. ***Activado*** utiliza la configuración predeterminada según la región del sistema. Los puertos de un módulo Phone V2 también pueden configurarse para su funcionamiento en ***101V***.
- Estos puertos no incluyen un capacitor de timbre. Por lo tanto, en los países que así lo requieran (por ejemplo, Reino Unido y Nueva Zelanda), la conexión de teléfonos analógicos de 4 vías deberá realizarse mediante una toma maestra con capacitores de timbre.
- El puerto serial DTE en la parte trasera del módulo ha sido cambiado por un enchufe para conector tipo D de 9 vías.

Función	Detalles
Localidades	Compatible con todas las localidades de IP Office
Nivel de software	Nivel mínimo de software nuclear IP Office Versión 2.1(36) .Archivo Bin = dvpots.bin.
Incluido	Unidad de suministro de energía (ver abajo) y cable de interconexión para expansiones.
Suministro de energía	El módulo está equipado con una unidad externa de suministro de energía aterrizada de 3 pins y 60W. La PSU cuenta con un cable de energía integrado para la conexión con el enchufe del módulo DC I/P. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
Montaje	El módulo se ha diseñado como un módulo independiente que puede combinarse con o bajo el comando de otros módulos IP Office. El módulo puede montarse en bastidor sobre un sistema de bastidor de 19" con ayuda del Kit opcional de montaje en bastidor IP400.
Dimensiones	Ancho: 445mm/17,5". Profundidad: 245 mm/9,7". Altura: 71mm/2.8"/2U.
Peso	Sin caja: 3.1Kg/6.94lbs. En caja: 4.4Kg/9.7lbs. (Con base en Phone 30 V2).

Parte delantera del módulo



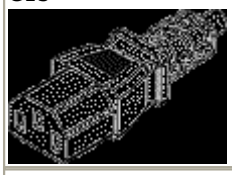
Parte trasera del módulo



Puertos	Descripción
DC I/P 286	Puerto de entrada de la corriente DC. Se utiliza para la conexión del cable de alimentación desde una unidad externa de suministro de energía aterrizada de 3 pines y 60 W incluida con el módulo de expansión. Se requiere un cable de energía IEC60320 C13 específico para la localidad 33 para la PSU externa, pero no viene incluido con el módulo.
DTE 293	Enchufe para conector tipo D de 9 vías. Solamente para uso con componentes Avaya.
EXPANSIÓN 288	Enchufe RJ45. Se utiliza para la conexión directa de un puerto de expansión en una unidad de control IP Office con ayuda del cable de interconexión para expansiones incluido con el módulo.
TELÉFONO 291	Enchufe RJ45. Se utiliza para conectar teléfonos analógicas. Se utiliza para conectar teléfonos analógicos de dos hilos. Para conectar con teléfonos analógicos de cuatro hilos, la conexión debe efectuarse con un enchufe maestro y capacitores de timbre. Cuando se conecta a una extensión fuera del edificio 39, la conexión debe equiparse con Cajas de protección IP Office 190 adicionales a la protección principal del edificio. El módulo debe asimismo conectarse a una conexión de tierra de protección.
⏚	Punto de la puesta a tierra de protección. Se requiere el uso de la conexión a tierra para protección en todas las instalaciones, consulte la sección Puesta a tierra 90. Cuando el módulo se conecta a extensiones analógicas en otro edificio, se requiere emplear una caja protectora IP Office Phone Barrier Box V2 (101V) en ambos extremos; consulte la sección Protección contra rayos/Conexiones fuera del edificio 39.

Códigos de piezas y equipos relacionados

Todos los módulos de expansión incluyen software de nivel básico y deben actualizarse para coincidir con el software nuclear en la unidad de control y el sistema IP Office. Los módulos de expansión incluyen una unidad externa de suministro de energía (PSU) y el cable de interconexión apropiado. No incluyen el cable de energía específico para la localidad para la PSU externa ni cables para extensión telefónica.

Artículo	Variante	País	Código SAP
IP400 Phone V2	8 puertos	Todos	700359896
	16 puertos		700359904
	30 puertos		700359912
Cable de energía IEC60320 C13 	CEE7/7	Europa	700289762
	BS1363	Reino Unido	700289747
	NEMA5-15P	América	700289770
Kit de montaje en bastidor IP400		Todos	700210800

13.7 Kits de montaje

Los siguientes son los tipos de kits de montaje disponibles para el uso con sistemas IP Office.

13.7.1 Kits de montaje en pared IP500

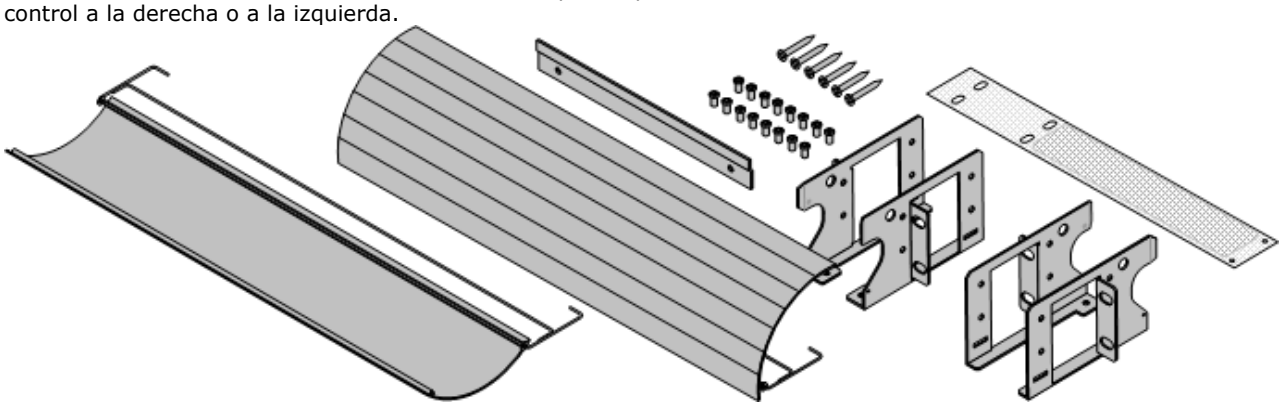
Las unidades de control IP500 V2 y los módulos de expansión externos IP500 pueden montarse en pared o bastidor. Para lograrlo, necesita un kit de montaje en pared, además de los aditamentos necesarios para fijarlos a la pared.

Además de los requerimientos ambientales 53 para el sistema IP Office, los siguientes requisitos adicionales aplican en la instalación en pared de una unidad:

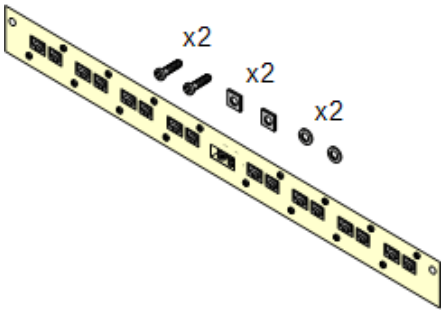
- La superficie de la pared debe ser vertical, plana y estar libre de vibraciones. No se permite la fijación a paredes temporales.
- Debe utilizar únicamente los tornillos incluidos en el kit de montaje para fijar la unidad de control a los soportes.

El siguiente kit de montaje para pared y soporte está disponible actualmente:

- **IPO IP500 WALL MNTG KIT V3** *(Código SAP 700503160)*
  Este kit se puede usar para montaje en la pared y en bastidor de una unidad de control IP500 V2 y módulos de expansión externos IP500. El kit incorpora el enrutamiento de los cables en la parte delantera y trasera de la unidad. En las unidades de control montadas en la pared, permite orientar las ranuras de la base de la unidad de control a la derecha o a la izquierda.



13.7.2 Kit de montaje en bastidor con cajas de protección



- **Kit de montaje en bastidor con cajas de protección** *(SAP 700293905)*
  Deben utilizarse cajas de protección en las extensiones de teléfono analógicas fuera del edificio 39. Este soporte admite hasta ocho cajas de protección IP Office montadas en bastidor y simplifica el número de conexiones hacia el punto de tierra de protección en el bastidor. Debe utilizar este kit cuando se utilizan más de tres cajas de protección, y admite un máximo de 16 cajas de protección para un solo módulo de expansión externo.

13.8 Teléfonos

El IP Office versión 10.1 admite los siguientes teléfonos y complementos. La disponibilidad puede depender según la ubicación y puede ser objeto de restricciones locales.

Punto y anillo (Tip y ring) mejorados (puertos ETR)

Estos teléfonos solo son compatibles en una tarjeta ETR6 en un sistema IP500 V2. Solo son compatibles en sistemas IP Office Basic Edition - modo PARTNER® y IP Office Basic Edition que funcionan en una región de Norteamérica y compansión U-Law.

- **Serie ETR:** ETR6, ETR6D, ETR18, ETR18D, ETR34D *(Los teléfonos ETR 34D tiene un límite máximo de 2 por tarjeta y 4 en total)*
- **PARTNER DECT:** 3910, 3920

Teléfonos digitales Avaya DS (puertos DS)

Estas estaciones digitales se conectan a IP Office vía los puertos DS 286. Son compatibles en todos los modos IP Office.

- **Serie 1400:** 1403, 1408, 1416
- **Serie 9500:** 9504, 9508

Los siguientes teléfonos adicionales del puerto DS solo son compatibles en modo estándar de IP Office:

- **Serie 2400:** 2402, 2410, 2420.
- **Serie 3800:** Teléfono inalámbrico 3810 (solo son compatibles con los módulos de expansión externos).
- **Serie T3:** T3 Compact, T3 Classic, T3 Comfort.

Teléfonos digitales Avaya BST (puertos BST)

Estas estaciones digitales se conectan al sistema IP500 V2 IP Office mediante puertos BST.

- **Serie 4100:** 4135, 4136, 4145, 4145EX, 4146, 4146EX - Conexión a puertos BST de IP Office mediante un sistema Digital Mobility Solution.
- **Serie 7400:** 7420, 7430, 7434, 7439, 7440, 7444, 7449 - Conexión a puertos BST de IP Office mediante un sistema Digital Mobility Solution.
- **ACU:** Unidad de audioconferencia
- **Serie M:** M7100, M7100N, M7208, M7208N, M7310, M7310N, M7324, M7324N.
- **Serie T:** T7000, T7100, T7208, T7316, T7316E, T7406, T7406E

Teléfonos analógicos

Los teléfonos y dispositivos analógicos se conectan a los puertos TELÉFONO 291 en el sistema de IP Office. Sin embargo, debido a la gran variedad de teléfonos y dispositivos analógicos disponibles, no ofrecemos garantía de su funcionamiento. Es responsabilidad de la persona a cargo de instalar y dar mantenimiento al sistema IP Office para comprobar y verificar el funcionamiento del equipo analógico propuesto.

- **Serie 6200:** 6211, 6219, 6221 *(Norteamérica)*.
- **Serie B100:** B149, B159, B169.
- **Interquartz Gemini:** 9330-AV, 9335-AV, 9281-AV *(Europa, Medio Oriente, África, Asia-Pacífico)*.

Teléfonos IP:

Los teléfonos IP (SIP y H323) se conectan al sistema de IP Office mediante el puerto LAN o WAN RJ45. Estos dispositivos requieren una licencia para terminales IP Avaya y recursos de compresión de voz.

H323:

- **Serie 1600:** 1603IP/SW, 1608, 1608-I, 1616, 1616-I
- **Serie 3600:** 3616, 3620, 3626, 3641, 3645
- **Serie 3700:** 3701, 3711 - Conexión por medio de estaciones base DECT. 3720, 3725, 3730, 3735, 3740, 3745, 3749 - Conexión por medio de estaciones base DECT R4.
- **Serie 9600:** 9608, 9608G, 9611G, 9620L, 9620C, 9621G, 9630G, 9640, 9640G, 9641G, 9641GS, 9650, 9650C.
- **Serie T3 IP:** T3 IP Compact, T3 IP Classic, T3 IP Comfort.

SIP:

- **Serie 1000:** 1010, 1040
- **Serie 1100:** 1120E, 1140E
- **Serie 1200:** 1220, 1230
- **Serie B100:** B179.
- **Serie D100:** Estos auriculares DECT (hasta 8) usan una estación base que se conecta al sistema IP Office usando una línea troncal SIP y aparecen en el IP Office como extensiones.
- **E129:** Un teléfono SIP simple, el E129 admite respuesta automática, funcionamiento de auricular y manos libres.
- **E159, E169:** Teléfono SIP compatible con el acoplamiento de dispositivos móviles.
- **H175:** Teléfono SIP de video.
- **J129:** Teléfono SIP de escritorio simple. Compatible con IP Office versión 10.0 SP2.

13.9 Complementos del teléfono

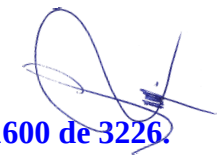
En versiones IP Office 5.0 y posteriores, la cantidad máxima combinada de los botones en módulos de botones es 1024 por sistema.. Los módulos DSS T3 no se incluyen en los límites combinados mencionados anteriormente, pero están limitados a 30 módulos DSS T3 (1080 botones).

- **1100 KEM:** *+18 (Max 3 por teléfono, 56 por sistema.)*
  Complemento para los teléfonos 1120E y 1140E. Cada módulo proporciona 18 botones programables adicionales.
- **1200 KEM:** *+12 (Max 7 por teléfono, 85 por sistema.)*
  Complemento para los teléfonos 1220 y 1230. Cada módulo proporciona 12 botones programables adicionales.
- **BM12:** *+24 (Máx. de 3 por teléfono, 42 por sistema).*
  Complemento para teléfonos 9508, 9608, 9611 y 9641. Proporciona 12 botones físicos que pueden asignarse en 2 páginas para lograr un total de 24 botones programables. Cuando se utilizan con teléfonos 9508, se debe suministrar alimentación al teléfono mediante un módulo de alimentación en línea.
- **BM32:** *+32 (Max 3 por teléfono, 32 por sistema.)*
  Complemento para los teléfonos 1616, proporcionando dos columnas de 16 botones. Hasta 3 módulos BM32 son compatibles con cualquier 1616. Sin embargo, cuando se lo utiliza con más de un módulo, el teléfono debe conectarse a una unidad de fuente de energía en vez de a PoE.
- **DBM32:** *+32 (Max 3 por teléfono, 32 por sistema.)*
  Complemento para los teléfonos 1416, proporcionando dos columnas de 16 botones. Se admiten hasta 3 módulos BM32 con cualquier 1416. Cuando se utiliza con un módulo de botón DBM32, el teléfono debe ser alimentado por una fuente de alimentación.
- **EU24:** *+24 (Max 1 por teléfono, 8 por sistema.)*
  Complemento para 2420, 4620, 4620SW, 4625, 5620, 5620SW y 5621. Proporciona 24 botones programables adicionales. Los iconos de visualización de los botones se encuentran en dos páginas alternables, con 12 iconos en cada página.
- **EU24BL:** *+24 (máx. 1 por teléfono, 8 por sistema)*
  Igual que el EU24 anterior, pero con luz de fondo como 4621. No es compatible con 2420.
- **KLM:** *+48 (Máx. 2 por teléfono, 21 por sistema).*
  Utilizado con los teléfonos M7324. Se admiten hasta 2 módulos de botones por teléfono. Cada módulo de botones proporciona 48 botones programables.
- **SMB24:** *+24 (Máx. 3 por teléfono, 42 por sistema)*
  Compatible con los teléfonos 9630G, 9640, 9640G, 9650 y 9650C. Para IP Office versión 9.0, también compatible con 9608, 9608G, 9611G, 9641G y 9641GS.
- **T3 DSS:** *+36 (Max 3 por teléfono, 30 por sistema.)*
  Se pueden conectar hasta tres unidades de este tipo a cualquier teléfono T3 IP Office T3. Cada una proporciona 36 botones programables. Cada botón incluye una sola luz LED de estado roja. Máximo 3 por teléfono, 30 por sistema. La conexión con el DSS T3 varía:
  - En los modelos distintos a IP, el primer DSS T3 se conecta directamente a un puerto de enlace en el teléfono. No requiere suministro de energía adicional.
  - En los modelos T3 IP, el primer DSS T3 se conecta a una unidad DSS Link instalada en el teléfono. La DSS requiere un suministro de energía.
- **T7316E KEM:** *+24 (Máx 9 por teléfono, 42 por sistema).*
  Utilizado con los teléfonos T7316E. Cada módulo de botones proporciona 24 botones programables. Se admiten hasta 4 módulos de botones por teléfono sin requerir un suministro adicional de energía. Pueden admitirse de 5 a 9 módulos con la adición de una fuente de energía. Máximo 9 por teléfono (4 sin fuente de energía adicional).

13.10 Aplicaciones

Esta sección describe los requisitos de las distintas aplicaciones de IP Office. Son sólo descripciones generales; para la información completa, consulte los manuales de instalación específicos de dichas aplicaciones, así como los Boletines Técnicos de IP Office.

- **IP Office Application Server** 265
- **Contact Recorder for IP Office** 265
- **one-X Portal for IP Office** 267
- **Avaya Communicator** 269
- **SoftConsole** 270
- **IP Office Video SoftPhone** 270
- **TAPI** 273
- **Voicemail Pro** 274
- **Colaboración web** 275
- **IP Office Manager** 267
- **System Monitor** 267
- **System Status Application (SSA)** 272



13.10.1 IP Office Application Server

El IP Office Application Server es un paquete de instalación para servidor único de las aplicaciones de IP Office enumeradas a continuación. El DVD instala un sistema operativo CentOS Linux, las aplicaciones de IP Office y un conjunto de páginas web para la administración del servidor. Tenga en cuenta que la instalación sobrescribe todo sistema operativo y datos existentes en la PC servidor.

- **one-X Portal for IP Office** 267
  El acceso de los usuarios y para configuración es mediante el navegador web, del mismo modo que para la instalación de un servidor Windows de one-X Portal for IP Office.
- **Voicemail Pro** 274
  El acceso a la configuración se realiza utilizando una instalación Windows del software de cliente Voicemail Pro. Se incluye un paquete de instalación para el cliente Voicemail Pro en el servidor IP Office Application Server.

Para el servidor Voicemail Pro que se ejecuta en una plataforma basada en Linux, no se admiten las siguientes funciones:

- **Secuencias de comandos VB**
- **Integración de base de datos de terceros**
- **VPNM**
- **Correo de voz UMS**
  (Sin embargo, existen las alternativas de acceso vía IMAP y one-X Portal for IP Office.)

Al iniciar sesión en el servidor de correo de voz con el cliente de Voicemail Pro, las características que no son compatibles aparecen en gris o están ocultas. Si las funciones están presentes en un flujo de llamadas importado, las funciones no operarán y las llamadas que intenten utilizarlas serán desconectadas.

Actualmente no se pueden utilizar las funciones de copia de seguridad y restauración del cliente Voicemail Pro para transferir datos de correo de voz entre un servidor Linux y un servidor Windows, y viceversa. Se pueden usar las funciones del cliente para importar y exportar un módulo y la base de datos de flujo de llamada.

En escenarios de pequeñas redes comunitarias donde hay varios servidores de correo de voz presentes, por ejemplo un servidor distribuido y uno de respaldo, está permitido combinar servidores con base en Linux y servidores con base en Windows.

Detalles	
DVD	IP Office Application Server Conjunto de DVD (2) 10.1 versión
Licencia	✓ - Depende de las aplicaciones IP Office seleccionadas durante la instalación. El servidor IP Office Application Server mismo no requiere ninguna licencia.

Requisitos de la PC

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.2 Contact Recorder for IP Office

Voicemail Pro 274 puede usarse para grabaciones de llamadas manuales y automáticas. Por lo normal, estas grabaciones se colocan en el correo de voz especificado para el usuario o el grupo de caza cuyas llamadas se están grabando, y después se comportan como mensajes normales. Contact Recorder for IP Office permite que esas grabaciones sean redireccionadas a una base de datos en el servidor que ejecuta Contact Recorder for IP Office. Esto permite archivar las grabaciones y realizar búsquedas en las mismas en forma separada de los mensajes de usuario. El acceso de usuario se realiza a través del navegador web.

Contact Recorder for IP Office es un servicio que puede ejecutarse en un IP Office Application Server (que también puede alojar Voicemail Pro y/o one-X Portal for IP Office. Sin embargo, el servidor debe configurarse con una partición o un disco por separado para el almacenamiento de las grabaciones de llamadas.

Detalles	
Licencia	✓ Administradores de grabaciones de VMPro. Consulte Licencias de Voicemail Pro 300.

13.10.3 IP Office Manager

Se utiliza esta herramienta para acceder a todas las partes de la configuración de IP Office. Pueden definirse distintos niveles de acceso para controlar cuáles partes de la configuración puede visualizar y modificar el usuario de IP Office Manager. También puede utilizar IP Office Manager para actualizar los archivos del software utilizado por el sistema IP Office. Durante la ejecución, actúa también como servidor TFTP, mediante el cual algunos teléfonos Avaya pueden solicitar nuevo software.

- ςερσι∫ν **IP Office Manager**
  Es importante que descargue e instale la versión actual de la suite de administración de IP Office, incluso IP Office Manager.
  - Para la instalación del sistema, debe usar la versión de IP Office Manager que coincide con la versión de IP Office que requiere el sistema. Esto configura la versión del software IP Office cargado al momento de la recreación de la tarjeta SD del sistema 75.
  - Para el mantenimiento del sistema, la versión que se usa de IP Office Manager configura la versión de software de IP Office que se carga a un sistema cuando se actualiza el sistema 179.
  - Para la configuración del sistema, IP Office Manager es compatible con las versiones anteriores. IP Office Manager versión 10.1 es compatible con las versiones anteriores para configurar los sistemas que ejecutan software desde IP Office versión 6.0 en adelante. IP Office Manager no puede cargar la configuración de un sistema IP Office que ejecuta una versión posterior del software

Detalles	
DVD	Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892) (Disco 1)
Idiomas	Inglés, portugués (Brasil), chino (simplificado), holandés, francés, alemán, italiano, ruso, español (México).
Licencia	✗ No se requieren licencias.

Requisitos de la PC

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.4 Monitor

Monitor (también conocida como System Monitor) es una herramienta que permite realizar un seguimiento minucioso de toda actividad producida en el sistema IP Office. Como consecuencia, la interpretación de los datos de Monitor requiere de un gran conocimiento de protocolos de datos y telefonía. Sin embargo, todos los técnicos a cargo de la instalación y mantenimiento de IP Office deben saber cómo ejecutar Monitor cuando sea necesario, ya que Avaya puede solicitar copias de los trazos de Monitor para resolver problemas de soporte técnico.

En IP Office 4.0 y versiones posteriores, se ha agregado System Status Application 272 para proporcionar información más fácil de interpretar que la proporcionada por Monitor.

Detalles	
DVD	Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892) (Disco 1)
Idiomas	Inglés solamente
Licencia	✗ No se requieren licencias.

Requisitos de la PC

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.5 one-X Portal for IP Office

Esta aplicación se instala en la PC del servidor conectado al sistema IP Office. Los usuarios acceden al one-X Portal desde su PC con ayuda de un navegador Web. La aplicación permite a los usuarios controlar sus teléfonos, acceder a los mensajes de correo de voz, registros de llamadas y directorios telefónicos.

Detalles	
DVD	Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892) (Disco 2) o IP Office Application Server Conjunto de DVD (2) 10.1 versión
Licencia	✓ Consulte la sección Licencias de usuario 298.

Idiomas	Portugués (Brasil), checo, holandés, inglés (RU), inglés (EE. UU.), francés, alemán, italiano, japonés, coreano, polaco, ruso, sueco, turco y español de América Latina.

Los detalles a continuación se refieren a una instalación de servidor con base en Windows de one-X Portal for IP Office. one-X Portal for IP Office puede también instalarse como parte de una instalación de servidor con base en Linux con ayuda del DVD IP Office Application Server 265. Los complementos adicionales que se admiten para uso con one-X Portal for IP Office tienen sus propios requisitos de sistema operativo; consulte la documentación del one-X Portal for IP Office para obtener detalles.

Requisitos de la PC

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.6 Avaya Communicator

Avaya Communicator es una aplicación softphone para usuario que le permite realizar y responder llamadas desde diversos dispositivos telefónicos. El software para cliente Avaya Communicator está disponible para dispositivos iPad y Windows.

Detalles	
Licencia	✓ Consulte la siguiente tabla.
Idiomas	Holandés, inglés (Reino Unido), inglés (Estados Unidos), francés, italiano, portugués de Brasil, ruso y español.

Las funciones disponibles para el usuario dependen de la licencia que el usuario posea para Avaya Communicator y si el sistema también incluye one-X Portal for IP Office 267 y Voicemail Pro 274.

		Modo Avaya Communicator	
		Modo Lite	**Modo Avanzado**
Funciones básicas		• Realizar, poner en espera, silenciar y transferir llamadas. • Directorio del sistema. • Registro de llamadas de aplicación local.	• Realizar, poner en espera, silenciar y transferir llamadas. • Directorio del sistema. • Registro de llamadas de aplicación local.
Funciones avanzadas *(Requiere one-X Portal for IP Office y Voicemail Pro)*		–	• Directorios de usuario y registros de llamada a través de one-X Portal for IP Office • Presencia (XMPP). • Mensajería instantánea de 2 participantes • Llamadas de video de 2 participantes. • Soporte de extensión doble.
Licencias requeridas	**Licencia de sistema**	• **Essential Edition**	• **Essential Edition*** • **Preferred Edition**
	Licencias de usuario	• **Avaya Softphone**	• **Office Worker** o bien • **Teleworker** o • **Power User**.
Modo del sistema	**IP Office Essential Edition**	✓ Sí	–
	IP Office Preferred Edition	✓ Sí	✓ Sí
Conexión de cliente		El sistema IP Office entrega soporte técnico para funciones básicas de modo.	El soporte técnico para funciones básicas de modo es otorgado por las aplicaciones one-X Portal for IP Office y Voicemail Pro.

- **Software para cliente**
  La fuente del software de cliente Avaya Communicator depende del dispositivo del usuario. Sin embargo, como Avaya Communicator es compatible con diversas plataformas Avaya, el instalador debe asegurar en todos los casos la obtención de un cliente Avaya Communicator que ofrezca soporte específicamente para IP Office.

Requisitos de PC Windows

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.7 SoftConsole

Esta es una aplicación que requiere licencia. Se le ha diseñado para el uso de operadoras o recepcionistas del sistema telefónico. La pantalla muestra los detalles de llamadas dirigidas al usuario y le permite comprobar rápidamente el estado del destino requerido por la llamada, y transferir la misma. El usuario de SoftConsole tiene la capacidad de acceder a una serie de detalles sobre el estado de usuario y grupos dentro del sistema de IP Office.

- IP Office SoftConsole funciona en combinación con un teléfono de extensión física de IP Office que proporcione una trayectoria de voz para las llamadas.
- Se pueden ingresar licencias para hasta cuatro usuarios SoftConsole simultáneos.

Detalles	
DVD	Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892) (Disco 1) o ficha Central de aplicaciones del servidor Linux.
Idiomas	Portugués (Brasil), Chino (simplificado), danés, holandés, inglés (RU), inglés (EE. UU.), finlandés, francés, alemán, italiano, coreano, japonés, español (América Latina), noruego, portugués (Europa), ruso, español y sueco.
Licencia	✓ Aplicación con licencia. Consulte más abajo.

Licencias

Licencia	Descripción	Nombre RFA	SAP
Recepcionista	Agrega un usuario SoftConsole adicional. Se pueden ingresar licencias para hasta cuatro usuarios SoftConsole.	IPO LIC RECEPTIONIST RFA	171987

Requisitos de la PC

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.8 IP Office Video SoftPhone

La aplicación IP Office Video SoftPhone es la SIP Softphone preferida para usar con sistemas IP Office. Incluye funciones específicas de IP Office que no están disponibles en otras aplicaciones que no son de Avaya SIP Softphone.

Asistencia técnica

Windows IP Office Video SoftPhone y MAC IP Office Video SoftPhone versión 3.2 no son compatibles con la versión 10.0 de IP Office.

Los usuarios de MAC que quieran ejecutar IP Office Video SoftPhone deben usar IP Office Video SoftPhone versión 4.0 que es compatible con Mac OS 10.8 y 10.9. Los nuevos usuarios de Windows deben usar Avaya Communicator.

Detalles	
DVD	Sólo Mac versión 4.0: Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892) (Disco 1) o ficha Central de aplicaciones del servidor Linux.

Licencia	✓
	Para usar IP Office Video SoftPhone el sistema IP Office debe contar con las siguientes licencias:
	• **Licencias del sistema**
	Los sistemas que no sean Server Edition deben tener licencias **Essential Edition** y **Preferred Edition**.
	• **Licencias de usuario**
	Sólo se puede habilitar usuarios para usar Softphone cambiando antes su perfil a **Power User** o **Teleworker**. Estos son modos de usuarios autorizados por las siguientes licencias:
	  • **Licencia Power User**.
	  • **Licencia Teleworker**.
	• **Licencias de aplicación**
	Con IP Office versión 9.1, las aplicaciones Softphone también usan las siguientes licencias adicionales:
	  • **IP Mac Softphone**
	Los Softphone versión 4.0 usan una licencia **Mac IP Softphone** individual.

Requisitos de PC del usuario

A continuación se indican los requisitos mínimos recomendados para IP Office Video SoftPhone.

Función	Computadora MAC
Sistema operativo	• **Versión 3.2:** Sólo sistema operativo Mac 10.6 a 10.7. • **Versión 4.0:** Sistemas operativos Mac 10.8 y 10.9.
Procesador	• Intel Core i5.
Memoria	• **Mínimo:** Memoria RAM de 1GB. • **Óptimo:** Memoria RAM de 2GB.
Espacio de disco duro	• 50MB.
Tarjeta de sonido	• Bidireccional, 16 bits o uso de auricular USB.
Adicional	–

13.10.9 System Status Application

Esta herramienta proporciona un amplio rango de información sobre el estado actual de un sistema IP Office 4.0 o superior. Incluye los recursos y componentes disponibles en el sistema. Esto incluye los detalles de la llamada actual en progreso. Registra los detalles de la cantidad de alarmas y la fecha y hora de las alarmas más recientes.

Cuando es necesario para la escalación de diagnóstico, la aplicación SSA tiene la capacidad de tomar una imagen instantánea del estado del sistema IP Office, incluyendo una copia de la configuración actual. El uso de la aplicación SSA requiere de un nombre y contraseña de usuario IP Office configurado para tener acceso a System Status en los ajustes de seguridad de IP Office.

- Para sistemas IP500 V2, la aplicación SSA se encuentra preinstalada en la tarjeta de memoria SD Avaya del sistema, y puede ejecutarse buscando la dirección IP del sistema IP Office.

Detalles	
DVD	Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892) (Disco 1)
Licencia	✗ No se requieren licencias.

Requisitos de la PC

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.10 TAPI

IP Office TAPI es una aplicación cliente de PC que permite las aplicaciones en cumplimiento con TAPI para interactuar con el sistema IP Office. El software de IP Office TAPI puede utilizarse en uno de dos modos, dependiendo de si cuenta o no con una licencia. Se instala el mismo software en cualquier caso. Las licencias, si se ingresan, se ingresan en la configuración del sistema de IP Office.

- **1st Party TAPI**
  En este modo sin licencia, el software TAPI admite el control de la extensión asociada a un usuario particular, permitiendo que una aplicación compatible con TAPI responda (requiere un teléfono que admita respuesta manos libres) y realice llamadas.
- **3rd Party TAPI**
  En este modo con licencia, se puede utilizar el software TAPI para controlar funciones de llamadas o extensiones con múltiples usuarios. Este modo se utiliza con aplicaciones CTI Developer.

Detalles	
DVD	Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892) (Disco 1)
Licencia	✗ Opcional. Las licencias requeridas para el modo de operación 3rd party. Consulte la sección Licencias CTI 301.

Requisitos de la PC

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.11 Voicemail Pro

Esta aplicación requiere ingresar varias licencias en la configuración de IP Office, con el fin de controlar las funciones que ofrece y la cantidad de conexiones simultáneas (IP500 = 40 (IP Office 5.0 o superior) o 30 (pre-IP Office 5.0), IP500 V2 = 40). Es posible personalizar el funcionamiento de Voicemail Pro para que proporcione servicios especiales. .

El cliente y el servidor de la aplicación Voicemail Pro pueden instalarse de forma separada. De esta forma, el servidor Voicemail Pro podrá administrarse de forma remota desde una computadora que solo tenga instalado el cliente Voicemail Pro. Con el servidor Voicemail Pro se instala de forma automática una copia del cliente a nivel local.

Origen	
DVD	Conjunto de DVD (2) para administrador/usuario de la versiónIP Office 10.1 (700512892) (Disco 1) o IP Office Application Server Conjunto de DVD (2) 10.1 versión
Idiomas	Chino mandarín, chino cantonés, danés, holandés, inglés (Reino Unido), inglés (Estados Unidos), finlandés, francés, francés (Canadá), alemán, griego, hebreo, húngaro, italiano, japonés, coreano, noruego, polaco, portugués, portugués (Brasil), ruso, español, español (Argentina), sueco, turco.
Licencia	✓ Consulte la sección Licencias de Voicemail Pro 300.

La siguiente información es para una instalación de servidor basada en Windows de Voicemail Pro. Voicemail Pro también puede instalarse como parte de la instalación de servidor basado en Linux mediante DVD IP Office Application Server 265 .

Además del software servidor principal, el servidor Voicemail Pro está formado por diversos componentes:

- **Campaigns**
  Voicemail Pro puede configurarse para ejecutar unja campaña. Una campaña consiste en una serie de preguntas, y la aplicación Voicemail Pro puede grabar las respuestas o las teclas presionadas por la persona que realiza la llamada. La grabación resultante puede se reproducida a continuación por el usuario. El aspecto Web de las campañas permite al usuario reproducir y procesar las grabaciones de la campaña mediante su navegador de Internet. Para ello se requiere un servidor Web IIS en la misma computadora que ejecuta el software Voicemail Pro.
- **Texto a voz (TTS)**
  Mediante la incorporación de licencias adicionales, la aplicación Voicemail Pro puede utilizar las funciones TTS de Windows para grabar avisos y reproducir texto y números a las personas que llaman. Esta función reviste especial importancia si Voicemail Pro obtiene valores de texto y números de una base de datos de clientes.
- **Servicio unificado de mensajes (UMS)**
  Voicemail Pro ofrece una función denominada correo electrónico de correo de voz, que permite enviar mensajes o alertas de mensajes al buzón de correo electrónico de un usuario. Sin embargo, esto es un proceso de una sola vía sin un enlace de vuelta al buzón de voz del correo electrónico del usuario para indicar si el mensaje ha sido leído o eliminado. UMS convierte al anterior en un proceso de dos vías, donde los usuarios pueden reproducir los mensajes de correo de voz en el buzón de su correo electrónico o de correo de voz.

Requisitos de la PC

Para averiguar los requisitos de PC consulte el manual de instalación o implementación de IP Office correspondiente para la aplicación. Para conocer la compatibilidad con sistemas operativos y navegadores, consulte Resumen del sistema operativo 276.

13.10.12 Colaboración web

Colaboración web es un servicio admitido por los servidores basados en IP Office Linux one-X Portal for IP Office (excepto por Unified Communications Module). Funciona en forma conjunta con one-X Portal for IP Office y Voicemail Pro.

Colaboración web proporciona al usuario funciones para compartir documentos, aplicaciones y su escritorio mediante una conferencia de colaboración web. Se ejecuta en paralelo a una conferencia de audio alojada por el sistema IP Office.

- La capacidad coincide con la capacidad de conferencias de audio de IP Office. Ancho de banda requerida 250 Kbps por usuario.
- Los usuarios de host deben tener licencia para one-X Portal for IP Office con un perfil de **Office Worker**, **Teleworker** o **Power User** además de una licencia de **Web Collaboration**.
- Programar una conferencia, por medio de one-X Portal for IP Office, requiere una licencia **Power User**.
- Los anfitriones pueden cargar documentos en formato PDF, JPEG y PNG.
  - 10 documentos por usuario
  - 6 MB por documento.
- No se admite el uso compartido de aplicaciones ni de escritorio para usuarios de equipos MAC.
- Abra desde la URL en el navegador 277 o directamente desde Avaya Communicator, one-X Portal, el complemento Outlook, y Call Assistant.
- Idiomas: Inglés, francés, español, alemán, italiano, portugués, ruso, sueco, chino, japonés, coreano.
- El video no es compatible.
- Para la versión 10.0 de IP Office, los usuarios internos con licencia para colaboración web pueden usar WebRTC para transmitir audio por medio de una conferencia de colaboración web en vez de tener que hacer una llamada telefónica paralela a la conferencia de audio.

13.10.13 Puertos IP Office

Encontrará detalles de la gama de puertos usados por IP Office y aplicaciones de IP Office en https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003.

La mayoría de los firewall de PC solicitan al usuario que permita varias excepciones cuando se ejecuta por primera vez una aplicación instalada recientemente. Sin embargo, puede que este no sea siempre el caso, especialmente si el firewall se encuentra en una ubicación distinta a la PC del usuario.

13.11 Resumen del sistema operativo

Esta sección contiene un resumen del soporte proporcionado a aplicaciones de IP Office por IP Office versión 10.1.

Algunas funciones específicas pueden tener requisitos adicionales. Estos requisitos se detallarán en el manual de instalación de la aplicación específica. A menos que se especifique lo contrario, el sistema operativo es la versión más reciente compatible del desarrollador del sistema operativo.

13.11.1 Compatibilidad con Windows

En la siguiente tabla se enumeran las aplicaciones IP Office que pueden instalarse en los sistemas operativos Windows compatibles. No incluye las aplicaciones navegables 277.

IP Office Application	Windows 7		Windows 8.1		Windows 10		2008 R2	2012/ 2012 R2	2016
Server Applications	**32**	**64**	**32**	**64**	**32**	**64**	**64**	**64**	**64**
one-X Portal for IP Office	–	–	–	–	–	–	–	✓	✓
IP Office Contact Center	–	–	–	–	–	–	–	✓	–
Voicemail Pro Server	✓	✓	✓	✓	✓	✓	–	✓	✓
... plus UMS	–	–	–	–	–	–	–	✓	✓
... plus campaigns	–	–	–	–	–	–	–	✓	✓
... MAPI service for Linux Voicemail Pro	✓	✓	–	–	–	–	–	✓	✓
User Applications									
one-X Portal plug-in for Outlook	✓	✓	✓	✓	✓	✓	–	–	–
" Call Assistant	✓	✓	✓	✓	✓	✓	–	–	–
" plug-in for MS Lync 2013	✓	✓	✓	✓	✓	✓	–	–	–
Avaya Communicator	✓	✓	✓	✓	✓	✓	–	–	–
SoftConsole	✓	✓	✓	✓	✓	✓	–	–	–
TAPI - 1st Party	✓	✓	✓	✓	✓	✓	–	✓	✓
TAPI - 3rd Party	✓	✓	✓	✓	✓	✓	–	✓	✓
TAPI WAV	✓	–	✓	–	✓	–	–	–	–
Web Conferencing Desktop Sharing	✓	✓	✓	✓	✓	✓	–	–	–
IP Office Video SoftPhone	–	–	–	–	–	–	–	–	–
Maintainer Applications									
IP Office Manager	✓	✓	✓	✓	✓	✓	–	✓	✓
System Monitor	✓	✓	✓	✓	✓	✓	–	✓	✓
System Status Application	✓	✓	✓	✓	✓	✓	–	✓	✓
Voicemail Pro Client	✓	✓	✓	✓	✓	✓	–	✓	✓

- Si es compatible, el soporte técnico de Windows 7 solo está disponible con las versiones Professional, Enterprise y Ultimate. El soporte técnico de Windows 8.1 y 10 solo está disponible en las versiones Pro y Enterprise.
- TAPI WAV no es compatible con sistemas operativos de 64 bits.

13.11.1.1 Compatibilidad con Outlook

Application\Outlook Version	2007	2010	2013	2016
Voicemail Pro UMS/IMAP	–	✓	✓	✓
TAPI Dialing	–	✓	✓	✓
one-X Portal for IP Office plug-in for Outlook	–	✓	✓[1]	✓[1]

1. No se admite Screen popping de los contactos de Outlook.

13.11.2 Compatibilidad con Apple MacOS

PC Apple

En la siguiente tabla se enumeran las aplicaciones IP Office que pueden instalarse en los sistemas operativos Mac compatibles. No incluye las aplicaciones navegables 277.

IP Office Application	10.8 Mountain Lion	10.9 Mavericks	10.10 Yosemite	10.11 El Capitan	10.12 Sierra
IP Office Video SoftPhone Version 4.0	✓	✓	✓	✓	–
Web Conferencing Desktop Sharing	✓	✓	✓	✓	✓

iPad

Avaya Communicator 269 es compatible con iOS 6.1 y posterior.

iPhone

one-X Mobile es compatible con iOS 7.0 y posterior.

13.11.3 Compatibilidad con Linux

Varias IP Office server applications (Voicemail Pro, one-X Portal for IP Office, Conferencias web y Contact Recorder for IP Office) pueden ejecutarse en sistemas operativos Linux. Sin embargo, solamente son compatibles si se ejecutan en IP Office Application Server 265 que incluye la instalación de su propio sistema operativo. Ninguna aplicación IP Office es compatible con otros sistemas operativos Linux de terceros.

13.11.4 Soporte de navegador

En la siguiente tabla se enumera la compatibilidad de las aplicaciones IP Office a las que se accede utilizando un navegador web.

Application\Browser	Internet Explorer 10.0	Internet Explorer 11.0	Edge	Firefox	Google Chrome	Safari 8 Safari 9 Safari 10
Voicemail Pro Campaigns	✓	✓	✓	–	–	–
Voicemail Pro UMS Webmail	✓	✓	✓	–	–	–
Contact Recorder Client	✓	✓	–	–	–	–
one-X Portal for IP Office [1]	✓	✓	✓	✓	✓	✓
IP DECT R4 Admin	✓	✓	✓	✓	✓	✓
D100 DECT Admin	✓	✓	✓	✓	✓	✓
Colaboración web [4]	✓	✓	✓	✓	✓	✓
IP Office Web Manager [3]						
" on PC	✓	✓	✓	✓	✓	✓
" on iPad tablet (iOS6+)	–	–	–	–	✓	✓
" on Android tablet (KitKat 4.4+)	–	–	–	–	✓	–
Avaya Communicator for Web	–	✓	–	–	✓	–

Notas:

1. La navegación en one-X Portal for IP Office no es admitida por los sistemas operativos servidores de Windows.

2. La versión de IE debe coincidir con el sistema operativo. Por ejemplo, un navegador de 32 bits en un sistema operativo de 32 bits.
3. Algunas funciones de IP Office Web Manager solamente se admiten en sistemas operativos Windows: respaldo, restauración, actualización, ejecución de System Status Application/Voicemail Pro/IP Office Manager, administración de archivos.
4. El audio de Web RTC solo es compatible con Chrome o Firefox.

13.12 Puertos físicos

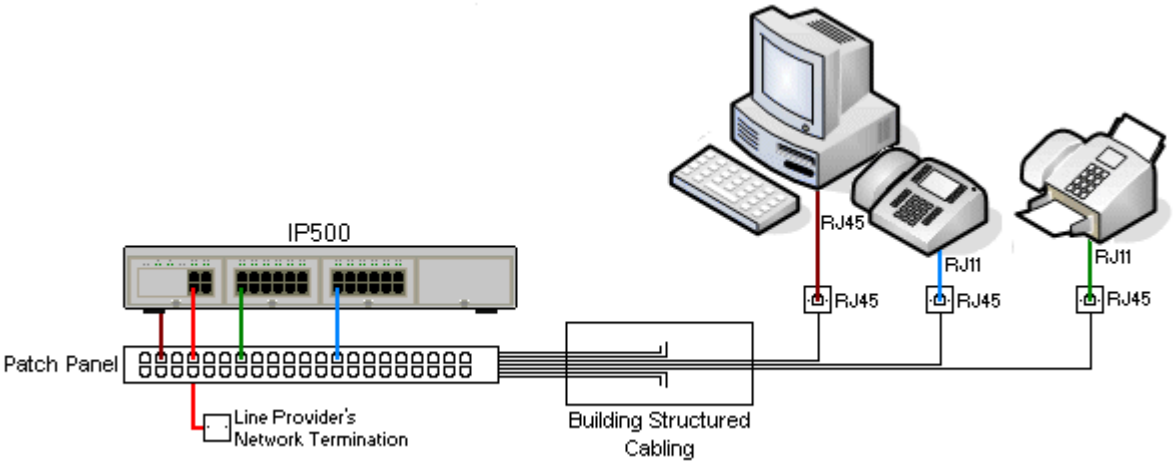
Los siguientes tipos de puertos se encuentran en la unidad de control y en los módulos de expansión de IP Office:

- **ANALÓGICO** 282
  Se utiliza para conectar troncales analógicas externas.
- **AUDIO** 282
  Se utiliza para la entrada de la fuente externa de música de espera.
- **BRI** 284
  Se utiliza para conectar troncales BRI (tarjeta de troncales Quad BRI). En los modos estándar de IP Office también pueden usarse para terminales ISDN (módulo So8).
- **BST (RJ21)** 285 y **BST (RJ45)** 285
  Conexiones para teléfonos serie M y serie T compatibles con IP Office. También compatible con sistema Digital Mobility Solution con soporte para teléfonos serie 4100 y 7400. Consulte Teléfonos digitales Avaya BST 41.
- **DC I/P** 286
  Entrada de corriente desde la unidad de suministro de energía
- **DS** 286
  Conexión de teléfonos de estación digital Avaya compatibles con IP Office.
- **RS232/DTE** 293
  Se utiliza para realizar operaciones de mantenimiento de la unidad bajo los lineamientos de Avaya. No se utiliza en los módulos de expansión.
- **EF** 287
  Los puertos de emergencia para cortes de energía puertos se encuentran en la tarjeta base ETR6.
- **ETR** 287
  Compatible únicamente con unidades de control IP500 V2 que se ejecutan en IP Office Basic Edition - modo PARTNER® o IP Office Basic Edition.
- **EXPANSIÓN** 288
  Se utiliza para interconectar módulos de expansión externos con las unidades de control.
- **EXT O/P** 192
  Se utiliza para controlar sistemas de relevadores externos. Este puerto proporciona dos controles con interruptor (activado, desactivado y pulso).
-
  Se utiliza para conectar la puesta a tierra funcional o de protección, de ser necesario.
- **LAN** 289
  Puertos 10/100Mbps Ethernet LAN.
- **PF** 290
  Puertos analógicos para fallo de energía
- **TELÉFONO** 291 **(POT)** 291
  Puertos de extensiones de teléfono analógicas. En unidades anteriores, estos puertos estaban marcados como puertos POT.
- **PRI** 292
  Puertos de troncales PRI

13.12.1 Cables

Los sistemas IP Office están diseñados principales para ser utilizados con un sistema de cableado estructurado RJ45 que emplea cable de par trenzado sin blindar (UTP) tipo CAT3 y enchufes RJ45.

Un sistema de cableado estructurado es aquel donde los cables emergen de un panel central de conexiones RJ45 dentro de la sala de comunicaciones/datos hacia enchufes RJ45 individuales en la ubicación de los usuarios individuales. Todos los cables dentro de cada cable entre el panel de conexiones y el enchufe de escritorio están conectados directamente. Esta organización permite que los dispositivos conectados al panel de conexiones puedan intercambiarse para adecuarse al tipo de dispositivo que necesita estar conectado en el enchufe del usuario. Por ejemplo, un enchufe de usuario puede ser un puerto telefónico y otro enchufe un puerto LAN para computadora, sin que esto requiera que se vuelvan a tender los cables entre el panel de conexiones y la ubicación del usuario.



- **Instalaciones de cableado tradicional IDC con ponchadora**
  De ser necesario, la clavija RJ45 del extremo lejano de los cables IP Office puede ser descubierta y cableada para conectarse a sistemas de cableado tradicional que emplean conectores con ponchadora. Este tipo de instalación debe realizarla un técnico de cableado experimentado.
- **Conexiones troncales**
  La mayoría de los puertos de troncales de IP Office emplean conectores RJ45 para admitir cables con terminales tipo RJ45 a RJ45. Sin embargo, es posible que la conexión en el extremo del proveedor de la línea requiera del uso de una clavija de enchufe diferente, con el fin de adecuarse al equipo del proveedor de la línea.
- **Conectores telefónicos RJ11**
  Muchos teléfonos emplean enchufes RJ11 y traen incluidos cables con terminales tipo RJ11 a RJ11. Las clavijas de enchufe RJ11 pueden insertarse en los enchufes RJ45, y la conexión funcionará correctamente en muchos casos. Sin embargo, esta práctica no se recomienda ni es admisible, ya que la unión de conexión no es completamente positiva y puede desconectarse fácilmente. Para este tipo de conexiones, existe un cable con terminales tipo RJ45 a RJ11 286 disponible.

Cables de IP Office Standard

Los siguientes son los tipos de cables estándar de Avaya, disponibles para el uso en sistemas IP Office. La longitud máxima aplica también cuando el cable estándar de Avaya es reemplazado por un cable alternativo.

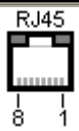
Cable	Descripción	Código SAP	Longitud estándar	Longitud máxima
Cable DTE de 9 terminales 293	Se conecta al puerto DTE de la unidad de control RS232. Con clavija de enchufe de 9 terminales tipo D a enchufe de 9 terminales tipo D	–	2m/6'6".	2m/6'6".
Cable de línea DS de cableado estructurado 286	Se conecta de los enchufes RJ45 a enchufes RJ11 y teléfonos DS y analógicos.	TT700047871	4m/13'2".	Consulte la tabla a continuación.
Cable de troncales BRI/PRI 284	Conecta los puertos de troncales BRI/PRI al punto de terminación de red del proveedor de línea. RJ45 a RJ45. Rojo.	700213440	3m/9'10".	–
Cable de interconexión para expansiones 288	Conecta la unidad de control a los módulos de expansión. RJ45 a RJ45. Azul. Puede reemplazarse por el cable de interconexión amarillo (2m - 700472871) incluido con la tarjeta IP500 4-Port Expansion 216, en casos donde se utilice esta tarjeta.	700213457	1m/3'3".	1m/3'3".
Cable LAN 289	Se conecta de los puertos LAN de IP Office a los dispositivos IP. RJ45 a RJ45. Gris.	700213481	3m/9'10".	100m/328'.

En la siguiente tabla se indican las distancias máximas totales de los cables para extensiones DS y analógicas utilizando cables de distintos espesores. Se debe usar cables de par trenzado no blindado Categoría 1 o superior.

Teléfono	Par trenzado no blindado (UTP) - 50 nf/km		
	AWG22 (0,65 mm)	AWG24 (0,5 mm)	AWG26 (0,4 mm)
Serie 1400	1.200m/3937'.	1.000m/3280'.	670m/2200'.
Serie 2400/5400	1.200m/3937'.	1.000m/3280'.	670m/2200'.
Serie 9500	1.200m/3937'.	1.000m/3280'.	670m/2200'.
Serie T3	1.000m/3280'.	1.000m/3280'.	400m/1310'.
BST	580m/1900'.	365 m/1200'.	228 m/750'
Teléfonos analógicos	1.000m/3280'.	1.000m/3280'.	400m/1640'.
Teléfonos ETR	305m/1000'.	305m/1000'.	122m/400'.

13.12.2 Puerto ANALÓGICO

Estos son puertos de líneas troncales analógicas. Las tarjetas de líneas troncales analógicas IP500 sólo son compatibles con líneas troncales de inicio de bucle. El módulo de línea troncal analógica ATM16 240 es compatible tanto con líneas troncales de inicio de bucle como de inicio básico, con la posibilidad de alternar entre ellas en la configuración de IP Office.

ANALÓGICO	Pin	Descripción
	1	No se utiliza.
	2	No se utiliza.
	3	No se utiliza.
	4	Negativo
	5	Tip.
	6	No se utiliza.
	7	No se utiliza.
	8	No se utiliza.

- **Corriente con teléfono descolgado:** 25mA.
- **IMPORTANTE**
  En todas las instalaciones de IP Office, cualquier módulo o unidad de control que utilice conexiones de troncales analógicas debe estar conectado a una puesta a tierra funcional 38.
- **PRECAUCIÓN**
  Dentro de la República de Sudáfrica y en áreas con alto riesgo de descargas eléctricas, todos los módulos o unidades de control que utilicen conexiones de troncales analógicas deben estar conectadas a una puesta a tierra de protección 38 y a un equipo de protección contra picos 39.

13.12.3 Puerto AUDIO

Este puerto se halla en la parte posterior del las unidades de control de IP Office. Se utiliza para la entrada de una fuente de sonido externa de música de espera. Observe que cuando se ha cargado un archivo de sonido interno para música en espera, se ignorará toda entrada desde este enchufe.

El puerto es un enchufe de clavija estéreo de 3.5 mm, adecuado para el uso con la mayoría de las terminales de audio estándar y para la conexión con el enchufe de saluda para "audífonos" disponible en la mayoría de los sistemas de audio.

El uso del enchufe de "audífonos" permite realizar ajustes sencillos del volumen. La conexión por medio del enchufe "Línea de salida" puede requerir equipo adicional para poder agregar el ajuste de nivel de volumen.

No. Pin	Descripción
Común	Común
Izquierdo	Entrada de audio - Canal izquierdo
Derecho	Entrada de audio - Canal derecho

- Impedancia de entrada: 10k /canal. Señal a.c. máxima – 200mV rms.

13.12.4 Puerto BRI (So)

Los puertos BRI en la parte delantera del módulo So8 son puertos de interfaz BRI So para proporcionar conexión a dispositivos de terminal ISDN. En IP Office 4.2+, las tarjetas de troncales auxiliares BRI IP500 pueden alternar entre el modo To y So.

IP Office			Cable	Terminal ISDN	
RJ45	Pin	BRI		PIN	RJ45
	1	–	Blanco/Anaranjado	1	
	2	–	Anaranjado/Blanco	2	
	3	⬅Rx-A	Blanco/Verde	3	
	4	➡Tx-B	Azul/Blanco	4	
	5	➡Tx-A	Blanco/Azul	5	
	6	⬅Rx-B	Verde/Blanco	6	
	7	–	Blanco/Café	7	
	8	–	Café/Blanco	8	

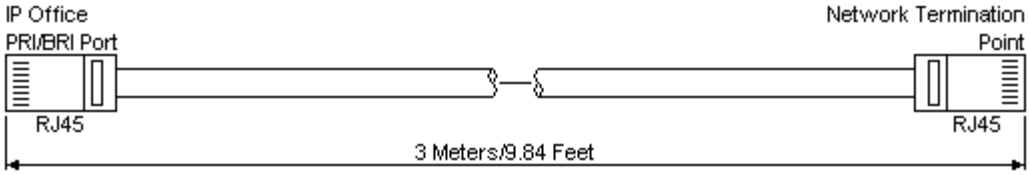
- **Resistores de terminación**
  Se necesitan resistores de terminación de 100ohm a lo largo de los pared de cables de transmisión y recepción a cada extremo del bus S.
  - Los puerto BRI del módulo So8 de IP Office incluyen resistores de terminación de 100ohm integrados.
  - En IP Office 4.2+, los puertos individuales de la tarjeta auxiliar BRI IP500 pueden alternarse al modo So. Esto se hace al configurar el **Subtipo de línea** a ***S-Bus*** en la configuración de IP Office. En este caso, los resistores de terminación deben agregarse en el extremo del IP Office, y en forma adicional a los presentes en el otro extremo de la conexión del bus S.
    - Puede agregar las terminaciones necesarias en el extremo de IP Office con ayuda de un Cable Convertidor IP500 BRI So (700458649). Este corto cable (25cm/10") incluye los resistores de terminación necesarios y el intercambio de terminales de cable.
  - Muchos dispositivos de terminales ISDN incluyen resistores de terminación. De no ser el caso, deben conectarse resistores de 100ohm (+/-5%) a lo largo del par de cables de recepción y el par de cables de transmisión en la caja de conexiones que precede inmediatamente a la última terminal ISDN en el bus S.

13.12.5 Puerto BRI (To)

Estos puertos son de tipo BRI para interfaz para la conexión a servicios de troncales BRI externos. Tenga en cuenta que los puertos BRI presentes en el módulo IP500 So8 son puertos de interfaz con BRI-S para la conexión de dispositivos de terminal ISDN. Consulte la sección Puerto BRI (So) 283.

Cable de troncales PRI/BRI

Este cable se utiliza para conectar de los puertos de troncales BRI/PRI de IP Office hacia el equipo de terminación de red del proveedor. Si este equipo no emplea enchufes tipo RJ45, es posible que haya que descubrir el cable y volver a cablear, o bien emplear otro tipo de cable. Las conexiones de clavija de señales y los colores de cable apropiados se describen a continuación.



IP Office				Cable	Terminación de red	
BRI	RJ45	BRI	PRI		PIN	RJ45
RJ45 8 1	1	–	⬅ Rx-A	Blanco/Anaranjado	1	RJ45 8 1
	2	–	⬅ Rx-B	Anaranjado/Blanco	2	
	3	➡ Tx-A	–	Blanco/Verde	3	
	4	⬅ Rx-A	➡ Tx-A	Azul/Blanco	4	
	5	⬅ Rx-B	➡ Tx-B	Blanco/Azul	5	
	6	➡ Tx-B	–	Verde/Blanco	6	
	7	–	–	Blanco/Café	7	
	8	–	–	Café/Blanco	8	

- Suministro: Las tarjetas de troncales BRI/PRI no incluyen estos cables.
- Color de cable: Rojo.
- Código SAP: 700213440.
- Longitud estándar: 3m/9'10".
- Longitud máxima: 5m/16'5".
- Aunque no se utilizan, las clavijas 7 y 8 están conectadas para facilitar la construcción.

13.12.6 Puerto BST (RJ21)

Estos puertos se encuentran en los módulos de expansión externos Estación digital IP500, 16A/30A 247. Estos son compatibles en sistemas IP500 V2 que funcionan en IP Office versión 7.0 y superiores. Consulte teléfonos digitales Avaya BST compatibles 41.

Primer conector RJ21

Puerto		Pin	Cable
1	Positivo	26	Blanco/Azul
	Negativo	1	Azul/Blanco
2	Positivo	27	Blanco/Anaranjado
	Negativo	2	Anaranjado/Blanco
3	Positivo	28	Blanco/Verde
	Negativo	3	Verde/Blanco
4	Positivo	29	Blanco/Café
	Negativo	4	Café/Blanco
5	Positivo	30	Blanco/Gris
	Negativo	5	Gris/Blanco
6	Positivo	31	Rojo/Azul
	Negativo	6	Azul/Rojo
7	Positivo	32	Rojo/Anaranjado
	Negativo	7	Anaranjado/Rojo
8	Positivo	33	Rojo/Verde
	Negativo	8	Verde/Rojo
9	Positivo	34	Rojo/Café
	Negativo	9	Café/Rojo
10	Positivo	35	Rojo/Gris
	Negativo	10	Gris/Rojo
11	Positivo	36	Negro/Azul
	Negativo	11	Azul/Negro
12	Positivo	37	Negro/Anaranjado
	Negativo	12	Anaranjado/Negro
13	Positivo	38	Negro/Verde
	Negativo	13	Verde/Negro
14	Positivo	39	Negro/Café
	Negativo	14	Café/Negro
15	Positivo	40	Negro/Gris
	Negativo	15	Gris/Negro
16	Positivo	41	Amarillo/Azul
	Negativo	16	Azul/Amarillo
No utilizado		42	Amarillo/Anaranjado
		17	Anaranjado/Amarillo
		43	Violeta/Gris
		08	Gris/Violeta

Segundo conector RJ21

Puerto		Pin	Cable
17	Positivo	26	Blanco/Azul
	Negativo	1	Azul/Blanco
18	Positivo	27	Blanco/Anaranjado
	Negativo	2	Anaranjado/Blanco
19	Positivo	28	Blanco/Verde
	Negativo	3	Verde/Blanco
20	Positivo	29	Blanco/Café
	Negativo	4	Café/Blanco
21	Positivo	30	Blanco/Gris
	Negativo	5	Gris/Blanco
22	Positivo	31	Rojo/Azul
	Negativo	6	Azul/Rojo
23	Positivo	32	Rojo/Anaranjado
	Negativo	7	Anaranjado/Rojo
24	Positivo	33	Rojo/Verde
	Negativo	8	Verde/Rojo
25	Positivo	34	Rojo/Café
	Negativo	9	Café/Rojo
26	Positivo	35	Rojo/Gris
	Negativo	10	Gris/Rojo
27	Positivo	36	Negro/Azul
	Negativo	11	Azul/Negro
28	Positivo	37	Negro/Anaranjado
	Negativo	12	Anaranjado/Negro
29	Positivo	38	Negro/Verde
	Negativo	13	Verde/Negro
30	Positivo	39	Negro/Café
	Negativo	14	Café/Negro
No utilizado		40	Negro/Gris
		15	Gris/Negro
		41	Amarillo/Azul
		16	Azul/Amarillo
		42	Amarillo/Anaranjado
		17	Anaranjado/Amarillo
		43	Violeta/Gris
		08	Gris/Violeta

13.12.7 Puerto BST (RJ45)

Estos puertos se encuentran en los módulos de expansión 16B y 30B de Estación digital IP500 250. Son compatibles con sistemas IP500 V2 que funcionan en IP Office versión 9.0 y superiores. Consulte Teléfonos digitales Avaya BST 41.

13.12.8 Puerto DC I/P

Este puerto está presente en todas las unidades de control y módulos de expansión de IP Office. Se utilizan para la conexión con la unidad de suministro de energía 33 incluida con la unidad de control o el módulo.

- No debe utilizarse otro tipo de unidad de suministro de energía o módulo a menos que Avaya lo indique específicamente.
- Los cables de energía no deben sujetarse a la superficie del edificio ni atravesar paredes, cielos rasos, pisos y otras aberturas similares.

13.12.9 Puertos DS (RJ45)

Estos puertos se utilizan para la conexión de un sistema de cableado estructurado RJ45 a los teléfonos digitales compatibles con el sistema IP Office. DS ports are provided by IP500 Digital Station Cards 224, Tarjetas combinadas IP500 219, Tarjetas combinadas IP500 221 y IP500 Digital Station 245 external expansion modules.

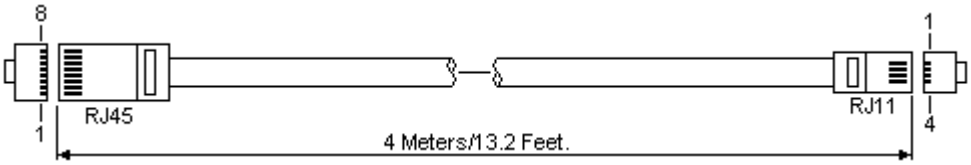
Si bien los cables RJ11 a RJ11 incluidos en la mayoría de los teléfonos DS pueden conectarse de forma directa con puertos RJ45 como los incluidos en los módulos de IP Office, esta conexión no resulta recomendable dado que no es realmente positiva y puede desconectarse.

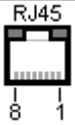
Los puertos DS en los módulos de expansión Digital Station se pueden conectar a out-of-building extensions 39. De ser este el caso, la conexión debe efectuarse con dispositivos de protección adecuados, en cada extremo y por medio de la protección principal del edificio. Además, el módulo Digital Station debe estar conectado a una tierra protectora.

Cables de línea para cableado estructurado

Se trata de un cable RJ45 a RJ11 apto para la conexión de un puerto RJ45 de un sistema de cableado estructurado a un teléfono DS. También pueden utilizarse para proporcionar extensiones telefónicas analógicas de dos hilos.

Este cable no es adecuado para efectuar conexiones entre una fuente de alimentación Avaya 1151D1/B2 y un teléfono DS con un módulo complementario EU24 o XM24. En esos casos, se deben utilizar los cables proporcionados con la unidad de la fuente de alimentación y el módulo adicional.



IP Office			Teléfono	
DS Puerto	**Pin**	**Descripción**	**Pin**	**Puerto**
	**1**	No se utiliza.	**–**	
	2	No se utiliza.	**1**	
	3	No se utiliza.	**2**	
	4	Señal 1.	**3**	
	5	Señal 2.	**4**	
	6	No se utiliza.	**5**	
	7	No se utiliza.	**6**	
	8	No se utiliza.	**–**	

- Código SAP: T700047871.

13.12.10 Puerto EF

Estos puertos se encuentran en la tarjeta base ETR6. Son puertos de troncales analógicas que solo pueden usarse cuando la tarjeta está equipada con una tarjeta auxiliar de troncales IP500. En caso de ocurrir un corte de energía, los puertos EF se conectan al puerto 12 de troncales analógicas.

13.12.11 Puerto ETR

La tarjeta base ETR6 proporciona los puertos ETR (Enhanced Tip and Ring). Se pueden utilizar para realizar la conexión entre dispositivos de teléfono analógicos DTMF y teléfonos ETR de Avaya.

- La compaginación en equipos de compaginación externos no se admite a través de puertos ETR6. No se admite a través de puertos POT.

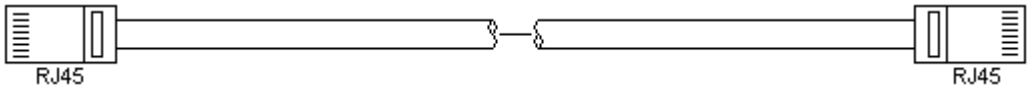
13.12.12 Puerto Expansión

Este tipo de puerto se encuentra en la parte trasera de las unidades de control IP Office y los módulos de expansión externos. Sirve para conectar los módulos de expansión externos a la unidad de control IP Office matriz.

Sólo debe utilizarse el cable de interconexión para expansiones proporcionado por Avaya para realizar estas conexiones. No debe usarse ningún otro tipo de cable.

- Cada módulo de expansión externo incluye un cable de interconexión para expansiones azul de 1 metro (3'3"). Este cable sedebe usar cuando se conecte a puertos de expansión en la parte trasera de una unidad de control.
- Al realizar la conexión con los puertos de expansión de una tarjeta IP500 4-Port Expansion card, puede utilizar el cable de interconexión para expansiones amarillo de dos metros (6'6") en vez del cable azul estándar. La tarjeta de expansión de 4 puertos IP500 contiene cuatro cables amarillos.

Cable de interconexión para expansiones
El cable de interconexión para expansiones se utiliza para conectar los puertos de expansión entre la unidad de control de IP Office y los módulos de expansión externos.



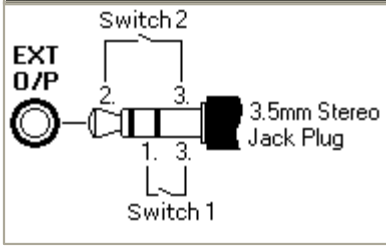
- Suministro: Todos los módulos de expansión externos incluyen normalmente un cable de este tipo.
- Código SAP: 1m (3'3") Cable azul - 700213457, 2m (6'6") Cable amarillo - 700472871.

13.12.13 Puerto EXT O/P

Estos puertos se hallan en la parte posterior de las unidades de control de IP Office. Se utilizan para la conexión con relevadores conmutadores externos. El puerto utiliza una clavija estéreo de 3.5 mm estándar para la conexión.

El sistema IP Office puede abrir (alta resistencia), cerrar (baja resistencia) o pulsar (cerrar por cinco segundos y luego abrir) los dos interruptores en el puerto. Cada interruptor puede operarse separadamente. Estos interruptores están diseñados para activar relevadores externos en sistemas como sistemas de apertura de puertas.

- **PRECAUCIÓN:**
  En instalaciones donde este puerto está conectado a un dispositivo externo al edificio, la conexión debe realizarse mediante un protector de pico MDS2 y debe haber una conexión con línea a tierra para protección en la unidad de control de IP Office. Cuando se utiliza el MDS2 en el puerto Ext O/P, utilice solo la Línea 1 y los conectores del Equipo 1. No utilice la Línea 2 ni los conectores del Equipo 2.

EXT O/P	Pin	Descripción
	1	Interruptor 1.
	2	Interruptor 2.
	3	0 Volts (Tierra/Chasís)

- Capacidad del interruptor: 0,7A.
- Voltaje máximo: 55V d.c.
- Resistencia efectiva: 0.7 ohms.
- Corriente de corto circuito: 1A.
- Capacidad de corriente de circuito inverso: 1.4A.
- Compruebe que los pins 1 y 2 llevan siempre un voltaje positivo con respecto al pin 3.

Los módulos sellados pre-construidos con frecuencia están equipados con clavijas de audio estéreo de 3.5 mm. Puede ser necesario emplear un multímetro para determinar las conexiones de cableado en una clavija disponible. Por lo general el cable de prueba es el 3 (común a ambos relevadores).

13.12.14 Puerto LAN

Estos puertos se hallan en las unidades de control de IP Office. Se utilizan para la conexión con dispositivos IP LAN e IP.

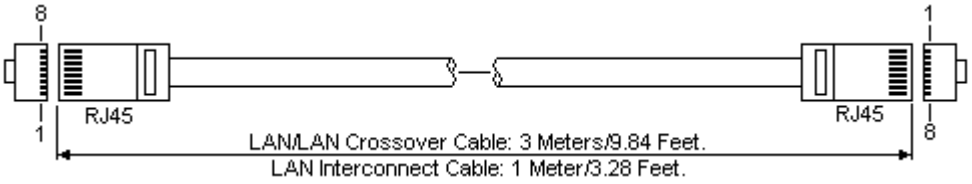
Todos los puertos LAN IP Office son puertos autosensibles de 10/100Mbps. Los puertos son cruzados MDI de detección automática, de 10/100 Mbps y dúplex completo. Forman una interruptor Ethernet capa 3 administrada.

El puerto WAN no se admite en sistemas que se ejecutan en el modo IP500 V2.

Las luces LED se usan de la siguiente manera.

- Verde: Encendido = Conectado, Parpadeando = Actividad.
- Amarillo: Encendido = 100Mbps, Apagado = 10Mbps.

Cables LAN
Se trata de cables UTP CAT5 para la conexión de distintos dispositivos IP en el sistema IP Office.



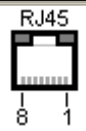
IP Office							
LAN	**Pin**	**MDIX (Normal)**	**MDI (Cruzado)**	**Cable**	**Estándar/ Interconexión**	**Cruzado**	
RJ45 8 1	1	⬅Rx-A	➡Tx-A	Blanco/ Anaranjado	1	3	RJ45 8 1
	2	⬅Rx-B	➡Tx-B	Anaranjado/ Blanco	2	6	
	3	➡Tx-A	⬅Rx-A	Blanco/Verde	3	1	
	4	No se utiliza.	No se utiliza.	Azul/Blanco	4	4	
	5	No se utiliza.	No se utiliza.	Blanco/Azul	5	5	
	6	➡Tx-B	⬅Rx-B	Verde/Blanco	6	2	
	7	No se utiliza.	No se utiliza.	Blanco/Café	7	7	
	8	No se utiliza.	No se utiliza.	Café/Blanco	8	8	

- **Código SAP:**
  - **Cable LAN - GRIS 700213481. 700213481.**
    Cable LAN directo estándar.
  - **Cable cruzado LAN - Negro 700213473. 700213473.**
    Cable cruzado LAN

13.12.15 Puerto PF

Estos puertos se encuentran en la parte trasera del módulo de expansión de línea troncal analógica 16 240. Son puertos de extensiones analógicas que pueden utilizarse en combinación con troncales analógicas de arranque por bucle durante cortes de energía en el sistema IP Office. Vea también Puertos de emergencia y para cortes de energía 50.

Todos los teléfonos conectados a estos puertos deben estar correctamente marcados como extensiones para cortes de energía y de acuerdo con los requisito legales nacionales y locales.

PF	Pin	Descripción
	1	No se utiliza.
	2	El pin 2 está conectado internamente al pin 5 vía un capacitor de timbre.
	3	No se utiliza.
	4	Negativo
	5	Tip.
	6	El pin 6 está conectado internamente al pin 5 vía un capacitor de timbre.
	7	No se utiliza.
	8	No se utiliza.

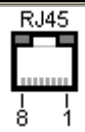
- Tamaño mínimo del cable: AWG 26.
- Longitud máxima del cable:
  - AWG26: 500m/1640'.
  - AWG24, AWG22: 1000 m/3280'.

13.12.16 Puerto PHONE (POT)

Estos puertos son puertos para extensiones analógicas. En unidades anteriores de IP Office, estos puertos estaban marcados como puertos POT en vez de puertos TELÉFONO.

Los puertos TELÉFONO en los módulos de expansión Phone V1/V2 pueden conectarse a extensiones fuera del edificio 39. De ser este el caso, la conexión debe efectuarse con dispositivos de protección adecuados (caja de protección de IP Office), en cada extremo y por medio de la protección principal del edificio. El módulo Phone debe asimismo conectarse a una conexión de tierra de protección.

Los puertos TELÉFONO de las unidades de control de IP Office no deben conectarse a extensiones fuera del edificio.

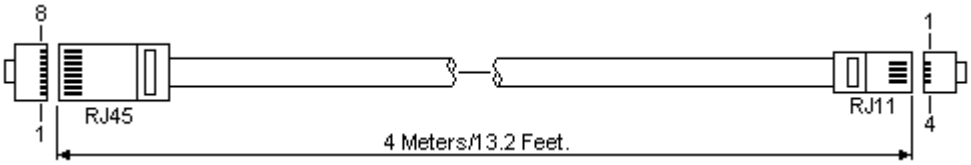
TELÉFONO	Pin	Descripción
	1	No se utiliza.
	2	No se utiliza.
	3	No se utiliza.
	4	Negativo
	5	Tip.
	6	No utilizado.
	7	No se utiliza.
	8	No se utiliza.

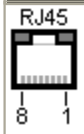
- Número REN: 2
- Corriente con teléfono descolgado: 25mA.
- Voltaje del negativo:
  - Unidad de control IP500 V2, módulos de teléfono IP500: 49V rms.
- Tamaño mínimo del cable: AWG 26.
- Longitud máxima del cable:
  - AWG26: 0,5 km / 1640 pies.
  - AWG24, AWG22: 1km./ 3280 pies.

Estos puertos no incluyen un capacitor de timbre. Por lo tanto, en los países que así lo requieran (habitualmente, Reino Unido y Nueva Zelanda), la conexión de teléfonos analógicos de 4 vías deberá realizarse mediante una toma maestra con capacitores de timbre.

Cable de línea de cableado estructurado

Este es un cable RJ45 a RJ11 adecuado para la conexión del puerto RJ45 de un sistema de cableado estructurado a un puerto DS. También pueden utilizarse para proporcionar extensiones telefónicas analógicas de dos hilos.



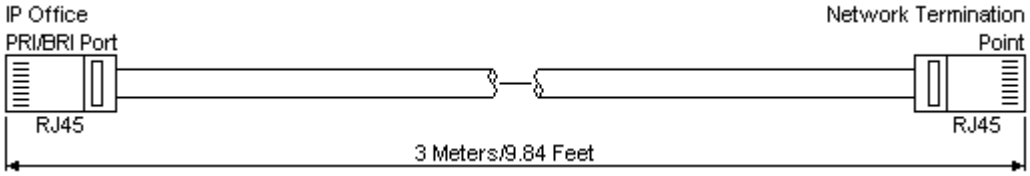
IP Office			Teléfono	
DS Puerto	Pin	Descripción	Pin	Puerto
	1	No se utiliza.	–	
	2	No se utiliza.	1	
	3	No se utiliza.	2	
	4	Señal 1.	3	
	5	Señal 2.	4	
	6	No se utiliza.	5	
	7	No se utiliza.	6	
	8	No se utiliza.	–	

13.12.17 Puerto PRI

Estos puertos se utilizan para la conexión con servicios de troncales PRI incluyendo E1, T1 y E1-R2.

Cable de troncales PRI

Este cable se utiliza para conectar de los puertos de troncales PRI de IP Office hacia el equipo de terminación de red del proveedor. Si este equipo no emplea enchufes tipo RJ45, es posible que haya que descubrir el cable y volver a cablear, o bien emplear otro tipo de cable. Las conexiones de clavija de señales y los colores de cable apropiados se describen a continuación.



IP Office			Cable	Terminación de red	
RJ45		PRI		PIN	RJ45
RJ45 8 1	1	⬅Rx-A	Blanco/Anaranjado	1	RJ45 8 1
	2	⬅Rx-B	Anaranjado/Blanco	2	
	3	–	Blanco/Verde	3	
	4	➡Tx-A	Azul/Blanco	4	
	5	➡Tx-B	Blanco/Azul	5	
	6	–	Verde/Blanco	6	
	7	–	Blanco/Café	7	
	8	–	Café/Blanco	8	

- Suministro: Las tarjetas de troncales PRI no incluyen estos cables.
- Color de cable: Rojo.
- Código SAP: 700213440.
- Longitud estándar: 3m/9'10".

13.12.18 Puerto RS232 (DTE)

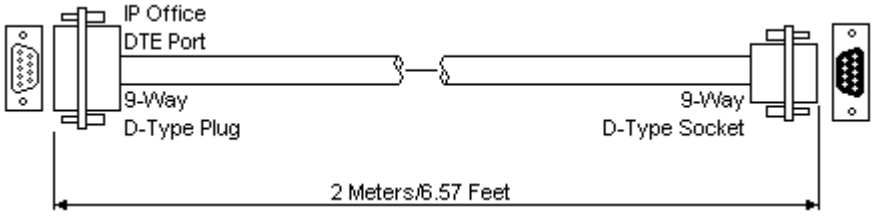
Estos puertos se hallan en la parte posterior de las unidades de control de IP Office. Los puertos similares ubicados en los módulos de expansión externos son de uso exclusivo de Avaya.

Los puertos RS232 DTE pueden usarse para diversos procesos de mantenimiento del sistema 202. Asimismo requiere un programa de terminales asíncronas, como HyperTerminal. Configúrelo para la operación mediante un puerto serial de PC, como se describe a continuación:

Bits por segundo	38,400	**Paridad**	Ninguno	**Control de flujo**	Ninguno
Bits de datos	8	**Bits de parada**	1	**Configuración | Emulación**	TTY

Cables DTE

Estos cables se utilizan para operaciones de mantenimiento y diagnóstico del sistema bajo los lineamientos de Avaya. También pueden utilizarse para conectar con un equipo con adaptador para terminal serial RS232 con la unidad de control de IP Office. El cable requerido dependerá de la unidad de control de IP Office. El cable es de tipo a "Cable serial hembra DB9 a macho DB9 directo".



Puerto DTE RS232 de 9 vías	Señal	PC/Adaptador de terminal
3	⬅ Recibir datos	3
2	➡ Transmitir datos	2
7	⬅ RTS (Petición para transmitir)	7
8	➡ CTS (Preparado para transmitir)	8
6	➡ DSR (Listo para transmitir)	6
5	⬤ Puesta a tierra	5
1	➡ DCD (Detección de portadora de datos)	1
4	⬅ DTR (Terminal de datos preparado)	4
9	➡ RI (Indicador de timbre)	9

13.13 Licencias

Esta sección abarca las licencias que se usan en los sistemas IP Office IP500 V2 que ejecutan la versión 10.0 de IP Office. No incluye detalles del uso de licencias de otros tipos de sistemas IP Office como Server Edition.

El sistema IP Office requiere licencia para algunas funciones. Consulte Licencias 294. El archivo de licencia puede cargarse manualmente o cargarse previamente en la tarjeta SD del sistema 77.

¿Cómo se le agrega una licencia al sistema?

- Se carga al sistema un archivo XML que contiene el conjunto completo de licencias PLDS. El archivo de licencia es exclusivo para el número de serie de clave de la función de la tarjeta System SD instalada en el sistema.
    - La Id. de host PLDS utilizada para el archivo de licencia debe coincidir la indicada por la **Id. PLDS** de 12 dígitos impresa en la etiqueta de la tarjeta SD. Las tarjetas más antiguas tienen un número de serie de clave de función de 10 dígitos que se muestra por **FK** o **FK SN**. Para estas tarjetas, agregue el prefijo ***11*** para obtener la Id. de PLDS.

Requerimientos mínimos de licencia

Para IP Office Essential Edition, el sistema requiere una licencia de sistema **Essential Edition** para la versión de IP Office específica que desea ejecutar.

Licencias de actualización

A partir de IP Office versión 10.0 en adelante, el archivo XML de licencia PLDS es específico para cada versión. Para que el sistema se actualice a una versión más nueva del software IP Office, se necesita un archivo de licencia nuevo específico para la versión deseada. Esto se aplica aunque el archivo contenga el mismo conjunto de licencias.

13.13.1 Licencias de edición del sistema

Estas licencias se utilizan para configurar el rango de funciones admitidas por el sistema IP Office.

- **Essential Edition:**
  Esta licencia es obligatoria para que el sistema se ejecute en el modo IP Office Essential Edition. Hasta que se introduzca, el sistema funcionará como un sistema IP Office Basic Edition.
    - Esta licencia también es un requisito previo a la licencia **Preferred Edition**.
    - Esta licencia activa el correo de voz integrado con hasta 2 conexiones simultáneas y 15 horas de almacenamiento.
- **Essential Edition Additional Voicemail Ports :**
  Esta licencia activa dos conexiones adicionales de correo de voz integrado y 5 horas adicionales de almacenamiento. Se pueden agregar distintas licencias para lograr un máximo de hasta 6 conexiones y 25 horas de almacenamiento.
- **Preferred Edition (Voicemail Pro) :**
  Esta licencia habilita la aplicación para Voicemail Pro como servidor de correo de voz de IP Office con cuatro puertos de correo de voz. La licencia **Preferred Edition** permite al servidor de correo de voz proporcionar los servicios que aparecen abajo. Para IP Office versión 8.0 y superiores, es necesarion **Essential Edition** como requisito para esta licencia en sistemas IP500 V2.
    - Buzones de correo para todos los usuarios y grupos de búsqueda.
    - Avisos para los usuarios y grupos de búsqueda.
    - Flujo de llamadas personalizable.
    - Grabación de llamadas a los buzones de correo.
    - Campañas.
    - Lectura de correo electrónico TTS para usuarios con licencias para perfiles **Mobile Worker** o **Power User**. También requiere licencias de TTS.
    - El uso de las funciones **Reunión en conferencia** funciones.
    - Acceso a la base de datos *(sólo para Voicemail Pro para Windows)*
    - Secuencias de comandos de Visual Basic *(sólo para Voicemail Pro para Windows)*

    1. Un sistema de licencias **Preferred Edition** 294 es un requisito previo para todas las licencias de perfil de usuario excepto las de **Basic User**.
        - En una Small Community Network, la **Preferred Edition** licencia del sistema central se comparte automáticamente con otros sistemas de la red, lo que activa las licencias de perfil de usuario en esos sistemas. Sin embargo, cada sistema que sea compatible con un servidor Voicemail Pro, como por ejemplo para los correos de voz distribuidos, también requiere una licencia **Preferred Edition**.

Página1630 de 3226.

2. Para un sistema IP500 V2 con una Unified Communications Module, la presencia de la tarjeta actúa automáticamente como una licencia **Preferred Edition**.

- **Sistema Branch**
  Esta licencia activa la compatibilidad con las funciones de sucursal empresarial. Estas funciones están relacionadas con el uso de un sistema IP Office como conmutador de una sucursal en una red Avaya Aura. Se necesitan licencias **de línea troncal SM** adicionales para las líneas SM configuradas entre la sucursal y Avaya Aura.

13.13.2 Licencias de actualización

Los sistemas IP Office existentes que se actualicen a la versión 10.1 de IP Office requieren una licencia de actualización de software.

- **ADVERTENCIA: Requisitos de actualización de licencia**
  En un sistema nuevo, al hacer la primera llamada el nivel de software en ejecución se escribe en la memoria permanente de la unidad de control. Cualquier actualización subsiguiente a una versión más nueva requiere la adición de la licencia **Essential Edition** para la versión de destino. Los sistemas actualizados sin dicha licencia muestran *"Sin licencia disponible"* en algunos teléfonos y no se permite ninguna función de telefonía.

- **Nota: Sistemas Server Edition**
  Las unidades de control IP500 V2 que se configuran como sistemas IP500 V2 Expansion sistema reciben licencias y actualizaciones a través de los menús de administración web de Server Edition. Consulte la documentación de Server Edition.

13.13.3 Licencias para troncales

Las siguientes licencias de troncales pueden usarse en un sistema IP500 V2.

- **IP500 Universal PRI (Canales adicionales)**
  Estas licencias sirven para habilitar canales B adicionales a los ocho básicos en una tarjeta PRI-U IP500. La tarjeta PRI-U IP500 es compatible con los modos E1, T1 y E1-R2 PRI. El sistema IP Office admite 8 canales B sin licencia en cada puerto PRI-U IP500 instalado. Los canales B adicionales, hasta donde lo permiten la capacidad de los puertos instalados y el modo PRI seleccionado, requieren la adición de licencias. Estos canales adicionales consumen licencias con base en los canales adicionales que sean configurados como en servicio, desde el puerto 9 de la ranura 1 en adelante. Los canales D no son afectados por las licencias. La licencia está disponible en versiones para 2, 8 y 22 canales, que pueden combinarse para alcanzar el total de canales necesarios.

- **Canales de línea troncal SIP**
  Estas licencias se utilizan para configurar la cantidad de llamadas simultáneas permitidas en las troncales SIP. Las licencias son consumidas por llamadas en progreso en un canal SIP. Para compatibilidad con SIP, el sistema también requiere Recursos de VCM 229. La licencia está disponible en versiones para 1, 5, 10 y 20 canales, que pueden combinarse para alcanzar el total de canales necesarios.

- **Redes de voz IP500**
  Estas licencias habilitan la compatibilidad con líneas troncales IP SCN, QSIG y H323. Para compatibilidad con redes de voz, el sistema también requiere recursos de VCM 229.

- **Canales de líneas troncales SM**
  Estas licencias se usan para habilitar líneas SM para la conexión a una red Avaya Aura. El sistema IP Office también necesita una licencia **sistema Branch**.

13.13.4 Licencias para teléfonos/terminales

Para utilizar teléfonos SIP y H323 con IP Office se requieren las siguientes licencias. Se utilizan distintas licencias para los teléfonos Avaya IP y los teléfonos de marcas distintas a Avaya, lo que incluye softphones de marcas distintas a Avaya.

Para los softphones IP, los requerimientos de licencia varían según la aplicación particular y no se tratan en esta sección. Consulte la documentación específica de la aplicación. Sin embargo, la mayoría de las aplicaciones de un softphone Avaya no requiere una licencia para terminales IP Avaya.

De forma predeterminada, cada teléfono IP que se registra en el sistema utiliza una licencia de terminal en el orden en que se van registrando los teléfonos. Sin embargo, es posible reservar una licencia para una determinada extensión a fin de garantizar que ese teléfono siempre obtenga primero una licencia si estuviera disponible. Esto se realiza mediante la configuración **Reservar licencia** de la configuración de la extensión en la configuración de sistema. Las licencias quedan liberadas cuando el teléfono registra su salida, a menos que se encuentren reservadas.

- **Advertencia**
  Los teléfonos Avaya IP sin una licencia aún pueden registrarse pero están limitados a realizar únicamente llamadas de emergencia (llamadas de código corto ***Marcar emergencia***). El usuario relacionado se trata como si hubiera cerrado sesión y el teléfono puede mostrar *"Sin licencia disponible"* y *"Llamada de emergencia únicamente".* Si hay disponible una licencia, se asigna a cualquier auricular DECT sin licencia primero y luego a cualquier otro teléfono IP Avaya sin licencia en el orden en el que los teléfonos se hayan registrado.

- **Licencia para terminales IP Avaya**
  Estas licencias se usan para autorizar otros teléfonos físicos IP Avaya. Esto incluye todos los teléfonos compatibles 1600, 9600, IP DECT, DECT R4, T3 IP Spectralink y VPN. La licencia está disponible en versiones para 1, 5 y 20 teléfonos, que pueden combinarse para alcanzar el total de teléfonos necesarios.

- **Licencia para terminales IP de terceros**
  Estas licencias se utilizan para admitir teléfonos de marcas distintas a Avaya IP, incluyendo extensiones SIP. Las licencias disponibles se utilizan en el orden de registro del teléfono. Si no hay licencias disponibles, el teléfono no puede realizar el registro. Esta licencia se llamaba anteriormente licencia **IP End-points**. La licencia está disponible en versiones para 1, 5 y 20 teléfonos, que pueden combinarse para alcanzar el total de teléfonos necesarios.

- **IP Mac Softphone**
  Esta licencia se usa para IP Office Video SoftPhone para Mac versión 4.0. El usuario también debe ser habilitado por licencias de usuario 298 **Power User** o **Teleworker.** .

13.13.5 Licencias de usuario

Las funciones disponibles para un usuario básico pueden optimizarse mediante la incorporación de licencias de usuario. Luego de que estas licencias estén presentes en la configuración del sistema, los perfiles correspondientes podrán aplicarse a los usuarios seleccionados mediante la opción **Usuario | Usuario | Perfil** de la configuración del sistema.

Tenga en cuenta que para todos los perfiles que no sean **Usuario básico**, una licencia de sistema **Preferred Edition** es un requisito previo para las licencias de usuario requeridas.

	Basic User	Empleado oficina	Teleworker	Mobile Worker	Power User
Servicios one-X Portal	–	✓	✓	–	✓
- Opciones de teletrabajo	–	–	✓	–	✓
Servicios Web UMS	–	✓	✓	–	✓
Funciones de movilidad	–	–	–	✓	✓
TTS para lectura de correo electrónico [4]	–	–	–	✓	✓
Trabajadores remotos [2]	–	–	✓	–	✓
Avaya Communicator [3]	✓[7]	✓	✓	–	✓
IP Office Video SoftPhone [5]	–	–	✓	–	✓
Colaboración web [6]	–	✓	✓	–	✓
- Programación de conferencias	–	–	–	–	✓

1. Un sistema de licencias **Preferred Edition** 294 es un requisito previo para todas las licencias de perfil de usuario excepto las de **Basic User**.
   - En una Small Community Network, la **Preferred Edition** licencia del sistema central se comparte automáticamente con otros sistemas de la red, lo que activa las licencias de perfil de usuario en esos sistemas. Sin embargo, cada sistema que sea compatible con un servidor Voicemail Pro, como por ejemplo para los correos de voz distribuidos, también requiere una licencia **Preferred Edition**.
2. La versión 8.0 admite usuarios que utilizan extensiones H323 remotas. Se admiten hasta 4 usuarios de Basic User en las extensiones remotas en el sistema. Los usuarios remotos adicionales se admiten si están autorizados o configurados para un perfil de usuario ***Teleworker*** o ***Power User***.
3. Controle que las aplicaciones one-X Portal for IP Office y Voicemail Pro también estén instaladas para funciones avanzadas.
4. TTS para lectura de correos electrónicos también requiere que el sistema de correo de voz cuente con licencia para el número necesario de sesiones simultáneas de TTS.
5. IP Office Video SoftPhone también requiere una licencia **IP Mac Softphone** para la aplicación, consulte Licencias para terminales/Teléfonos 297.
6. También requiere una licencia **Web Collaboration**.
7. Para usuarios básicos de Avaya Communicator, también requiere una licencia **Avaya Softphone** y solo recibe funciones de telefonía básicas.

Licencias de usuario

- **Licencia Teleworker**
  Estas licencias establecen el número de usuarios que pueden tener su perfil definido como ***Teleworker***. Los usuarios que cuentan con esta licencia opcional pueden acceder a valores de configuración adicionales para los siguientes servicios: one-X Portal for IP Office con la opción Telecommuter, Avaya Communicator y los servicios de web UMS. Una licencia de sistema 294 **Preferred Edition** es un requisito previo para esta licencia.
- **Licencia Mobile Worker**
  Estas licencias definen la cantidad de usuarios que pueden tener su perfil configurado como ***Mobile Worker***. Los usuarios que cuentan con esta licencia opcional pueden acceder a valores de configuración adicionales para los siguientes servicios: Funciones de movilidad y TTS para lectura de correo electrónico. Para IP Office versión 8.0 y posterior, las funciones de movilidad están habilitadas para todos los usuarios por la licencia **Essential Edition**. Una licencia de sistema 294 **Preferred Edition** es un requisito previo para esta licencia.
- **Licencia Office Worker**
  Estas licencias definen la cantidad de usuarios que pueden tener su perfil configurado como ***Office Worker***. Los usuarios que cuentan con esta licencia opcional pueden acceder a valores de configuración adicionales para los siguientes servicios: one-X Portal for IP Office (sin funciones de telecomunicación) y Servicios Web UMS. Una licencia de sistema 294 **Preferred Edition** es un requisito previo para esta licencia.

- **Licencia Power User Profile**
  Estas licencias definen la cantidad de usuarios que pueden tener un perfil configurado como ***Power User***. Para los usuarios con esta licencia opcional, se habilitan los mismos servicios adicionales que para los usuarios Teleworker y Mobile Worker. Una licencia de sistema 294 **Preferred Edition** es un requisito previo para esta licencia.

Otras licencias de usuario

Además de las licencias de perfil de usuario mencionadas, están disponibles las siguientes licencias de usuario individual:

- **Receptionist:**
  Esta licencia permite habilitar la aplicación IP Office SoftConsole. Esta licencia solo puede ser utilizada por usuarios configurados como **Recepcionist** en la configuración de IP Office. Se admite un máximo de cuatro recepcionistas. Anteriormente, esta licencia se denominaba **SoftConsole**. Cada usuario configurado como **Recepcionista** consume una instancia de esta licencia.

- **Colaboración web**
  Esta licencia se puede usar para permitir la compatibilidad con la aplicación Colaboración web 275. Se requiere una licencia por cada usuario configurado para colaboración web. Compatible con usuarios con licencia **Office Worker**, **Teleworker** o **Power User**.

13.13.6 Licencias de Voicemail Pro

Voicemail Pro se habilita mediante la adición de las siguientes licencias.

- **Preferred Edition (Voicemail Pro) :**
  Esta licencia habilita la aplicación para Voicemail Pro como servidor de correo de voz de IP Office con cuatro puertos de correo de voz. La licencia **Preferred Edition** permite al servidor de correo de voz proporcionar los servicios que aparecen abajo. Para IP Office versión 8.0 y superiores, es necesarion **Essential Edition** como requisito para esta licencia en sistemas IP500 V2.

  - Buzones de correo para todos los usuarios y grupos de búsqueda.
  - Avisos para los usuarios y grupos de búsqueda.
  - Flujo de llamadas personalizable.
  - Grabación de llamadas a los buzones de correo.
  - Campañas.
  - Lectura de correo electrónico TTS para usuarios con licencias para perfiles **Mobile Worker** o **Power User**. También requiere licencias de TTS.
  - El uso de las funciones **Reunión en conferencia** funciones.
  - Acceso a la base de datos *(sólo para Voicemail Pro para Windows)*
  - Secuencias de comandos de Visual Basic *(sólo para Voicemail Pro para Windows)*

  1. Un sistema de licencias **Preferred Edition** 294 es un requisito previo para todas las licencias de perfil de usuario excepto las de **Basic User**.
     - En una Small Community Network, la **Preferred Edition** licencia del sistema central se comparte automáticamente con otros sistemas de la red, lo que activa las licencias de perfil de usuario en esos sistemas. Sin embargo, cada sistema que sea compatible con un servidor Voicemail Pro, como por ejemplo para los correos de voz distribuidos, también requiere una licencia **Preferred Edition**.
  2. Para un sistema IP500 V2 con una Unified Communications Module, la presencia de la tarjeta actúa automáticamente como una licencia **Preferred Edition**.

- **Puertos adicionales de correo de voz Preferred Edition**
  La licencia requerida para habilitar el servidor Voicemail Pro (Preferred Edition (Voicemail Pro)) también permite habilitar cuatro puertos de correo de voz. Estas licencias se pueden usar para agregar puertos de correo de voz adicionales hasta alcanzar la capacidad máxima del sistema IP Office (en IP500 V2, 40). Esta licencia se llamaba anteriormente **Additional Voicemail Pro (puertos)**. Estas licencias están disponibles en versiones de 2, 4, 8 y 16 puertos que se pueden combinar para alcanzar el total de puertos necesarios.

- **Administradores de grabaciones VMPro:** .
  Para habilitar ContactStore en una Small Community Network, los sistemas IP Office distintos al sistema central IP Office necesitan su propia licencia.

- **Mensajes de red VMPro:**
  Habilita la funcionalidad VPNM (mensajería de red de Voicemail Pro) dentro de Voicemail Pro. Esto permite el intercambio de mensajes con sistemas Voicemail Pro remotos y los sistemas de intercambio Avaya.

- **TTS VMPro (Genérico) :**
  Esta licencia legada permite habilitar funciones de texto a voz mediante el software TTS de terceros con Voicemail Pro en un servidor de Windows. Se requiere una licencia por instancia simultánea de uso TTS. Tenga en cuenta que la licencia IP Office Advance Edition también admite 8 puertos de TTS genérico pero que solo se pueden usar con Speak Text.

- **VMPro TTS (ScanSoft):**
  Esta licencia legada permite habilitar funciones de texto a voz mediante el software TTS suministrado por Avaya con Voicemail Pro en un servidor de Windows. Se requiere una licencia por instancia simultánea de uso TTS.

- **VMPro TTS profesional:**
  Esta licencia permite habilitar las funciones de texto a voz suministradas por Voicemail Pro en un servidor basado en Linux. Se requiere una licencia por instancia simultánea de uso TTS.

- **Servicios Web UMS**
  Estas licencias sirven para habilitar los servicios de correo de voz UMS para usuarios configurados con el perfil ***Basic User***. Se habilita UMS para otros usuarios mediante la licencia de su perfil de usuario. Estas licencias también se emplean para dar licencia a los servicios de correo de voz UMS para grupos de búsqueda. Cada licencia habilita a un usuario.

13.13.7 Licencias de prueba

Se pueden solicitar licencias de prueba. Cada una es válida por 60 días a partir de su emisión; en tal sentido, se emitirá una única licencia de prueba por número de serie de tarjeta SD del sistema. Con excepción de esta restricción, la licencia de prueba funciona de la misma manera que una licencia completa.

13.13.8 Licencias CTI

- **CTI Link Pro:**
  Habilita las funcionalidades de CTI Link Pro (TAPI Link Pro y DEVLink Pro).
- **Usuario Wave:**
  Permite descargar archivos WAV en torrente con ayuda de TAPILink Pro para aplicaciones de voz de proveedores externos. Esta es una licencia por usuario. Observe que TAPI WAV requiere el uso de los canales de datos del sistema, tomados de los mismos recursos que los puertos de correo de voz. La cantidad máxima de llamadas de usuarios TAPI WAV y usuarios de correo de voz admitida de forma simultánea está determinada por el tipo de unidad de control IP Office; con IP500 V2 es de 40.

13.13.9 Otras licencias

- **Correo de voz Audix:**
  Habilita a IP Office para utilizar un sistema remoto Intuity Audix o de mensajería modular, en vez de requerir un servidor de correo de voz local.
- **Túneles IPSec:**
  Habilita al sistema IP Office para iniciar y terminar túneles IPSec y L2TP.
- **Avaya Contact Center Select**
  Esta es la licencia requerida para la compatibilidad de Avaya Contact Center Select.

13.14 Compatibilidad con hardware y software

Esta página resume los componentes de hardware y software compatibles con las diferentes versiones del software de base IP Office. Puede obtener información adicional sobre otros productos Avaya, incluidas versiones de software compatibles, en el sitio web **Matriz de compatibilidad de productos** (https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml).

- **Unidades de control** 302
- **Plataformas de servidor** 302
- **Módulos de expansión externos** 303
- **Tarjetas de base y de línea troncal** 304
- **Teléfonos** 305
- **Aplicaciones** 308

Unidades de control

Unidad de control	Código de material	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
Small Office Edition	–	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
IP403	700350382	–	–	–	–	–	–	–	–	–	–	–	–	–
IP406 V1	700210776	–	–	–	–	–	–	–	–	–	–	–	–	–
IP406 V2	700359946	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]		–	–	–	–	–	–	–
IP412	700350408	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
IP500 (version 1)	700417207	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP500 V2	700476005	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. Para que una unidad de control IP406 V2 ejecute el software IP Office versión 4.0 o posterior hasta IP Office versión 6.1, la unidad de control debe ser PCS 8 o posterior.

Plataformas de servidor

Plataforma de servidor	Código de material	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
DL120G7 SRVR IPO R8+	269810	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
DL120G7 SRVR IPO R8+ FRANCE TELECOM	270391	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
DL120G7 SRVR IPO R8.1 + SE EXP	270395	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
R210 II XL SERVER IP OFFICE UNIFIED COMMUNICATIONS	302786	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
R210 II XL SERVER IP OFFICE FRANCE TELECOM	302787	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
R210 II XL SERVER IP OFFICE SERVER EDITION EXPANSION	302788	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓
R210 II XL SERVER IP OFFICE CONTACT CENTER SERVER	306626	–	–	–	–	–	–	–	–	–	–	✓	✓	✓
R220 II XL SERVER IP OFFICE UNIFIED COMMUNICATIONS	380223	–	–	–	–	–	–	–	–	–	–	✓	✓	✓
R220 II XL SERVER IP OFFICE FRANCE TELECOM	380224	–	–	–	–	–	–	–	–	–	–	✓	✓	✓
R220 II XL SERVER IP OFFICE SERVER EDITION EXPANSION	380225	–	–	–	–	–	–	–	–	–	–	✓	✓	✓
R220 II XL SERVER IP OFFICE CONTACT CENTRE	380226	–	–	–	–	–	–	–	–	–	–	✓	✓	✓
DL360G7 SRVR IPO R8.1 + PRIMARY	270393	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓

Plataforma de servidor	Código de material	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
R620 SRVR IPO SE PRIMARY	306961	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓
R630 SRVR IPO SE/UC	383542										✓	✓	✓	✓
R630 SRVR IPOCC	383555										✓	✓	✓	✓

Módulos de expansión externos

Módulo	Código de material	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
IP400 ATM16[3]	700211360	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 DS16	700184807	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP400 DS30	700184880	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP400 DS16 V2[3]	700359839	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 DS30 V2[3]	700359847	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 Phone 8	700184773	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP400 Phone 16	700184781	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP400 Phone 30	700184799	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP400 Phone 8	700359896	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP400 Phone 16 V2[3]	700359904	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 Phone 30 V2[3]	700359912	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 So8	700185077	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP400 WAN3[1]	–	–	–	–	–	–	–	–	–	–	–	–	–	–
IP400 WAN3 10/100[1]	700262009	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
IP500 ATM16[2]	700449473	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 So8	700449515	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS16	700449499	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS30	700426216	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS16A (RJ21)	700500699	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
IP500 DS30A (RJ21)	700500698	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
IP500 DS16B	700501585	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
IP500 DS30B	700501586	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
IP500 DS16B2	700511093	–	–	–	–	–	–	–	–	–	–	–	–	✓
IP500 DS30B2	700511094	–	–	–	–	–	–	–	–	–	–	–	–	✓
IP500 Phone 16 V2	700449507	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Phone 30 V2	700426224	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. No admitido en los sistemas IP500 e IP500 V2.
2. Solo en América del Norte, a menos que se acepte en un país de destino.
3. Las variantes IP400 todavía son compatibles en IP Office versión 9.1 y posterior.

Base y tarjetas

Tarjetas base	Código de material	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
IP500 Phone 2	700431778	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Phone 8	700417231	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Digital Station 8	700417330	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Card Carrier[6]	700417215	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
IP500 VCM 32[6]	700417389	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 VCM 64[6]	700417397	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 VCM 32 V2[6]	700504031	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
IP500 VCM 64 V2[6]	700504031	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
IP500 4-Port Expansion[6]	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 ETR6[1][2]	700476039	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 ATM4 Combo Card[1]	700476013	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
" PCS04 310 and higher[5]	700476013	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
IP500 ATM4 Combo Card V2[1]	700504556	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
IP500 BRI Combo Card BRI[1]	700476021	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 TCM 8[1]	700500758	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Unified Communications Module v1[1][6]	700501442	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Unified Communications Module v2[1][6]	700507449	–	–	–	–	–	–	–	–	–	–	✓	✓	✓

Tarjetas de línea troncal	Código de material	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
IP500 Alog Trunk Card	700417405	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
" PCS10 310 and higher[4]	700417405	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Alog Trunk Card V2[1][3]	700503164	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
IP500 BRI 4 Trunk Card	700417413	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 BRI 8 Trunk Card	700417421	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 PRI-1U	700417439	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 PRI-2U	700417462	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 T1(J) PRI Dual	700509377	–	–	–	–	–	–	–	–	–	–	✓	✓	✓

1. solo sistemas IP500 V2.
2. solo se admite en los modos IP Office Basic Edition - modo PARTNER® o IP Office Basic Edition (U-Law) que funcionan en una región de Norteamérica.
3. Compatible con 8.1 Feature Pack 1 y posteriores.
4. Estas tarjetas son compatibles con IP Office versión 4.0 y posteriores. No obstante, las tarjetas PCS10 y posteriores solo son compatibles con sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) ú 8.0 y posteriores. Consulte el Consejo técnico de Avaya IP Office 237.
5. Estas tarjetas son compatibles con IP Office versión 6.0 y posteriores. No obstante, las tarjetas PCS04 y posteriores solo son compatibles con sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) ú 8.0 y posteriores. Consulte el Consejo técnico de Avaya IP Office 237.
6. No compatible con sistemas en modo IP Office Basic Edition.

Teléfonos

Serie 1000

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
1010	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
1040	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Serie 1100/1200

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
1120E	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
1140E	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
1220	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
1230	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Serie 1400

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
1403	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1408	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1416	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 1600

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
1603[1]	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603-I	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603SW	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603SW-I	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1608[1]	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1608-I	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1616[1]	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1616-I	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. 4.2 T4 2008+.

Serie 2400

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
2402D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2410D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2420	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 3600

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
3616	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3620	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3626	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3641	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3645	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 3700

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
3701	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3711	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3720	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3725	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3730													✓
3735													✓
3740	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
3745	–	–	–	–	–	–	–	–	–	–	–	✓	✓
3749	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓

Página1641 de 3226.

Serie 3800/3900

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
3810	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3910	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
3920	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

Serie 4100

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
4135	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
4136	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
4145	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
4145EX	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
4146	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
4146EX	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓

Serie 4400

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
4406D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
4412D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
4424D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Serie 4600

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
4601	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
4602IP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
4602SW	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
4606	–	–	–	–	–	–	–	–	–	–	–	–	–
4610SW	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
4612	–	–	–	–	–	–	–	–	–	–	–	–	–
4620	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
4621	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
4624	–	–	–	–	–	–	–	–	–	–	–	–	–
4625	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Serie 5400

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
5402	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
5410	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
5420	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Serie 6400

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
6408D	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
6416D0	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
6424D	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–

Serie 5600

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
5601	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
5602IP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
5602SW	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
5610SW	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
5620	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
5621	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Serie 7400

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
7420	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
7430	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
7434	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
7439	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
7440	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
7444	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
7449	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓

Serie 9500

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
9504	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9508	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓

Serie 9600

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
9608	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
9611	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
9620L	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
9620C	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
9621G	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
9630G	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
9640	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
9640G	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
9641G	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
9650	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
9650C	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. Versión 8.0 2012 Q1 service pack y versiones posteriores.

Serie B100

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
B149	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
B159	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
B169	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
B179	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓

Serie D100

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
D160	–	–	–	–	–	–	–	–	✓[1]	✓	✓	✓	✓

1. Compatible con 8.1 Feature Pack 1 y posteriores.

Serie E100

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
E129	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓
E169	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓

Serie H100

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
H175	–	–	–	–	–	–	–	–	–	–	–	✓	✓

Serie J100

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
J129	–	–	–	–	–	–	–	–	–	–	–	✓	✓

1. Compatible desde R10 SP2.

Serie M

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
M7100	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
M7100N	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
M7208	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
M7208N	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
M7310	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
M7310N	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
M7324	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
M7324N	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓

Serie T

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
T7000	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
T7100	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
T7208	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
T7316	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
T7316E	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
T7406	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
T7406E	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
ACU	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓

Series T3/T3IP

Teléfono	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
T3 Compact	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T3 Classic	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T3 Comfort	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T3 IP Compact	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T3 IP Classic	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T3 IP Comfort	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Aplicaciones IP Office

Aplicación	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
Registros de detalle de llamada (CDR)	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Centro de conferencias	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Compact Business Center	✓	✓	–	–	–	–	–	–	–	–	–	–	–
Contact Recorder	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
ContactStore	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
Customer Call Reporter	–	–	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Compact Contact Center	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Data Migration Manager	–	–	–	–	–	–	✓	✓	✓	✓	–	–	–
Servidor Delta	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Avaya Communicator	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
IP Office Contact Center	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓
Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MS-CRM	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Phone Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
- Pro	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
- Pro Softphone	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
one-X Mobile Preferred	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
one-X Portal	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
- Call Assistant	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
- Plug-in Lync	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓
- Plug-in de Outlook	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
- Plug-In de Salesforce	–	–	–	–	–	–	–	✓	✓	✓	✓	–	–
Outbound Call Express	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓

Aplicación	4.0	4.1	4.2	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1
SoftConsole	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
System Status Application	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
System Monitor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TAPI Link Lite	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TAPI Link Pro	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mensajería integrada	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Video Softphone (Mac)	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
- (Windows)	–	–	–	–	✓	✓	✓	✓	✓	✓	✓	–	–
Voicemail Lite	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
VoiceMail Pro	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Conferencias web	–	–	–	–	–	–	–	–	–	–	✓	✓	✓

13.15 Niveles PCS

Cada elemento del hardware de IP Office tiene un nivel de Estado de cambio del producto (PCS). Por lo general, éste figura en la etiqueta en el prefijo del hardware con **PCS**.

El nivel de PCS aumenta cada vez que se realiza un cambio a los componentes de ese hardware específico. Por ejemplo, el nivel de PCS puede aumentar cuando reemplace un componente por otro de un proveedor distinto.

Por lo general, los cambios en un nivel de PCS no son importantes y los elementos del mismo hardware pero con distintos niveles de PCS siguen siendo idénticos en su funcionamiento y se pueden intercambiar. Sin embargo, existen algunas excepciones que señalamos a continuación.

Restricciones del nivel de PCS

- **Tarjeta de troncales analógicas IP500 V1**
  Estas tarjetas son compatibles con IP Office versión 4.0 y posteriores. No obstante, las tarjetas PCS10 y posteriores solo son compatibles con sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) ú 8.0 y posteriores. Consulte el Consejo técnico de Avaya IP Office 237.
- **Tarjeta combinada ATM4 IP500 V1**
  Estas tarjetas son compatibles con IP Office versión 6.0 y posteriores. No obstante, las tarjetas PCS04 y posteriores solo son compatibles con sistemas que ejecutan IP Office versión 6.1(20), 7.0(12) ú 8.0 y posteriores. Consulte el Consejo técnico de Avaya IP Office 237.
- **Unidad de control IP500 V2**
  Para tener compatibilidad con la versión 9.1 de IP Office o posterior, las unidades PCS 14 o anterior debe instalar primero la versión 8.1 (65) (o superior a 8.1) o cualquier versión 9.0 y luego actualizar a la versión 9.1 o superior. Debe tomarse la precaución de asegurarse de que no se hagan llamadas antes de la actualización final, de lo contrario el sistema requerirá una licencia de actualización.

13.16 TAA

Aquellos elementos etiquetados como TAA, satisfacen los requisitos de Trade Agreements Act, estos son un requisito previo para las compras federales en los Estados Unidos de América. A menos que se especifique lo contrario, las variantes TAA del equipo son física y funcionalmente iguales a las variantes no TAA.

		Código SAP
Unidad de control	**IPO IP500 V2 CNTRL UNIT TAA** 209	700501510
Tarjetas base	**IPO IP500 EXTN CARD DGTL STA 8 TAA** 224	700501512
	TARJETA COMBINADA ATM IPO IP500 V2, VERSIÓN TAA 219	700501513
	IPO IP500 VCM 32 TAA 229	700501518
	IPO IP500 VCM 32 TAA V2 229	700504033
Tarjetas auxiliares de troncales	**TRONCAL IPO IP500 BRI 4 UNI TAA** 235	700501515
	TRONCAL IPO IP500 PRI UNVRSL SNGL TAA 236	700501514
	IPO IP500 TRNK PRI UNVRSL DUAL TAA 236	700501517
Módulos de expansión externos	**IPO IP500 EXP MOD ANLG TRNK 16 TAA** 240	700501511
	IPO IP500 EXP MOD DGTL STA 16 TAA 245	700501516
Teléfonos	**Teléfono de escritorio IP 9608 TAA universal**	700501428, 700507947
	Teléfono de escritorio IP 9608G TAA universal	700507946
	Teléfono de escritorio IP 9611G TAA universal	700501429, 700507948
	Teléfono de escritorio IP 9621G TAA universal	700500254, 700506516
	Teléfono de escritorio IP 9641G TAA universal	700501431, 700506519

Capítulo 14.
Declaraciones de seguridad

14. Declaraciones de seguridad

Los módulos Avaya IP500 Office están diseñados para ser instalados por "Personal de Servicio" y es responsabilidad del Personal de servicio comprobar que todos los equipos subsidiarios interconectados estén cableados correctamente y que cumplan con los requerimientos de seguridad de IEC60950 o UL60950 cuando esto es aplicable.

- CE
  La marca CE adherida a este equipo significa que el módulo cumple con las directivas 1999/5/EC (R&TTE), 89/336/EEC (EMC) y 72/23EEC (LVD).
- Las Declaraciones de Conformidad (DoC) de los productos IP500 se encuentran disponibles en el DVD de aplicaciones IP Office.
- ⚠ Este símbolo de advertencia se encuentra en la base de los módulos IP500.
- Consulte la sección Módulos de interfaz de troncales 313 para más información sobre las variantes de módulos de interfaz de troncales correctos para cada país.

En Finlandia, Noruega y Suecia es necesario conectar un conductor de tierra de protección al punto de tierra de protección en la parte trasera de las unidades de control IP500 V2. Consulte la sección Puesta a tierra 90 Información adicional. Además, el Servidor debe estar localizado en una ubicación de acceso restringido, en donde se haya aplicado unión equipotencial, por ejemplo, en un centro de telecomunicaciones.

14.1 Protección contra rayos/símbolos de peligro

Protectores contra rayos

Debe verificarse los protectores contra rayos del edificio como sigue:

1. Verifique los protectores contra rayos en el punto de entrada del cable de troncales al edificio que aloja el sistema Avaya IP Office, prestando especial atención a la puesta a tierra de protección contra rayos. Informe sobre cualquier problema por escrito a la empresa telefónica.
2. Los equipos diseñados para conectarse mediante cableado interno por lo general no están equipados con protección contra rayos. Por lo tanto, los cables para extensión de Avaya IP Office no deben abandonar el edificio. En instalaciones donde existen teléfonos y/o otros dispositivos estándar (positivo/negativo) instalados en otro edificio, es necesario incluir protección contra rayos (consulte la sección Instalaciones telefónicas fuera del edificio 39).

Símbolo de peligro

El símbolo de peligro de choque eléctrico está diseñado para alertar al personal de riesgos de tipo eléctrico o de daños al equipo. Deben observarse las siguientes precauciones adicionales al instalar equipos telefónicos:

1. Nunca instale cableado de teléfono durante una tormenta eléctrica.
2. Nunca instale los enchufes de teléfono en lugares húmedos, a menos que el enchufe esté especialmente diseñado para ubicaciones de este tipo.
3. Nunca toque los cables o terminales de teléfono sin aislar, a menos que la línea de teléfono esté desconectada de la interfaz de red.
4. Tenga siempre precaución cuando trabaja con líneas telefónicas.

14.2 Módulos de interfaz de troncales

A fin de asegurar la validación de las autorizaciones, sólo deben equiparse los siguientes tipos de tarjetas de interfaz de troncales en las siguientes unidades de control de IP Office.

EUA/Canadá						
Producto	Quad BRI	PRI E1		PRI T1		Tarjeta de troncales analógicas
		Individual	Dual	Individual	Dual	
IP500 V2	✗	✗	✗	✓	✓	✓
IP500	✗	✗	✗	✓	✓	✓

Resto del mundo						
Producto	Quad BRI	PRI E1/E1R2		PRI T1		Tarjeta de troncales analógicas
		Individual	Dual	Individual	Dual	
IP500 V2	✓	✓	✓	✗	✗	✓
IP500	✓	✓	✓	✗	✗	✓

Notas

- Las troncales E1R2 sólo se admiten en CALA y en Corea.

14.3 Información adicional y actualizaciones de productos

Puede obtener información adicional, incluyendo las actualizaciones a Manuales de Productos y de Referencia, de los Vendedores y Distribuidores de Avaya o de su sitio web en: http://www.avaya.com.

Puede obtener asimismo esta guía en el sitio Web de soporte de Avaya: http://support.avaya.com.

Números de teléfono de soporte técnico
Para obtener ayuda y soporte técnico iniciales, contacte a su distribuidor o proveedor. Los siguientes puntos de contacto están disponibles para los asociados autorizados de Avaya.

- Únicamente en Estados Unidos,
  Avaya ofrece una línea de Ayuda al Cliente 24 horas al día sin costo:
  - Nombre: Organización de Soporte Técnico Avaya (TSO)
  - Línea de ayuda al cliente: 1 800 628-2888
  - Dirección: 8744 Lucent Blvd., Highlands Ranch, Colorado, 80129 USA
  - URL: http://support.avaya.com
    Si requiere asistencia durante la instalación, programación o el uso de su sistema, llame a la Línea de Ayuda o a su representante de Avaya. Es posible que apliquen cargos por consulta.

- Fuera de EUA
  Si requiere asistencia durante la instalación, programación o el uso de su sistema, contacte a su representante de Avaya.
  - URL: http://support.avaya.com

14.4 Clasificación de seguridad de los puertos

Los sistemas Avaya IP Office tienen los siguientes puertos, clasificados como sigue:

Nombre de puerto	Descripción de puerto	Clasificación de puerto
Puerto PRI	Conexión ISDN PRI (NET)	TNV (Operando dentro de los límites de SELV)
Puertos BRI	Conexión ISDN BRI (NET)	TNV (Operando dentro de los límites de SELV)
Puertos analógico	Dos troncales analógicas de dos hilos	TNV3
Puertos para cortes de energía	Dos troncales analógicas de dos hilos	TNV3
Puerto RS232 DTE	Conexión con Async Data.	SELV
Puertos de teléfono analógico	Puertos de extensión telefónica	TNV2
Puertos de teléfono digital	Puertos de extensión telefónica	SELV
Puertos LAN	Complemento 10/100 BaseT para LAN.	SELV
Puertos de expansiones	Conector del módulo de expansión	SELV
Puerto Audio	Conector para la música de espera	SELV
Puerto de control externo	Conector para los circuitos de Control auxiliar.	SELV
Puerto de entrada de la corriente DC.	Conector para la corriente DC de entrada.	SELV

Deben seleccionarse los circuitos de interconexiones para que proporcionen un cumplimiento continuado con los requerimientos de la cláusula 2.3 de EN 609050:1992/A3:1995 para los circuitos SELV y con los requerimientos para la cláusula 6 sobre circuitos TNV, después de realizar las conexiones entre equipos.

14.5 Directiva EMC

889/336/ CE (Directiva CE) CISPR 22:1993 incluyendo A1 + A2, AS/NZ 3548:1995 (ROW)

- ⚠ **PRECAUCIÓN**
  Este es un producto clase A. En un entorno doméstico, el producto puede provocar interferencia de radio, en cuyo caso puede requerirse que el usuario tome las medidas adecuadas.

Comisión Federal de Comunicaciones (FCC)

Este equipo ha sido sometido a pruebas y cumple con los límites descritos para los dispositivos digitales Clase A, en lineamiento con la Parte 15 del Reglamento FCC. Estos límites se han diseñado para proporcionar una protección razonable contra interferencias perjudiciales durante la operación del equipo dentro de un entorno comercial. Este equipo genera, utiliza, e irradia energía en forma de frecuencias de radio y puede ocasionar interferencia de radio perjudicial a las comunicaciones por radio de no ser instalado de acuerdo con el manual de instrucciones. La operación de este equipo en áreas residenciales probablemente provocará interferencias perjudiciales, en cuyo caso se solicitará al usuario que corrija esta interferencia por su cuenta.

Departamento de Comunicaciones de Canadá (DOC)

NOTIFICACIÓN: Este equipo cumple con las Especificaciones Técnicas para Equipos Terminales de Industry Canada aplicables. Esto lo confirma el número de registro. La abreviatura IC que precede al número de registro significa que este registro se realizó con base en una Declaración de Conformidad indicando que se cumplieron las especificaciones técnicas estipuladas por Industry Canada. Lo anterior no implica que Industry Canada ha autorizado el equipo.

Precauciones de CE para China

警示

注意：此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。仅适用于商业或工业环境。

14.6 Instrucciones regulatorias para su uso

14.6.1 Australia

Conexiones
La conexión de los productos IP Office debe realizarse mediante un módulo de aislamiento de línea con una etiqueta que certifique su cumplimiento con las leyes de telecomunicaciones.

Interfaz BRI
Durante la configuración, compruebe que el número de emergencia "000" no está restringido realizando los pasos siguientes:

- Código corto: 000
- No. de teléfono: 000;
- Función: MarcarEmergencia

En las conexiones a TS013, no deben utilizarse las siguientes Capacidades de portadora:

- Audio, Video, Información digital restringida 7kHz.

Si se utiliza un tipo de número desconocido en el número de la partida que llama, la red utilizará el CLI determinado.

El sistema debe estar configurado para conexiones punto a punto múltiple, a fin de cumplir con los requerimientos de Austel para la conexión de circuitos TS013.

Dado que el sistema de IP Office no admite la marcación de emergencia después de haber perdido potencial, debe reconocerse la siguiente notificación de advertencia:

- **PRECAUCIÓN**
  Este equipo es inoperable cuando hay un corte de la energía central.

Interfaz PRI
Durante la configuración, compruebe que el número de emergencia "000" no está restringido realizando los pasos siguientes:

- Código corto: 000
- No. de teléfono: 000;
- Función: MarcarEmergencia

- **PRECAUCIÓN**
  Este equipo es inoperable cuando hay un corte de la energía central.

14.6.2 Canadá

Este equipo está en cumplimiento con las Especificaciones Técnicas para Equipos Terminales de Industry Canada. Esto lo confirma el número de registro. La abreviatura IC que precede al número de registro significa que este registro se realizó con base en una Declaración de Conformidad indicando que se cumplieron las especificaciones técnicas estipuladas por Industry Canada.

Esto no implica que Industry Canada ha autorizado el equipo.

NOTIFICACIÓN: El Número de equivalencia de timbre (REN) de este equipo terminal es 1. El REN asignado a cada equipo de terminal proporciona una indicación de la cantidad máxima de terminales que pueden ser conectadas a una interfaz de teléfono. La terminación de una interfaz puede consistir de cualquier combinación de dispositivos, con el único requisito que la suma de sus Números de equivalencia de timbre no sobrepase cinco.

14.6.3 China

AVAYA

700433220
February 2007
Copyright© 2007, Avaya Inc. All Rights Reserved

所有在中华人民共和国境内进口或销售的电子信息产品必须附上本文件

Include this document with all Electronic Information Products imported or sold in the People's Republic of China

部件名称 (Part Name)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 (Metal Parts)	×	○	○	○	○	○
电路模块 (Circuit Modules)	×	○	○	○	○	○
电缆及电缆组件 (Cables & Cable Assemblies)	×	○	○	○	○	○
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	○
电路开关/断路器 (Circuit Switch/Breakers)	○	○	○	○	○	○
电源组件 (Power Assemblies)	×	○	○	○	○	○
显示器 (LCD, Monitor)	○	○	○	○	○	○
玻璃 (Glass)	○	○	○	○	○	○

○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363 2006 标准规定的限量要求以下。
Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363 2006 standard.

×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363 2006 标准规定的限量要求。
Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363 2006 standard.

本表显示，所附的亚美亚电子信息产品中，从生产日期起，可能包含这些物质。注意：所附产品可能包含或不含以上所列的某些组件。
This table shows where these substances may be found in Avaya's electronic information products, as of the date of manufacture of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

除非有另外特别的标注,此标志将作为所附产品及零部件的环保使用期标志. 某些产品会有一个不同的环保使用期(例如,电话机)并贴在其产品上.此环保使用期限只适用于产品在产品手册中所规定的条件下使用

The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain products have a different EFUP (for example, telephones) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

14.6.4 Japón

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるように要求されることがあります

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取扱をして下さい

14.6.5 Unión Europea

1. No deben restringirse las llamadas a los números 999 y 112. Esto invalidará la autorización.
2. Todas las conexiones al MDF deben estar identificadas mediante etiquetas apropiadas.
3. La marca de CE sobre el equipo de IP Office indica el cumplimiento del sistema con las directivas, reglas y normas técnicas de EMC, LVD, g R&TTE para ISDN de tasa primaria y tasa básica.
4. Todos los puertos para conexiones de dispositivos distintos a telecomunicaciones tienen un estado de seguridad de extra bajo voltaje (SELV).

CE Declaraciones de conformidad de la Unión Europea

Avaya Inc. declara que el equipo especificado en este documento y que lleva la marca "CE" (Conformité Europeénne) se ajusta a la Directiva de la Unión Europea sobre equipos radioeléctricos y equipos terminales de telecomunicación (1999/5/CE), incluida la Directiva de compatibilidad electromagnética (2004/108/CE) y la Directiva sobre baja tensión (2006/95/CE).

Puede comunicarse con el representante de ventas local para obtener copias de estas declaraciones de conformidad (DoC), que están disponibles en el siguiente sitio web: http://support.avaya.com/DoC.

Directiva de la Unión Europea sobre baterías

Avaya Inc. respalda la Directiva sobre baterías 2006/66/CE de la Unión Europea. Determinados productos de Avaya Inc. poseen baterías de litio. Estas baterías no pueden ser reemplazadas por el cliente ni en campo. No las desarme. Las baterías pueden ser peligrosas si se las manipula incorrectamente.

14.6.6 Nueva Zelanda

El certificación Telepermit sobre cualquier equipo de terminal indica solamente que Telecom ha aceptado que el producto cumple con las condiciones mínimas para la conexión con su red. No indica una recomendación del producto por parte de Telecom, ni proporciona ningún tipo de garantía. Por sobre todo, no ofrece seguridad alguna de que el producto operará correctamente en todos los aspectos en conjunto con otros equipos con certificación Telepermit, otras marcas o modelos, ni implica que el productos es compatible con todos los servicios de la red de Telecom.

14.6.7 Notificación de la FCC

Este equipo cumple con la Parte 68 del reglamento de la FCC y los requerimientos adoptados por el Consejo Administrador de Dispositivos Terminales (ACTA). En la parte trasera de los equipos se encuentra una etiqueta que contiene, entre otros datos, un identificador del producto con el formato US:AAAEQ##TXXX. Debe proporcionar este número a la compañía telefónica, si ésta lo solicita.

El REN se utiliza para determinar la cantidad dispositivos que pueden conectarse a la línea telefónica. Una cantidad excesiva de números REN en una línea telefónica puede resultar en que los dispositivos no timbren en respuesta a una llamada entrante. En la mayoría de las áreas, pero no en todas, la suma de todos los REN no debe ser mayor a 5.0. Para conocer con seguridad la cantidad de dispositivos que pueden contactarse a una línea según lo determina la cantidad de números REN totales, contacte a la compañía telefónica local. En productos autorizados después del 23 de julio de 2001, el número REN de estos productos forma parte del identificador de producto con el formato US:AAAEQ##TXXX. Los dígitos representados con ## son el REN sin el número decimal (por ejemplo, 03 es un REN de 0.3). En productos anteriores, el REN aparece sobre la etiqueta en un número separado.

Medio de conexión

La siguiente tabla muestra la conexión de este equipo a la red telefónica.

Puerto	FIC	SOC	Enchufe USOC	REN
IP500 PRI 1U, IP500 PRI2U	04DU9.BN, 04DU9. DN, 04DU9.IKN, 04DU9. ISN	6.0Y	RJ48C	NA
IP500 ATM4U	OL13A, OL13B, OL13C, 02AC2, 02LA2, 02LB2, 02LC2, 02LR2, 02LS2	9.0Y	RJ45S	0,1B
IP500 ATM16	OL13A, OL13B, OL13C, 02AC2, 02GS2, 02LA2, 02LB2, 02LC2, 02LR2, 02LF2 02GS2, 02LS2	9.0Y	RJ45S	0,1B

Si este equipo provoca daños a la red telefónica, la compañía telefónica le notificará con anticipación que es posible que sea necesario descontinuar temporalmente el servicio. En caso que una notificación anticipada no sea una alternativa válida, la compañía telefónica notificará al cliente lo antes posible. También se le notificará de su derecho a presentar una queja con la FCC si lo considera necesario.

La compañía telefónica puede realizar cambios en sus instalaciones, equipos, operaciones y procedimientos que pudieran afectar el funcionamiento de los equipos. De ocurrir esto, la compañía telefónica deberá enviar una notificación por adelantado a fin de que pueda hacer las modificaciones necesarias para mantener un servicio ininterrumpido.

En caso de experimentar problemas con este equipo, contacte el Centro de Servicio Técnico al -800-242- 2121 o contacte a su representante local de Avaya. Si el equipo provoca daños a la red telefónica, la compañía telefónica puede solicitarle que desconecte el equipo hasta resolver el problema.

El enchufe y clavija empleados para conectar este equipo al cableado de las instalaciones y la red telefónica deben cumplir con las reglas aplicables de la Parte 68 de la FCC, así como los requerimientos estipulados por el ACTA.

La conexión al servicio de líneas colectivas está sujeta a las tarifas estatales. Contacte a la comisión estatal de servicios públicos, la comisión de servicios públicos o a la comisión corporativa para obtener más información.

Equipos con Marcación Entrante Directa ("DID"):

Permitir que este equipo opere de tal forma que no proporcione la correcta supervisión de respuesta es una infracción de la Parte 68 del reglamento de la 'FCC.

La correcta supervisión de respuesta ocurre cuando:

A. El equipo devuelve supervisión de respuesta a la red telefónica de conmutador público (PSTN) cuando las llamadas DID son:
   - respondidas por la estación a la que se marcó,
   - respondida por la operadora,
   - enrutadas hacia un anuncio grabado que puede ser administrado por el usuario del equipo en las instalaciones del cliente (CPE).
   - Enrutamiento hacia un tono de marcar

B. El equipo devuelve señales de supervisión de respuesta para todas las llamadas (DID) desviadas de vuelta a la PSTN.
   Algunas excepciones permitidas son:
   - La llamada no es respondida.
   - Se recibe tono de ocupado.
   - Se recibe un torno de reordenar.

Avaya certifica que su equipo registrado es capaz de proporcionar a los usuarios acceso a proveedores y servicios de operadora interestatales mediante el uso de códigos de acceso. La modificación de estos equipos mediante agregadores de llamadas para bloqueado los códigos de marcación de accesos es una infracción de la Ley de consumidores de operadores telefónicos de 1990.

Marcadores automáticos:

Cuando programe números de emergencia y (o) realice llamadas de prueba a números de emergencia:

1. Permanezca en la línea y explique brevemente al operador la razón de su llamada.
2. Realice estas actividades en horas de baja demanda, como temprano por la mañana o a primera hora de la noche.

Equipos de restricción de tarifas y de enrutamiento de costo mínimo:

Es necesario actualizar el software contenido en este equipo para permitir acceso a la red para reconocer los códigos de área establecidos recientemente e intercambiar estos códigos conforme entran en servicio.

De no realizarse las actualizaciones en los sistemas de las instalaciones o el equipo periférico para que puedan reconocer los nuevos códigos conforme estos se establecen ocasionará restricciones al cliente e impedirá a sus empleados'el acceso a la red para obtener estos códigos.

Declaraciones de conformidad con la Parte 68 de la FCC 'por parte del proveedor

Avaya Inc. en Estados Unidos de América certifica por el presente que los equipos descritos en este documentos y con número de identificación TIA TSB-168 cumplen con las reglas y normas 'de la FCC, 47 CFR Parte 68, así como los criterios técnicos adoptados por el Consejo Administrador de Dispositivos Terminales (ACTA).

Avaya asimismo asevera que el equipo terminal equipado con auricular Avaya descrito en este documento está en cumplimiento con el Párrafo 68.316 de las reglas y normas de la FCC en cuanto a la Compatibilidad con Prótesis Auditivas, por lo que se le considera compatible con prótesis auditivas.

14.6.8 Cumplimiento de las normas de la FCC

Transmisión y recepción de la configuración de ganancia para puertos PRI/T1 y analógicos

La configuración de Ganancia está controlada por contraseña y sólo debe modificarla personal de instalación calificada, sin estar disponible al usuario final. Una configuración de ganancia predeterminada de 0dB asegura el cumplimiento con la parte 68 sección 68.308(b)(5) del reglamento de la FCC y la Sección 4.5.2.5 de TIA/EIA-IS-968. "Vía amplificación de la transmisión de los puertos para la conexión de equipos registrados separadamente o de otros puertos de conexión de la red". Los ajustes realizados a la configuración de Ganancia por personal no calificado pueden resultar en infracciones al reglamento de la FCC. El personal calificado puede ajustar la configuración de ganancia por sobre estos niveles solamente cuando:

1. Se han realizado mediciones para asegurar que los niveles de potencia enviados a línea en cada interfaz de red conectada no exceden los niveles máximos especificados en la parte 68 sección 68.308(b) del reglamento de la FCC y la Sección 4.5 de TIA/EIA-IS-968 para el tipo de interfaz específico.
2. Cuando se realizan ajustes a la ganancia distintos a los valores predeterminados, es necesario tomar precauciones para asegurar que las conexiones al equipo terminal son controladas por personal de instalación calificado.
3. A fin de acomodar el Índice de sonoridad objetiva en recepción en distancias mayores a 2.7km de la oficina central, debe fijarse una ganancia de recepción de 1.5dB en las troncales analógicas.

Índice

A

Analógico
- Cajas de protección para teléfonos 190
- Disponibilidad por regiones del teléfono 41, 262
- Puerto 279, 282

Aplicación
- Call Center 48
- CD/DVD 45
- ContactStore 265
- Correo de voz 47
- CTI 48
- Manager 267
- Mantenimiento 46
- Monitor 267
- Registro de llamadas 48
- SoftConsole 270
- System Status Application 272
- TAPI 273
- Usuario 47
- VoiceMail Pro 274

Aplicación DevLink 48
Aplicación TAPIlink Pro 48
Aplicaciones para registro de llamadas 48
Audio
- Coversión de códec 43
- Puerto 279

B

BRI
- Puerto 279
- Puerto (So) 283
- Puerto (Troncal) 284

C

Cable
- Requisitos de acceso 54
- Requisitos de espacio de seguridad 54

Cableado
- Protección contra rayos 39, 188

Cables
- Distancias máximas de los cables 36, 280
- IP Office Standard 36, 280

Cajas de protección
- Montaje en bastidor 191
- Teléfono analógico 190

Call Status
- Aplicación 46

Canales
- Compresión 43

Canales de compresión 43
Canales de compresión de voz 43
Castle Rock 197
Clave de funciones paralela 23
Clave de funciones serial 23
Compact Business Center
- Aplicación 48

Compact Contact Center
- Aplicación 48

Compatibilidad
- Idioma 45
- Localidades 45

Conexiones
- Fuera del edificio 39, 188
- Puesta a tierra 38

Conference Center
- Aplicación 47

Configuración
- Crear nueva 76
- Eliminar 168

Configuración de seguridad
- Predeterminado 172

ContactStore
- Aplicación 47
- Componentes 265
- Requisitos de la PC 265
- Requisitos de licencia 265

Copia de seguridad
- Tarjeta SD 143

Copiar
- Tarjeta SD 147

Crear configuración 76
Cursos de capacitación 49

D

DC I/P
- Puerto 279

Declaraciones
- Homologación 312
- Seguridad 312

Declaraciones de homologación 312
Declaraciones de seguridad 312
DECT
- Disponibilidad por regiones 41, 262
- Teléfono 41, 262

Disponibilidad del equipo 13
Disponibilidad por regiones
- Teléfono analógico 41, 262
- Teléfono DECT 41, 262
- Teléfono DS 41, 262
- Teléfono H323 41, 262

DS
- Disponibilidad por regiones 41, 262
- IROB 189
- Puerto 279, 286
- Teléfono 41, 189, 262

E

Eliminar
- Tarjeta SD 136

Embedded Voicemail
- Aplicación 47

Evaluaciones
- Red 42
- VoIP 42

Evaluaciones de red 42
Evaluaciones de VoIP 42
Excepciones de Firewall 275
Expansión
- Puerto 279

EXT O/P
- Puerto 279

F

Feature Key Server
- Aplicación 46

Fuera del edificio
- Conexiones 39, 188

H

H323
- Disponibilidad por regiones 41, 262
- Teléfonos 41, 262

HP OpenView 197

Página1659 de 3226.

I

Información general
- Cursos de capacitación 49
- Sitios Web 49

Instalación IP500
- Aplicaciones Admin 64
- Comprobación de la luz LED de tarjeta 92
- Conexión de Manager 67
- Desembalaje 59
- Documentación 59
- Herramientas 58
- Inicio Manager 68
- Montaje en bastidor 87
- Puesta a tierra 90
- Tarjeta 80

IP500
- Botón Restaurar 201
- Tarjeta auxiliar de troncales 27
- Tarjeta auxiliar de troncales analógicas 27
- Tarjeta auxiliar de troncales BRI 27
- Tarjeta auxiliar de troncales PRI-U 27
- Tarjeta base de estación digital 24, 213
- Tarjeta base de tarjeta portadora legada 24, 213
- Tarjeta base de teléfono analógico 24, 213
- Tarjeta base VCM 24, 213

L

LAN
- Puerto 279

Licencias
- ContactStore 265
- Manager 267
- Monitor 267
- PC-Base 23
- PC-Less 23
- SoftConsole 270
- System Status Application 272
- TAPI 273
- VoiceMail Pro 274

Licencias PC-Base 23
Licencias PC-Less 23
Llave de funciones de Smart Card 23
Llaves de funciones
- Paralelo 23
- Serial 23
- Smart Card 23
- USB 23

M

Manager
- Actualización de software 179
- Aplicación 46
- Calidad del reloj 106
- Componentes 267
- Líneas troncales 104
- Marcación de prefijos 108
- Requisitos de la PC 267
- Requisitos de licencia 267

Mantenimiento
- Aplicaciones 46

MIB de SNMP
- Aplicación 46

Módulo
- Polycom Video 195

Módulo Polycom Video 195
Módulos
- Interfaz de troncales 313

Módulos de expansión
- Estación digital IP400 V2 257
- Estación digital IP500 29, 245
- IP400 Phone V2 259
- IP500 Phone 29, 252
- IPO 500 BRI So8 29
- So8 de BRI de IP500 243
- Troncal analógica de 16 líneas IP400 255
- Troncal analógica de 16 líneas IP500 240
- Troncal analógica IP500 29

Módulos de expansión externos 29
Módulos de interfaz de troncales 313
Monitor
- Aplicación 46
- Componentes 267
- Protocolos 275
- Requisitos de la PC 267
- Requisitos de licencia 267

MS-CRM
- Aplicación 47

N

Nueva configuración 76
Numeración de las extensiones
- Intercambio 187

O

Operación de IP Office en
- Australia 316
- Canadá 316
- China 317
- EUA 320
- Nueva Zelanda 319
- Unión Europea 318

P

País
- Idiomas 45
- Localidades compatibles 45

PF
- Puerto 279

Precauciones de compatibilidad electromagnética (CE)
- Comisión Federal de Comunicaciones 315
- Departamento de Comunicaciones de Canadá 315
- Precauciones de CE para China 315

PRI
- Puerto 279

Protección contra rayos 39, 188, 312
Protocolos 275
Puerto
- Analógico 279, 282
- Asignado 275
- Audio 279, 282
- BRI 279
- BRI (So) 283
- BRI (Troncal) 284
- Clasificación de seguridad 314
- DC I/P 279
- DCI I/P 286
- DS 279, 286
- DTE RS323 293
- Expansión 279, 288
- EXT O/P 192, 279, 288
- IP Office 275
- LAN 279, 289
- PF 279, 290
- PRI 279, 292
- Puerta 192

Página1660 de 3226.

Puerto
RS232/DTE 279
Teléfono (POT) 279, 291
USB 279
Utilizado 275
WAN 279
Puerto Audio 282
Puerto DC I/P 286
Puerto DTE 202
Configuración 293
Requerimientos del cable 293
RS232 293
Puerto Expansión 288
Puerto EXT O/P 192, 288
Puerto LAN 289
Puerto PF 290
Puerto PHONE (POT) 291
Puerto PRI 292

R

Reglamento de la FCC 322
Reloj 106
Requerimientos para el montaje en pared 53
Requisitos
Acceso de cables 54
Ambientales 53
Distancias de seguridad de los cables 54
Espacio 54
Montaje en pared 53
Requisitos ambientales 53
Requisitos de espacio 54
Restaurar
Tarjeta SD 145
RoHS 13
RS232/DTE
Puerto 279

S

Símbolos de peligro 312
Sitios Web 49
SNMP 197
Envío de trampas 200
Habilitar 200
Instalación 198
Puerto 200
respuesta 200
So8
Ejemplo de terminal ISDN 194
Ejemplo de videoconferencia 195
SoftConsole
Aplicación 47
Componentes 270
Requisitos de la PC 270
Requisitos de licencia 270
Software
Eliminación del software nuclear 203
Suministros de energía
1151C1 33
1151C2 33
Cables 34
PSU tipo 40W 33
PSU tipo 45w Aterrizada 33
PSU tipo 60W Aterrizada 33
Suministro de energía ininterrumpido 35
Sustancias peligrosas 13
System Status
Aplicación 46
System Status Application
Componentes 272
Requisitos de la PC 272
Requisitos de licencia 272

T

TAPI
Aplicación del driver WAV 48
Componentes 273
Requisitos de la PC 273
Requisitos de licencia 273
TAPILink Lite
Aplicación 47
Tarjeta base
Estación digital 24, 213
Tarjeta portadora legada 24, 213
Teléfono analógico 24, 213
VCM 24, 213
Tarjeta de memoria
Extracción 136
Tarjeta SD
Copia de seguridad 143
Copiar 147
Extracción 136
Restaurar 145
Tarjetas
Base de estación digital IP500 224
Tarjeta base de teléfono analógico IP500 217
VCM IP500 229
Tarjetas auxiliares
de troncales PRI 236
Troncal 27
Troncal analógica 27, 233
Troncal BRI 27, 235
Troncal PRI-U 27
Teléfono (POT)
Puerto 279

U

Unidad de control
IP406 V2 20
IP412 20
Montaje en bastidor 40
Montaje en pared 40
SOE 20
Unidad de control IP500 20
Unidades de control de la conexión a tierra 38
Unidades de control para montaje en bastidor 40
Unidades de control para montaje en pared 40
Unidades defectuosas 13
USB
Clave de funciones 23
Puerto 279

V

Voicemail Lite
Aplicación 47
VoiceMail Pro
Aplicación 47
Componentes 274
Requisitos de la PC 274
Requisitos de licencia 274

W

WAN
Puerto 279

© 2017 Avaya Inc. Reservados todos los derechos.

Traducido del inglés al español - www.onlinedoctranslator.com

Plataforma IP Office™ 11.0

Directrices de seguridad de la plataforma IP Office

Contenido

1. Introducción

1.1 Audiencia a la que se dirige 6

1.2 Cambio de documento 6

2. Resumen

2.1 Descargo de responsabilidad 8

2.2 Clasificaciones de información y requisitos de NDA 8

2.3 Aplicabilidad 9

2.4 Responsabilidad por la PI 9

2.5 Responsabilidad por seguridad 9

3. Fundamentos de seguridad de IP Office

3.1 Cifrado 13

3.1.1 Mensaje 14

3.1.2 Seguridad de datos 14

3.2 Privacidad de datos 15

3.3 Autenticación y Autorización 16

3.4 Plataforma Linux Seguridad 17

3.5 Servicios de IP Office 18

3.6 Seguridad predeterminada 19

4. Cuentas de usuario y derechos de acceso

4.1 Usuarios del servicio 23

4.1.1 Cambio de usuarios administrativos, grupos de derechos y Autenticación 24

4.1.2 Usuarios administrativos predeterminados y grupos de derechos 24

4.2 Configuración de seguridad 29

5. Gestión de contraseñas y PIN

5.1 Contraseña y PIN 33

5.2 Usuario administrativo 34

5.3 Contraseña de usuario de IP Office 36

6. Certificados y Fideicomiso

6.1 Término del certificado 39

6.1.1 Componentes de certificación 40

6.1.2 Certificados de seguridad 41

6.1.3 Certificados de host 41

6.1.4 Certificados y protocolo de seguridad de la capa de transporte (TLS) 41

6.1.5 Certificados de Web 42

6.2 Certificados de IP Office 43

6.2.1 Interfaces de certificados 44

6.2.2 Certificado inicial 44

6.2.3 Certificados de CA 50

6.2.4 Certificados de host 52

6.2.5 Certificados de identificación 53

6.2.6 Determinar mediante programación 56

6.2.7 IP Office Key 57

6.2.8 Selección IP Office 59

6.2.9 Implementación de IP Office 59

6.2.10 Certificados de autoridades de certificación externas 62

6.2.11 Certificado de autenticación 64

7. Seguridad VoIP

7.1 Plataforma IP Office 68

7.2 Señalización VoIP Seguridad 70

7.3 Aprovisionamiento de punto final Seguridad 70

7.4 Desempeño SRTP Capacidad 71

7.5 Indicaciones de llamadas seguras 71

7.6 Seguridad de VoIP Plan 72

8. Protección de la solución de la plataforma IP Office

8.1 Directrices generales 75

8.2 Evaluación de las oficinas de propiedad intelectual 76

8.3 Administración de la seguridad 76

8.4 Cambiar Security Default 76

8.5 Quitar Unnecesarios Archivos 76

8.6 Desactivar Unused Services/Interfaces 77

8.7 Asegurar Mínimo 78

8.8 Hacer cumplir una Contraseña Policy 79

8.9 Actualizar Certificados 80

8.10 Asegurar Telephony User Services 81

8.11 Endurecimiento para Web Server 82

8.12 Aseguramiento de los baúles/Lenguetas 83

8.13 Voz segura Media 83

8.14 Previniendo Unwanted Calls 84

8.14.1 Llamada Barring 84

8.14.2 Usar Barring 85

8.14.3 Protección Phone 86

8.14.4 Hacer Calls de Calls Made Prior to Login 86

8.14.5 Forwarding Protection 87

8.14.6 Remote Forwarding Configuration 87

8.14.7 SMDR Records Report todo 87

8.14.8 Error Handling 87

8.15 Protección de los interfaces de CTI 88

8.16 Asegurar la propiedad intelectual de la oficina 88

8.16.1 Security Manager 89

8.16.2 Protección de IP Office Web Manager/Web Control 89

8.16.3 Seguridad Web 89

8.16.4 Seguridad Settings 90

8.16.5 Seguridad Monitor 90

8.16.6 Seguridad Voice 91

8.16.7 Security Email 92

8.16.8 Seguridad Configuración 92

8.16.9 Seguridad para Exchange Office 93

8.16.10 Seguridad Web Browser 94

8.16.11 Seguridad Manager 94

8.16.12 Seguridad Profile 94

8.16.13 Protección de las aplicaciones de Avaya Contact Center 94

8.17 Configuración Data 94

8.18 Limitación de redes IP 95

8.18.1 Cortafuegos todos 95

8.18.2 Session Border Controller 95

8.18.3 Remote Access 95

8.19 Secure Maintenance Interfaces 96

8.20 Restricción Physical Ports 96

8.21 Protección del servidor Edition 97

Página1666 de 3226.

8.22 Protección del servidor de aplicaciones Linux/ M..o..d..u..... 99

9. Supervisión de la plataforma IP Office

9.1 Comprobaciones y Pruebas 103

9.2 Activación de Reporte..... 106

9.2.1 Oficial de PI e...R . . e..p...o..rtin..g..... 106

9.2.2 Voz.e.m. . . a..il.P . ro..R. e..p..o.r..ting 106

9.2.3 Con.ta.c..t..R . . e..c..o...rd.e...r..R. e..p...o..rtin..g..... 106

9.2.4 uno-.X. . . P..o...rta.l..para..r..IP. . ..O. ffic.e...R . e..p...o..rtin..g..... 107

9.2.5 Linu.x..-.B . . a..s..e...d...S . . e..rv.e..r...R...e..p..o...rtin.g 107

9.2.6 Otros..r..C . . o..m. p..o...n..e..n...ts..R . . e..p...o..rtin..g..... 107

9.3 Avaya Security...A..d..v..is.o...rie.s....a..n..d....IP..O . . . ffic.e....U...p..d..a...te.s..... 107

9.4 Respuesta a In.c.i.e.n..... 107

10.Apéndices

10.1 Apéndice A - .A..v..a..y..a...P . . . rod.d...u..c..t..S . e..c..u..r..ity.S . u..p..p..o..r..t..... 111

10.1.1 Acc..e.s.s...ing...A . va..ya...S..e...c..u..rity..A . d...vis..o..rie..s..... 111

10.1.2 Inter..rp..re.tin..g...a..n....A..v..a..y..a...S . . . e..c..u..r..ity.A . d..v..is.o..r..y..... 111

10.2 Apéndice B - .D. . . e..fa..u..lt.T..r..u..s..te..d...C . e..r..tific.a.s..... 112

10.2.1 Symantec Class 3 Secure Server CA - G4 en formato PEM.a..t..... 113

10.2.2 Autoridad de Certificación Entrust - L1K en formato PEM 113

10.2.3 GT.S...R . o..o..t..R . 1...en...P.E METROforma . a.t..... 114

10.2.4 GT.S...R . o..o..t..R . 2...en...P.E METROforma . a.t..... 114

10.2.5 Glo..b..a..lS. . ig.n....R...o..o..t..C . A . - . .R . 2...en...P.E METROforma . a..t..... 115

10.2.6 ISR..G. . . R o..o...t..X..1...en...P..E . . METROforma . a..t..... 115

10.2.7 Dig..iC..e..rt.G. . lo..b..a..l..R . o..o..t..C . Aen... educación METROforma . a..t..... 116

10.2.8 DigiCert SHA2 Secure Server CA en formato PEM. 116

10.2.9 Let.'.s...E. . n..c..ry.p..t..A. . u..th.o.ridad..X..3...en...P..E METROforma . a..t..... 117

10.2.10 Re.m. . o..v..ing.g...a....D...e..fa.u...lt.T..ru..s..te.d....C. ..e..artific.a....te..... 117

10.3 Apéndice C -.W. . . in.d..o..w Carolina.del.sur.tific.a..te...M. a..n..a...g..e..m . . e..n.t..... 118

10.3.1 Win..d...o..w. . Carolina.del.sur.tífico.a..te...S..para..re..O. r..g..a..n...iza..tio.n..... 118

10.3.2 Certific.a..te...S..to..re..Im . . . . p..o..... 119

10.3.3 Certificado.a..te...S..a..re..E . . . x..p..o..r..t..... ... 119

10.3.4 A.test..de.certificados...C . . o..n..s.o..le..... 120

10.4 Apéndice D -.S. . R T..P. . Solución de problemas..... 121

10.4.1 Tro.u...b..le.s...h..o..o...tin.g...T . . . o..o..ls..... 121

10.4.2 Tro.u...b..le.s...h..o..o...tin.g...T . . . ip.s..... 121

10.5 Apéndice E - .IP . . . .O. ffic.e...In.te..rfa.c..e....C...e..rtific.a...te..S . u..p..p...o..rt.. 123

10.6 Apéndice F - .IP..O. . ffic.e....V..o..IP. pu . n..d..p...o..in.t..S . . e..c.u.ridad..... 127

10.7 Apéndice G: uso de la autoridad de certificación de IP Office 131

10.7.1 Generación del Certificado de Identidad Propio del Servidor CA..... 131

10.7.2 Generación de certificados de identidad para otros dispositivos 132

10.7.3 Exp.o.r..t.g...th..e...S. . ig.n..in..g...C . . e..r..tific.a..... 132

10.7.4 Re.n..e..w. . en..g../.R e..p...la.c..ing.g....th.e...S. ig.n....ing.g...C. e...rtific.a..te... 133

10.8 Apéndice H -.C. . e...rtific.a..te...S..ig..n..ing.g....R...e..q..u...e..s..ts 134

10.8.1 Creación de una CSR mediante Microsoft MMC Certificate.s....S..n...a..p..-..in..... 135

10.8.2 Crear una CSR utilizando OpenSSL Paquete 138

10.8.3 Creación de una CSR mediante el comando del servidor Linux....L..in.e..... 140

10.8.4 Co.n..v..e..rtin..g...C. . e..r..tific.a..te..F . ile.s..... 141

10.9 Apéndice I: Aprovisionamiento seguro de la serie 9600 Teléfonos H.323 142

10.9.1 Re.c..o..m. . . metro e...n..d..e...d...S . etiqueta.g..in..g...P . . ro.c..e.s..s..... 142

10.9.2 Autom... a..te..d...P. . ro.c..e.s..s..... 143

10.9.3 Cambi...a....R...o..o..t..C. . A. . C..e..artific.a..... 143

10.10 Apéndice J: dependencias de seguridad de la aplicación/ cliente. 144

11.Historial del documento

Índice 155

¿Comentarios sobre este documento? infodev@avaya.com

Capítulo 1. Introducción

1. Introducción

Este documento proporciona pautas para implementar y mantener la seguridad de la plataforma IP Office. Contiene una descripción general de la política de seguridad y describe las herramientas de seguridad disponibles para una solución de plataforma IP Office.

1.1 Público objetivo

Este documento está destinado al personal de instalación, administración, servicio y soporte que requiere conocimiento de las herramientas de seguridad de IP Office disponibles e información sobre cómo implementar una política de seguridad de IP Office.

1.2 Cambios en el documento desde la última emisión

Actualizaciones para la versión 11.1 de IP Office

- Privacidad de datos
- Valores predeterminados de configuración de seguridad de IP Office
- Certificados de confianza predeterminados
- Política SBC
- Enlaces actualizados

Actualizaciones para la versión 11.1 FP1 de IP Office

- La contraseña del correo de voz utilizada para proteger la conexión entre los servicios de IP Office y Voicemail Pro ahora tiene una longitud fija de 31 caracteres.
  - En instalaciones nuevas, se genera automáticamente una contraseña adecuada de 31 caracteres en la primera conexión entre los dos servicios.
  - Los sistemas existentes pueden continuar con contraseñas más cortas existentes. Sin embargo, en cualquier cambio de contraseña, se aplica el requisito de longitud de contraseña de 31 caracteres.

Capitulo 2.

Visión general

2. Resumen

El siguiente documento es una guía práctica para la planificación, las comprobaciones y los cambios de configuración necesarios para ayudar a proteger la solución IP Office. Todas las instalaciones nuevas y existentes de IP Office, independientemente del uso, se deben evaluar con las siguientes secciones y se deben tomar medidas inmediatas cuando se indique.

La implementación de estas recomendaciones reducirá sustancialmente el riesgo de compromiso por amenazas de seguridad como la denegación de servicio, el fraude de llamadas y el robo de datos.

Este documento no proporciona un análisis de temas relacionados con la seguridad, define la política de seguridad ni discute la teoría; tampoco puede garantizar la seguridad. Sin embargo, este documento tiene como objetivo proporcionar información útil y comprensible que pueda ser utilizada por el personal de instalación, servicio y soporte, así como por los clientes, para ayudar a proteger IP Office contra los ataques.

2.1 Descargo de responsabilidad

Avaya ha realizado todos los esfuerzos razonables para garantizar que la información proporcionada aquí sea precisa en la fecha de publicación. Avaya puede cambiar cualquier proceso subyacente, arquitectura, producto, descripción o cualquier otra información descrita o contenida en este documento. Avaya renuncia a cualquier intención u obligación de actualizar o revisar el documento, ya sea como resultado de nueva información, eventos futuros u otros. Este documento se proporciona "tal cual" y Avaya no ofrece ninguna garantía de ningún tipo, expresa o implícita.

2.2 Clasificaciones de información y requisitos de NDA

Avaya proporciona información relacionada con la seguridad de acuerdo con las siguientes clasificaciones de información:

Clasificación	Descripción
Avaya restringido	Esta clasificación es para información comercial extremadamente confidencial, destinada estrictamente para su uso dentro de Avaya. La divulgación no autorizada de esta información puede tener un impacto adverso grave en Avaya y los clientes, los socios comerciales y los proveedores de Avaya.
Avaya Confidencial	Esta clasificación se aplica a la información empresarial menos confidencial destinada a su uso dentro de Avaya. La divulgación no autorizada de esta información puede tener un impacto adverso significativo en Avaya y los clientes, los socios comerciales y los proveedores de Avaya. En esta clasificación se incluye información que puede ser privada para algunas personas.
Propiedad de Avaya	Esta clasificación se aplica a toda otra información que no encaja claramente en las dos clasificaciones anteriores y se considera confidencial solo fuera de Avaya. Si bien la divulgación puede no tener un impacto adverso grave en Avaya y los clientes, socios comerciales y proveedores de Avaya, esta información pertenece a Avaya y la divulgación no autorizada va en contra de la política de Avaya.
Público	Esta clasificación se aplica a la información aprobada explícitamente por la gerencia de Avaya como información no confidencial disponible para publicación externa.

Dado que este documento está generalmente disponible, la información contenida en este documento se considera**Público**. Este documento contiene referencias a fuentes de información adicionales que pueden divulgar información tanto confidencial como patentada y requieren un acuerdo de confidencialidad (NDA) con Avaya.

2.3 Aplicabilidad

La siguiente información se aplica a IP Office IP500 V2, IP Office Server Edition, aplicaciones IP Office y terminales para las versiones 9.1, 10.0, 10.1, 11.0 y 11.1.

El Boletín técnico 169 de IP Office cubre las versiones 9.0 y anteriores, y se puede encontrar en: https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/bulletins/techbulls/tb169.pdf .

Las siguientes áreas no están cubiertas en este documento:

- Medidas de seguridad física
- Seguridad de componentes que no son de Avaya
- Definición de política de seguridad
- Cumplimiento normativo

2.4 Responsabilidad por la seguridad de IP Office

Avaya es responsable de diseñar y probar la seguridad de todos los productos de Avaya. Cuando Avaya vende un producto como un paquete de hardware/software, el proceso de diseño y prueba del producto de Avaya también incluye la prueba del sistema operativo.

El cliente es responsable de las configuraciones de seguridad apropiadas de las redes de datos. El cliente también es responsable de usar y configurar las funciones de seguridad en los sistemas, puertas de enlace, aplicaciones y teléfonos de IP Office.

2.5 Responsabilidad por las actualizaciones de seguridad

Cuando las aplicaciones relacionadas con la seguridad o las actualizaciones de software operativo están disponibles, Avaya prueba las actualizaciones, si corresponde, antes de ponerlas a disposición de los clientes. En algunos casos, Avaya modifica el software actualizado antes de ponerlo a disposición de los clientes.

Avaya notifica a los clientes sobre la disponibilidad de actualizaciones de seguridad a través de Avisos de seguridad. Los clientes pueden suscribirse a recIV e notificación sobre avisos de seguridad por correo electrónico. Para más información, verSoporte de seguridad de productos de Avaya 111.

Cuando las actualizaciones de seguridad del software de IP Office estén disponibles, el cliente puede instalar las actualizaciones o emplear un instalador del grupo de soporte de servicios al cliente para instalar las actualizaciones. Cuando Avaya instala las actualizaciones, el instalador es responsable de seguir las mejores prácticas de seguridad para el acceso al servidor, las transferencias de archivos y la copia de seguridad y restauración de datos.

Capítulo 3.

Seguridad de IP Office

Fundamentos

¿Comentarios sobre este documento? infodev@avaya.com

3. Fundamentos de seguridad de IP Office

Toda la telefonía, administración, datos, servicios e interfaces que ofrece la solución IP Office tienen características de seguridad para ayudar a prevenir amenazas de seguridad como:

- Acceso no autorizado o modificación de datos
- robo de datos
- Ataques de denegación de servicio (DoS)
- Virus y gusanos
- Ataques basados en web como Cross-Site Scripting y Cross-Site Forgery
- Detección de intentos de ataque

La siguiente tabla enumera los métodos y técnicas que se utilizan para ayudar a contrarrestar las amenazas de seguridad:

Mecanismo	Uso	Ejemplos de IP Office
Identificación y Autenticación	La identificación es la capacidad de identificar de manera única a un usuario, sistema o aplicación de un sistema o una aplicación que se ejecuta en el sistema. La autenticación es la capacidad de demostrar que una entidad es realmente quien dice ser.	• Cuentas de Usuarios de Telefonía y Servicios • Autenticación de mensajes • Certificados digitales X509
Autorización	La autorización protege los recursos al limitar el acceso solo a usuarios, sistemas o aplicaciones autorizados.	• Controles de acceso a cuentas de Usuarios de Telefonía y Servicios
Revisión de cuentas	La auditoría es el proceso de registrar y verificar eventos para detectar si se ha producido alguna actividad o intento inesperado.	• Pista de auditoría • Alarmas de aplicación de estado del sistema • Informes de registro del sistema
Confidencialidad	La confidencialidad mantiene la información confidencial privada, protegiéndola de la divulgación no autorizada.	• Cifrado TLS/SRTP • Cifrado de base de datos de seguridad
Integridad de los datos	La integridad de los datos detecta si ha habido una modificación no autorizada de los datos.	• Autenticación de mensajes TLS/SRTP

Tabla 1: Métodos de seguridad

3.1 Cifrado

El cifrado garantiza que todos los datos almacenados en un sistema o enviados por un sistema a otro no puedan ser "leídos" por nadie más. Hay dos tipos principales de encriptación

- **Cifrado simétrico**es la aplicación de un proceso matemático en el extremo de origen y un proceso inverso en el extremo receptor. Los procesos en cada extremo usan la misma 'clave' para cifrar y descifrar los datos.
- **Cifrado asimétrico**usa diferentes claves para encriptar y decrypti en. Un uso común es la clave privada y pública de una autoridad de certificación. VerCertificados y Fideicomiso 38para más información.

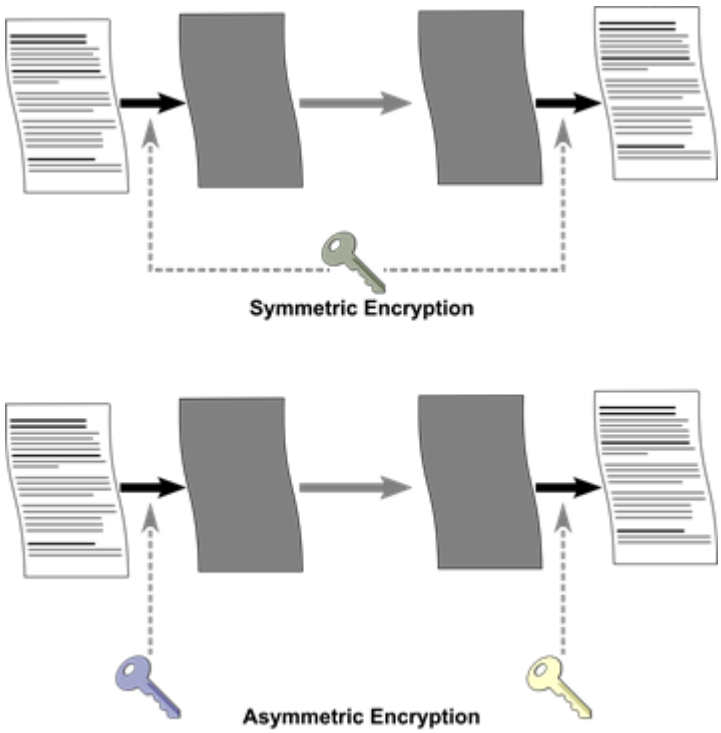


Figura 1: Cifrado simétrico/asimétrico

La mayor parte del cifrado de datos de mensajes es simétrico. Los datos enviados pueden cifrarse opcionalmente utilizando una serie de algoritmos conocidos:

Algoritmo	Tamaño de clave efectivo (bits)	Usar
DES-40	40	No soportado – fuerza insuficiente
DES-56	56	No soportado – fuerza insuficiente
3DES	112 (también conocido como DES de dos teclas)	No soportado – fuerza insuficiente
3DES	168 (también conocido como DES de tres teclas)	Seguridad 'baja'.
RC4-128	128	Seguridad 'baja'.
AES-128	128	Seguridad 'media'.
AES-256	256	Seguridad 'fuerte'.

Tabla 2: Algoritmos de cifrado

En general, cuanto mayor sea el tamaño de la clave, más seguro será el cifrado. Sin embargo, los tamaños de clave más pequeños generalmente requieren menos procesamiento.

IP Office admite el cifrado mediante:

- Seguridad de la capa de transporte (TLS v1.2 con v1.0 y v1.1 para legado)
- Shell seguro (SSH v2)
- RTP seguro (SRTP)

3.1.1 Autenticación de mensajes

La autenticación de mensajes garantiza que todos los datos enviados por el sistema o el administrador no puedan ser modificados (o sustituidos) por nadie más sin ser detectados. Esto implica que el originador de los datos produzca una firma (denominada 'hash') de los datos enviados y también los envíe. El receptor obtiene los datos y la firma, y verifica que ambos coincidan.

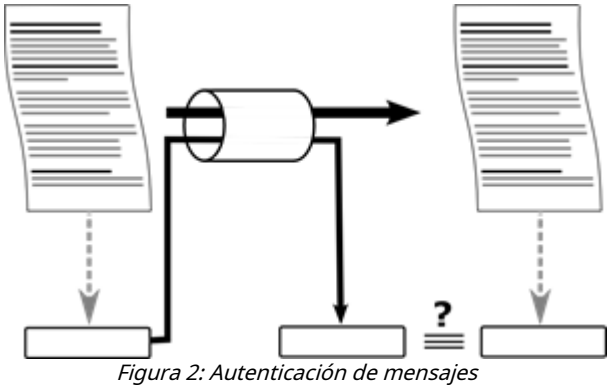


Figura 2: Autenticación de mensajes

Cualquier dato enviado puede autenticarse opcionalmente utilizando una serie de algoritmos conocidos y criptográficamente seguros:

algoritmo metro	Hachís efectivo tamaño (bits)	Usar
MD5	128	No soportado – fuerza insuficiente
SHA-1	160	Seguridad 'Baja/Media' para la autenticación de mensajes.
SHA-2	224, 245, 384, 512	Seguridad 'fuerte'

Tabla 3: Autenticación de mensajes

En general, cuanto mayor sea el tamaño del hash, más segura será la firma. Sin embargo, los tamaños de hash más pequeños generalmente requieren menos procesamiento. IP Office admite la autenticación de mensajes mediante los protocolos Transport Layer Security (TLS v1.0, v1.1 y v1.2), Secure Shell (SSH v2), Secure RTP (SRTP) e IPsec.

3.1.2 Base de datos de seguridad

Una base de datos de seguridad está ubicada en IP Office que controla todo el acceso local, además del acceso remoto a otros componentes de IP Office. Estas configuraciones de seguridad tienen valores predeterminados iniciales, pueden ser modificadas por IP Office Manager o IP Office Web Manager y cubren las siguientes áreas:

- cuentas administrativas
- Una cuenta de administración de seguridad inviolable
- Política de cuentas y contraseñas de los usuarios
- Almacén de confianza (almacén de certificados de confianza)
- Certificados de identidad
- Comprobaciones de certificados recibidos
- Controles de seguridad de la interfaz de servicio
- Controles de interfaz heredados

Los ajustes de seguridad son independientes de la configuración de IP Office, siempre están protegidos y no se pueden guardar ni editar sin conexión.

Además de la configuración de seguridad de IP Office, one-X Portal for IP Office, Voicemail Pro, Contact Recorder, WebLM y Web Control tiene cuentas administrativas locales utilizadas en condiciones de respaldo, consulteCuentas de usuario y derechos de acceso 22.

3.2 Privacidad de datos

En los últimos años, la legislación como la Ley de Privacidad del Consumidor de California (CCPA) y el Reglamento General Europeo de Protección de Datos (GDPR) han destacado la necesidad de mantener los datos personales, es decir, la información que se puede rastrear hasta un individuo, en un alto grado. de mando

IP Office puede, bajo ciertas condiciones, procesar y guardar datos personales. Algunos ejemplos son:

- Los registros de detalles de llamadas (SMDR) pueden contener el número de teléfono personal de una persona
- Las grabaciones de llamadas pueden contener información personal hablada por una persona que llama

La responsabilidad de mantener dichos datos protegidos es, en última instancia, responsabilidad del 'Controlador de datos'. Para IP Office, el controlador de datos normalmente sería la empresa que utiliza el sistema. es decir, el cliente o su agente. Bajo CCPA esto se conoce como 'Negocio'

Avaya IP Office, cuando se utiliza como parte de una solución para procesar y guardar datos personales en nombre del cliente, se denomina "Procesador de datos". Según la CCPA, esto se denomina "Proveedor de servicios". Tenga en cuenta que IP Office formará solo una parte de los aspectos del Procesador de datos, generalmente combinado con otros procesos automatizados o manuales.

IP Office no se puede certificar individualmente para cumplir con un requisito específico de privacidad de datos, pero el Procesador de datos puede configurarlo y operarlo para lograr el cumplimiento de varios regímenes de privacidad de datos, como GDPR y CCPA.

La plataforma IP Office se adhiere a los siguientes principios establecidos de privacidad de datos:

- Diseñado y diseñado teniendo en cuenta la privacidad de los datos
- No se capturan datos personales por defecto
- Controla qué datos personales se pueden capturar y cuánto tiempo se conservan.
- Notificaciones a las personas antes de la captura de datos personales, junto con un registro de aceptación.
- Todos los datos personales seguros tanto en reposo como en tránsito
- Los datos personales permanecen locales en los servidores; El almacenamiento en la nube de IP Office permanece dentro de la región geográfica.
- Acceso a todos los datos personales controlados a través delyo Marco de autenticación y autorización de P Office, consulte Marco de autenticación y autorización dieciséis.
- Los datos personales se pueden exportar, modificar o eliminar en respuesta a solicitudes de privacidad de datos.
- Acceso a los datos personales registrados. El cliente puede ver estos registros para proporcionar una pista de auditoría del acceso a los datos personales.

Puede encontrar una Declaración de privacidad del producto para IP Office en: https://downloads.avaya.com/css/P8/documents/101049410 .

Protección de la solución de la plataforma IP Office 74contiene información para proteger la solución IP Office y debe seguirse desde una perspectiva de seguridad y privacidad de datos. Además, se deben leer los siguientes documentos antes de implementar la solución:

- Declaración de privacidad del producto IP Office de Avaya
- Declaración de privacidad del producto Avaya IX Workplace
- Declaración de privacidad del producto Avaya Communicator for Web
- Declaración de privacidad del producto de colaboración Avaya IX
- Declaración de privacidad del producto Avaya Contact Center Select
- Informe de llamadas de Avaya para la declaración de privacidad del producto Avaya IP Office™

Es útil al revisar estos documentos para comprender los siguientes términos. Estas definiciones tienen un alcance amplio y pueden variar según las normas de privacidad de datos vigentes en un país o región en particular.

- **Información personal:**Significa cualquier información relativa a una persona física identificada o identificable. Esto podría incluir números de teléfono personales, información registrada durante las llamadas, direcciones de correo electrónico, datos de ubicación, domicilio, etc.
- **Sujeto de datos:**Una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre
- **Controlador de datos:**La persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o junto con otros, determine los fines y medios del Tratamiento de Datos Personales. Un ejemplo podría ser el cliente que opera el sistema IP Office.
- **Procesador de datos:**Una persona física o jurídica, autoridad pública, agencia u otro organismo que Procesa Datos Personales en nombre del Controlador. El sistema IP Office podría formar parte del procesamiento de datos.

Página1679 de 3226.

3.3 Marco de autenticación y autorización

IP Office tiene su propio marco de autenticación y autorización (AA), y las solicitudes a los servicios de IP Office se enrutan a través del marco AA. El marco AA evita el acceso no autorizado y no autenticado a los servicios y datos de IP Office.

El siguiente diagrama muestra las interfaces de servicio cubiertas por este marco:

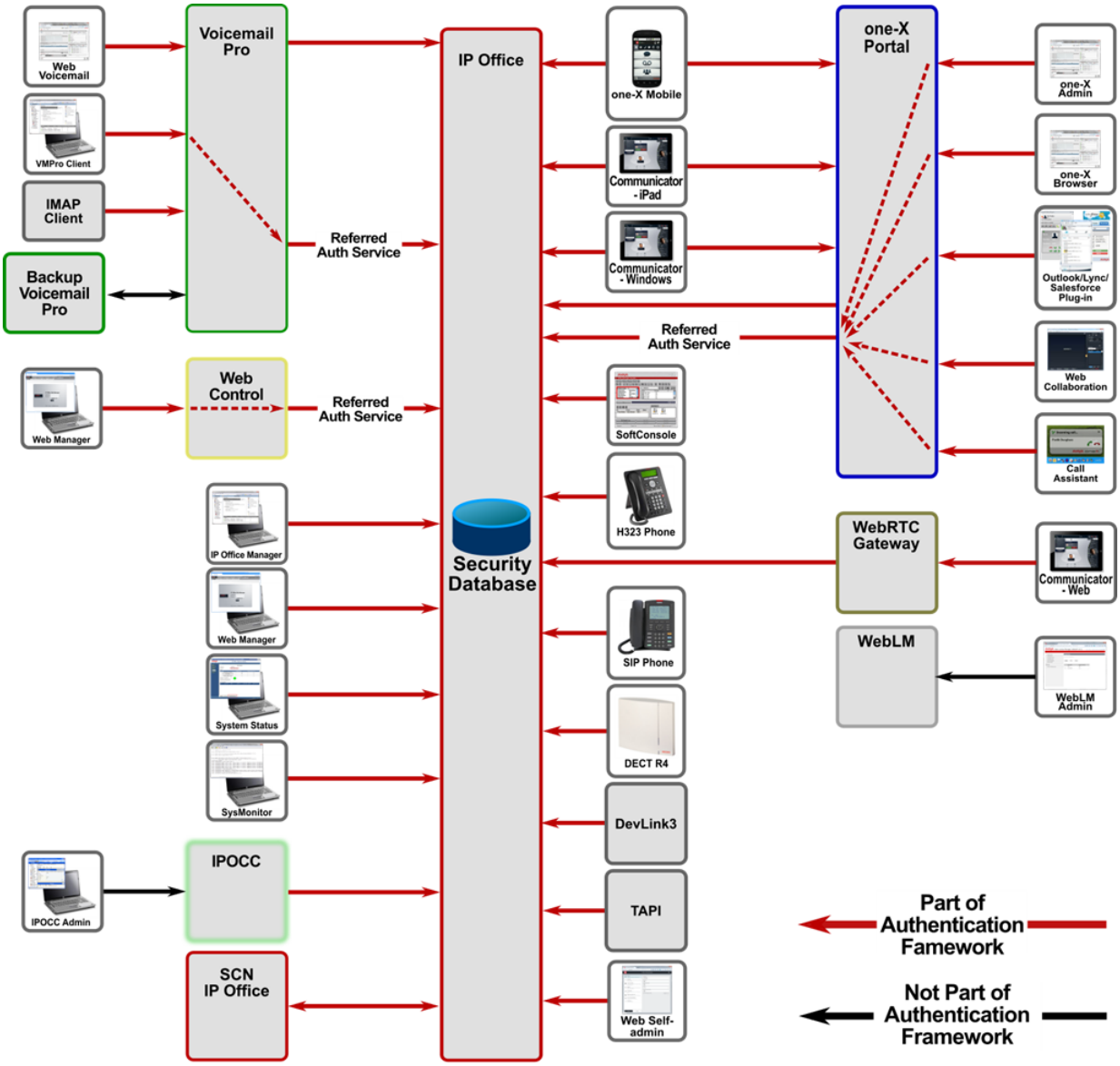


Figura 3: Marco de autenticación y autorización

Portal one-X para IP Office, Voicemail Pro y Web Control remiten cualquier inicio de sesión administrativo a IP Office a través de un servicio web de autenticación/autorización.

Hay algunas interfaces heredadas que no pasan por el marco AA:

- Directorios y listas de usuarios TFTP
- Transferencia de archivos TFTP
- SNMP (Nota: no se admiten operaciones SET)

Estos están deshabilitados de forma predeterminada, pero se pueden habilitar dentro de un entorno protegido por otros medios.

Página1680 de 3226.

3.4 Seguridad de la plataforma Linux

Varios productos de IP Office se ejecutan en el sistema operativo Linux. Avaya utiliza el sistema operativo Linux de código abierto como base segura para las comunicaciones.

La base de código abierto es beneficiosa por las siguientes razones:

- Expertos en seguridad de todo el mundo revisan el código fuente en busca de defectos o vulnerabilidades.
- Avaya trabaja diligentemente para monitorear tanto las mejoras como las mejoras creadas por la comunidad de Linux y para revisar cuidadosamente los cambios antes de incorporarlos a los productos de Avaya.
- Los servidores Avaya basados en Linux ayudan a proteger contra muchos ataques DoS, como inundaciones SYN, inundaciones de ping, paquetes con formato incorrecto, paquetes de gran tamaño y falsificación de números de secuencia, entre otros.

Avaya ha modificado o fortalecido el sistema operativo Linux de las siguientes maneras para minimizar las vulnerabilidades y mejorar la seguridad:

- **Instalación mínima:**
  Se eliminan todos los RPM innecesarios. Además de hacer que las imágenes de los archivos de software sean más pequeñas y más manejables, el sistema operativo es más seguro porque los atacantes no pueden comprometer los RPM que no están presentes.
- **Privilegios mínimos:**
  Todas las aplicaciones de IP Office se ejecutan como no root. El acceso SSH raíz está deshabilitado.
- **Puertos:**
  Puertos IP innecesarios cerrados.
- **Sistema operativo Linux:**
  Linux con seguridad mejorada (SELinux) está habilitado, lo que proporciona una mayor seguridad utilizando mecanismos a nivel de kernel que reducen la amenaza de compromiso y limitan el daño potencial de aplicaciones maliciosas o defectuosas.
- **Protección de cortafuegos:**
  Los productos basados en Linux de Avaya usan el firewall IPTables que protege el sistema contra varios ataques basados en la red.
- **Compatibilidad con puerta de enlace de seguridad de acceso mejorada (EASG):**
  EASG es un sistema de autenticación basado en certificados que reemplaza las contraseñas de las cuentas de soporte técnico.
- **Protección de partición de unidad:**
  Los procesos que pueden escribir cantidades significativas de datos en el disco duro, como el servidor HTTPS de respaldo/restauración y Voicemail Pro, tienen cuotas asignadas para garantizar que el espacio del disco no se agote por acciones malintencionadas o no intencionales.

Paquetes/herramientas de administración y seguridad de terceros

Hay disponibles varios antivirus y otros paquetes de seguridad para Linux; sin embargo, Avaya no admite el uso de dicho software en el producto IP Office, ya que tiene un nivel de inmunidad natural y los paquetes pueden afectar gravemente el rendimiento.

3.5 Servicios de IP Office

Todas las interfaces de servicios administrativos y de mantenimiento de IP Office están controladas por la base de datos de seguridad en cuanto a disponibilidad y nivel de seguridad. Estos servicios incluyen:

Servicio	Uso
Configuración	Acceso a la configuración de IP Office Manager y Server Edition Manager
Administración de Seguridad	Acceso a la configuración de seguridad (base de datos) de IP Office Manager y Server Edition Manager
Interfaz de la aplicación de estado del sistema	Acceso a la aplicación de estado del sistema (SSA)
TSPI mejorado	Acceso one-X Portal para IP Office CTI
HTTP	Teléfono y acceso a archivos de IP Office Manager, Voicemail Pro, IP Office Line, System Monitor (seguro)
Servicios web	Administrador web de IP Office y SMGR
Externo	Servicios externos a la aplicación IP Office.

Tabla 4: Servicios de IP Office

Cada servicio tiene un Nivel de Seguridad del Servicio configurable:

Nivel de seguridad del servicio	Uso
Desactivado	El servicio y los puertos TCP correspondientes están inactivos
Solo no seguro	Esta opción permite solo el acceso no seguro al servicio. El puerto TCP seguro del servicio, si lo hay, está deshabilitado. Esta o Deshabilitada son las únicas opciones compatibles con el servicio TSPI mejorado
Inseguro + Seguro	Esta opción permite el acceso no seguro y seguro (bajo).
Seguro, Bajo	Esta opción permite el acceso seguro a ese servicio mediante TLS y exige un cifrado y una autenticación más débiles (por ejemplo, 3DES) o superiores. El puerto TCP no seguro del servicio está deshabilitado.
Seguro, Medio	Esta opción permite el acceso seguro a ese servicio mediante TLS y exige un cifrado y una autenticación moderados (por ejemplo, AES-128) o superiores. El puerto TCP no seguro del servicio está deshabilitado.
Seguro, Alto	Esta opción permite el acceso seguro a ese servicio mediante TLS y exige un cifrado y una autenticación más sólidos (por ejemplo, AES-256), o superiores. Además, se requiere un certificado d.f. desde el cliente (para autenticación mutua). Ver Controles de comprobación de certificados 52 para las pruebas realizadas en el certificado recibido. Si no se recibe ningún certificado del cliente, se rechaza la conexión. El puerto TCP no seguro del servicio está deshabilitado.

Tabla 5: Niveles de seguridad del servicio

Se controla la actividad de otras interfaces de servicio.

3.6 Configuración de seguridad predeterminada

Los valores predeterminados para la configuración de seguridad de IP Office se cargan en el primer inicio y en el reinicio. Tienen un nivel de seguridad e incluyen cambios de contraseña obligatorios para las cuentas.

- **Nota:**La versión 9.0 y anteriores de IP Office requieren cambios adicionales de los valores predeterminados para hacerlos más seguros.

Es posible restablecer la configuración de seguridad de IP Office a través de una interfaz de administración, el puerto serial IP500 V2 o los botones de reinicio de encendido; por este motivo, es importante que la instalación de IP Office sea físicamente segura.

Para obtener información sobre los valores predeterminados de usuario administrativo de IP Office, consulteUsuarios administrativos predeterminados y grupos de derechos 24. Para obtener información sobre los valores predeterminados de los certificados, consulteConfiguración inicial del certificado 44.

Las siguientes configuraciones de seguridad predeterminadas se aplican a las diversas interfaces de servicio de IP Office.

Interfaz	Configuración predeterminada	Defecto ¿Seguridad?	notas
Configuración	Seguro, Medio	✓	Acceso a la configuración de IP Office Manager
Seguridad Administración	Seguro, Medio	✓	Acceso a la configuración de seguridad de IP Office Manager
Estado del sistema Interfaz de la aplicación	Seguro, Medio	✓	acceso a la SSA
TSPI mejorado	Solo no seguro	✗	Acceso one-X Portal para IP Office CTI
HTTP	Inseguro + Seguro	✗	Teléfono y acceso a archivos de IP Office Manager, Voicemail Pro, IP Office Line, System Monitor (seguro)
Servicios web	Seguro, Medio	✓	Administrador web de IP Office y SMGR
Servidor TFTP	Activo (IP500 V2) Inactivo (Linux)	✗	Permite el acceso para la actualización de Manager y el descubrimiento UDP whois
Lectura de directorio TFTP	Inactivo	n / A	Directorio del sistema DECT R4
Correo de voz TFTP	Inactivo	n / A	Usado para Voicemail Pro R9.0 y anteriores
Código de programa	Activo (IP500 V2) Inactivo (Linux)	✗	Acceso de actualización del administrador
Devlink	Inactivo	n / A	Acceso a DevLink y System Monitor UDP/TCP
Devlink3	Activo	✓	Acceso a DevLink3.
TAPI	Inactivo	n / A	Solo interfaces TAPI de primera y tercera parte.
Lectura de directorio HTTP	Activo	✗	Portal one-X para acceso al directorio de IP Office, función de directorio externo
Escritura de directorio HTTP	Activo	✗	one-X Portal para acceso al directorio de IP Office

Tabla 6: Configuración de seguridad predeterminada

La configuración de seguridad local para one-X Portal for IP Office, Voicemail Pro, IPOCC y Contact Recorder se puede restablecer mediante la CLI de la consola de Linux y el acceso raíz.

Capítulo 4.

Cuentas de usuario y derechos de acceso

4. Cuentas de usuario y derechos de acceso

Hay dos tipos principales de cuentas de usuario en la solución IP Office.

- Un usuario de telefonía se denomina**Usuario de IP Office**.
- Un usuario administrativo se llama**Usuario del servicio**.

Los usuarios de IP Office se definen en los ajustes de configuración principales. Los usuarios del servicio se definen en la configuración de seguridad.

Un tipo especial de usuario del servicio es el administrador de seguridad, con acceso permanente a todas las configuraciones de seguridad. Un sistema IP Office no puede tener usuarios de servicio o de IP Office configurados, pero el administrador de seguridad no puede eliminarse ni deshabilitarse.

Con el fin de proporcionar una base de datos de autenticación central para el marco de autenticación y autorización (AA), IP Office proporciona un servicio web seguro a otras aplicaciones. Linux one-X Portal para IP Office, Voicemail Pro y Web Management usan este servicio para 'Referir' inicios de sesión administrativos a la base de datos.

4.1 Usuarios del servicio

El acceso a la configuración del sistema está controlado por usuarios de servicio y grupos de derechos almacenados en la configuración de seguridad de la unidad de control. Estos se almacenan por separado de los ajustes de configuración del sistema. Todas las acciones relacionadas con las comunicaciones entre Manager y el sistema requieren un nombre de usuario y una contraseña de servicio. Ese usuario del servicio debe ser miembro de un grupo de derechos con permisos para realizar la acción requerida.

Administrador de seguridad:

El administrador de seguridad puede acceder a la configuración de seguridad del sistema y la cuenta no se puede eliminar ni desactivar.

Además, una configuración de seguridad adicional puede obligar a esta cuenta a tener derechos de seguridad exclusivos, evitando que otros usuarios del servicio accedan a la configuración de seguridad.

Usuarios del servicio:

Cada usuario del servicio tiene un nombre, una contraseña y es miembro de uno o más grupos de derechos. Las cuentas pueden estar en uno de varios estados, incluidos habilitado, deshabilitado, bloqueado y cambio de contraseña forzado.

IP Office admite un máximo de 64 usuarios de servicio.

Grupos de derechos:

Los grupos de derechos a los que pertenece un usuario del servicio determinan qué acciones puede realizar. Se puede considerar como un rol, pero tiene mucha más flexibilidad. Las acciones disponibles para los grupos de derechos incluyen configuración, acciones de seguridad y acciones de mantenimiento. Cuando un usuario del servicio se ha configurado como miembro de más de un Grupo de derechos, combina las funciones disponibles en los Grupos de derechos separados

IP Office admite un máximo de 32 grupos de derechos.

Funciones de la aplicación:

Además de los derechos de acceso al servicio de IP Office, los grupos de derechos también pueden contener 'Funciones' para IP Office Manager e IP Office Web Manager; la configuración de estos roles determina qué derechos de acceso tiene el usuario del servicio dentro de esa aplicación. Permite una mayor granularidad de control de acceso dentro de esa aplicación que los derechos de acceso al servicio básico. Por ejemplo, el servicio de configuración de IP Office tiene dos derechos básicos de acceso: Leer todo y Escribir todo. Sin embargo, los roles de Administrador y Operador pueden restringir aún más lo que se puede escribir, ver o editar.

Ejemplo de asignación de derechos:

Figura 4: Asignación de grupos de derechos de servicios

En el ejemplo ilustrado arriba:

- El usuario del servicio X puede leer y escribir la configuración. Sin embargo, solo pueden editar la configuración del Operador y solo pueden realizar cambios que se puedan fusionar.
- El usuario del servicio Y puede leer y escribir la configuración, editar todas las configuraciones y realizar cambios que requieran reinicios o fusiones. También pueden acceder a la configuración de Voicemail Pro.
- El usuario del servicio Z puede leer y escribir la configuración, editar todas las configuraciones y realizar cambios que requieren reinicios. También pueden acceder a la configuración de seguridad y de Voicemail Pro.
- La cuenta de administrador de seguridad solo puede acceder a la configuración de seguridad.

4.1.1 Cambio de usuarios administrativos, grupos de derechos y autenticación

IP Office Manager e IP Office Web Manager permiten la modificación de usuarios de servicios y grupos de derechos. Antes de cualquier cambio, se debe considerar lo siguiente:

- Una implementación de Server Edition o IP500 V2 de varios sitios debe tener usuarios de servicio y grupos de derechos coherentes. IP Office Manager e IP Office Web Manager tienen herramientas de sincronización para ayudar.
- Para todos los servidores basados en Linux, habilite la autenticación referida para permitir que la aplicación de IP Office use la IP Office local.
- Todos los cambios deben seguir las mejores prácticas de seguridad, como la política de contraseñas y los derechos mínimos de acceso.

4.1.2 Usuarios administrativos predeterminados y grupos de derechos

Las siguientes configuraciones de usuario de servicio predeterminadas están presentes en el primer inicio o después de un restablecimiento de la configuración de seguridad.

- Administrador de seguridad predeterminado 24
- Usuarios de servicio predeterminados 25
- Grupos de derechos predeterminados 26
- Asignaciones de grupos de derechos predeterminados 27

4.1.2.1 Administrador de seguridad predeterminado

El seguimiento**Administrador de seguridad**la cuenta está presente en el primer inicio y restablecimiento de la configuración de seguridad:

Nombre	Defecto Cuenta Estado	Uso	Grupo de derechos Afiliación	notas
seguridad	Activado, Fuerza clave cambio	Esta es la cuenta de administración de seguridad predeterminada. Tiene todos los derechos sobre todos los servicios de administración y mantenimiento de la seguridad.	implícito todo derechos de seguridad	No se puede quitar ni deshabilitar.

Tabla 7: Administrador de seguridad predeterminado

4.1.2.2 Usuarios de servicios predeterminados

El seguimiento**Usuario del servicio**las cuentas están presentes en el primer inicio y restablecimiento de la configuración de seguridad:

Nombre de la cuenta	Defecto Cuenta Estado	Uso	Grupo de derechos Afiliación	notas
Administrador	Activado, Fuerza clave cambio	Esta es la cuenta predeterminada utilizada para la configuración del sistema mediante las aplicaciones IP Office e IP Office Web Manager, incluido one-X Portal for IP. Office/Voicemail Pro administración. Tiene todos los derechos sobre todos los servicios de administración y mantenimiento, incluida la configuración de seguridad.	Administrador, Estado del sistema Solicitud, Socio de negocios	No debe ser eliminado o deshabilitado No debe ser renombrado
EnhTcpaService	Activado	Esta cuenta se usa para las conexiones one-X Portal for IP Office al sistema.	Grupo TCPA	Aunque no se cumpla, la contraseña debe cambiarse tan pronto como posible tanto en IP Office como en one-X Portal for IP Office Activar solo cuando one-X Portal for IP Office desplegada
Servicio IPDECT	Desactivado	Esta cuenta se utiliza para el aprovisionamiento del sistema DECT R4	Grupo IPDECT	Activar solo cuando DECT R4 implementado y modo de aprovisionamiento activo
Administrador de sucursal	Desactivado	Esta cuenta se usa para el acceso del administrador del sistema (SMGR) en una implementación de sucursal	Administrador de SMGR	Habilitar solo cuando se implementa SMGR; se habilitará cuando el Inicial Utilidad de configuración Se ha seleccionado la ejecución (ICU) y la administración de SMGR. No debe ser renombrado
Socio de negocios	Desactivado	Derechos de acceso similares a los de administrador y se pueden usar como una cuenta separada para socios comerciales	Socio de negocios	Debiera ser eliminado/deshabilitado a menos que sea necesario
mantenedor	Desactivado	Cuenta de mantenimiento sin editar configuración ni acceso de seguridad. Se puede usar para Manager (solo lectura), IP Office Web Manager (solo lectura), System Status Application (SSA), Copia de seguridad/restauración, monitor del sistema, actualización	mantenedor	Debiera ser eliminado/deshabilitado a menos que sea necesario

Tabla 8: Usuarios de servicio predeterminados

4.1.2.3 Grupos de derechos predeterminados

El seguimiento**Grupos de derechos**están presentes en la primera puesta en marcha y restablecimiento de la configuración de seguridad:

Nombre del grupo	Uso	Grupo de derechos Usuarios	notas
Administrador Grupo	Permite el acceso completo a la aplicación IP Office Manager para configurar el sistema. Sin acceso de seguridad o mantenimiento	Administrador	Todas las operaciones de IP Office Manager están permitidas Puede usar el administrador de archivos integrado
Gerente de grupo	Permite el acceso limitado a la aplicación IP Office Manager para configurar el sistema.	–	Se permiten todas las operaciones de IP Office Manager excepto: - Eliminar código corto - Ver configuración de LAN2 Puede usar el administrador de archivos integrado
Grupo de operadores	Permite el acceso limitado a la aplicación IP Office Manager para configurar el sistema.	–	Se permiten todas las operaciones de IP Office Manager excepto: - Nuevas creaciones de objetos - Ver configuración de LAN2 - Eliminar directorio - Eliminar ruta de llamada entrante No se puede usar el administrador de archivos incorporado
Estado del sistema Solicitud Grupo	Permite acceso limitado a SSA y Sys System Monitor aplicaciones	Administrador	El derecho de acceso de Sys Monitor solo se verifica cuando se usan usuarios de servicio con Sys Monitor
Grupo TCPA	La aplicación one-X Portal for IP Office utiliza este grupo.	EnhTcpaService	
Grupo IPDECT	La estación base maestra DECT R4 utiliza este grupo para extraer la configuración DECT de IP Office.	Servicio IPDECT	
Administrador de SMGR	SMGR utiliza este grupo para configurar IP Office.	Administrador de sucursal	No cambie los derechos de acceso
Administrador de seguridad	Solo permite el acceso a la configuración de seguridad	–	
Administrador de respaldo	Permite el acceso únicamente a todos los servicios de copia de seguridad y restauración, incluido one-X Portal for IP Office	–	
Actualizar administrador	Permite el acceso al servicio de actualización	–	Permite la actualización de las aplicaciones y el sistema operativo de IP Office
Administrador del sistema	Permite la configuración de IP Office, one-X Portal para IP Office y Voicemail Pro	–	
Administrador de mantenimiento	Permite la configuración de IP Office, one-X Portal for IP Office y Voicemail Pro junto con respaldo, restauración y actualización	–	Normalmente se utiliza para el personal de mantenimiento
Socio de negocios	Acceso completo a todos los servicios de configuración, seguridad y mantenimiento.	Administrador, Socio de negocios	
Administrador de clientes	Administración web, one-X Portal para administración de IP Office y Voicemail Pro	–	Sin acceso al administrador de IP Office
mantenedor	Solo permite la vista de configuración, junto con SSA, copia de seguridad, restauración y actualización de Sys Monitor	–	Normalmente se utiliza para el personal de mantenimiento sin necesidad de cambios de configuración.

Tabla 9: Grupos de derechos predeterminados

4.1.2.4 Asignaciones de grupos de derechos predeterminados

El seguimiento**Grupo de derechos**las asignaciones están presentes en el primer inicio y restablecimiento de la configuración de seguridad:

Servicio	Grupo de Derechos > Derecho de acceso V	Administrar grupo	Gerente Grupo	Operador Grupo	Sistema Estado Aplicación en grupo	TCPA Grupo	IPDECT Grupo	SMGR Administración
Configuración	Leer toda la configuración	✓	✓	✓				
	Escribir toda la configuración	✓	✓	✓				
	Combinar configuración	✓	✓	✓				
	Configuración por defecto	✓	✓	✓				
	Reiniciar/Apagar inmediatamente	✓	✓	✓				
	Reiniciar cuando esté libre	✓	✓	✓				
	Reiniciar a la hora del día	✓	✓	✓				
Administrador de seguridad	Leer toda la seguridad ajustes							
	Escriba toda la seguridad ajustes							
	Restablecer toda la seguridad ajustes							
	Escriba su propia contraseña de usuario de servicio							
Estado del sistema Solicitud	Estado del sistema Acceso a la aplicación				✓			
	Leer toda la configuración				✓			
	Control de sistema				✓			
	Monitor del sistema				✓			
API de telefonía	Acceso TSPI mejorado					✓		
	Enlace de desarrollo 3							
	API de ubicación							
HTTP	Aprovisionamiento DECT R4						✓	
Servicios web	Seguridad Leer Todo							✓
	Seguridad Escribir todo							✓
	Seguridad Escritura Propia Clave							✓
	Configuración Leer todo							✓
	Configurar escribir todo							✓
	Respaldo							✓
	Restaurar							✓
	Mejora							✓
Externo	Correo de voz Pro básico							
	Correo de voz Pro estándar							
	Buzón de voz profesional Administrador							✓
	Administrador de one-X Portal para IP Office							

Servicio	Grupo de Derechos > Derecho de acceso V	Administrar grupo	Gerente Grupo	Operador Grupo	Sistema Estado Aplicación en grupo	TCPA Grupo	IPDECT Grupo	SMGR Administración
	Portal one-X para superusuario de IP Office							
	control web Administrador							
	Seguridad de control web							
	Administrador WebRTC							

Servicio	Grupo de Derechos > Derecho de acceso V	Seguridad Administración	Respaldo Administración	Mejora Administración	Sistema Administración	Mantenimiento Administración	Negocio Compañero	Disfraz ejem Administración	Mantenimiento ainer
Configuración	Leer toda la configuración				✓	✓	✓		✓
	Escribir toda la configuración				✓	✓	✓		
	Combinar configuración				✓	✓	✓		
	Configuración por defecto						✓		
	Reiniciar/Apagar inmediatamente						✓		
	Reiniciar cuando esté libre						✓		
	Reiniciar a la hora del día						✓		
Administrador de seguridad	Leer toda la seguridad ajustes	✓					✓		
	Escriba toda la seguridad ajustes	✓					✓		
	Restablecer toda la seguridad ajustes	✓					✓		
	Escriba su propia contraseña de usuario de servicio	✓					✓		
Estado del sistema Solicitud	Estado del sistema Acceso a la aplicación						✓		✓
	Leer toda la configuración						✓		✓
	Control de sistema						✓		✓
	Monitor del sistema						✓		✓
API de telefonía	Acceso TSPI mejorado								
	Enlace de desarrollo 3								
	API de ubicación								
HTTP	Aprovisionamiento DECT R4								
Servicios web	Seguridad Leer Todo	✓					✓		
	Seguridad Escribir todo	✓					✓		
	Seguridad Escritura Propia Clave	✓			✓		✓	✓	
	Configuración Leer todo				✓		✓	✓	
	Configurar escribir todo				✓		✓	✓	
	Respaldo		✓			✓	✓	✓	✓
	Restaurar		✓			✓	✓	✓	✓

Servicio	Grupo de Derechos > Derecho de acceso V	Seguridad Administración	Respaldo Administración	Mejora Administración	Sistema Administración	Mantenimiento Administración	Negocio Compañero	Disfraz ejem Administración	Mantenimiento ainer
	Mejora			✓		✓	✓	✓	✓
Externo	Correo de voz Pro básico								✓
	Correo de voz Pro estándar				✓	✓		✓	
	Buzón de voz profesional Administrador						✓		
	Administrador de one-X Portal para IP Office				✓	✓	✓	✓	
	Portal one-X para superusuario de IP Office		✓						✓
	control web Administrador						✓		✓
	Seguridad de control web	✓					✓		
	Administrador WebRTC								

Tabla 10: Asignaciones de grupos de derechos predeterminados

4.2 Configuración de seguridad en la actualización

Cuando se actualiza el sistema IP Office y se agregan nuevos grupos de derechos o servicios, a los usuarios existentes solo se les otorgarán los nuevos derechos si las cuentas de los usuarios del servicio están predeterminadas. Esto evita cambios inesperados de derechos en la actualización. Si se requiere acceso a estos nuevos derechos o servicios, deben agregarse manualmente después de que se haya completado el proceso de actualización.

Capítulo 5.
Contraseña y PIN administración

¿Comentarios sobre este documento? infodev@avaya.com

5. Gestión de contraseñas y PIN

En general, la resistencia de contraseñas y PIN a Guessing (ataques que usan contraseñas predeterminadas, palabras de diccionario o fuerza bruta) y Cracking (ataques que intentan hacer coincidir el cálculo de inicio de sesión sin necesidad de conocer la contraseña real) se puede mejorar considerablemente con contraseñas "fuertes". y una política de cambio de contraseña.

Una contraseña segura suele ser aquella que:

- Es largo (por ejemplo, al menos 8 caracteres)
- Complejo (por ejemplo, contiene caracteres superiores, inferiores y numéricos)
- No contiene secuencias ni caracteres repetidos
- No es fácil de adivinar. Las contraseñas adivinables incluyen:
  - Contraseña igual que el nombre de cuenta o el número de extensión (o al revés)
  - Palabras del diccionario
  - Palabras de diccionario con sustitución de números
  - palabras al revés
  - Información personal o corporativa
  - Fecha de nacimiento
  - Contraseñas predeterminadas

Un PIN/código de inicio de sesión fuerte suele ser uno que:

- Es largo. Un PIN de 13 dígitos es similar en fuerza a una contraseña de 8 caracteres que distingue entre mayúsculas y minúsculas
- No contiene secuencias ni dígitos repetidos
- No contiene secuencias de teclado (por ejemplo, 2580)
- No es fácil de adivinar. Los PIN adivinables incluyen:
  - PIN igual que el número de extensión (o al revés)
  - Información personal o corporativa
  - Fecha, predominante cuando se aplica una longitud mínima de 4, 6 u 8 dígitos
  - Códigos de inicio de sesión predeterminados

La seguridad y la administración de contraseñas y PIN no se tratan en detalle aquí, pero existen muchas publicaciones que incluyen:

- **Publicación especial de NIST (SP) 800-118, Guía para la gestión de contraseñas empresariales (borrador):** ttp://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
- **Centro para la Protección de la Infraestructura Nacional (CPNI), SISTEMAS DE PROTECCIÓN Y DATOS, ASESORAMIENTO DE CONTRASEÑA**
  http://www.cpni.gov.uk/documents/publications/2012/2012029-password_advice.pdf
- **Consejo de seguridad de US-CERT (ST04-002), elección y protección de contraseñas:**
  https://www.us-cert.gov/ncas/tips/ST04-002

5.1 Política de contraseñas y PIN

En una nueva instalación de IP Office, cuando enciende un servidor Linux o inicia sesión por primera vez en Manager o IP Office Web Manager, debe cambiar las tres contraseñas de la cuenta del sistema: Administrador, Administrador de seguridad y contraseña del sistema.

Tanto la política de contraseñas de usuario de servicio como de IP Office se configura en el**Configuración de seguridad | General**ficha de IP Office Manager. La configuración de la política incluye:

- Longitud mínima del nombre y la contraseña del usuario del servicio
- Complejidad mínima de la contraseña del usuario del servicio
- Número de intentos de falla consecutivos y la acción posterior; nada, registro, desactivación temporal, desactivación permanente
- Asegúrese de que no se reutilicen contraseñas anteriores
- Cambio de contraseña obligatorio, tanto inmediato como periódico
- Tiempo de espera de cuenta inactiva
- Conjunto separado de configuraciones de políticas de usuario de IP Office para permitir la diferenciación

Los PIN se utilizan en IP Office para el inicio de sesión del usuario de telefonía (Código de inicio de sesión), el registro de la extensión de VoIP (Contraseña del teléfono) y el acceso al buzón de correo de voz (Código de inicio de sesión del correo de voz). La política se configura usando**Sistema | Correo de voz | Complejidad del código de correo de voz**y**Sistema | Telefonía | Complejidad del código de inicio de sesión**:

- Código mínimo de inicio de sesión y longitud de registro de extensión
- Código mínimo de inicio de sesión y complejidad de registro de extensión
- Longitud mínima del código de correo de voz
- Complejidad mínima del código de correo de voz

5.2 Contraseñas de usuarios administrativos

Hay varias cuentas que se utilizan para el acceso administrativo, de mantenimiento y de máquinas/servicios. Las siguientes tablas cubren esas interfaces, sus atributos de contraseña y dónde se encuentran las configuraciones de la cuenta:

Interfaz de inicio de sesión	Configuraciones de la cuenta	notas
· **Gerente** · **Administrador de la edición del servidor** · **Administrador web de IP Office** · **Estado del sistema Solicitud (SSA)** · **control web** · **Cliente Voicemail Pro** · **Monitoreo del sistema***	Servicio Nombre de usuario y contraseña. Diversos derechos de acceso Contraseña: 1-31 caracteres Unicode	Cambiar usando Manager en el modo de configuración de seguridad o Web Security Manager Se aplica la configuración de seguridad para la política de contraseñas del usuario del servicio Bloqueo temporal o permanente al número de intentos fallidos consecutivos. El estado de bloqueo actual se puede ver en Manager en Seguridad | Usuarios del servicio | Detalles del usuario del servicio * System Monitor usará esta cuenta cuando el **Seguridad | Sistema | Interfaces no seguras | Usar credenciales de usuario del servicio**está activo
· **Actualización del administrador**	Contraseña del sistema Contraseña: 1-31 caracteres ASCII imprimibles	Cambiar usando Manager en el modo de configuración de seguridad
· **Monitoreo del sistema*** · **DevLink**	Contraseña del monitor del sistema Contraseña: 1-31 ASCII 0-9, az, caracteres AZ	Cambiar usando Manager en el modo de configuración de seguridad * System Monitor usará esta contraseña cuando el**Seguridad | Sistema | Interfaces no seguras | Usar credenciales de usuario del servicio**está inactivo
· **Cliente Voicemail Pro**	Tres roles de administrador: - Administrador - Estándar - Básico Contraseña: 5-31 caracteres ASCII imprimibles excepto \ / : * ? < > | , ;.	Cambiar usando el cliente VMPro, pestaña Administradores de Voicemail Pro Se utiliza para Voicemail Pro como cuenta alternativa cuando la autenticación recomendada de IP Office no está disponible.
· **Registrador de contactos**	Dos roles de administrador: - Administrador del sistema - Administrador restringido Contraseña: 1-99 caracteres Unicode excepto espacio	Cambiar usando la página de administración web de Contact Recorder, pestaña del sistema
· **one-X Portal para administración de IP Office**	Dos roles de administrador: - Administrador - Copia de seguridad de restauracion Contraseña: 1-31 caracteres Unicode	Cambiar usando one-X Portal para la página web de administración de IP Office, **Configuración | Usuarios**panel. Se usa para one-X Portal for IP Office como respaldo cuando la autenticación referida de IP Office no está disponible
· **Shell seguro de Linux (SSH)**	Un rol de administrador: 'Administrador' Contraseña: 1-31 caracteres ASCII imprimibles	Cambiar usando la pantalla de inicio de sesión de Control web Solo se puede cambiar la contraseña
· **Interfaz de consola de Linux (CLI)**	Dos roles de administrador: - Administrador - raíz Contraseña: 1-31 caracteres ASCII imprimibles	Cambiar usando la pantalla de inicio de sesión de Control web Cambiar usando Web Control,**Configuración | Sistema**pestaña Solo puede cambiar contraseñas
· **VMPro <-> interfaz de servicio de IP Office**	Contraseña de VMPro Contraseña: 31 caracteres ASCII imprimibles	Cambiar usando Manager en el modo de configuración de seguridad Cambiar usando el cliente VMPro,**Preferencias del sistema | General**pestaña.
· **one-X Portal para IP Office <-> servicio de IP Office interfaz**	Servicio Nombre de usuario y contraseña Contraseña: 1-31 caracteres Unicode	Cambie usando Manager en el modo de configuración de seguridad o Web Security Manager. Cambiar usando one-X Portal para la página web de administración de IP Office, **Configuración | Proveedores | Proveedor predeterminado de CSTA | Editar** panel

Página1698 de 3226.

Interfaz de inicio de sesión	Configuraciones de la cuenta	notas
· **TAPI Link Pro (TAPI de terceros)**	Contraseña del sistema Contraseña: 1-31 caracteres ASCII imprimibles	Cambiar usando Manager en el modo de configuración de seguridad TAPI Link Lite está cubierto enOficina de PI Contraseñas y códigos de inicio de sesión de los usuarios .
· **Aprovisionamiento DECT R4**	Servicio Nombre de usuario y contraseña Contraseña: 1-31 caracteres Unicode	Cambiar usando Manager en el modo de configuración de seguridad Cambiar usando la interfaz de administración web de la estación base
· **API DevLink3** · **API de ubicación** · **API de supervisión de servicios** · **API de SDK de administración web**	Servicio Nombre de usuario y contraseña Contraseña: 1-31 caracteres Unicode	Cambiar usando Manager en el modo de configuración de seguridad

Tabla 11: Contraseñas de usuarios administrativos

5.3 Contraseñas de usuario y códigos de inicio de sesión de IP Office

La siguiente tabla indica qué componentes de IP Office usan qué contraseña, PIN de correo de voz o código de inicio de sesión al iniciar sesión en las diversas interfaces.

- La contraseña se define en el campo de configuración**Usuario | Usuario | Clave**y normalmente se usa durante el inicio de sesión de la aplicación.
- El código de correo de voz está definido por el campo de configuración**Usuario | Correo de voz | Código de correo de voz**y se utiliza para iniciar sesión en el buzón.
- El código de inicio de sesión está definido por el campo de configuración**Usuario | Telefonía | Configuración del supervisor | Código de inicio de sesión**y se utiliza para iniciar sesión en el teléfono. Un nuevo campo en la versión 9.0+ permite el inicio de sesión del teléfono VoIP en la extensión, no en el registro del usuario:**Extensión | Ext. | Contraseña del teléfono**.

Todas las contraseñas y códigos de inicio de sesión se pueden cambiar en IP Office e IP Office Web Manager.

Interfaz de inicio de sesión	Configuración de cuenta	notas
• **SoftConsole** • **Navegador one-X Portal** • **Preferido de one-X Mobile** • **Comunicador Windows/iPad** • **Softphone de vídeo de IP Office** • **Complemento de Outlook, Asistente de llamadas** • **Complemento de Salesforce y Lync** • **TAPI Link Lite (TAPI original)** • **Usuarios de RAS (llamada entrante)** • **Autoadministración web** • **Colaboración web** **propietario de la conferencia** • **Agente/Supervisor de Reportero de Contacto Integrado** • **Cliente web de IP Office**	• Nombre:**Usuario	Usuario	Nombre** • Clave:**Usuario	Usuario	Clave** • Atributos: 0-31 ASCII 0-9, az, caracteres AZ	Se aplica la configuración de seguridad para la política de contraseñas de usuario de IP Office TAPI Link Pro y DevLink son cove rojo en Contraseñas de usuarios administrativos34. Bloqueo temporal o permanente al número de intentos fallidos consecutivos.
• **Buzón Voicemail Pro** • **Buzón de correo de voz incorporado**	• Extensión de usuario:**Usuario	Usuario	Extensión** • Código de correo de voz:**Usuario	Correo de voz	Código de correo de voz** • Atributos: 0-15 dígitos ASCII	Se aplican las configuraciones de correo de voz para la política de contraseña/PIN:**Sistema	Correo de voz	Complejidad del código de correo de voz**. No se requiere ingresar el código del correo de voz del usuario si accede al correo de voz desde una extensión confiable.
• **Inicio de sesión del teléfono del usuario de IP Office**	• Extensión de usuario:**Usuario	Usuario	Extensión** • Código de inicio de sesión:**Usuario	Telefonía	Configuración del supervisor	Código de inicio de sesión** • Atributos: 0-31 dígitos ASCII	Se aplica la configuración del sistema para la política de contraseña/PIN:**Sistema	Telefonía	Complejidad del código de inicio de sesión**. Bloqueo temporal al número de intentos fallidos consecutivos.
• **Registro de teléfono H323** • **Registro de teléfono SIP**	• Extensión telefónica:**Extensión	Ext.	Extensión de base** • Código de inicio de sesión:**Usuario	Telefonía	Configuración del supervisor	Código de inicio de sesión** • Atributos: 0-31 dígitos ASCII	Se aplica la configuración del sistema para la política de contraseña/PIN:**Sistema	Telefonía	Complejidad del código de inicio de sesión**. Bloqueo temporal por número de intentos fallidos consecutivos Para R9.0+, H323**Extensión	Ext.	Contraseña del teléfono**el campo se utiliza si está establecido. El estado de bloqueo actual se puede ver y restablecer en SSA en**Sistema	Seguridad VoIP	Extensiones en la lista negra**y**Direcciones en la lista negra**.

Tabla 12: Contraseñas de usuario y códigos de inicio de sesión

Capítulo 6.

Certificados y Fideicomiso

6. Certificados y Fideicomiso

Los certificados digitales se utilizan dentro de la solución IP Office para una serie de propósitos:

- Firma de firmware, aplicaciones y applets de Java para asegurar su origen.
- Identificar IP Office para otros sistemas, aplicaciones y usuarios.
- Verificación de la identidad de otros sistemas, aplicaciones y usuarios.
- Configuración de enlaces de seguridad de la capa de transporte (TLS), incluidos HTTPS y SIP.
- Incorporación de IP Office en un dominio de confianza más amplio.

Los certificados digitales están definidos por el formato X509v3 y se han convertido en el estándar de facto para la mayoría de las operaciones de seguridad que involucran la verificación de identidad. La identidad de personas, sistemas y aplicaciones puede afirmarse mediante un certificado con una clave 'pública' y su correspondiente clave 'privada'. La clave pública es parte del certificado, junto con otra información de identidad y otros datos de seguridad digital.

Por ejemplo, Avaya firma sus aplicaciones con su clave privada y hace público el certificado correspondiente. Cualquiera que desee comprobar la solicitud, puede tomar el certificado y usar la clave pública para desbloquear la firma y verificar:

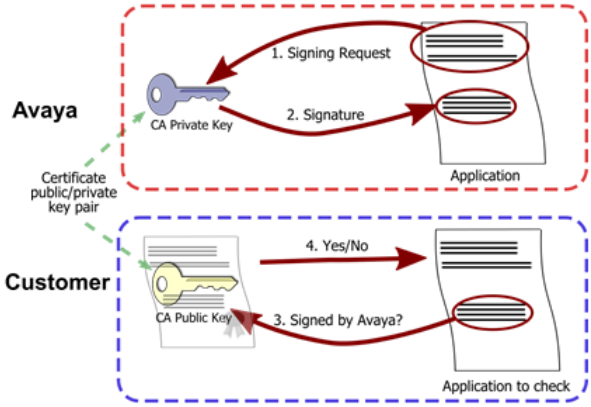


Figura 5: Comprobación de clave de aplicación de Avaya

Un punto del ejemplo anterior es que la clave privada debe permanecer privada; cualquier persona con acceso a la clave puede hacerse pasar por Avaya.

Para garantizar una mayor confianza, una parte de confianza puede firmar la clave pública y la información sobre su propietario. Una parte confiable que emite certificados digitales se denomina autoridad de certificación (CA), similar a una agencia gubernamental que emite licencias de conducir. Una CA puede ser un proveedor de servicios de certificación externo o un gobierno, o la CA puede pertenecer a la misma organización que las entidades a las que sirve. Las CA también pueden emitir certificados a otras CA subordinadas, lo que crea una confianza de certificado en forma de árbol denominada Infraestructura de clave pública (PKI):

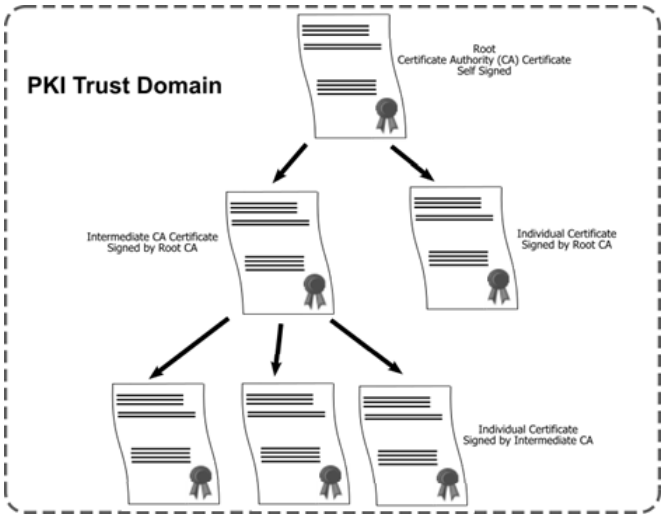


Figura 6: Dominio de confianza de PKI

Página1702 de 3226.

6.1 Terminología del certificado

A lo largo de este documento, se utilizarán los siguientes términos y definiciones en el contexto de los certificados:

- **Certificado**
  Un certificado digital que contiene información de identidad, una clave pública y otros datos de seguridad digital conforme al estándar X.509 v3.
- **Autoridad de certificación (CA)**
  Una entidad que puede emitir certificados de identidad firmados por otro certificado.
- **Certificado de CA raíz**
  Un certificado 'autofirmado' (es decir, un certificado que ha sido firmado por sí mismo) que representa la raíz de la autoridad de certificación de la jerarquía de certificados cuya clave privada se puede usar para firmar otros certificados. La mayoría de los sistemas operativos y navegadores se envían con muchos certificados de CA raíz de autoridades públicas en los que se confía de forma predeterminada.
- **Certificado CA Intermedio**
  Un certificado que ha sido creado por firmado por una CA con el propósito de firmar otros certificados.
- **Certificado de Identidad**
  Un certificado utilizado para representar la identidad de una entidad. Para ser utilizado como certificado de identidad, también debe estar presente la clave privada asociada.
- **Certificado de confianza**
  Un certificado en el que confía una entidad.
- **Almacén de confianza (almacén de certificados de confianza/TCS)** Un almacén de certificados de confianza.
- **Raíz de confianza/anclaje de confianza**
  El certificado de nivel superior en el que confía una entidad.
- **Cadena de certificados**
  Una lista de certificados, comenzando con el Certificado de identidad seguido de uno o más certificados de CA (generalmente el último es el certificado de CA raíz) donde cada certificado de la cadena está firmado por el certificado posterior.
- **Dominio de confianza**
  Una única estructura de confianza de PKI, por ejemplo, una 'isla de autoridad'.
- **Autenticación del servidor**
  La comprobación del certificado de un servidor por parte de un cliente.
- **Autenticacion mutua**
  La comprobación del certificado de un cliente por parte de un servidor.
- **Verificación de identidad del certificado**
  El origen del certificado (dirección IP, URL, etc.) se compara con el contenido de los campos Nombre y Nombre alternativo del sujeto del certificado.
- **Certificado de dominio único**
  Un certificado creado para un solo servidor con solo un campo de nombre/dominio (es decir, una identidad).
- **Certificado multidominio**(también llamado**'SAN múltiple**o**'Comunicaciones Unificadas'**certificado)
  Un certificado creado para un solo servidor con muchos dominios/identidades, cada identidad es una entrada de nombre.
- **Certificado comodín**
  Un certificado creado para varios servidores o un solo servidor con muchos dominios/identidades. La entrada de nombre tiene el formato '*.example.co metro'. Los certificados comodín conllevan riesgos y limitaciones de seguridad adicionales. Ver Contenido del nombre del certificado 50.

6.1.1 Componentes de un Certificado

Los certificados se componen de una serie de campos, algunos obligatorios y otros opcionales:

- **Versión**
  Por lo general, V3: indica el formato X.509 v3
- **Número de serie**
  Un número único que se utiliza para identificar de forma única el certificado. No hay ningún requisito de que el número esté realmente serializado, solo que sea único.
- **Tema**(alias**emitido a**)
  La entidad (persona, sistema, etc.) identificada por el certificado. Esto se divide en una serie de subcampos: nombre común (CN), unidad organizativa (OU), correo electrónico, etc. Por lo general, se hace referencia al CN como el 'Nombre' del certificado.
- **Nombre alternativo del sujeto**
  Nombres alternativos por los que se puede identificar a la entidad. Estas entradas a menudo se prueban para asegurar al destinatario la fuente del certificado. Por ejemplo, la dirección IP del servidor remoto debe coincidir con uno de los nombres de este campo.
- **Editor:**(alias**Emitido por**)
  La entidad CA que verificó la información y emitió el certificado. Esto también se divide en una serie de subcampos como Asunto.
- **Válida desde**
  La hora/fecha UTC a partir de la cual el certificado es válido por primera vez.
- **Válido hasta**
  La hora/fecha de caducidad.
- **Uso de clave**
  Finalidad para la que se puede utilizar la clave pública (por ejemplo, firma de certificados, cifrado, etc.).
- **Algoritmo de firma**
  El algoritmo criptográfico utilizado para crear la firma.
- **Firma**
  Los datos de la firma para comprobar que procede del emisor. Cifrado con la clave privada del emisor, se puede descifrar con la clave pública del emisor que se encuentra en el certificado del emisor.
- **Algoritmo de clave pública**
  El tipo de clave pública (por ejemplo, RSA, DSA, etc.).
- **Llave pública**
  La clave pública.

Hay otros campos que pueden estar presentes, consulteRFC5280 para más información.

6.1.2 Seguridad del Certificado

El tamaño de la clave pública y el algoritmo de huella digital utilizados determinan en parte qué tan resistente es el certificado a ser comprometido. Muchos organismos gubernamentales ahora determinan que los certificados con algoritmos de huella digital MD5 y SHA-1, o claves públicas de menos de 2048 bits, no son seguros.

6.1.3 Comprobaciones de certificados

Cuando se recibe un certificado con vistas a verificar la identidad, se pueden realizar una serie de pruebas y controles:

- Se evalúa la validez básica del certificado, como la integridad, la fecha de inicio/finalización, la información de uso, la solidez de la clave pública, etc.
- El asunto del certificado recibido y los nombres alternativos se verifican con la fuente del certificado; por ejemplo, la dirección IP o el nombre de dominio. Esto se denomina 'Verificación de identidad del certificado'.
- Se extrae el emisor y se busca en el almacén de certificados de confianza (TCS) un certificado que coincida. Cuando se encuentra, la firma del certificado recibido se comprueba utilizando la clave pública del certificado de confianza. Esto se repite hasta que se encuentra un certificado de CA raíz de confianza.
- Si la información de revocación está presente en el certificado de la CA raíz, el certificado recibido se verifica con la CA para ver si ha sido revocado (es decir, si la autoridad canceló o retiró el certificado).

Debido a la variedad de implementaciones, el contenido del certificado, la configuración configurable y la herencia, muchos sistemas y aplicaciones difieren mucho en la aplicación de dichas pruebas.

6.1.4 Certificados y el protocolo de seguridad de la capa de transporte (TLS)

TLS utiliza los certificados de varias maneras:

- Intercambio de claves utilizadas para el cifrado simétrico al inicio de la sesión.
- Verificación de la identidad del servidor TLS
- Verificación de la identidad del cliente TLS

Debido a la forma en que funciona TLS, el servidor siempre debe tener un certificado; de lo contrario, la sesión TLS no puede iniciarse y ese certificado siempre se presenta al cliente. Para obtener el certificado del cliente, el servidor debe solicitarlo explícitamente.

Normalmente, la verificación de identidad tanto del cliente como del servidor es configurable, junto con el conjunto exacto de comprobaciones realizadas en los certificados recibidos. Sin tales controles, TLS puede ser susceptible a ataques de intermediarios.

La plataforma IP Office es compatible con TLS v1.0, v1.1 y v1.2. Todas las interfaces TLS comienzan con TLS v1.2 pero pueden permitir la negociación hasta v1.1 o v1.0 por compatibilidad. Hay configuraciones de administrador de IP Office, Voicemail Pro, IP Office Web Manager y one-X Portal para IP Office para la 'versión mínima de TLS' que aplican v1.2 . Tenga en cuenta que algunos clientes de Avaya no son compatibles con v1.2 en la actualidad. VerApéndice F: seguridad de terminales VoIP de IP Office 127.

6.1.5 Nombre y formato del archivo de certificado

Como tantos otros aspectos de los certificados, existen varias opciones y estándares (tanto formales como informales) asociados con los archivos de certificados.

Formatos de archivo

Hay cuatro codificaciones/formatos internos principales para los archivos de certificado. Tenga en cuenta que estas son codificaciones, no convenciones de nomenclatura de archivos:

Formato	Descripción
DER	Formato Distinguished Encoding Rules (DER), que es un formato binario utilizado para representar un certificado. Por lo general, se usa para describir solo un certificado y no puede incluir una clave privada.
PEM	Privacy Enhanced Mail (PEM) es una codificación Base 64 (es decir, texto ASCII) de DER, un certificado se incluye entre '-----BEGIN CERTIFICATE-----' y '-----END CERTIFICATE- ----' declaraciones. Puede contener una clave privada encerrada entre las sentencias '-----BEGIN PRIVATE KEY -----' y '-----END BEGIN PRIVATE KEY -----'. Se puede incluir más de un certificado. PEM se identifique visualizando el archivo en un editor de texto. • Este es un formato no seguro y no se recomienda para el uso de claves privadas a menos que esté protegido con una contraseña.
PKCS#12	Estándar de criptografía de clave pública (PKCS) #12. Un formato binario seguro, encriptado con una contraseña. Por lo general, se usa para describir un certificado y su clave privada asociada, pero también puede incluir otros certificados, como los certificados de firma. Este es el formato recomendado para el uso de claves privadas.
PKCS#7	Una codificación Base 64 (es decir, texto ASCII) definida por RFC 2315, uno o más certificados se incluyen entre las declaraciones '—–BEGIN PKCS—–' y '—–END PKCS7—–'. Solo puede contener certificados y certificados de cadena, pero no la clave privada. Se puede identificar viendo el archivo en un editor de texto.

Tabla 13: Formatos de archivo de certificado

Extensiones de nombre de archivo

Hay muchas extensiones de nombre de archivo comunes en uso:

Extensión	Descripción
. tubo de rayos catódicos	Puede ser DER o PEM. Extensión típica utilizada por los archivos de certificados públicos de los sistemas Unix/Android en formato DER.
. RCE	Puede ser DER o PEM. Extensión típica utilizada por los archivos de certificados públicos de los sistemas Microsoft/Java en formato PEM.
. PEM	Solo debe estar codificado con PEM
. DER	Solo debe estar codificado en DER
. p12	Solo debe estar en formato PKCS#12. Extensión típica utilizada por los certificados de identidad de los sistemas Unix/Android/ archivos de pares de claves privadas. Mismo formato que .pfx, por lo tanto, simplemente se puede cambiar el nombre.
. pfx	Solo debe estar en formato PKCS#12. Extensión típica utilizada por los archivos de pares de claves privadas/certificados de identidad de los sistemas de Microsoft. El mismo formato que .p12, por lo tanto, se puede renombrar simplemente.
. pb7	Solo debe estar en formato RFC 2315. Extensión típica utilizada por los sistemas Microsoft y Java para cadenas de certificados.

Tabla 14: Extensiones de nombre de archivo de certificado

Se pueden usar herramientas de terceros, como OpenSSL y el complemento Certificado de la consola de administración de Windows, para convertir entre los distintos formatos., C se debe tomar para no exponer ninguna clave privada. VerCreación de una CSR mediante la línea de comandos del servidor Linux 140para obtener información sobre la conversión de formato OpenSSL.

6.2 Compatibilidad con certificados de IP Office

La plataforma IP Office admite certificados de varias maneras, la mayoría de las cuales se pueden configurar a través de la configuración de seguridad:

- Un certificado de identidad para cada sistema y sus aplicaciones locales, incluido un certificado de identidad independiente opcional para las interfaces de gestión y telefonía.
- Certificado de identidad único autogenerado por todos los sistemas cuando sea necesario.
- El certificado de identidad puede administrarse a través de IP Office Manager o IP Office Web Manager, u obtenerse automáticamente mediante el Protocolo simple de inscripción de certificados (SCEP) o PKCS#10 (solo IP Office Linux).
- DER y PEM para importar/exportar archivos de certificados, y PKCS#12 para importar/exportar pares de certificados/claves privadas.
- Una autoridad de certificación en el servidor de aplicaciones Linux principal y Linux, incluida la compatibilidad con el nombre alternativo del sujeto.
- El procesamiento de certificados puede admitir claves RSA públicas de 1024, 2048 y 4096 bits, y hash SHA-1, SHA-256, SHA-224 y SHA-512.
- Un almacén de certificados de confianza (TCS) de 64 entradas como mínimo.
- Contenido de TCS predeterminado configurable, restaurado al restablecer la configuración de seguridad.
- Controles individuales por servicio para hacer cumplir la autenticación de certificados mutuos donde se solicita y prueba el certificado del cliente.
- La gestión separada y la telefonía recibieron niveles de verificación de certificados que brindan pruebas cada vez más rigurosas. Esto incluye una configuración 'alta' que prueba no solo la cadena de confianza sino también la presencia del certificado recibido en el TCS.
- Compatibilidad con certificados de CA intermedios, tanto para las CA como para la cadena de certificados de identidad que ofrece IP Office y sus aplicaciones.
- Errores, alarmas y advertencias para ayudar a identificar problemas de certificados.

Actualmente, la compatibilidad con certificados de IP Office no incluye lo siguiente:

- Las aplicaciones de Linux (incluido one-X Portal for IP Office, Voicemail Pro y Contact Recorder) no se pueden configurar para la autenticación mutua. es decir, no pueden cotejar ningún certificado recibido con el TCS.
- No se solicitan certificados de clientes SIP.
- Las pruebas de certificados recibidos de IP Office no incluyen comprobaciones de revocación como OCSP o CRL.
- Las pruebas de certificados recibidos de IP Office no incluyen asegurar la fuente del certificado mediante entradas de nombre alternativo del sujeto. es decir, Certificado de verificación de identidad.
- No se admiten certificados de clave pública DSA o EC-DSA, ni claves públicas RSA superiores a 4096 bits. Se recomienda utilizar claves públicas RSA de 2048 bits.
  - Los servidores IP500 V2 no admiten la generación manual de una solicitud de firma de certificado (CSR) donde la clave privada se conserva dentro del servidor. O unw Se puede utilizar una solicitud basada en formularios eb o una herramienta de terceros para crear un CSR. VerSolicitudes de firma de certificado 134para obtener más información sobre cómo generar una CSR para IP Office.

6.2.1 Soporte de certificado de interfaz

Los certificados son compatibles con todas las interfaces TLS y SSH de IP Office, incluido HTTPS, ya sea cliente o servidor.

- **Nota:**SSLv2 y SSLv3 no son compatibles con IP Office.

Para obtener información sobre la funcionalidad básica de TLS, consulteCertificados y la seguridad de la capa de transporte (TLS) 41.

Hay una serie de configuraciones de IP Office que afectan la operación del certificado

la mesa enCompatibilidad con certificados de interfaz de IP Office 123enumera todos los enlaces TLS en la solución de la plataforma IP Office y sus capacidades de seguridad, incluida la compatibilidad con certificados.

la mesa enSeguridad de punto final VoIP de IP Office 127enumera los clientes de VoIP en la solución de la plataforma IP Office y sus capacidades de seguridad.

6.2.2 Configuración inicial del certificado

- **Soporte de certificado de interfaz** 44
- **Contenido del nombre del certificado** 50
- **Controles de comprobación de certificados** 52
- **Distribución de certificados** 53
- **Determinación de la política de confianza** 56
- **Enfoques de confianza de IP Office PKI** 57
- **Selección de PKI de IP Office** 59
- **Implementación de PKI de IP Office** 59
- **Certificados de autoridades de certificación externas** 62
- **Mantenimiento de certificados** 64

6.2.2.1 Configuración del certificado inicial de IP500 V2

IP500 V2 siempre creará un certificado de CA autofirmado único en la puesta en marcha inicial y en el restablecimiento de la configuración de seguridad. Contendrá los campos del certificado que se enumeran a continuación.

Este certificado se puede utilizar para operaciones de PKI de manera limitada; tiene cierto valor de seguridad, pero no forma parte de una PKI más amplia y, por lo tanto, nadie más puede confiar en él, a menos que este certificado esté instalado en el TCS pertinente.

Campo de certificado	Contenido	notas
Versión	V3	Siempre formato X.509 V3
Número de serie	Gran número aleatorio	Asegura que el número de serie sea único No más de 20 bytes
Asunto (Emitido para)	CN = ipoffice-nnnnnnnnnn.avaya.com O = Avaya Inc. OU = GC L = Basking Ridge S = Nueva Jersey C = EE. UU. E = soporte@avaya.com	Dónde*nnnnnnnnnn*es la dirección mac LAN 1, por ejemplo*ipoffice-00e00705918e.avaya.com*
Sujeto Alternativo Nombres	1: Nombre DNS=ipoffice-nnnnnnnnnn.avaya.com 2: Dirección IP=abcd 3: dirección IP = efgh	Dónde: - nnnnnnnnnn es la dirección mac de LAN 1 - abcd es la dirección IP de LAN 1 en el momento de la creación del certificado - efgh es la dirección IP de LAN 2 en el momento de la creación del certificado
Emisor (Emitido por)	CN = ipoffice-nnnnnnnnnn.avaya.com O = Avaya Inc. OU = GC L = Basking Ridge S = Nueva Jersey C = EE. UU. E = soporte@avaya.com	Mismo contenido que Asunto: Certificado autofirmado
Válida desde	DD/MM/AA HH:MM:SS	Reflejará la hora/fecha UTC menos 24 horas cuando se creó el certificado. Si el reloj de tiempo real estaba dañado o no estaba configurado, la hora se fijará a las 00:00:00 del 1 de enero del año en que se lanzó el software.
Válido hasta	Válido desde más 825 días	
Uso de clave	acuerdo clave Cifrado clave firma digital, no repudio, Cifrado de datos keyCertSign	Marcado no crítico El certificado se puede utilizar para el conjunto de operaciones de certificado de IP Office
Uso extendido de claves	id-kp-serverAuth id-kp-clientAuth	Marcado no crítico El certificado se puede utilizar para el conjunto de operaciones de certificado de IP Office
Restricciones básicas	CA: cierto pathLenConstraint: 0	Marcado crítico El certificado se puede utilizar de forma aislada como una CA, este no puede firmar ningún otro certificado.
Algoritmo de firma	sha256rsa	
Firma	Datos de firma	
Algoritmo de clave pública	RSA	
Llave pública	Tamaño 2048 bits	

Tabla 15: Configuración del certificado inicial de IP500 V2

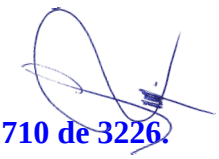
Nota

1. La dirección correcta de LAN 1 y LAN 2 debe configurarse durante la instalación inicial y el certificado de identidad debe regenerarse manualmente.

6.2.2.2 Servidores Linux antes de la ignición

Las distribuciones de Unified Communications Module y Server Edition predeterminadas antes de que se complete el encendido no tienen un certificado único. Para conectar un navegador para encender, este certificado requiere ser aceptado temporalmente. Nunca debe almacenarse permanentemente. Está autofirmado y contiene un asunto y un emisor de '*ipofficedefault.avaya.com*'.

Una vez que se completa el encendido, se reemplaza por el certificado de identidad correspondiente según el tipo de servidor resultante.



6.2.2.3 Configuración del certificado inicial del servidor de aplicaciones Linux/principal de Server Edition

El servidor de aplicaciones principal y Linux tienen una autoridad de certificación incorporada. Durante el proceso de encendido, el instalador puede optar por mantener el certificado raíz de CA predeterminado que se usa para firmar o importar otro como un par de claves pública/privada. Este certificado importado puede ser una CA raíz o una CA intermedia.

Si se conserva la CA interna, tiene los contenidos que se enumeran a continuación.

Campo de certificado	Contenido	notas
Versión	V3	Siempre formato X.509 V3
Número de serie	Gran número aleatorio	Asegura que el número de serie sea único No más de 20 bytes
Asunto (Emitido para)	CN = ipoffice-raíz-AsuntoNombre.avaya.com O = Avaya Inc. OU = GC L = Basking Ridge S = Nueva Jersey C = EE. UU. E = soporte@avaya.com	Dónde*Nombre del tema*es el nombre de host configurado durante el encendido de la siguiente manera: · Utilice el administrador web de IP Office | Vista de la plataforma | Configuración | Sistema | Red | campo Nombre de host si está configurado en algo distinto a: · servidor local · localhost.localdomain · el instalador predeterminado (dirección mac) · Si no se usa el nombre de host, use una resolución de DNS de LAN1; si no, LAN2. · Si no se usa el nombre de host y la resolución de DNS no es exitosa, use el nombre predeterminado de 'Eth0 mac', por ejemplo, 'ipoffice-root-00e007057307.avaya.com' · El nombre de host correcto debe configurarse durante el encendido; de lo contrario, será necesario regenerar el certificado de CA raíz.
Sujeto Alternativo Nombres	1: Nombre DNS= ipoffice-roothostname.avaya.com	Una copia del Asunto CN
Emisor (Emitido por)	CN = ipoffice-raíz-hostname.avaya.com O = Avaya Inc. OU = GC L = Basking Ridge S = Nueva Jersey C = EE. UU. E = soporte@avaya.com	Mismo contenido que Asunto: Certificado autofirmado
Válida desde	DD/MM/AA HH:MM:SS	Reflejará la hora/fecha UTC menos 24 horas cuando se creó el certificado. Si el reloj de tiempo real estaba dañado o no estaba configurado, la hora se fijará a las 00:00:00 del 1 de enero del año en que se lanzó el software.
Válido hasta	Válido Desde más 10 años	
Uso de clave	firma digital keyCertSign cRLSign cRLSign fuera de línea	Marcado no crítico El certificado se puede utilizar para el conjunto de operaciones de certificado de IP Office
Uso extendido de claves		No presente
Restricciones básicas	CA: cierto pathLenConstraint: 1	Marcado crítico El certificado de CA puede firmar más certificados de CA intermedios o de identidad
Identificador de clave de sujeto	Identificador clave	Este valor se coloca en el Identificador de clave de autoridad de cualquier certificado firmado
Algoritmo de firma	sha256rsa	
Firma	Datos de firma	
Algoritmo de clave pública	RSA	
Llave pública	Tamaño 2048 bits	

Tabla 16: Certificado de CA principal predeterminado

También como parte del encendido, se crea un certificado de identidad firmado por la CA interna con las propiedades que se enumeran a continuación.

Campo de certificado	Contenido	notas
Versión	V3	Siempre formato X.509 V3
Número de serie	Gran número aleatorio	Asegura que el número de serie sea único No más de 20 bytes
Asunto (Emitido para)	CN = Nombre del sujeto O = Avaya Inc. OU = GC L = Basking Ridge S = Nueva Jersey C = EE. UU. E = soporte@avaya.com	Dónde*Nombre del tema*es el nombre de host configurado durante el encendido de la siguiente manera: · Utilice el administrador web de IP Office | Vista de la plataforma | Configuración | Sistema | Red | campo Nombre de host si está configurado en algo distinto a: oservidor local olocalhost.localdomain oel instalador predeterminado (dirección mac) · Si no se usa el nombre de host, use una resolución de DNS de LAN1; si no, LAN2. · Si no se usa el nombre de host y la resolución de DNS no es exitosa, use el nombre predeterminado de 'Eth0 mac', por ejemplo, 'ipoffice-root-00e007057307.avaya.com' · El nombre de host correcto debe configurarse durante el encendido; de lo contrario, será necesario regenerar el certificado de CA raíz.
Sujeto Alternativo Nombres	1: Nombre DNS= Nombre del sujeto 2: Dirección IP=abcd 3: dirección IP = efgh	Dónde: - DN es el nombre de host configurado durante el encendido - abcd es la dirección IP de LAN 1 en el momento de la creación del certificado - efgh es la dirección IP de LAN 2 en el momento de la creación del certificado (si está presente) Ver Nota 1.
Emisor (Emitido por)	Campos de asunto del certificado de CA	Certificado firmado por la CA interna
Válida desde	DD/MM/AA HH:MM:SS	Reflejará la hora/fecha UTC menos 24 horas cuando se creó el certificado. Si el reloj de tiempo real estaba dañado o no estaba configurado, la hora se fijará a las 00:00:00 del 1 de enero del año en que se lanzó el software.
Válido hasta	Válido desde más 825 días	
Uso de clave	acuerdo clave Cifrado clave firma digital, no repudio, Cifrado de datos	Marcado no crítico El certificado se puede utilizar para el conjunto de operaciones de certificado de IP Office
Uso extendido de claves	id-kp-serverAuth id-kp-clientAuth	Marcado no crítico El certificado se puede utilizar para el conjunto de operaciones de certificado de IP Office
Restricciones básicas	tipo de sujeto: entidad final pathLenConstraint: 0	Marcado crítico Indica Certificado de identidad
Clave de autoridad identificador	Identificador clave	Coincide con el campo Identificador de clave de asunto del certificado de CA
Algoritmo de firma	sha256rsa	
Firma	Datos de firma	
Algoritmo de clave pública	RSA	
Llave pública	Tamaño 2048 bits	

Tabla 17: Certificado de identidad principal predeterminado

Nota 1:

- La dirección correcta de LAN 1 y LAN 2 debe configurarse durante el encendido; de lo contrario, será necesario regenerar el certificado de identidad.
- La regeneración del certificado de identidad se realiza automáticamente si IP Office Web Manager | Vista de la plataforma | Configuración | generales | Certificados | El ajuste Renovar automáticamente está activo (predeterminado).

Página1712 de 3226.

6.2.2.4 Configuración del certificado inicial de expansión secundaria/Linux de Server Edition

El servidor secundario y la expansión de Linux no tienen una autoridad de certificación incorporada. El proceso de ignición crea un certificado de identidad autofirmado único con las propiedades que se enumeran a continuación.

Este certificado de identidad tiene un valor limitado y debe ser reemplazado por uno generado por el servidor primario u otra CA externa.

Campo de certificado	Contenido	notas
Versión	V3	Siempre formato X.509 V3
Número de serie	Gran número aleatorio	Asegura que el número de serie sea único No más de 20 bytes
Asunto (Emitido para)	CN = Nombre del sujeto O = Avaya Inc. OU = GC L = Basking Ridge S = Nueva Jersey C = EE. UU. E = soporte@avaya.com	Dónde*Nombre del tema*es el nombre de host configurado durante el encendido de la siguiente manera: • Utilice el administrador web de IP Office | Vista de la plataforma | Configuración | Sistema | Red | campo Nombre de host si está configurado en algo distinto a: oservidor local olocalhost.localdomain oel instalador predeterminado (dirección mac) • Si no se usa el nombre de host, use una resolución de DNS de LAN1; si no, LAN2. • Si no se usa el nombre de host y la resolución de DNS no es exitosa, use el nombre predeterminado de 'Eth0 mac', por ejemplo, 'ipoffice-root-00e007057307.avaya.com' • El nombre de host correcto debe establecerse durante el encendido, de lo contrario, será necesario el certificado de CA raíz. regenerado
Sujeto Alternativo Nombres		Ninguna
Emisor (Emitido por)	CN = Nombre del sujeto O = Avaya Inc. OU = GC L = Basking Ridge S = Nueva Jersey C = EE. UU. E = soporte@avaya.com	Mismo contenido que Asunto: Certificado autofirmado
Válida desde	DD/MM/AA HH:MM:SS	Reflejará la hora/fecha UTC menos 24 horas cuando se creó el certificado. Si el reloj de tiempo real estaba dañado o no estaba configurado, la hora se fijará a las 00:00:00 del 1 de enero del año en que se lanzó el software.
Válido hasta	Válido Desde más 7 años	
Uso de clave		Ninguna
Uso extendido de claves		Ninguna
Restricciones básicas		Ninguna
Algoritmo de firma	sha256rsa	
Firma	Datos de firma	
Algoritmo de clave pública	RSA	
Llave pública	Tamaño 2048 bits	

Tabla 18: Certificado secundario/de expansión predeterminado

6.2.3 Contenido del nombre del certificado

Los campos del certificado**Nombre del tema**(campo Nombre común) y**Nombre alternativo del sujeto**tienen un significado particular para IP Office y sus diversos clientes.

Aunque IP Office no procesa el campo Nombre alternativo del sujeto (SAN), se requiere contenido específico para el extremo SIP.oye nts y otros clientes, generalmente como verificación de la fuente del certificado. VerSeguridad de punto final VoIP de IP Office 127para obtener más información sobre los clientes de Avaya.

Al solicitar o crear certificados de identidad para los sistemas IP Office, todos los sistemas conectados que procesan el certificado IP Office recibido deben revisarse en cuanto a sus requisitos de Nombre y SAN. Esto también debe incluir cualquier posible sistema futuro conectado durante la vigencia del certificado. En caso de duda, se deben incluir todas las posibles entradas de nombres.

Las consideraciones típicas incluyen:

- **FQDN del sistema como nombre del sujeto**
  El nombre de dominio completo (FQDN) del sistema para el nombre del sujeto. Si no hay un nombre de dominio relevante, se debe usar un nombre de texto significativo y único para el sistema, ya que este campo se puede mostrar a los usuarios. El campo Nombre nunca debe estar vacío.**Ejemplo:***ejemplo.com*
- **FQDN del sistema como entrada SAN DNS**
  El nombre de dominio completo (FQDN) del sistema como una entrada SAN en formato DNS. Esto siempre debe estar presente si se requieren otras entradas de SAN. Los navegadores web y otros clientes suelen utilizar esta entrada cuando acceden a IP Office mediante la resolución de DNS. Cuando la usan terminales SIP, a partir de la versión 10.0 de IP Office, esta entrada normalmente debe tener el valor configurado en Manager | LANx | VoIP | Registrador SIP | Registrador SIP FQDN.**Ejemplo:** *DNS: ejemplo.com*
- **Otros nombres de dominio y FQDN como entradas SAN DNS**
  Cualquier otro nombre de dominio o FQDN del sistema como una entrada SAN en formato DNS. Esta entrada se usa normalmente cuando se puede acceder al sistema usando DNS 'dividido'.**Ejemplo:***DNS:ipoffice.ejemplo.com*
- **Dominios SIP como entradas SAN DNS**
  Cualquier dominio SIP en uso como una entrada SAN para cada dominio SIP, en formato DNS. Este suele ser el valor configurado en Manager | LANx | VoIP | Registrador SIP | Registrador SIP FQDN. Esta entrada suele ser utilizada por puntos finales SIP, como el H175, que verifica el certificado del servidor con el dominio SIP en el que se está registrando. **Ejemplo:** *DNS:sip.ejemplo.com*
- **Dominios SIP como entradas SAN DNS SIP**
  Cualquier dominio SIP en uso como una entrada SAN para cada dominio SIP, en formato URI. Este suele ser el valor configurado en Manager | LANx | VoIP | Registrador SIP | Registrador SIP FQDN. Esta entrada generalmente la usan los terminales SIP cuando acceden a IP Office mediante la resolución de DNS.**Ejemplo:***URI: sorbo: sorbo.ejemplo.com*
- **Dirección IP de LAN1 como entrada de IP de SAN**
  La dirección IP de LAN 1 como una entrada SAN en formato IP. Los navegadores web y otros clientes suelen utilizar esta entrada cuando acceden a IP Office mediante la dirección IP de LAN 1. Ejemplo: IP:192.168.42.1 Los campos de dirección IP no son compatibles con muchas autoridades de certificación públicas. Consulte las notas a continuación.
- **Dirección IP de LAN2 como entrada de IP de SAN**
  La dirección IP de LAN 2 como una entrada SAN en formato IP. Los navegadores web y otros clientes suelen utilizar esta entrada cuando acceden a IP Office mediante la dirección IP de LAN 2. Ejemplo: IP:192.168.43.1 Los campos de dirección IP no son compatibles con muchas autoridades de certificación públicas. Consulte las notas a continuación.
- **NAT y direcciones IP públicas como entradas IP de SAN**
  Cualquier NAT o dirección IP pública como una entrada SAN en formato IP. Esta entrada suele ser utilizada por teléfonos 96x1 H.323 en implementaciones en la nube o de trabajo remoto, navegadores web y otros clientes al acceder a IP Office mediante la dirección IP directa externa/pública. Tenga en cuenta que esta entrada no se agrega de forma predeterminada a los certificados de identidad generados por la CA del servidor primario de IP Office. Esta entrada es necesaria si los teléfonos u otros clientes están configurados para conectarse a la dirección IP pública de IP Office y no a su FQDN. Ejemplo: IP:135.11.53.53 Los campos de dirección IP no son compatibles con muchas autoridades de certificación públicas. Consulte las notas a continuación.
- **Dirección IP SIP como entradas SAN URI**
  Cualquier dirección IP SIP en uso como una entrada SAN para cada dominio SIP, en formato URI. Esta entrada la utiliza el terminal SIP E129 de Avaya cuando accede a IP Office mediante una dirección IP. Ejemplo: URI:sip:135.11.53.53 Los campos de dirección IP no son compatibles con muchas autoridades de certificación públicas. Consulte las notas a continuación.
- **Entradas comodín**
  En determinadas circunstancias, podría considerarse el uso de nombres 'comodines'. Un campo de nombre comodín contiene un asterisco en el nombre (por ejemplo, '*.example.com') y cubre todos los subdominios. IP Office puede admitir dichos campos tanto en el nombre del sujeto como en los campos de nombre comodín de SAN, pero conlleva riesgos y limitaciones de seguridad adicionales
  y por lo tanto no se recomiendan. Consulte las notas a continuación.

Notas de contenido del nombre del certificado:

- Las autoridades de certificación públicas no admiten direcciones IP ni dominios privados. Se deben usar DNS y dominios públicos para todos los clientes si se va a usar una CA pública. No usar la dirección IP puede comprometer la administración de 96xx y otros puntos finales. Los teléfonos de la serie 11xx/12xx no admiten FQDN y, por lo tanto, no se pueden usar con certificados proporcionados por autoridades de certificación públicas.
- Los certificados comodín (o certificados con campos de nombre comodín) conllevan los siguientes riesgos adicionales:
  - **Seguridad:**Si un servidor o subdominio se ve comprometido, todos los subdominios pueden verse comprometidos.
  - **Seguridad:**Si se usa para más de un servidor, la clave privada puede quedar expuesta.
  - **Administración:**Si es necesario revocar el certificado comodín, todos los subdominios necesitarán un nuevo certificado.
  - **Compatibilidad:**Es posible que los certificados comodín no funcionen con todas las configuraciones de servidor-cliente.
  - **Proteccion:**Los certificados Wildcard no están protegidos por la validación o garantía extendida de CA.
  - **Seguridad:**No deben usarse para proteger más de un servidor de IP Office en una implementación; cada servidor debe tener un certificado de identidad único.
- Los certificados comodín no son compatibles con los clientes SIP de Avaya, como las series Equinox, Vantage o J1xx.

IP500 V2 y Server Edition Primary/Linux Application Server admiten la creación de certificados con hasta 8 campos SAN con las siguientes opciones:

- **DNS**–utilizado para nombre de host o FQDN
- **URL**–utilizado para URL y URI
- **IP**–Dirección IP en formato v4
- **Correo electrónico**–dirección de correo electrónico

Estos campos SAN también se pueden utilizar para solicitudes de firma de certificados a través de SCEP.

VerConfiguración inicial del certificado 44para los campos Nombre SAN predeterminados agregados en la creación del certificado inicial.

Para muchas implementaciones sencillas, solo se requiere un único FQDN como nombre de asunto, como one-X Portal para IP Office y Voicemail Pro en Windows, Unified Communications Module o Linux Application Server, donde el DNS siempre se resuelve en el mismo FQDN.

Otras implementaciones donde la identidad del sistema difiere según el acceso (por ejemplo, LAN o WAN) o el uso de puntos finales SIP o H323 con señalización segura, normalmente se requerirán SAN.

6.2.4 Controles de verificación de certificados

Existen tres niveles de verificación de certificados recibidos realizados por IP Office en las interfaces admitidas; estos se aplican a cualquier certificado recibido de cualquier cliente o servidor TLS remoto.

- **Bajo**
  Solo se comprueba la validez (en fecha) y la fuerza (clave pública >=1024 bits) del certificado recibido. Esto no tiene ningún valor para determinar la confianza.
- **Medio**
  Se comprueba la validez (en fecha) y la fuerza (clave pública >=1024 bits) del certificado recibido, luego se busca en el TCS una cadena de confianza completa a una CA raíz. Esto es típico de la forma en que los navegadores comprueban los certificados. Tenga en cuenta que estas pruebas no incluyen comprobaciones de identidad de certificado mediante los campos Nombre y Nombre alternativo del sujeto.
- **Alto**
  Esto no solo realizará comprobaciones bajas y medias, sino que también comprobará la clave pública >= 2048 bits y que haya una copia del certificado recibido en el almacén. Esto permite implementar un dominio de confianza mucho más pequeño donde solo se aceptan certificados individuales. Esta es una forma de 'fijación de certificados' y supera una de las limitaciones de la estructura de árbol estándar de PKI; todos los certificados emitidos por la CA raíz siempre son de confianza.

Ver "*Administración de la plataforma Avaya IP Office™ con Manager*" para obtener una lista detallada de las comprobaciones realizadas.

Las verificaciones de confianza extendidas 'Alta' se activan con la configuración:

- **Gerente de Seguridad | Sistema | Certificados | Comprobaciones de certificados recibidos (Telefonía)**=***Alto*** Se aplica a todos los certificados recibidos en las interfaces SIP-TLS
- **Gerente de Seguridad | Sistema | Certificados | Comprobaciones de certificados recibidos (Gestión)**=***Alto*** Se aplica a todos los certificados recibidos en las interfaces de gestión TLS y HTTPS.
- **Configuración del administrador | Línea | Línea | Seguridad**=***Alto***
  Se aplica a los certificados recibidos en esa línea WebSocket de IP Office, independientemente de las verificaciones de certificados recibidas por la administración (las líneas WebSocket utilizan el servidor HTTP/S de IP Office).

Autenticacion mutua

Cuando IP Office actúa como un servidor TLS/HTTPS, ciertas configuraciones de seguridad activan una solicitud de certificado del cliente. Si no se recibe ningún certificado, IP Office rechazará la conexión. Si se recibe uno, se aplicarán controles de certificado. Este es el mecanismo principal utilizado para hacer cumplir las verificaciones de confianza por parte de IP Office.

- **Nota:**En la actualidad, IP Office nunca solicita certificados de terminales SIP o H323 que se conectan a través de TLS.

La autenticación mutua se activa con la configuración:

- **Gerente de Seguridad | Servicios | Configuración | Nivel de seguridad del servicio**=***Alto***
  Se aplica a los valores de configuración de IP Office Manager y a las interfaces DevConnect del servicio web de configuración (XO) en el puerto 50805.
- **Gerente de Seguridad | Servicios | Administración de Seguridad | Nivel de seguridad del servicio**=***Alto*** Se aplica a la configuración de seguridad de IP Office Manager en el puerto 50809.
- **Gerente de Seguridad | Servicios | HTTP | Nivel de seguridad del servicio**=***Alto***
  Se aplica a clientes HTTPS que se conectan al puerto 443 y 411, generalmente teléfonos H323, DECT R4, líneas de IP Office, Voicemail Pro, System Monitor, etc.
- **Gerente de Seguridad | Servicios | Servicios web | Nivel de seguridad del servicio**=***Alto*** Se aplica a la interfaz de IP Office Web Manager en el puerto 8443.
- **Gerente de Seguridad | Sistema | Certificados | Comprobaciones de certificados recibidos (Telefonía)**=***Bajo***, ***Medio*** o ***Alto***
  Se aplica a líneas SIP y SM en el puerto 5061.
- **Configuración del administrador | Línea | Línea | Seguridad**=***Alto***
  Se aplica a las líneas del servidor WebSocket de IP Office en el puerto 443. Es independiente del **Seguridad | Servicios | HTTP | Nivel de seguridad del servicio** yo controlo

Ver Compatibilidad con certificados de interfaz de IP Office [13] para más información.

6.2.5 Distribución de certificados

Esta sección cubre los procesos de distribución de certificados.

- Soporte de certificado de interfaz 44
- Configuración inicial del certificado 44
- Contenido del nombre del certificado 50
- Controles de comprobación de certificados 52
- Determinación de la política de confianza 56
- Enfoques de confianza de IP Office PKI 57
- Selección de PKI de IP Office 59
- Implementación de PKI de IP Office 59
- Certificados de autoridades de certificación externas 62
- Mantenimiento de certificados 64

6.2.5.1 Distribución de certificados de identidad

IP Office admite tres mecanismos principales para distribuir certificados de identidad, cuya selección dependerá de la política de confianza elegida. Se requiere un certificado de identidad único para cada IP Office; dos si se requiere un dominio de confianza de telefonía por separado.

Manual de una CA externa

Se crea una solicitud de firma de certificado manual (CSR) y se envía a una CA externa que verificó el contenido y crea un certificado de identidad firmado por la CA.

Una vez que se obtiene el certificado de identidad/clave privada, se puede usar Manager o IP Office Web Manager para administrarlo en IP Office:

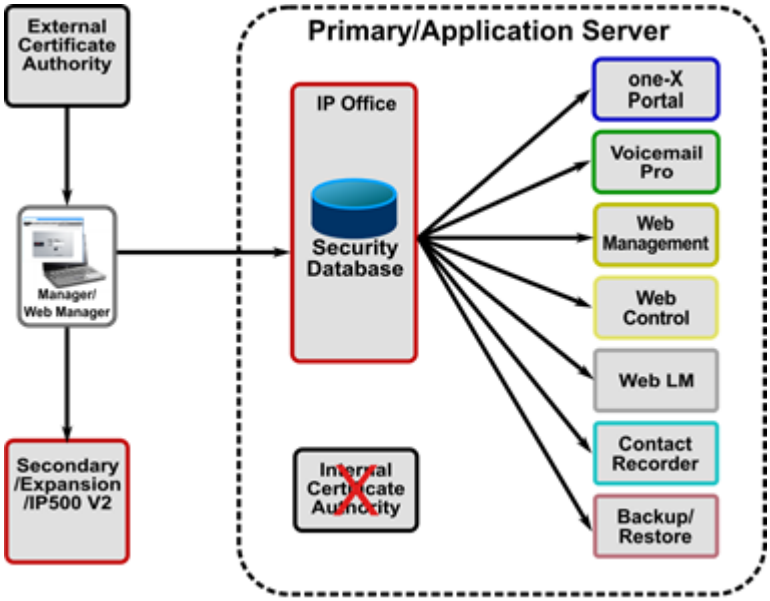


Figura 7: Distribución de certificación - Autoridad de certificación externa

Para obtener más información sobre la creación de una PKI basada en una CA externa, consulteImplementación de PKI de IP Office 59.

Para obtener más información sobre las autoridades de certificación externas, consulteCertificados de autoridades de certificación externas 62

La autoridad de certificación interna se puede utilizar para crear un conjunto de certificados de identidad únicos en el formato de archivo seguro PKCS#12. El archivo PKCS#12 también incluye el certificado CA.
Estos certificados de identidad se pueden utilizar para cualquier entidad, incluidos IP Office, teléfonos, PC Manager, etc. Una vez que el certificado de identidad/archivo de clave privada se guarda en la PC local, se puede usar Manager o IP Office Web Manager para administrarlo en IP Office.

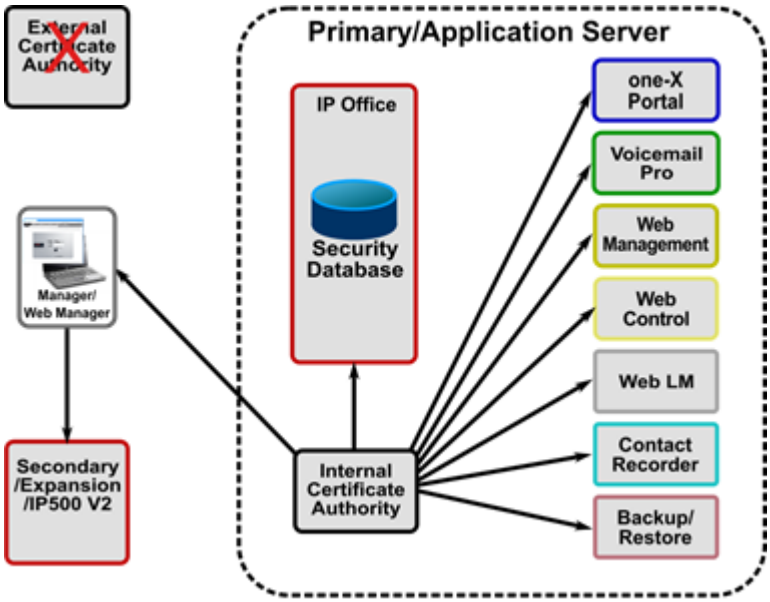


Figura 8: Distribución de certificados - Autoridad de certificación interna

Para obtener más información sobre la creación de una PKI basada en una CA interna, consulteImplementación de PKI de IP Office 59.

Automático utilizando el Protocolo simple de inscripción de certificados (SCEP)

Cada IP Office se configura con la ubicación del servidor SCEP junto con una contraseña. IP Office realizará periódicamente un CSR hasta obtener su certificado de identidad. La clave privada se mantiene internamente. El servidor SCEP debe administrarse para aceptar la solicitud de firma y emitir el certificado correcto.

Como parte del proceso de inscripción, el certificado de CA utilizado para firmar la solicitud de SCEP se coloca en el TCS, después de lo cual IP Office confiará en cualquier otro certificado firmado por esa CA. Este es el mecanismo utilizado en las implementaciones de sucursales de IP Office con System Manager (SMGR).

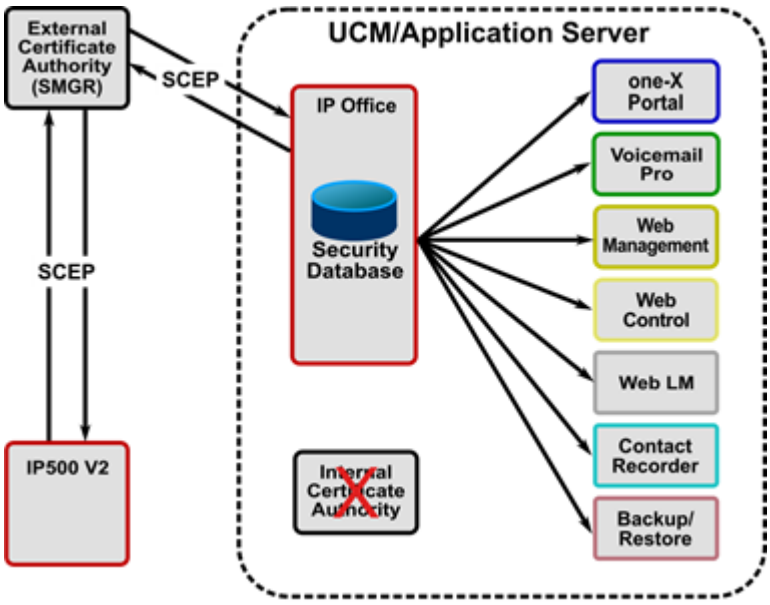


Figura 9: Distribución de certificados: inscripción simple de certificados Protocolo (SCEP)

En todos los casos (CA externa, CA interna, SCEP), cuando IP Office recibe un nuevo certificado de identidad, todas las interfaces/aplicaciones relevantes se actualizan.

Para obtener más información sobre la creación de una PKI basada en SCEP, consulteImplementación de PKI de IP Office 59.

Manual de uso de un CSR PKCS#10

Se crea una solicitud de firma de certificado (CSR) PKCS#10 en el servidor IP Office Linux a través de la interfaz de línea de comandos (CLI). La clave privada se conserva dentro del servidor. El CSR se envía a una CA externa que verifica el contenido y crea un certificado de identidad firmado por la CA.

Una vez que se devuelve el certificado de identidad, la CLI se usa para combinar con la clave privada y se distribuye con el servidor.

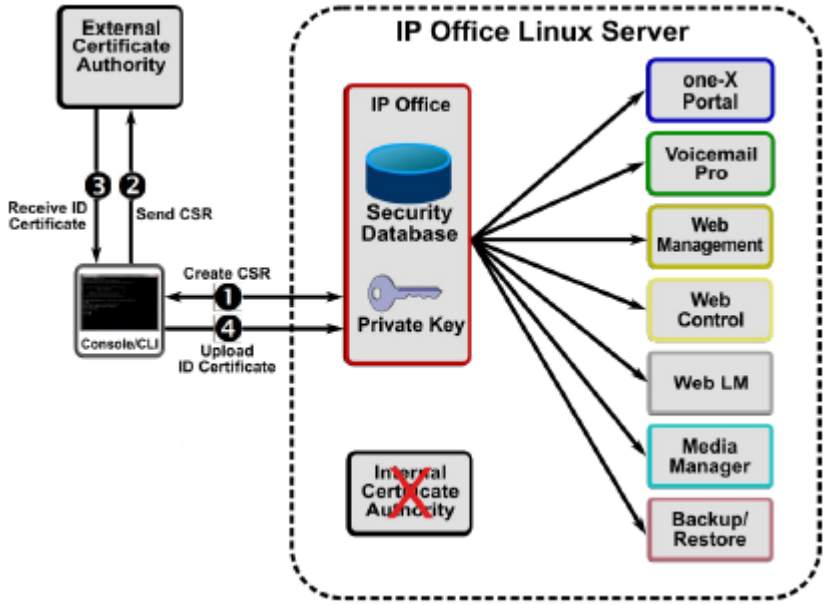


Figura 10: Distribución de certificados - Autoridad de certificación externa

Para obtener más información sobre la creación de una PKI basada en una CA externa, consulteImplementación de PKI de IP Office 59.

Para obtener más información sobre las autoridades de certificación externas, consulteCertificados de autoridades de certificación externas 62

6.2.5.2 Distribución de certificados de CA raíz

Si la política de confianza seleccionada utiliza una CA pública conocida (como Verisign™), sus certificados raíz normalmente ya están instalados en los sistemas operativos y navegadores correspondientes. Sin embargo, IP Office no tiene certificados de CA públicos conocidos en su TCS; estos pueden descargarse del sitio web de la CA y administrarse manualmente a través de Manager o IP Office Web Manager para cada IP Office.

Para obtener más información sobre la distribución de certificados de CA raíz, consulteImplementación de PKI de IP Office 59.

6.2.5.3 Distribución de certificados de CA intermedia

Si la implementación de confianza también utiliza certificados de CA intermedios, se puede activar la función de encadenamiento de certificados de IP Office y se deben agregar los CA intermedios al TCS. Esta cadena de certificados de ID se propaga a todas las interfaces TLS locales.
Esto eliminará la necesidad de administrar certificados de CA intermedia en los almacenes de certificados de confianza de varios clientes.

Para obtener más información sobre la distribución de certificados de CA intermedia, consulteImplementación de PKI de IP Office 59.

6.2.6 Determinación de la política de confianza

Con los requisitos de comunicación segura de hoy en día, no es posible ignorar el uso de certificados para implementar relaciones de confianza, incluso si las necesidades identificadas son mínimas. Se debe seleccionar e implementar una política de confianza antes de exponer los servicios de IP Office. Esta sección proporciona información para ayudar en la determinación de dicha política; sin embargo, no puede proporcionar una guía definitiva ni incluir factores externos.

Nota: Las implementaciones de sucursales de IP Office tienen un entorno y requisitos especializados. Ver los documentos:

- **Implementación de Avaya IP Office Platform como una sucursal empresarial con Avaya Aura Session Manager** Número de documento 18-603853,https://downloads.avaya.com/css/P8/documents/101004861
- **Administración de usuarios centralizados para una sucursal de IP Office™ Platform Enterprise** Número de documento 15-604263,https://downloads.avaya.com/css/P8/documents/101004857
- **Avaya IP Office Platform en una configuración de referencia de entorno de sucursal** Número de documento 15-604253,https://downloads.avaya.com/css/P8/documents/101004855

Al considerar una política de confianza para IP Office, se pueden considerar las siguientes preguntas:

- ¿Qué requisitos fiduciarios internacionales, nacionales, corporativos u otros existen?
- ¿Existe una infraestructura de confianza/PKI de la que IP Office deba ser parte?
- ¿Los servicios de IP Office están expuestos en las interfaces públicas?
- ¿Los componentes de la plataforma IP Office se implementan en plataformas o entornos no seguros?
- ¿Se implementan los terminales/clientes de IP Office en plataformas o entornos no seguros?
- ¿Cuáles son los requisitos de confianza para los sistemas de terceros que se conectan a IP Office?
- ¿Es importante la capacidad de confiar en IP Office sin administrar certificados en clientes/terminales?
- ¿Existe la necesidad de un dominio de confianza de administración y telefonía separado?
- ¿Qué interfaces y servicios necesitan usar comprobaciones de confianza y cuáles no?
- ¿La confianza debe ser unidireccional (por ejemplo, el cliente verifica el servidor) o bidireccional (por ejemplo, el cliente y el servidor se verifican entre sí)?
- ¿Existe la necesidad de proporcionar las verificaciones de confianza extendidas de IP Office donde todos los certificados de los clientes deben estar presentes en el TCS? Esto es útil cuando la estructura de confianza del árbol PKI es insuficiente.
- ¿Cuántos certificados de identificación se requieren? Al menos un certificado único por servidor de IP Office, dos si se necesita un dominio de confianza de telefonía independiente.
- ¿Cómo se obtienen, distribuyen y recuperan los certificados?
- ¿Qué métodos de renovación y distribución de certificados deben admitirse?
- ¿Puede la CA proporcionar el contenido del certificado correcto? Por ejemplo, el contenido del nombre alternativo del sujeto

Esta lista no es exhaustiva, para más información verEvaluación de los requisitos de seguridad de IP Office 76.

6.2.7 Enfoques de confianza de PKI de IP Office

Existen cinco enfoques principales que se pueden utilizar con la plataforma IP Office:

1. Dominio de confianza de PKI basado en la CA raíz interna principal o del servidor de aplicaciones de Linux.
2. Dominio de confianza de PKI basado en la CA primaria o intermedia interna del servidor de aplicaciones Linux.
3. Dominio de confianza de PKI basado en una autoridad de certificación externa.
4. Dominio de confianza de PKI basado en una autoridad de certificación externa a través de SCEP.
5. Sin dominio de confianza PKI.

Enfoque 1: Dominio de confianza de PKI basado en la CA raíz principal o del servidor de aplicaciones de Linux

Esta opción permite generar certificados de identidad utilizando el certificado CA raíz del servidor.

Las ventajas relativas incluyen:

- Costo sobre una CA comercial.
- El control de la CA es interno.
- Formato de contenido del certificado compatible con otros componentes de Avaya.
- La política de certificados es flexible y no está sujeta a consideraciones comerciales.
- Las relaciones de confianza no se extienden fuera de la implementación, es decir, sigue siendo un dominio privado.

Las desventajas relativas incluyen:

- Los terceros y otros componentes de IP Office no confían en el certificado de CA raíz y, por lo tanto, debe distribuirse.
- El proceso de creación y distribución de certificados es manual.

Enfoque 2: Dominio de confianza de PKI basado en una entidad emisora de certificados primaria o intermedia del servidor de aplicaciones de Linux

Esta opción permite generar certificados de identidad en el servidor de aplicaciones Linux o principal mediante un certificado de CA intermedio obtenido de una autoridad de certificación externa.

Ventajas potenciales para el certificado de CA intermedio en el servidor de aplicaciones principal/Linux:

- Los certificados de identificación generados son parte de una confianza más amplia
- El control de la CA es interno.
- Formato de contenido del certificado de identificación compatible con otros componentes de Avaya.
- Certificados de identificación con dominios privados y rangos de direcciones Se pueden crear direcciones IP
- El certificado de CA raíz es (normalmente) de confianza para terceros y, por lo tanto, no es necesario distribuirlo.

Las posibles desventajas incluyen:

- Costo: si utiliza un proveedor comercial. Los certificados de firma suelen ser más caros.
- La política de certificados está sujeta a consideraciones comerciales.
- Muchas autoridades de certificación públicas no emitirán certificados de CA intermedios para dominios privados o rangos de direcciones IP.
- Los componentes de IP Office no confían en el certificado CA raíz y, por lo tanto, debe distribuirse.
- El proceso de creación y distribución de certificados es manual.
- Todos los clientes deben admitir cadenas de certificados en el intercambio TLS; de lo contrario, se debe distribuir el certificado de CA intermedio.

Enfoque 3: dominio de confianza de PKI basado en una autoridad de certificación externa

Esta opción permite obtener certificados de identidad directamente de una Autoridad de Certificación externa mediante un proceso manual.

Posibles ventajas de los certificados de identidad de una CA externa:

- Útil para implementaciones pequeñas cuando no existe un servidor de aplicaciones principal o Linux.
- Los certificados de identificación generados forman parte de un dominio de confianza más amplio.
- El certificado de CA raíz es (normalmente) de confianza para terceros y, por lo tanto, no es necesario distribuirlo.

Las posibles desventajas incluyen:

- Las autoridades de certificación pública no emitirán certificados para dominios privados o rangos de direcciones IP.
- Costo: si utiliza un proveedor comercial.
- El control de la CA es externo.
- La política de certificados está sujeta a consideraciones comerciales. Es posible que el formato del contenido del certificado de ID no sea compatible con los componentes de Avaya.
- Los componentes de IP Office no confían en el certificado CA raíz y, por lo tanto, debe distribuirse.
- El proceso de creación y distribución de certificados es manual.

Enfoque 4: dominio de confianza de PKI basado en una autoridad de certificación externa a través de SCEP

Esta opción permite obtener certificados de identidad directamente de una Autoridad de Certificación externa mediante un proceso automatizado.

Posibles ventajas de los certificados de identidad obtenidos mediante SCEP:

- Los certificados de identificación generados forman parte de un dominio de confianza más amplio.
- Formato de contenido del certificado de identificación compatible con los componentes de Avaya.
- El certificado de CA raíz es (normalmente) de confianza para terceros y, por lo tanto, no es necesario distribuirlo.
- Los componentes de IP Office siempre confían en el certificado de CA raíz y, por lo tanto, no es necesario distribuirlo.
- El proceso de creación y distribución de certificados está automatizado y admite muchos sistemas de manera eficiente.

Las posibles desventajas incluyen:

- Actualmente, la compatibilidad con los servidores SECP se limita a EJBCA, la CA presente en Avaya Aura System Manager (SMGR).
- Las autoridades de certificación pública no emitirán certificados para dominios privados o rangos de direcciones.
- Costo: si utiliza un proveedor comercial.
- El control de la CA es externo.
- La política de certificados está sujeta a consideraciones comerciales.

Enfoque 5: Sin dominio de confianza

Esto solo se puede considerar usado cuando un solo IP500 V2 o servidor primario no tiene interfaces externas/públicas y está completamente dentro de un entorno seguro/cerrado.

La instalación/creación se logra conservando el certificado de identidad predeterminado.

No hay relaciones de confianza activas, no se comprueban los certificados.

El Mantenimiento de PKI consistirá en renovar el certificado de identidad eliminando el existente mediante IP Office Manager o IP Office Web Manager; esto creará un nuevo certificado para los próximos 7 años. Será necesario volver a afirmar cualquier excepción de navegador existente.

6.2.8 Selección de PKI de IP Office

La política de seguridad del cliente existente ya puede definir el enfoque necesario. Cuando esto aún no se haya definido, una evaluación de los requisitos debería ayudar a identificar la opción adecuada. La siguiente guía puede ser útil:

- Una implementación con interfaces externas y muchos clientes externos sugeriría una autoridad de certificación pública externa (enfoque 3).
- Una implementación sin interfaces externas o con pocos clientes externos sugeriría una autoridad de certificación interna (enfoque 1).
- Una implementación que requiere direcciones IP o nombres de dominio privados en los campos del certificado no puede usar una autoridad de certificación pública, por lo que el enfoque 1 puede ser adecuado.
- Una implementación que ofrece cualquier servicio al público debe utilizar una entidad de certificación pública externa (enfoque 3).
- Una implementación de sucursal con System Manager generalmente usará SCEP (Método 4)

Aunque arriba se describen cinco enfoques, una combinación puede ser apropiada; por ejemplo, CA pública externa para servidores públicos, CA interna para todos los demás. No se puede utilizar un enfoque híbrido cuando la resiliencia de terminales de VoIP está activa; la CA raíz para el servidor principal y el de copia de seguridad debe ser la misma.

6.2.9 Implementación de IP Office PKI

Una vez determinada la política de confianza, el proceso de implementación dependerá de la opción seleccionada:

Enfoque 1: Dominio de confianza de PKI basado en la CA raíz principal o del servidor de aplicaciones de Linux

1. La CA del servidor principal debe usarse para las implementaciones de Server Edition. El servidor de aplicaciones de Linux para implementaciones que no son de Server Edition. Se debe usar la misma CA para todos los sistemas en una implementación.
2. Habilite la configuración**Vista de la plataforma | Configuración | generales | Certificados | Certificados de Identidad | Renovar automáticamente**en el servidor de aplicaciones principal/Linux.
3. Para cada dispositivo (servidor, IP 500V2, etc.) use la CA para crear un certificado de ID único para cada uno con el contenido de nombre correcto y guárdelo en un directorio local. El nombre fieviejo s del certificado son importantes para la correcta interoperabilidad concli entes; verContenido del nombre del certificado 50para más información. VerUso de la autoridad de certificación de IP Office 131.
4. Guarde el certificado de CA raíz en formato PEM y DER en un directorio local mediante la configuración de IP Office Web Manager.**Vista de la plataforma | Configuración | generales | Certificados | Certificado CA | Descargar (codificación PEM)**y**Descargar (codificado en DER)**.
5. Use IP Office Web Manager o IP Office Manager para guardar el certificado de CA en cada TCS.
6. Utilice IP Office Web Manaedad r o IP Office Manager para guardar el certificado de identificación en el servidor de IP Office correspondiente. VerActualizar certificados 80.
7. Si los teléfonos SIP o H.323 utilizan HTTPS para el aprovisionamiento o TLS para la señalización, el certificado CA raíz de IP Office debe estar presente en cada teléfono. VerSeguridad VoIP 68.
8. Distribuya el certificado de CA raíz a todos los clientes y navegadores. Los mecanismos varían y algunos requieren formato PEM, algunos requieren DER. Consulte la documentación relevante del cliente y del navegador.
9. Verifique que se haya aplicado el certificado de ID correcto en cada dispositivo usando un navegador u otra herramienta de diagnóstico.
10. Habilite la comprobación de certificados en la configuración de seguridad de IP Office y en las líneas de IP Office.
11. Verifique con SE Manager que todos los sistemas IP Office estén en línea sin alarmas.
12. Habilite las conexiones seguras para los clientes.
13. Verifique que cada cliente pueda conectarse correctamente.
14. Asegúrese de que todos los archivos de certificados de ID se almacenen de forma segura.
15. Una vez realizadas todas las comprobaciones, se debe realizar una copia de seguridad de la configuración.

Enfoque 2: Dominio de confianza de PKI basado en una entidad emisora de certificados primaria o intermedia del servidor de aplicaciones de Linux

1. La CA del servidor principal debe usarse para las implementaciones de Server Edition. El servidor de aplicaciones de Linux para implementaciones que no son de Server Edition. Se debe usar la misma CA para todos los sistemas en una implementación.
2. Habilite la configuración**Plataforma | Configuración | generales | Certificados | Certificados de Identidad | Renovar automáticamente**en el servidor de aplicaciones principal/Linux.
3. Seleccione una autoridad de certificación adecuada que pueda cumplir con los requisitos de confianza y certificado de la implementación.t. Para obtener más información sobre las autoridades públicas externas, consulteCertificados de autoridades de certificación externas 62.
4. Solicite un par de certificado de CA intermedia/clave privada de una autoridad de certificación de confianza en formato PCKS#12. Un certificado de CA intermedio difiere en contenido de una CA raíz o un certificado de identidad de dispositivo. Para obtener más información sobre las autoridades públicas externas, consulteCertificados de autoridades de certificación externas 62 .
5. Descargue el certificado de CA raíz (y cualquier otro certificado de CA intermedio) de la autoridad de certificación en formato PEM y DER a un directorio local.
6. Instale el certificado de CA intermedia en el servidor de aplicaciones principal o Linux. Esto se puede hacer durante el encendido o después del encendido a través de la configuración de IP Office Web Manager.**Vista de la plataforma | Configuración | generales | Certificados | Certificado CA | Importar**.
7. Para cada dispositivo (servidor, IP 500V2, etc.) use la CA para crear un certificado de ID único para cada uno con el contenido de nombre correcto y guárdelo en un directorio local. El nombre fieviejo s del certificado son importantes para la correcta interoperabilidad concli entes; verContenido del nombre del certificado 50para más información. VerUso de la autoridad de certificación de IP Office 131.
8. Guarde el certificado de CA intermedio en formato PEM y DER en un directorio local mediante la configuración de IP Office Web Manager.**Vista de la plataforma | Configuración | generales | Certificados | Certificado CA | Descargar (codificación PEM)**y**Descargar (codificado en DER)**.
9. Use IP Office Web Manager o IP Office Manager para:
   - Guarde el certificado CA raíz e intermedio en el TCS, luego
   - Active la función de encadenamiento de certificados Cadena de certificados de ID de oferta.
10. Utilice IP Office Web Manaedad r o IP Office Manager para guardar el certificado de identificación en el servidor de IP Office correspondiente. VerActualizar certificados 80.
11. La distribución del certificado de CA raíz a teléfonos, clientes y navegadores se realiza de acuerdo con el Dominio de confianza de PKI basado en la CA raíz principal o del servidor de aplicaciones de Linux en la sección anterior.
12. Los pasos de verificación y habilitación son según el dominio de confianza de PKI basado en la CA principal o raíz del servidor de aplicaciones de Linux, con la nota de que muchas CA externas brindan herramientas de verificación en línea.
13. Una vez realizadas todas las comprobaciones, se debe realizar una copia de seguridad de la configuración.

Enfoque 3: dominio de confianza de PKI basado en una autoridad de certificación externa

1. No se utiliza la CA en el servidor de aplicaciones Linux o principal.
2. Habilite la configuración**Plataforma | Configuración | generales | Certificados | Certificados de Identidad | Renovar automáticamente**.
3. Seleccione una autoridad de certificación adecuada que pueda cumplir con los requisitos de confianza y certificado de la implementación.t. Para obtener más información sobre las autoridades públicas externas, consulteCertificados de autoridades de certificación externas 62.
4. Para cada dispositivo (servidor, IP 500V2, etc.), solicite a la CA que cree un certificado de identificación único para cada uno con el contenido de nombre correcto y guárdelo en un directorio local. El nombre fieviejo Los datos del certificado son importantes para la correcta interoperabilidad con los clientes; verContenido del nombre del certificado 50para más información. Para obtener más información sobre las autoridades públicas externas, consulteCertificados de autoridades de certificación externas 62.
5. Para los dispositivos IP500 V2, se debe utilizar un CSR basado en un formulario externo. Para dispositivos IP Office Linux, un CSR PKCS#10 puedeser creado usando la CLI. Para obtener más información sobre el proceso de RSE, consulteSolicitudes de firma de certificado 134.
6. Descargue el certificado CA raíz y cualquier certificado intermedio de la entidad emisora de certificados en formato PEM y DER a un directorio local.
7. Use IP Office Web Manager o IP Office Manager para:
   - Guarde el certificado CA raíz e intermedio en el TCS, luego
   - Active la función de encadenamiento de certificados Cadena de certificados de ID de oferta.
8. Utilice IP Office Web Manaedad r o IP Office Manager para guardar el certificado de identificación en el servidor de IP Office correspondiente. VerActualizar certificados 80.
9. La distribución del certificado de CA raíz a teléfonos, clientes y navegadores se realiza de acuerdo con el Dominio de confianza de PKI basado en la sección CA raíz principal o del servidor de aplicaciones Linux anterior.
10. Los pasos de verificación y habilitación son según el Dominio de confianza de PKI basado en la CA raíz principal o del servidor de aplicaciones de Linux, con la nota de que muchas CA externas brindan herramientas de verificación en línea.
11. Una vez realizadas todas las comprobaciones, se debe realizar una copia de seguridad de la configuración.

Enfoque 4: dominio de confianza de PKI basado en una autoridad de certificación externa a través de SCEP

1. No se utiliza la CA en el servidor de aplicaciones Linux o principal; deshabilitar la configuración**Vista de la plataforma | Configuración | generales | Certificados | Certificados de Identidad | Renovar automáticamente**.
2. Seleccione una autoridad de certificación adecuada que pueda cumplir con los requisitos de confianza y certificado de la implementación, incluido un servicio SCEP basado en EJBCA.
3. Los pasos necesarios para habilitar el funcionamiento de SCEP se describen en la documentación de la sucursal de IP Office.

6.2.10 Certificados de autoridades de certificación externas

Una autoridad de certificación (CA) externa proporciona una forma de obtener certificados de identidad en los que confían terceros. Estos proveedores de CA suelen realizar las siguientes funciones:

- Valida la identidad del solicitante del certificado y la propiedad del dominio
- Emite certificados
- Mantiene la información del estado del certificado
- Actualizaciones de listas de revocación de certificados

La mayoría de las CA comerciales forman parte de una o más organizaciones industriales, como:

- **El Consejo de Seguridad de la Autoridad de Certificación:**https://casecurity.org/
- **El foro CA/navegador:**https://cabforum.org/

Ambos tienen recursos en línea que pueden ayudar a seleccionar y usar una CA. Además, hay otros recursos web de los propios proveedores de CA.

6.2.10.1 Selección de una autoridad de certificación

Nota: Una autoridad de certificación externa no puede emitir certificados con contenido de nombre que no se pueda verificar externamente. Esto incluye cualquier nombre de dominio local y direcciones IP privadas. Si se requieren nombres de dominio locales o direcciones IP privadas, se debe usar la CA del servidor de aplicaciones principal o Linux.

Seleccione una autoridad de certificación que pueda cumplir con los requisitos de confianza y certificado de la implementación. Los criterios de selección están fuera de este documento, pero deben incluir para las implementaciones de IP Office:

- ¿Se confía en la Autoridad de Certificación?
- ¿Puede la autoridad de certificación proporcionar certificados de identidad RSA de 2048 bits + SHA-256 para servidores web? La firma de código y otros tipos de certificados no son utilizados por IP Office.
- ¿La autoridad de certificación admite una solicitud de firma de certificado (CSR) basada en un formulario web seguro? Sino t, se requieren herramientas externas para proporcionar a la CA un CSR basado en texto. VerSolicitudes de firma de certificado 134para obtener más información sobre cómo crear CSR basados en texto.
- ¿Puede la autoridad de certificación proporcionar certificados de identidad en formato PKCS#12? De lo contrario, se requieren herramientas externas para convertir el certificado de identidad al formato correcto para importarlo a IP Office.
  - VerNombre y formato del archivo de certificado 42para obtener más información sobre los formatos de archivo de certificado.
  - VerCreación de una CSR mediante la línea de comandos de IP Office Linux 140.
- Si es necesario, ¿puede la autoridad de certificación proporcionar certificados multidominio (también conocido como 'Multi-SAN' o 'Comunicaciones unificadas')?
- Si es necesario, ¿puede la autoridad de certificación proporcionar un certificado de CA de firma? La opción sería necesaria para el Método 2: Dominio de confianza de PKI basado en la CA primaria o intermedia del servidor de aplicaciones de Linux anterior.
- ¿La CA raíz ya estará en los navegadores y sistemas operativos del cliente? ¿Están cubiertos todos los navegadores y sistemas operativos de los clientes?
- ¿Se utilizan certificados de firma intermedios? Esto puede aumentar la complejidad de la implementación si se utilizan intermediarios.
- ¿Se proporcionan los certificados de firma en formato PEM y DER? VerNombre y formato del archivo de certificado 42 para obtener más información sobre los formatos de archivo de certificado.
- ¿Qué nivel de notificación/garantía se requiere? Los proveedores suelen ofrecer varios niveles con varios nombres:
  - Básico, también conocido como 'Validación de dominio': solo se valida el nombre de dominio, no la empresa en sí. Los navegadores no deberían generar un error/advertencia, pero no se muestra información de la empresa. Este nivel no se recomienda para las interfaces de IP Office donde la verificación de la identidad de la empresa es importante.
  - Intermedio, también conocido como 'Validación de la organización': se validan el dominio y la empresa. Los navegadores no deben generar un error/advertencia, se muestra la información de la empresa.
  - Mejorado, también conocido como 'Validación extendida': el dominio y la empresa se validan en detalle. Los navegadores deben mostrar un fondo verde verificado y se muestra la información de la empresa. Debido a sus problemas de seguridad, los certificados Wildcard no están permitidos para la 'Validación extendida'.
- ¿Por cuánto tiempo son válidos los certificados de identidad y firma? Los períodos más cortos aumentan los gastos generales de mantenimiento.

- ¿Se puede obtener un certificado de prueba gratuito para verificar el correcto funcionamiento? IP Office se probó con éxito con varios certificados de proveedores, pero debido a la cantidad de proveedores, no se puede garantizar que todos los certificados de proveedores se admitan correctamente.
- ¿Se proporcionan pruebas y otras utilidades de soporte?

6.2.10.2 Obtención de Certificados de Identidad

Una vez que se ha seleccionado un proveedor, se deben identificar los requisitos del certificado:

- el nombremi los campos del certificado son vitales para la correcta interoperabilidad con los clientes; verContenido del nombre del certificado 50para más información.
- El certificado debe ser RSA2048 bit, con algoritmo de firma SHA-256
- La cantidad y duración
- El nivel de seguridad
- Ya sea dominio único o multidominio
- El certificado debe ser para un servidor web y no un certificado de firma.

Una vez identificados los requisitos, se realiza una solicitud de firma de certificado (CSR) a la CA. Esto puede usar varios métodos:

- Basado en formularios, utilizando el sitio web de la CA o utilidades descargadas: la CA crea la clave privada y el certificado y el cliente los envía o descarga.
- Basado en texto, usando el paquete OpenSSL: OpenSSL crea la clave privada y la guarda en la PC. El certificado lo crea la CA y se utiliza OpenSSL para unir las dos partes en un archivo PKCS#12.
- Basado en texto, utilizando las herramientas de Microsoft Windows: la clave privada se crea con las herramientas del sistema operativo de Microsoft y se guarda en la PC. El certificado lo crea la CA y las herramientas del SO de Microsoft que se utilizan para unir las dos partes en un archivo PKCS#12.
- Automatizado a través de SECP: IP Office crea la clave privada y la guarda en el sistema. El certificado lo crea la CA e IP Office une las dos partes.
- Basado en formularios web, utilizando un sitio de terceros. Esto no es recomendable.

Actualmente, los servidores IP Office Linux e IP500 V2 no admiten la generación de una CSR donde la clave privada se conserva dentro del servidor IP Office. Esto significa que si la CA noAntiguo Testamento Admite CSR basado en formularios, OpenSSL o métodos de herramientas de Microsoft Windows deSolicitudes de firma de certificado 134debe ser usado.

Una vez que se envía una CSR a la CA, esta revisará la solicitud y, si tiene éxito, emitirá el certificado de identidad junto con los certificados de firma. El formato requerido de los certificados de identidad de IP Office es PKC S#12. Los formatos requeridos para los certificados de firma son PEM y DER. VerNombre y formato del archivo de certificado 42.

Si los formatos de archivo no son los requeridos por las utilidades de IP Office, se pueden usar para convertir; estos pueden ser proporcionados por la CA o 3rd party se pueden utilizar herramientas. EnSolicitudes de firma de certificado 134.

6.2.11 Mantenimiento de certificados

Independientemente de la estructura de certificado/fideicomiso utilizada, todos los certificados caducan y, en circunstancias excepcionales, pueden verse comprometidos. Además, debido a los requisitos de nomenclatura del certificado de identidad, puede ser necesaria una actualización debido al cambio de nombre de host o dirección IP. La política de certificados debe incluir disposiciones para el reemplazo/actualización de CA y certificados individuales, tanto de confianza como de identidad.

Si se deja en la configuración predeterminada, los certificados de identidad de IP Office caducan siete años después de la instalación y el certificado de CA raíz en diez. Para los certificados obtenidos de una autoridad externa, puede ser tan solo 12 meses.

Para los certificados de identidad derivados de una CA, el reemplazo es relativamente sencillo ya que la CA (y, por lo tanto, la relación de confianza básica) no cambia: obtenga el reemplazo correspondiente antes de que caduque con el mismo contenido y reemplace. Si es necesario cambiar la CA raíz o intermedia, el proceso puede ser más extenso dependiendo de si el par de claves pública/privada asociado también cambia. La CA interna de IP Office en la primaria retendrá opcionalmente el par de claves pública/privada si el certificado de la CA se vuelve a crear a través de Administración web (el**renovar existente** opción).

Si se cambia el par de claves pública/privada de la CA raíz, todos los certificados de identidad deben renovarse y debe hacerse mucho antes de que caduque la CA. La nueva CA debe instalarse en las tiendas de confianza relevantes junto con la anterior; esto permite un período de transición durante el cual se pueden reemplazar todos los certificados de identidad.

Los inicios de sesión administrativos en Manager e IP Office Web Manager mostrarán una advertencia de caducidad del certificado de identidad, junto con la cantidad de días restantes. La versión 10.0 de IP Office y en adelante generará una alarma (un evento diario del sistema en SSA, SNMP, syslog, correo electrónico) cada vez que un certificado esté dentro de los 60 días de vencimiento.

6.2.11.1 Renovación de un certificado IP500 V2/secundario/de expansión

Si se utiliza el certificado autofirmado predeterminado o SCEP, eliminar el actual o reiniciar el sistema obligará a generar/obtener otro. Al crear el nuevo certificado, los archivos de nombre común y nombre alternativo del sujeto se pueden especificar en la configuración de seguridad del administrador; de lo contrario, se utilizarán los valores predeterminados. Para Server Edition, todos los procesos se reiniciarán, para IP500 V2, la transición será fluida.

Si el certificado de ID se obtuvo de una CA externa, se puede administrar un reemplazo mediante IP Office Manager o IP Office Web Manager.

6.2.11.2 Renovación de un certificado de ID de servidor de aplicaciones principal/Linux

Si el certificado de ID ha sido creado por la CA interna, la configuración Administración web**Plataforma | Configuración | generales | Certificados | Renovar automáticamente**determina si la creación y la aplicación son automáticas debido a la caducidad o al cambio de nombre de host o dirección IP. Si no es automático, se pueden usar Generar y Aplicar.

Si el certificado de ID se obtuvo de una CA externa, se puede administrar un reemplazo mediante IP Office Manager o IP Office Web Manager.

6.2.11.3 Renovación de un certificado de CA de aplicación principal/Linux

Se puede crear uno nuevo usando Administración web**Vista de la plataforma | Configuración | generales | Certificado CA | Crear nuevo**. Este comando debe usarse con precaución, ya que creará un certificado de CA raíz completamente nuevo; también requerirá nuevos certificados de identificación para todas las entidades y la distribución de certificados de CA a todos los dispositivos. Para conservar todos los certificados de identidad existentes, se debe seleccionar Renovar los existentes; esto creará un nuevo certificado con el mismo contenido y claves públicas/privadas, pero con un número de serie y una fecha de inicio/finalización diferentes. Solo esta nueva CA raíz requiere distribución; los certificados de identificación actualizados existentes firmados por la CA anterior seguirán siendo válidos. Se debe tener cuidado de no abusar de la comodidad de esta función, ya que cuanto más tiempo permanezcan sin cambios las claves públicas/privadas, mayor será el riesgo de compromiso.

VerUso de la autoridad de certificación de IP Office 131

6.2.11.4 Recuperación de un certificado

Todos los certificados forman parte del proceso de copia de seguridad/restauración de la configuración de seguridad. Para recuperar un certificado de ID, se debe restaurar el último conjunto de copias de seguridad. Para Server Edition, todos los procesos se reiniciarán.

6.2.11.5 Solución de problemas de certificados

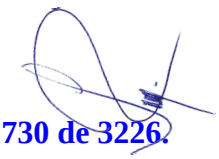
Los certificados intercambiados por cualquier interfaz de IP Office se pueden mostrar utilizando herramientas de terceros como Wireshark. El certificado de identidad de IP Office también se puede mostrar en Manager, IP Office Web Manager y navegadores.

La falla de las verificaciones de certificados recibidos por parte de IP Office genera un evento de alarma que contiene la causa. Estas alarmas también incluyen fallas de verificación de certificados según lo informado por el otro extremo a través de mensajes de alerta TLS. IP Office Manager y los navegadores también informan fallas en las comprobaciones de certificados.

Si una interfaz HTTP/TLS parece tener problemas con el certificado, es posible desactivar temporalmente la comprobación de certificados o activar una versión no segura de esa interfaz.

La interfaz de configuración de seguridad de IP Office Manager para IP Office siempre debe estar accesible; IP Office siempre se asegurará de tener un certificado de identidad (creando uno autofirmado si el anteriorsi se eliminó o se corrompió), y Manager se puede configurar para aceptar cualquier certificado. VerProtección de IP Office Manager 89.

Se ha encontrado en raras ocasiones que los enrutadores de gama baja al realizar la traducción de direcciones de red (NAT) modificarán las direcciones IP dentro de los campos de nombre del certificado, corrompiéndolos. Cambiar el firewall/enrutador es la mejor solución, pero una solución temporal puede ser eliminar cualquier entrada de dirección IP sujeta a NAT.



Capítulo 7.

Seguridad VoIP

7. Seguridad VoIP

La seguridad de medios de VoIP proporciona un medio por el cual dos puntos finales capaces de comunicarse pueden participar en intercambios de medios más seguros. Hay una serie de enfoques que se pueden utilizar:

- Protocolo de transporte seguro en tiempo real (SRTP)
- Seguridad de la capa de transporte de datagramas (DTLS)
- Una Red Privada Virtual (VPN) implementada usando IPsec u otra tecnología VPN como SSL VPN.
- Otros transportes IP con soporte de seguridad como Multiprotocol Label Switching (MPLS).

VPN y otra seguridad de transporte IP se analizan brevemente enLimitación de la exposición de la red IP 95,sin embargo, los méritos relativos de cada enfoque de seguridad de los medios están fuera del alcance de este documento.

SRTP es compatible con la protección de medios RTP punto a punto, proporcionando confidencialidad, autenticación de mensajes y protección de reproducción. SRTP también admite autenticación y protección de reproducción para el Protocolo de control RTP (RTCP). Tenga en cuenta que RTCP no se utiliza como canal de señalización para llamadas VoIP, pero contiene información de calidad de servicio (QoS).

La confidencialidad (implementada por el cifrado de clave simétrica) y la autenticación (implementada por el código de autenticación de mensajes hash, HMAC) son opcionales e independientes entre sí.

El cifrado SRTP se basa en claves seguras generadas dinámicamente para enviarse al extremo remoto. Esto no se puede lograr a través del protocolo SRTP, por lo que se requiere un mecanismo seguro alternativo, generalmente a través del canal de señalización asociado, por ejemplo, SIP-TLS para SIP y 'Anexo H' para H.323.

Como SRTP es punto a punto, todos los enlaces individuales involucrados en la llamada de VoIP, incluido el intercambio de claves/señalización, deben ser seguros para que la llamada sea segura de extremo a extremo.

7.1 Seguridad de medios de la plataforma IP Office

IP Office es compatible con SRTP e IPsec para la seguridad de los medios de VoIP. Se puede utilizar la función IPsec de IP Office, pero no se recomienda ya que se limita a la plataforma IP500 V2 y utiliza un mecanismo de intercambio de claves heredado (IKEv1).

La seguridad de medios de VoIP mediante SRTP es compatible con IP Office en Standard Edition, Server Edition, Select y alojada, sin necesidad de licencias adicionales, para las conexiones:

- Línea IP Office
- Línea SIP
- Línea SM
- Extensiones Avaya H.323: 9608, 9611, 9621, 9641
- Extensiones SIP de Avaya: 9608, 9611, 9621 y 9641 (en implementaciones de sucursales centralizadas), serie 1100, serie 1200, B179, E129, H175, serie J100, serie K100 (Vantage), serie Scopia XT
- Avaya Communicator para iPad y Windows
- one-X Mobile preferido para iOS y Android
- Extensiones SIP de terceros que admiten SRTP

Algunas conexiones de IP Office no admiten la seguridad de medios SRTP:

- Extensiones analógicas y digitales
- Líneas/troncales analógicas y digitales
- Enlace de IP Office <-> Voicemail Pro
- Troncos H.323
- Extensiones Avaya H.323: 96x0, 16xx, 36xx, 46xx, 56xx
- Extensiones SIP de Avaya: D100, E159, E169
- IP DECT y DECT R4 de Avaya
- Softphone de IP Office de Avaya (Mac)
- Extensiones SIP de terceros que no admiten SRTP

Las siguientes opciones de SRTP configurables son compatibles con IP Office:

función SRTP	Opciones	Apoyo	Defecto	notas
Operación SRTP	Desactivado	✓	✓	Todas las configuraciones de SRTP son por sistema con una anulación por línea y por extensión
	En: Mejor esfuerzo	✓		
	Activado: Hacer cumplir	✓		
Cifrado RTP	Apagado	✓		
	Encendido: AES128-CTR	✓	✓	
	Encendido: AES128-F8	✗		
Autenticación RTP	Apagado	✓		La autenticación RTP no debe deshabilitarse
	En: SHA-1/32	✓		
	En: SHA-1/80	✓	✓	SHA-1/80 proporciona una autenticación más fuerte para un pequeño aumento de ancho de banda
Cifrado RTCP	Apagado	✓	✓	
	Encendido: AES128-CTR	✓		Algunos terminales de Avaya y de terceros no admiten RTCP encriptado
	Encendido: AES128-F8	✗		
Autenticación RTCP	En: SHA-1/32	✓		Autenticación RTCP siempre activa
	En: SHA-1/80	✓	✓	SHA-1/80 proporciona una autenticación más sólida para un pequeño aumento de ancho de banda.

Tabla 19: Opciones de SRTP

IP Office es compatible con un conjunto de controles SRTP por sistema, con anulación por línea y extensión, incluida la configuración de encriptación y autenticación. De forma predeterminada, la operación de SRTP está deshabilitada; sin embargo, las actualizaciones de los sistemas de sucursal de IP Office de versiones anteriores que utilizan la línea SM y SRTP mantendrán su configuración.

El control de operación SRTP es la configuración Media Security y tiene los siguientes valores:

- **Desactivado**–SRTP no está disponible
- **Hacer cumplir**–RTP no está disponible en ese tramo de llamada. Nota: Esto no aplica SRTP de extremo a extremo, solo SRTP en el tramo de llamada configurado como**Hacer cumplir**.
- **Mejor esfuerzo**–siempre ofrezca tanto SRTP como RTP y si tiene la opción, elija SRTP.

Cuando los clientes de software SIP se conectan a IP Office en modo de registro simultáneo (es decir, otro dispositivo está registrado para el mismo usuario), no tienen una anulación por extensión de la configuración de seguridad de medios. IP Office manejará las llamadas de estos dispositivos de acuerdo con su configuración de seguridad de medios a nivel del sistema

IP Office considera cada tramo de una llamada de forma independiente para el control de SRTP; la configuración adecuada de la Línea o Extensión SRTP determinará el apoyo de cada pata. Las conferencias o grabaciones de llamadas con tramos SRTP por parte de IP Office conservarán SRTP siempre que sea posible.

En ordena proporcionar una seguridad de llamada completa, el intercambio de claves SRTP también debe estar protegido, consulteSeguridad de Señalización VoIP 70.

7.2 Seguridad de señalización de VoIP

La protección de la señalización de los enlaces de VoIP es necesaria cuando SRTP está habilitado y es una medida de seguridad en sí misma: debe habilitarse cuando el registrador SIP o H323 Gatekeeper está expuesto en una interfaz pública, con las otras opciones no seguras deshabilitadas.

El mecanismo de seguridad depende del tipo de enlace:

Tipo de vínculo	Mecanismo de seguridad clave	notas
Línea IP Office	WebSocket HTTPS	Solo se debe utilizar la línea de IP Office con transporte WebSocket y la configuración de seguridad Media o Alta.
Línea SIP	SIP-TLS	Se requiere una configuración de línea adicional para habilitar SIP-TLS. También es compatible con el esquema SIPS URI
Línea SM	SIP-TLS	Se requiere una configuración de línea adicional para habilitar SIP-TLS. También es compatible con el esquema SIPS URI.
Avaya H.323 extensiones	H.323-TLS	Compatible desde R10.0. Se requiere configuración adicional para habilitar H.323-TLS.
	H.323-Anexo H	No requiere configuración adicional Esto no asegura el canal de señalización H.323 completo, solo el registro, el intercambio de claves y los dígitos marcados.
Extensiones SIP de Avaya	SIP-TLS	Se requiere una configuración de registrador SIP adicional para habilitar SIP-TLS

Tabla 20: Seguridad de Señalización VoIP

Para las extensiones SIP, la configuración del protocolo de capa 4 del registrador SIP de la LAN relevante debe ser co Configurado para habilitar el protocolo TLS. SIP-TLS requiere la administración de certificados; verCertificados y Fideicomiso38.

Para las líneas SIP o SM, la configuración de transporte de la línea debe configurarse para usar el protocolo TLS y las verificaciones de certificados habilitadas. Otra consideración es el uso del esquema URI de SIPS según lo definido por RFC 3261 y RFC 5630. Habilitar la configuración Tipo de URI de SIPS hará que todas las sesiones originadas desde el enlace troncal usen SIPS, lo que indica el requisito de enlaces SIP seguros para la llamada. El sistema de ajuste del sistema | Seguridad VoIP | SIPS estricto cuando está activo, hace que IP Office rechace cualquier llamada a una línea SIP o SM que no esté configurada para SIP-TLS y el esquema SIPS URI. Cuando no está configurada, IP Office permite la 'reducción de categoría' de una llamada SIP-TLS a una llamada SIP no segura.

Se debe tener cuidado al usar el esquema SIPS URI y Strict SIPS, ya que el soporte de los clientes de Avaya y los ITSP varía, lo que podría resultar en llamadas fallidas. Esto es de gran importancia para la planificación de llamadas de emergencia.

El soporte SIPS actual de los clientes de Avaya está cubierto enSeguridad de punto final VoIP de IP Office127.

VerAprovisionamiento seguro de 9609, 9611, 9621 y 9641 H.323144teléfonos para obtener información sobre el aprovisionamiento de teléfonos seguros 9608, 9611, 9621 y 9641 H323.

Para obtener más detalles, consulte la documentación del cliente correspondiente.

7.3 Seguridad de aprovisionamiento de terminales

Cuando se utiliza seguridad de medios o de señalización, se requieren configuraciones en los propios puntos finales. Parte del aprovisionamiento de terminales remotos es compatible directamente con IP Office y se puede transmitir de manera más segura a través de HTTPS en lugar del HTTP predeterminado.

El soporte de punto final del aprovisionamiento remoto seguro se trata enSeguridad de punto final VoIP de IP Office127.

Cuando un punto final no admite el aprovisionamiento de punto final remoto, se utiliza la configuración local del dispositivo.

Para obtener más detalles, consulte la documentación del cliente correspondiente.

7.4 Rendimiento y capacidad de SRTP

SRTP es más intensivo en procesamiento que RTP en la medida en que la capacidad de llamadas simultáneas de un IP500 V2 se reduce en un 66 % y los servidores Linux en un 50 %. Consulte la sección Planificación de la capacidad en "*Implementación de la solución IP Office Server Edition*". Estas reducciones solo ocurren cuando el flujo de medios termina o se origina en IP Office. Por esta razón, es importante usar medios directos siempre que sea posible.

Los medios directos de SRTP ocurrirán cuando las capacidades de SRTP de ambos terminales externos coincidan; si no es así, IP Office terminará ambas transmisiones y realizará la conversión. Esto reducirá la capacidad de llamadas SRTP concurrentes en dos. Esto, a su vez, otorga gran importancia a las diversas configuraciones de SRTP dentro de IP Office y los diversos puntos finales.

Las siguientes recomendaciones de IP Office deben seguirse como punto de partida y solo modificarse si es necesario:

- El cifrado RTP y la autenticación deben mantenerse activados; algunos puntos finales no negociarán en absoluto si cualquiera de los dos está desactivado.
- La configuración de autenticaciones/cifrado RTP debe ser AES-128/CTR más SHA-1/80.
- El cifrado RTCP debe mantenerse desactivado; algunos sistemas (incluido Avaya Communication Manager) no admiten el cifrado RTCP.
- Todas las extensiones SIP, cuando sea posible, deben configurarse para el mejor esfuerzo (negociación de capacidad o 'cap-neg'); esto permite que la configuración de IP Office dicte el comportamiento de SRTP.
    - **Nota:**Cuando los archivos de configuración generados automáticamente que IP Office proporciona a las series 1100/1200 y los tipos de dispositivos B179 siempre indican a los teléfonos que hagan el mejor esfuerzo, cuando la configuración de SRTP de IP Office es Best Effort o Enforce.
- Garantice la consistencia entre el sistema y la configuración de SRTP por extensión para los clientes de software SIP que se conectan a IP Office en modo de registro simultáneo (Avaya Communicator y one-X Portal for IP Office Mobile).
- Todas las configuraciones de medios directos activadas.
- Selecciones de códec predeterminadas que deberían garantizar que el códec G711 obligatorio esté siempre disponible.

Otra consideración de rendimiento es el ancho de banda adicional que se genera cuando SRTP está activo; la autenticación agrega 4 o 10 bytes a cada paquete para RTP y RTCP. Dado un período de muestra de 20 ms, el SRTP activo usa el siguiente ancho de banda de IP aproximado para una sola llamada:

códec	Sin SRTP	+ autorización RTCP	+ autorización RTP/RTCP	notas
G.711	84 kbps	SHA1/80: 85 kbps SHA1/32: 84,5 kbps	SHA1/80: 86 kbps SHA1/32: 85 kbps	aumento del 2,4% aumento del 1,2%
G.729	25 kbps	SHA1/80: 26 kbps SHA1/32: 25,5 kbps	SHA1/80: 27 kbps SHA1/32: 26 kbps	aumento del 8% aumento del 4%
G.722	84 kbps	SHA1/80: 85 kbps SHA1/32: 84,5 kbps	SHA1/80: 86 kbps SHA1/32: 85 kbps	aumento del 2,4% aumento del 1,2%

Tabla 21: Ancho de banda SRTP

7.5 Indicaciones de llamadas seguras

No hay indicaciones directas en las pantallas de los teléfonos que indiquen que la llamada es segura. Si se requiere garantía, Media Security debe establecerse en Enforce y Strict SIPS activado.

El tramo de llamada SRTPAGS El estado se puede mostrar mediante la aplicación de estado del sistema y el monitor del sistema, consulteSolución de problemas de SRTP 121.

7.6 Consideraciones sobre la planificación de la seguridad de VoIP

La señalización y los medios seguros deben tenerse en cuenta cada vez que las terminales VoIP o las interfaces VoIP de IP Office transiten o sean potencialmente accesibles a través de redes no confiables, incluida Internet.

Antes de implementar medios seguros o señalización mediante IP Office, se debe revisar lo siguiente:

- La función SRTP de IP Office es compatible con la seguridad de los medios de forma nativa sin requisitos de licencia o infraestructura de IP, pero puede agregar una complejidad de interoperación adicional con varios puntos finales.
- La seguridad de la señalización debe tenerse en cuenta siempre que se contemple SRTP. La seguridad de la señalización puede considerarse por sí sola como un mecanismo de mejora de la seguridad.
- Se debe considerar el aprovisionamiento seguro de teléfonos siempre que se contemple la seguridad de los medios o la señalización.
- Cuando la resiliencia de puntos finales de VoIP está activa con señalización o aprovisionamiento seguro, el certificado de CA raíz para el servidor principal y el de respaldo debe ser el mismo.
- SRTP reducirá la capacidad de llamadas simultáneas de los sistemas IP Office, por lo tanto, se deben usar medios directos siempre que sea posible. También puede reducir la capacidad y el rendimiento de otros sistemas conectados.
- Se debe evaluar el soporte SRTP exacto de cada tipo de punto final para determinar la mejor manera de lograr la seguridad, los medios directos y otros criterios de rendimiento.
- La configuración de SRTP predeterminada de IP Office debe conservarse siempre que sea posible y solo modificarse en circunstancias excepcionales.
- Las implementaciones de sucursales de IP Office tienen un entorno y requisitos especializados. Ver:
  - Implementación de la plataforma Avaya IP Office™ como una sucursal empresarial con Avaya Aura® Session Manager, número de documento 18-603853,https://downloads.avaya.com/css/P8/documents/101004861
  - Administración de usuarios centralizados para una sucursal empresarial de la plataforma IP Office™, número de documento 15-604263,https://downloads.avaya.com/css/P8/documents/101004857
  - Configuración de referencia de Avaya IP Office™ Platform en un entorno de sucursal, número de documento 15-604253,https://downloads.avaya.com/css/P8/documents/101004855

Capítulo 8.

Protección de la solución de la plataforma IP Office

8. Protección de la solución de la plataforma IP Office

IP Office puede convertirse en un producto muy seguro; sin embargo, solo una cierta cantidad de funciones están activas de forma predeterminada o en la actualización de versiones anteriores. Esto es para facilitar la instalación inicial, pero no ayudará a proteger el sistema sin seguir las sugerencias enumeradas en este documento, otras publicaciones de seguridad de Avaya y los manuales de instalación/administración de IP Office relevantes. Por lo tanto, es necesario verificar e implementar las opciones de configuración enumeradas aquí.

Puede ser necesaria una configuración adicional para asegurar aún más la implementación individual. Avaya presenta esta información solo como guía; el cliente es responsable de garantizar que su sistema sea seguro.

- Reglas generales 75
- Evaluación de los requisitos de seguridad de IP Office 76
- Administración de Seguridad 76
- Cambiar valores predeterminados de seguridad 76
- Eliminar cuentas innecesarias 76
- Deshabilitar servicios/interfaces no utilizados 77
- Garantizar derechos mínimos de acceso 78
- Hacer cumplir una política de contraseñas 79
- Actualizar certificados 80
- Protección de usuarios y extensiones de telefonía 81
- Endurecimiento para la operación de trabajadores remotos 82
- Protección de troncales/líneas 83
- Medios de voz seguros 83
- Prevención de llamadas no deseadas 84
- Protección de las interfaces CTI 88
- Protección de las aplicaciones de IP Office 88
- Configuración y otros datos confidenciales 94
- Limitación de la exposición de la red IP 95
- Interfaces de mantenimiento seguras 96
- Restricción del acceso físico 96
- Protección de servidores Server Edition 97
- Protección del servidor de aplicaciones Linux/módulo de comunicaciones unificadas 99

8.1 Directrices generales

El proceso recomendado para mejorar la seguridad de IP Office es: Evaluar los requisitos, implementar cambios según sea necesario, luego monitorear el sistema y responder de manera oportuna a cualquier amenaza detectada.

Se deben seguir todas las pautas y pasos, independientemente de la implementación real de IP Office.

Evaluar:

- Revisar las instalaciones existentes
- Planificar nuevos despliegues
- Identificar riesgos y requisitos de seguridad.

Implementar:

- Cambiar los valores predeterminados de seguridad
- Eliminar cuentas innecesarias
- Deshabilitar servicios/interfaces no utilizados
- Hacer cumplir la política de contraseñas
- Actualizar Certificados de Identidad y PKI
- Usuarios y extensiones seguras
- Líneas/troncales seguras
- Medios de voz seguros
- Prevenir llamadas no deseadas
- Correo de voz seguro y one-X Portal para IP Office
- Limite la exposición de la red IP
- Aplicaciones de gestión seguras y datos de configuración
- Servidores seguros
- Activar informes/supervisión
- Comprobaciones y pruebas

Monitor:

- Supervisar alarmas y registros
- Detectar otra actividad inusual
- Revise los avisos de seguridad de Avaya
- Revise las actualizaciones y los boletines técnicos del software Avaya IP Office
- Supervisar la comunicación del proveedor de telefonía
- Reevaluación periódica de la seguridad

Responder:

- Investigar y reaccionar ante cualquier incidente.
- Informe a las organizaciones apropiadas
- Asegúrese de que estén instaladas las últimas actualizaciones de software/paquetes de servicio

8.2 Evaluación de los requisitos de seguridad de IP Office

Es vital que se lleve a cabo una evaluación de riesgos de seguridad en todas las instalaciones de IP Office, tanto inicial (antes de la implementación o para implementaciones existentes si aún no se ha realizado), como periódicamente después de la evaluación inicial para revisar cualquier cambio.

Un diferenciador principal del riesgo de seguridad para IP Office es si el sistema es potencialmente accesible desde redes o personas externas o no seguras, especialmente Internet.

Este documento no cubre las evaluaciones de seguridad en detalle; sin embargo, hay muchos recursos disponibles que cubren este proceso, incluidos, por ejemplo:

- **Publicación especial (SP) 800-30 del Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST), Guía de gestión de riesgos para el sistema de tecnología de la información**
  http://dx.doi.org/10.6028/NIST.SP.800-30r1
- **Reino Unido British Standards Institute (BSI) ISO/IEC 27001, Cuestionario de autoevaluación** http://www.bsigroup.co.uk/en-GB/iso-27001-information-security/ISO-27001-for-SME/
- SANS Institute también proporciona una amplia gama de información relacionada con la seguridad, incluidas evaluaciones de riesgos y auditorías:
  http://www.sans.org/sala-de-lectura

8.3 Administración de seguridad

Los ajustes de seguridad se almacenan en el sistema y son independientes de los ajustes de configuración del sistema. Para cambiar la configuración de seguridad de un sistema, Manager primero debe cambiarse al modo de seguridad seleccionando**Archivo | Avanzado | Configuraciones de seguridad**desde la barra de menú.

La configuración de seguridad solo se puede cargar directamente desde un sistema. Estas configuraciones no se pueden guardar como un archivo en la PC local, ni aparecen como un archivo temporal en ningún momento. De manera predeterminada, Manager y el sistema siempre intentarán usar un enlace seguro para los intercambios de configuraciones y ajustes de seguridad.

8.4 Cambiar valores predeterminados de seguridad

Todas las contraseñas predeterminadas deben cambiarse a una contraseña única y "fuerte". VerGestión de contraseñas y PIN para obtener más 32 información sobre la seguridad de la contraseña.

En IP Office Manager**Configuración de seguridad | General**pestaña:

1. Para la cuenta de administrador de seguridad:

   una. Cambio**Clave**a una contraseña 'fuerte' de 8 o más caracteres.

   b. Establecer**Complejidad mínima de la contraseña**a***alto***.

2. Cambiar la cuenta de usuario del servicio '**Administrador**' contraseña a una contraseña 'fuerte' de 8 o más caracteres.
3. Si es necesario, agregue una cuenta de administración del cliente (nuevamente con una contraseña segura) con los derechos mínimos de acceso. el estado de la cuenta**Forzar nueva contraseña**debe establecerse. Esto impondrá un cambio de contraseña en el próximo inicio de sesión (es decir, durante la instalación del cliente/ingeniería).
4. Cambie las contraseñas del sistema, VM Pro y Monitor a contraseñas 'fuertes' de 8 o más caracteres.

8.5 Eliminar cuentas innecesarias

Todas las cuentas de administración y de usuario de IP Office innecesarias deben eliminarse o deshabilitarse para reducir la probabilidad de que las cuentas predeterminadas olvidadas se utilicen para acceso no autorizado.es s. Las cuentas restantes deben tener sus contraseñas cambiadas. Ver Cuentas de usuario y derechos de acceso 22para obtener más información sobre los diferentes tipos de cuentas y ubicaciones.

1. En IP Office Manager |**Configuración de seguridad | Usuario del servicio**pestaña, elimine todas las cuentas de usuario de servicio innecesarias; conservar únicamente las cuentas que sean imprescindibles. El usuario del servicio puede eliminarse o el estado de la cuenta puede establecerse como Deshabilitado.

2. Para todas las cuentas de usuario de servicio activas restantes, cambie pass palabra a una fuerte de 8 o más caracteres. Si utiliza Server Edition, consulteProtección de servidores Server Edition 97para la administración de usuarios de servicios alternativos mediante IP Office Web Manager

3 en**Configuración | Usuarios**: elimine cualquier cuenta de usuario de telefonía RAS (por ejemplo, 'RemoteManager') que no sea necesaria. Para cualquiera que sea necesario, cambie la contraseña a una segura de 8 o más caracteres.

Página1740 de 3226.

8.6 Deshabilitar servicios/interfaces no utilizados

Todas las interfaces y servicios que no sean necesarios deben desactivarse. Además, considere habilitar interfaces y servicios solo cuando sea necesario.

1. En IP Office Manager**Configuración de seguridad | Sistema | Interfaces no seguras**pestaña: Desmarque todos los controles de la aplicación y habilite solo el mínimo de acuerdo con la siguiente tabla:

Control de aplicaciones	Aplicación afectada	notas
Servidor TFTP	Administrador de actualización de IP Office Manager Phone Manager DECT R4* Correo de voz Pro heredado Whois UDP** Visor de red	Deshabilita todo el acceso TFTP, incluida la lectura de directorio TFTP, el correo de voz TFTP y el código de programa. * Cuando está inactivo, DECT seguirá funcionando pero sin la función de directorio del sistema. * * El descubrimiento de TCP whois debe usarse en Manager.
Directorio TFTP Leer	Administrador de teléfono DECT R4* Instalación TAPI**	También se utiliza para aplicaciones heredadas: IP DECT*, DECT analógico, centro de conferencias, CRM, MMM * Cuando está inactivo, DECT seguirá funcionando pero sin la función de directorio del sistema * * La instalación de TAPI generará una advertencia, pero se puede ignorar También controlado por la configuración general del servidor TFTP anterior.
Correo de voz TFTP	Correo de voz Pro heredado	Habilitar solo cuando se usa Voicemail Pro R9.0 y versiones anteriores No aplicable al correo de voz integrado También controlado por la configuración general del servidor TFTP anterior.
Código de programa	Actualización del administrador de IP Office	Se utiliza para actualizaciones desde IP Office Manager, debe deshabilitarse cuando no se requiera También controlado por la configuración general del servidor TFTP anterior.
DevLink	DevLink Monitoreo del sistema*	Debe estar deshabilitado cuando no se requiera * Cuando está inactivo, System Monitor todavía puede usar el método de acceso HTTP/S.
TAPI	TAPI Link Lite (TAPI de terceros) TAPI Link Pro (TAPI de terceros) Avaya Contact Center Select IP Office Contact Center	Habilite solo cuando se requiera TAPI; tenga en cuenta que la instalación del controlador TAPI fallará si la interfaz TAPI no está activa. Esta configuración afectará a IPOCC y ACCS CTI Link; cuando está inactivo, cualquier sesión de IPOCC y ACCS requerirá TLS y un certificado de confianza de IPOCC/ACCS. Esta configuración no afectará one-X Portal for IP Office CTI Link.
Directorio HTTP Leer	Directorio centralizado de IP Office Teléfono J129*	Habilite solo cuando se use J129 o el directorio centralizado de IP Office. Acceso solo a través de HTTPS. El puerto HTTP 80 debe estar deshabilitado. * Cuando está inactivo, J129 seguirá funcionando pero sin la función de directorio
Directorio HTTP Escribe	J129*	Habilitar solo cuando J129. Acceso solo a través de HTTPS. El puerto HTTP 80 debe estar deshabilitado. * Cuando está inactivo, J129 seguirá funcionando pero sin la función de actualización de directorio

Tabla 22: Efecto de los Servicios de Inhabilitación

8.7 Garantizar derechos mínimos de acceso

Restringir los derechos de acceso de los Usuarios al Servicio al mínimo necesario. VerCuentas de usuario y derechos de acceso más 22 por información sobre los diferentes niveles de acceso.

1. En IP Office Manager |**Configuración de seguridad | Grupos de derechos**, elimine todos los derechos de acceso innecesarios; sólo conservan los derechos que son esenciales.
2. En IP Office Manager |**Configuración de seguridad | Usuarios del servicio | Membresía del grupo de derechos**, elimine toda la pertenencia a grupos de derechos innecesarios.
3. Si es necesario, cree nuevos grupos de derechos con acceso mínimo.
4. Los grupos de derechos que están definidos pero no asignados a ningún usuario del servicio no presentan un riesgo de seguridad.
5. En IP Office Manager**Configuración de seguridad | Servicios**pestaña: habilite solo los servicios mínimos en los recomendados**Nivel de seguridad del servicio**de acuerdo con la siguiente tabla:

Nombre del Servicio	Solicitud	Servicio Seguridad Nivel	notas
Configuración	Gerente, Configuración Servicio web (DevConnect)	Seguro, Medio	Siempre debe estar habilitado
Seguridad Administración	Gerente	Seguro, Medio	Siempre debe estar habilitado
Estado del sistema Solicitud Interfaz	SSA	Seguro, Medio	Deshabilitar si SSA no está presente
TSPI mejorado	Portal one-X para IP Office	Solo no seguro	Deshabilitar si one-X Portal for IP Office no está presente
HTTP	Teléfonos H323 (HTTP o HTTPS) Administrador de archivos integrado (HTTP), Softphone de IP Office (HTTP o HTTPS) Monitor de sistema (HTTP o HTTPS) VM Pro (HTTPS) Línea IP Office (HTTP o HTTPS)		Controla el servidor HTTP de IP Office. Deshabilite si no es necesario, de lo contrario, si solo requiere HTTPS, configure en Seguro, Medio. Si se debe habilitar HTTP, configure el**Sistema | Sistema | Solo cliente HTTP de Avaya**configuración activa. Esto rechazará a todos los clientes que no sean de Avaya.
Servicios web	Administrador web de IP Office	Seguro, Medio	Deshabilitar si no se usa Administración web o Administrador del sistema (SMGR)
Externo	buzón de voz profesional, one-X Portal para IP Office, control web, WebRTC	n / A	No es una verdadera interfaz de servicio

Tabla 23: Derechos de Acceso Mínimos

6. En IP Office Manager**Configuración | Sistema | Sistema**pestaña, verifique la configuración de la dirección IP del escritor de archivos. Esto especifica la dirección IP permitida para escribir archivos en IP Office (IP500 V2 y Linux) usando los protocolos HTTP y TFTP. Debe establecerse en 0.0.0.0 (deshabilitado) y establecerse solo cuando sea necesario transferir archivos.

8.8 Hacer cumplir una política de contraseñas

Cambie la configuración de seguridad para hacer cumplir la complejidad mínima de la contraseña, deshabilite a los usuarios del servicio temporalmente y a los usuarios de IP Office de forma permanente en los inicios de sesión incorrectos.

Si un usuario del Servicio no inicia sesión 3 veces en 10 minutos, la cuenta se bloqueará durante 60 segundos. Si un usuario de IP Office no inicia sesión 5 veces en 10 minutos, la cuenta se bloqueará de forma permanente y el administrador deberá desbloquear la cuenta mediante Manager.

- **NOTA:**Esta política de contraseñas de usuario de IP Office recomendada siempre debe aplicarse si el sistema es potencialmente accesible desde redes no seguras, incluido Internet; por ejemplo, cuando se admiten extensiones/ trabajadores remotos de VoIP o troncales SIP.

En Seguridad de IP Office Manager**Configuración | General**pestaña:

1.**Establecer los detalles del usuario del servicio:**

- **Longitud mínima del nombre**a 6
- **Longitud mínima de la contraseña**a 8
- **Acción de rechazo de contraseña**a '***Registro y deshabilitación temporal***'.
- **Complejidad mínima de la contraseña**a '***Medio***'.
- **Límite de contraseña anterior (entradas)**para 4.

2.**Establezca los detalles del usuario de IP Office:**

- **Aplicación de contraseña**a encendido
- **Longitud mínima de la contraseña**a 8
- **Complejidad mínima de la contraseña**a 'Medio'.
- **Límite de rechazo de contraseña**a 5
- **Acción de rechazo de contraseña**a '***Iniciar sesión y desactivar cuenta***'.

- **Nota:**La política de contraseñas de usuario de IP Office onl y se aplica al campo de la contraseña, no al correo de voz ni al código de inicio de sesión del usuario. VerGestión de contraseñas y PIN 32para más información.

8.9 Actualizar certificados

1. Es fundamental comprender la información y recomendaciones deCertificados y Fideicomiso los requisitos 38 para determinar de certificado y confianza del sistema antes de la instalación.
2. Si es necesario, administre un nuevo certificado de identidad de plataforma:
   - El nuevo certificado de identidad debe estar en un archivo 'p12' o 'pfx'.
   - Idealmente, todos los certificados utilizados para firmar el nuevo certificado de identidad deberían estar en el mismo archivo.
   - Si los certificados de firma están en archivos separados, use Manager**Seguridad | Sistema | Certificados | Almacén de certificados de confianza | Agregar**para subir cada uno.
   - Activar la configuración del Administrador**Seguridad | Sistema | Certificados | Certificado de Identidad | Cadena de certificados de ID de oferta**.
   - Administrador de uso**Seguridad | Sistema | Certificados | Certificado de Identidad | Establecer**para cargar el archivo del certificado de identidad.
   - El certificado de identidad se propagará automáticamente a todas las interfaces TLS/HTTPS del servidor, todos los certificados de firma se colocarán en el almacén de certificados de confianza (TCS).
   - Si se requiere un certificado de identidad de telefonía independiente, debe administrarse utilizando la configuración de seguridad de Manager.
3. Los certificados predeterminados en los que confía IP Office deben eliminarse si no se requieren. Esto se logra colocando una copia del certificado en el***sistema/primario/certificados/tcs/eliminar***directorio utilizando el Administrador de archivos de Manager o IP Office Web Manager.
   Cualquier certificado predeterminado en el que IP Office confíe debe agregarse a la ***sistema/primario/certificados/tcs/añadir***directorio. VerCertificados de confianza predeterminados 112para obtener más información y cómo crear los archivos de certificado.
4. Si hay un cambio en la dirección IP de la LAN, el dominio SIP o el FQDN del servidor, será necesario volver a generar el certificado de identidad. Un servidor de expansión IP500 V2, Unified Communications Module, secundario o Linux siempre requerirá una regeneración manual. Un servidor de aplicaciones primario o Linux será automático si el**Administrador web de IP Office | Plataforma | Configuración | generales | Certificados | Renovar automáticamente**el ajuste está activo (predeterminado).
5. Después de asegurarse de que todos los demás certificados de identidad de los componentes de IP Office estén configurados correctamente, configure los niveles de verificación de certificados recibidos de manera adecuada mediante la configuración de Manager.**Seguridad | Sistema | Certificados | Comprobaciones de certificados recibidos (Gestión)**y**Seguridad | Sistema | Certificados | Comprobaciones de certificados recibidos (Telefonía)**.

8.10 Protección de usuarios y extensiones de telefonía

Los usuarios y las extensiones deben configurarse para restringir el acceso a las funciones necesarias, cambiar los códigos de inicio de sesión predeterminados y deshabilitar la creación automática.

1. Todos los usuarios no utilizados deben eliminarse, excepto NoUser.

2. Las siguientes configuraciones de creación automática se deben deshabilitar cuando no se requieran:

   - **LAN1 | VoIP | Portero H323 | Extensión de creación automática**
   - **LAN1 | VoIP | Portero H323 | Usuario de creación automática**
   - **LAN1 | VoIP | Registrador SIP | Crear automáticamente extensión/usuario**
   - **LAN2 | VoIP | Portero H323 | Extensión de creación automática**
   - **LAN2 | VoIP | Portero H323 | Usuario de creación automática**
   - **LAN2 | VoIP | Registrador SIP | Crear automáticamente extensión/usuario**
   - **Línea | DECT IP | puerta de enlace | Extensión de creación automática**
   - **Línea | DECT IP | puerta de enlace | Usuario de creación automática**

3. Si se utiliza alguna función de creación automática para ayudar en la instalación, la configuración debe desactivarse lo antes posible. Tenga en cuenta que a partir de la versión 9.1, estos ajustes se desactivarán automáticamente 24 horas después de configurarlos para evitar la exposición inadvertida.

4. Si no se admiten extensiones H.323, el**LAN1/LAN2 | VoIP | H323 Gatekeeper Habilitar**debe configurarse deshabilitado. Si se admiten las extensiones H.323, solo se debe habilitar el controlador de acceso de la LAN correspondiente.

5. Si no se admiten trabajadores remotos H.323, el**LAN1/LAN2 | VoIP | Portero H323 | Habilitar extensión remota H323**debe configurarse deshabilitado. Si se admiten trabajadores remotos H.323, solo se debe habilitar la extensión remota de la LAN correspondiente.

6. Si no se admiten extensiones SIP, el**LAN1/LAN2 | VoIP | Habilitar registrador SIP**debe configurarse deshabilitado. Si se admiten las extensiones SIP, solo se debe habilitar el registrador de la LAN correspondiente.

7. Si no se admiten trabajadores remotos SIP, el**LAN1/LAN2 | VoIP | Registrador SIP | Habilitar extensión remota SIP**debe configurarse deshabilitado. Si se admiten trabajadores remotos SIP, solo se debe habilitar la extensión remota SIP de la LAN correspondiente.

8. Haga cumplir una política de código de inicio de sesión (PIN) para todos los usuarios y extensiones configurando**Sistema | Telefonía | Complejidad del código de inicio de sesión | Longitud mínima**a la longitud mínima aceptable y activando**C** pruebas de complejidad. Para obtener más información sobre la seguridad del PIN y el código de inicio de sesión, consulteGestión de contraseñas y PIN 32.

9. Todos los usuarios de VoIP (SIP, H323, DECT)**Usuario |Telefonía | Configuración del supervisor | Código de inicio de sesión**o**Extensión | Ext. | Contraseña del teléfono**se debe establecer.

10. Si algún registrador SIP o gatekeeper H323 está expuesto directa o indirectamente**a** una red no segura, incluso a través de un SBC, los pasos adicionales deEndurecimiento para la operación de trabajadores remotos 82debe seguirse.

11. Todas las extensiones SIP'**Ext. | Forzar autorización**la configuración debe estar habilitada.

12. Todos los usuarios de VoIP creados automáticamente deben tener su**Usuario | Telefonía | Configuración del supervisor | Código de inicio de sesión** cambiado desde el valor predeterminado. Todos los usuarios no VoIP (Digital, Analógico) creados automáticamente deben cambiar su nombre y extensión de los predeterminados.

13. Cada usuario debe tener solo lo necesario**Usuario | Usuario | Perfil**funciones habilitadas, todas las demás deshabilitadas.

14. Cada usuario debe tener solo lo mínimo necesario**Usuario | Autoadministración web**características de la interfaz habilitadas, todas las demás deshabilitadas. La autoadministración web es una característica nueva de R9.1 y está deshabilitada de manera predeterminada. Cada pestaña de la página de autoadministración web se puede controlar para ver y editar por usuario:

Pestaña	Configuración del usuario
Perfil	Usuario
Mensaje de voz	Mensaje de voz
No molestar	No molestar
Movilidad	Movilidad
Reenvío	Reenvío
Directorio personal	Directorio personal
Programación de botones	Programación de botones
Descargar	ninguno (siempre disponible)

15. Para IP Office versión 8.1 y anteriores, deshabilite todos**Usuario | Opciones del administrador del teléfono**a menos que sea necesario. Esto se puede lograr mediante la aplicación de Derechos de usuario (Derechos de usuario | Administrador de teléfono).

16. Si difierenNuevo Testamento desde la configuración de todo el sistema, cambie el**Ext. | VoIP | Seguridad de los medios**ajuste. VerSeguridad VoIP 68.

Página1745 de 3226.

17. Si la extensión de VoIP se va a configurar para medios seguros (SRTP) o funciona en un entorno no seguro, cualquier archivo de configuración proporcionado por IP Office se debe convertirmi yed a través de HTTPS no HTTP. Esto requerirá además la administración de certificados; verCertificados y Fideicomiso 38.

8.11 Fortalecimiento para la operación de trabajadores remotos

Siempre que se admita la operación de trabajador remoto SIP o H323, o si cualquier registrador SIP o gatekeeper H323 está expuesto directa o indirectamente a una red no segura, incluso a través de un SBC, se requieren consideraciones adicionales para garantizar que el acceso externo no comprometa la seguridad de IP Office.

- **Importante:**
  IP Office solo debe conectarse externamente a través de un Firewall configurado correctamente. Nunca debe conectarse directamente.

1. El rango de puertos RTP en la interfaz LAN debe establecerse en no más de 50750. Si se requieren más puertos RTP, se puede cambiar el valor mínimo.
   - **LAN1/LAN2 | VoIP | Rango de número de puerto | Máximo**
   - **LAN1/LAN2 | VoIP | Rango de número de puerto (NAT) | Máximo**
2. Cualquier registrador SIP expuesto o H323GRAMO atekeeper debe tener la opción TLS aplicada y cualquier opción no segura deshabilitada. VerSeguridad VoIP 68.Para reducir los gastos generales de seguridad y administración de certificados, se puede usar un registrador de LAN para la interfaz externa y la otra LAN para extensiones internas.
3. Los puertos del registrador SIP deben cambiarse del predeterminado 5060/5061
4. Cualquier archivo de configuración proporcionado por IP Office debe ser convocado.y ed a través de HTTPS no HTTP. Esto requerirá además la administración de certificados; verCertificados y Fideicomiso 38.
5. Se debe considerar SRTP para la seguridad de los medios, consulteSeguridad VoIP 68.
6. Si cualquier H323 Gatekeeper o registrador SIP está expuesto directa o indirectamente a una red no segura, todos los trabajadores remotos **Extensión | Ext. | Contraseña del teléfono**se debe establecer. El código no debe ser una secuencia, dígitos repetidos o el mismo que el número de extensión. No debe tener menos de 9 dígitos, preferiblemente 13 dígitos. Para R8.1 y anteriores, la configuración**Usuario | Telefonía | Configuración del supervisor | Código de inicio de sesión**puede ser usado.
7. Cada extensión de trabajador remoto H323 o SIP**Extensión | VoIP | Dirección IP**debe establecerse en la dirección IP pública del teléfono.
   - **Nota:**Esto no se puede usar si hay más de un teléfono detrás del mismo firewall/NAT, o si cambia la dirección IP remota.
8. Los pasos deProtección de usuarios y extensiones de telefonía 81debe seguirse.
9. Los pasos dePrevención de llamadas no deseadas 84debe seguirse.
10. Se debe considerar un controlador de borde de sesión (SBC) para mejorar la seguridad de los trabajadores remotos SIP: Avaya SBC for Enterprise (ABSCE) es una solución diseñada específicamente para trabajadores remotos SIP de IP Office y troncales SIP. Para más información, ver "*Configuración de Avaya Session Border Controller para trabajadores remotos de IP Office*" en "*Administración de Avaya IP Office Platform™ con Manager*".
    - **Nota:**
      Si se implementa una puerta de enlace de nivel de aplicación (ALG) SBC o SIP, algunas de las medidas de seguridad de IP Office deben trasladarse de IP Office a SBC/ALG; la lista negra de direcciones IP de origen de IP Office debe deshabilitarse con el número de origen sin usuario 'B_DISABLE_SIP_IPADDR'. La lista blanca/negra de SBC/ALG debe estar activada para compensar.

8.12 Protección de troncales/líneas

El enlace troncal SIP y el interruptor de apagado o los reenvíos/transferencias de troncal a troncal deben desactivarse cuando no se requieran, y se debe usar un controlador de borde de sesión (SBC) para mejorar la seguridad de SIP. Los enlaces entre los sistemas IP Office se pueden proteger opcionalmente.

1. Si usa troncales SIP, IP Office debe estar conectado externamente a través de un Firewall correctamente configurado; verLimitación de la exposición de la red IP 93para más información. Nunca se debe conectar IP Office directamente.
2. A menos que los troncales SIP estén configurados para una interfaz LAN en particular, el**LAN1/LAN2 | VoIP | Habilitar Troncal SIP**el ajuste debe estar deshabilitado.
3. Muchos clientes de IP Office confían en los proveedores de servicios para proporcionar un entorno de troncal SIP seguro. Para una postura de seguridad más sólida, se recomienda la implementación de Avaya Session Border Controller for Enterprise (Avaya SBCE) como mejor práctica. Avaya SBCE también proporciona servicios avanzados, como Secure Remote Worker y Encryption Service, que admiten el acceso sin VPN a IP Office para terminales SIP fuera del firewall de la empresa. Avaya SBC for Enterprise es una solución diseñada específicamente para IP Office. Para más información, ver:

   http://www.avaya.com/usa/product/avaya-session-border-controller-for-enterprise .

   - **Nota:**
     Si se implementa una puerta de enlace de nivel de aplicación (ALG) SBC o SIP, algunas de las medidas de seguridad de IP Office deben trasladarse de IP Office a SBC/ALG; la lista negra de direcciones IP de origen de IP Office debe deshabilitarse con el número de origen sin usuario 'B_DISABLE_SIP_IPADDR'. La lista blanca/negra de SBC/ALG debe estar activada para compensar.
4. Los reenvíos/transferencias sin interruptor deben deshabilitarse por sistema o por usuario, con la configuración del sistema prevaleciendo sobre el usuario.
   - La configuración por usuario es:**Usuario | Telefonía | Configuración del supervisor | Inhibir Desactivar Reenviar/ Transferir**. Esto también se puede configurar a través de los derechos de usuario.
   - La configuración de todo el sistema es:**Sistema | Telefonía | Telefonía | Inhibir Desactivar Reenviar/Transferir**.
5. Los desvíos/transferencias de troncal a troncal analógica deben deshabilitarse por línea a menos que se requiera, usando**Línea | Opciones analógicas| Conexión analógica de troncal a troncal**.
6. Otros cambios para restringir llamadas están contenidos enPrevención de llamadas no deseadas 84.
7. Las líneas de IP Office (también conocidas como troncales SCN) pueden protegerse mediante el**Línea | Línea | Tipo de transporte**de***Cliente/ Servidor WebSocket***, y un**Línea | Línea | Configuración de seguridad**de***Medio***o***Alto***.
   - Un sistema IP Office debe ser el cliente WebSocket y el otro el servidor. El primario y el secundario siempre deben ser el servidor WebSocket.
   - Para el***Alto***configuración, se requiere configuración de certificado; verCertificados y Fideicomiso 38para más información.
8. Para las implementaciones de Server Edition, siempre se deben usar las líneas seguras de IP Office.

8.13 Medios de voz seguros

En un entorno inseguro sin otra seguridad de VoIP, la seguridad de medios de VoIP de IP Office debe estar habilitada.

- **Nota:**Habilitar la seguridad de los medios de VoIP reducirá considerablemente la capacidad de llamadas simultáneas de la plataforma. También requerirá seguridad de señalización de llamadas SIP.

Para más información, verSeguridad VoIP 68.Esto debe revisarse antes de habilitar cualquier seguridad de medios VoIP de IP Office.

¿Comentarios sobre este documento? infodev@avaya.com

8.14 Prevención de llamadas no deseadas

Las siguientes recomendaciones no pueden ser precisas debido a la gran variedad de planes de marcación nacionales, internacionales y de clientes, sin embargo, se pueden adaptar según sea necesario para implementaciones específicas.

- **Nota:**Se recomienda enfáticamente que todas las implementaciones de IP Office estén protegidas contra llamadas no deseadas, independientemente del riesgo percibido.

El fraude telefónico, los ataques de marcación directa o las llamadas entrantes o salientes no deseadas en general se pueden mitigar en IP Office mediante:

- Bloqueo de llamadas
- Códigos de autorización
- Registro y monitoreo de llamadas
- Bloqueo de teléfono
- Cierre de sesión automático
- Salvo fuera de horario
- Bloqueo de transferencias de apagado automático y de troncal a troncal
- Eliminación del control de llamadas móviles
- Asegurarse de que los números de emergencia estén definidos
- Corregir el manejo de errores en los flujos de llamadas de Voicemail Pro.

8.14.1 Restricción de llamadas

La forma normal de restricción de llamadas es tener una ruta saliente predeterminada y luego bloquear los números no deseados. Al bloquear números no deseados, es importante tener en cuenta las reglas de marcación de IP Office y agregar una N después de cualquier cadena de marcación que intente bloquear.

Por ejemplo para bloquear llamadas a números de tarifa Premium (1900-xxx-xxxxx US o 09... UK):

	A NOSOTROS	Reino Unido
Número de teléfono	1900N	09N o 909N
Rasgo	Prohibido	Prohibido

Es importante asegurarse de que el número de teléfono vaya seguido de una N para que coincida incluso cuando se marque en bloque (o se vuelva a marcar).

Muchos países tienen prefijos que se pueden marcar antes de los números PSTN normales, por ejemplo, para forzar la presentación del identificador de llamadas, (*67 (EE. UU.)/141 (Reino Unido) para retener el identificador de llamadas, *82 (EE. ID) es importante incluir versiones de todos los códigos cortos bloqueados, incluidos estos prefijos, o simplemente bloquear cualquier intento de llamada que use estos prefijos.

8.14.2 Restricción basada en el usuario

Existen varios métodos potenciales para lograr diferentes reglas de enrutamiento/restricción para los usuarios.

Un método efectivo que minimiza la configuración por usuario y puede ser parte de las plantillas de derechos de usuario, centraliza la configuración de enrutamiento/restricción y mantiene características como el tono de marcado secundario, es crear copias del ARS "50:Principal" para los diferentes niveles de acceso requeridos.

Como 50:Main es el predeterminado, tiene sentido que sea el que se use para la mayoría de los usuarios, o en sitios con preocupaciones específicas sobre la seguridad, el más restringido.

Para este ejemplo, definiremos dos entradas ARS alternativas para Local y Larga Distancia, y Sin restricciones, copiando el Principal predeterminado y luego restringiendo el Principal para que sea solo local. Todas las tablas ARS deben enrutar Llamadas de Emergencia.

Los nuevos Códigos Cortos en el ARS Principal serán:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0N;	0N	Barred	0
1N;	1N	Barred	0
XN;	N	Dial 3K1	0
XXXXXXXXXXN	N	Dial 3K1	0
*67N		Barred	0
*82N		Barred	0

el 0N; y 1N; los códigos se cambiaron a barras y se agregaron códigos de barras para *67 y *82. Tenga en cuenta la adición de la N para garantizar una coincidencia para volver a marcar, etc. Se pueden agregar códigos cortos para áreas donde la marcación local de 7 dígitos todavía está disponible si es necesario, también podría ser útil crear códigos cortos para atrapar códigos de área locales que han sido marcado con un 1 inicial, también marcación gratuita.

Los códigos Cortos Locales y de Larga Distancia serán:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0N;	0N	Barred	0
1XXXN;	1N	Dial 3K1	0
XN;	N	Dial 3K1	0
XXXXXXXXXXN	N	Dial 3K1	0
1900N		Barred	0
*67N		Barred	0
*82N		Barred	0

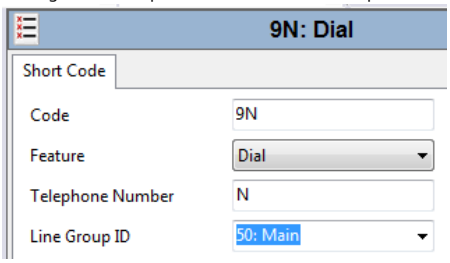
Esto permitirá que todas las llamadas comiencen en '1' excepto Tarifa Premium (números 1-900), el 1N; El código corto se modifica a 1XXXN; para evitar que las personas hagan una pausa durante la marcación haciendo coincidir un simple código corto "1N;". Se repite la restricción para *67 y *82.

Los códigos cortos de ARS sin restricciones serán:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
N;	N	Dial 3K1	0

Esto es totalmente ilimitado, en funcionamiento real es poco probable que haya llamadas externas totalmente ilimitadas.

El código de acceso predeterminado del sistema para marcar no ha cambiado:



Agregue códigos cortos de usuario específicos para los usuarios a los que se les permiten mayores privilegios de marcación, similares al código corto del sistema predeterminado pero que apuntan a la entrada ARS adecuada. Esto se puede hacer a través de Plantillas de derechos de usuario.

Para obtener más información sobre el funcionamiento de ARS, consulte las descripciones de los campos de la ficha Manager ARS en Administración de Avaya IP Office ™ Platform con Manager.

Página1749 de 3226.

8.14.3 Protección de teléfonos

En algunos entornos, uno de los riesgos no proviene de los usuarios normales de los teléfonos, sino de las personas que tienen acceso físico al teléfono pero no desea que los usen. Hay varios mecanismos que se pueden usar para proteger los teléfonos cuando los usuarios normales no están en sus escritorios:

- **Bloqueo de teléfono**
  Los teléfonos se pueden bloquear utilizando la función Bloquear en el menú Funciones del teléfono. Bloquear el teléfono también bloquea el menú Funciones. Los teléfonos de las series 1400, 9500 y 9600 tienen una opción para especificar un temporizador en el que el teléfono se bloqueará automáticamente después de un período específico de inactividad.
- **Códigos cortos**
  El código corto "Prohibición de llamadas salientes activada" evita que el teléfono se utilice para realizar llamadas salientes. Se permiten llamadas internas y de emergencia. "Barra de llamadas salientes desactivada" con el código de inicio de sesión del usuario desbloquea el teléfono
- **Cerrar sesión/Hot Desking**
  Los usuarios pueden cerrar sesión en el teléfono, lo que dejará el teléfono con la cuenta especial 'NoUser' asociada a él. Este NoUser tiene restricción de llamadas salientes. Los usuarios deben tener un código de inicio de sesión para poder cerrar sesión en su teléfono predeterminado (el teléfono con su número de extensión).
- **Cierre de sesión automático**
  los**Extensión | Telefonía | Configuración del supervisor | Período de inactividad de inicio de sesión**se puede usar para obligar a un usuario a cerrar la sesión si su teléfono está inactivo durante un período de tiempo.
- **Enrutamiento de llamadas fuera de horario**
  Se puede asociar un perfil de tiempo a un ARS de modo que cuando el perfil de tiempo esté inactivo, se use un ARS diferente para enrutar llamadas; para nuestro ejemplo anterior, configuraremos las tablas de ARS adicionales para que apunten a Principal fuera de horario para que solo Local y Emergencia Se pueden hacer llamadas.
- **Fuente de correo de voz confiable**
  Cuando un teléfono se encuentra en un área no controlada, también se recomienda eliminar el número de origen confiable predeterminado para el acceso al correo de voz, de modo que todo acceso al correo de voz de IP Office requiera ingresar el código de acceso al correo de voz, incluso desde la extensión de la casa del usuario.

8.14.4 Realización de llamadas desde teléfonos protegidos

Una vez que los teléfonos tienen la marcación saliente bloqueada, a menudo es necesario proporcionar excepciones ocasionales. Desde la versión 5.0, un usuario privilegiado (recepcionista, por ejemplo) puede transferir un tono de marcación secundario a un usuario restringido para permitirle realizar una llamada que, de otro modo, no podría realizar.

Una solución más versátil es usar Códigos de Autorización. Los Códigos de Autorización permiten a un usuario con un Código ir a un teléfono restringido y hacer una llamada con sus privilegios sin necesidad de Hot Desking para la llamada. Esto a veces se denomina "Clase de servicio de roaming" en otros sistemas. Para obtener información, consulte las descripciones de los campos de la pestaña Códigos de autorización del administrador en*Administración de la plataforma Avaya IP Office™ con Manager*.

Tenga en cuenta que las llamadas de emergencia siempre están permitidas, de ahí la necesidad de asegurarse de que la marcación de emergencia se haya definido correctamente.

8.14.5 Protección de reenvío

Cuando un usuario tiene el desvío activo, se aplicará cualquier enrutamiento de llamadas, incluida la restricción de llamadas a ese usuario. Si un usuario no puede realizar una llamada de larga distancia e intenta desviar a un número de larga distancia, la llamada fallará. Como el enrutamiento/restricción de llamadas puede variar según la hora del día, no es posible bloquear el intento de configurar larga distancia como destino de desvío.

Usar la configuración**Sistema | Telefonía | Telefonía | Inhibir Desactivar Reenviar/Transferir**para inhibir todos los reenvíos y transferencias de apagado. Cuando está habilitado, tiene prioridad sobre todas las configuraciones del usuario.

Esta configuración también se puede establecer por usuario usando**Usuario | Telefonía | Configuración del supervisor | Inhibir Desactivar Reenviar/Transferir**.

8.14.6 Controles de reenvío remoto

De manera predeterminada, IP Office y las aplicaciones de correo de voz de IP Office no brindan ningún mecanismo para la modificación remota de la configuración de Reenvío de usuarios. Sin embargo, Mobile Call Control se puede habilitar para dar acceso. Para obtener más información, consulte "Control de llamadas móviles" en Administración de la plataforma Avaya IP Office ™ con Manager.

También hay un Voicemail Pro**Menú de opciones personales**opción que se puede agregar a un flujo de llamadas personalizado para permitir a los usuarios cambiar de forma remota su reenvío y otras configuraciones.

Antes de habilitar cualquiera de estas opciones, se deben considerar las advertencias en los manuales y hacer un juicio para decidir si el beneficio vale la pena el riesgo de acceso no autorizado.

8.14.7 Informe SMDR de llamadas restringidas

Para habilitar la detección de intentos de llamada no autorizados, se puede incluir la cadena 'SMDR' en el campo de teléfono del código corto prohibido. Cuando se incluya, se generará un informe SMDR con el campo relevante que indica la parte que llama, el destino de la llamada, etc. La llamada tendrá duración cero, tiempo de timbre cero, con la palabra 'Prohibido' en el campo de información de la segunda parte.

8.14.8 Manejo de errores en los flujos de llamadas de Voicemail Pro

Todos los flujos de llamadas que pueden realizar llamadas internas o externas, transferencias u otras posibles operaciones de llamadas deben garantizar que solo se permitan los destinos de llamadas esperados de usuarios válidos. Todas las posibles operaciones no válidas deben detectarse y evitarse mediante el uso de la lógica de flujo de llamadas.

8.15 Protección de las interfaces CTI

1. Si no es necesario, deslicenciado en Derecho e TAPI Link Lite/Pro (TAPI de 1.er/3.er fabricante) segúnDeshabilitar servicios/ interfaces no utilizados 77.
2. Para asegurar el enlace entre ACCS o IPOCC e IP Office, la configuración IP Office Manager |**Configuración de seguridad | Sistema | Interfaces no seguras | TAPI**debe estar deshabilitado. Esto habilitará TLS y solicitará un certificado de confianza de IPOCC/ACCS.
3. Administrar IPOCC/ACCS con certificado de identidad. Consulte la documentación pertinente de IPOCC/ACCS.
4. Administre el almacén de certificados confiables (TCS) de IP Office con el certificado de CA raíz de IPOCC/ACCS.

8.16 Protección de las aplicaciones de IP Office

Para ayudar a proteger las aplicaciones de IP Office, use las siguientes recomendaciones:

- Reglas generales 75
- Evaluación de los requisitos de seguridad de IP Office 76
- Administración de Seguridad 76
- Cambiar valores predeterminados de seguridad 76
- Eliminar cuentas innecesarias 76
- Deshabilitar servicios/interfaces no utilizados 77
- Garantizar derechos mínimos de acceso 78
- Hacer cumplir una política de contraseñas 79
- Actualizar certificados 80
- Protección de usuarios y extensiones de telefonía 81
- Endurecimiento para la operación de trabajadores remotos 82
- Protección de troncales/líneas 83
- Medios de voz seguros 83
- Prevención de llamadas no deseadas 84
- Protección de las interfaces CTI 88
- Configuración y otros datos confidenciales 94
- Limitación de la exposición de la red IP 95
- Interfaces de mantenimiento seguras 96
- Restricción del acceso físico 96
- Protección de servidores Server Edition 97
- Protección del servidor de aplicaciones Linux/módulo de comunicaciones unificadas 99

8.16.1 Protección de IP Office Manager

1. Aplique los siguientes ajustes de configuración en el Administrador**Archivo | Preferencias | Seguridad**para garantizar comunicaciones de IP Office más seguras y ayudar a mantener los datos de configuración fuera del alcance de usuarios no autorizados:

Configuración	Parámetro Ajuste
Solicitar inicio de sesión al guardar	Activado
Cerrar configuración/ajustes de seguridad después de enviar	Activado
Guardar archivo de configuración después de la carga	Desactivado
Copia de seguridad de archivos al enviar	Desactivado
Habilitar el temporizador de inactividad de la aplicación (5 minutos)	Activado
Comunicaciones seguras	Activado

2. El**Comprobación del certificado de administrador**sobre el**Archivo | Preferencias | Seguridad**La pestaña debe configurarse de acuerdo con la política de seguridad. Debe estar configurado para***Ninguna*sólo con fines de recuperación.

3. Para más información verCertificados y Fideicomiso 38yGestión de certificados de Windows 118.

4. Si se requiere autenticación de certificado mutuo (es decir, el servicio de configuración o administración de seguridad de IP Office solicitará un certificado de Manager), el**Archivo | Preferencias | Seguridad | CertificadoC comió**ofrecido a IP Office debe configurarse con un certificado de identidad. VerGestión de certificados de Windows 118.Si se selecciona Usuario actual, solo se aplicará al usuario actual de Windows. Si se selecciona Máquina local, se utilizará para todos los usuarios de Windows de esa PC.

5. Para evitar que otros administradores modifiquen el**Archivo | Preferencias | Seguridad**configuración de la pestaña, asegúrese de que esos usuarios del servicio no tengan los derechos para editar la configuración de seguridad o que tengan el rol de operador de administrador administrador.

6. En IP Office Manager**Archivo | Preferencias | Directorios**pestaña, cambie la**Directorio de trabajo (archivos .cfg)**ser diferente a la**Directorio binario (archivos .bin)**. Si la configuración de los dos directorios es la misma, potencialmente permite el acceso remoto de archivos TFTP/HTTP a la carpeta que contiene copias de los archivos de configuración.

7. Asegúrese de que todos los archivos de configuración fuera de línea, los archivos exportados u otros datos de configuración estén controlados.

8.16.2 Protección de IP Office Web Manager/Web Control

Web Manager y el panel de control web de Linux son herramientas de administración en línea basadas en navegador que siempre usan comunicación HTTPS.

1. Cualquier navegador que se utilice para la administración basada en web debe tener el certificado de CA/certificado de ID de IP Office instalado en el almacén de certificados de confianza correspondiente. Es posible en algunos navegadores proporcionar excepciones temporales o permanentes, pero este shoul ser evitado. Para obtener más información acerca de los certificados y la compatibilidad con navegadores, consulteCertificados y Fideicomiso 38.

2. Asegúrese de que todos los archivos de configuración fuera de línea, los archivos exportados u otros datos de configuración estén controlados.

8.16.3 Proteger el Administrador de licencias web

Las cuentas administrativas de Web License Manager (WebLM) son independientes de IP Office y los inicios de sesión en WebLM no están integrados en el marco IP Office AA.

La administración de WebLM se basa en el navegador y siempre utiliza comunicación HTTPS.

1. Cambie la contraseña de la cuenta predeterminada lo antes posible.

2. Todas las contraseñas deben ser 'fuertes' y de 8 o más caracteres (VerGestión de contraseñas y PIN 32).

3. Para la administración posterior de contraseñas, vaya a la página 'Administrar usuarios' de WebLM. Todas las cuentas de administrador no utilizadas deben eliminarse.

   - Nota: WebLM no admite la autenticación referida; las cuentas de usuario locales se utilizan en todo momento.

4. Cualquier navegador que se utilice para la administración basada en web debe tener el certificado de CA/certificado de ID de IP Office instalado en el almacén de certificados de confianza correspondiente. Es posible en algunos navegadores proporcionar excepciones temporales o permanentes, pero este shoul ser evitado. Para obtener más información acerca de los certificados y la compatibilidad con navegadores, consulteCertificados y Fideicomiso 38.

5. Si la aplicación no se usa, debe deshabilitarse usando Web Control**Configuración | Sistema | Servicios | Inicio automático** ajuste.

8.16.4 Protección de la aplicación de estado del sistema

SSA siempre intentará conectarse a IP Office mediante el servicio TLS seguro primero si la configuración de la página de inicio de sesión **Conexión segura**es seleccionado. Sin embargo, si falla el intento de conexión TLS, ofrecerá al usuario la opción de conectarse a través de la conexión no segura.

1. Para evitar el uso de una conexión no segura, la configuración de seguridad del Administrador**Servicios | Interfaz de la aplicación de estado del sistema | Nivel de seguridad del servicio**debe establecerse en***Seguro, Bajo***o***Seguro, Medio*.
   - **Nota:**El uso de SSA con la conexión TLS limitará la capacidad de monitoreo de estado, particularmente en la plataforma IP500 V2. Si se anticipan eventos de SSA o tasas de llamadas altas, la conexión no segura debe usarse con arreglos de seguridad alternativos.
2. SSA no verifica el certificado de IP Office cuando se usa la conexión TLS, por lo tanto, no es posible configurar el certificado en SSA.
3. Si no lo requiere el personal de apoyo que utiliza SSA, los derechos:**Grupos de Derechos | Aplicación de estado del sistema | Leer toda la configuración**y**Grupos de Derechos | Aplicación de estado del sistema | Control de sistema** debe eliminarse de la cuenta de usuario del servicio.
4. Cualquier otra instancia de SSA puede leer cualquier archivo de instantánea guardado por SSA sin autorización. Este archivo puede incluir configuración y otra información confidencial y, por lo tanto, se debe controlar el acceso al archivo.

8.16.5 Protección del monitor del sistema

System Monitor tiene varios métodos de conexión: dos heredados (UDP y TCP) y dos contemporáneos (HTTP y HTTPS). Solo el método HTTPS es completamente seguro, pero tiene la sobrecarga de procesamiento más alta. UDP tiene lo mínimo.

La compatibilidad de IP Office con los diversos métodos de conexión de System Monitor se controla mediante la configuración de seguridad de la siguiente manera:

Seguridad del servicio HTTP Nivel	HTTP	HTTPS	UDP	TCP
Desactivado	Desactivado	Desactivado	n / A	n / A
Solo no seguro	Activado	Desactivado	n / A	n / A
Inseguro + Seguro	Activado	Activado	n / A	n / A
seguro bajo	Desactivado	Activado	n / A	n / A
Medio seguro	Desactivado	Activado	n / A	n / A
Seguro alto	Desactivado	Activado	n / A	n / A

Interfaces no seguras | DevLink	HTTP	HTTPS	UDP	TCP
Desactivado	Desactivado	Activado	Desactivado	Desactivado
Activado	Activado	Activado	Activado	Activado

1. Se debe usar una cuenta de usuario de servicio en lugar de la contraseña de monitor heredada, la seguridad del administrador usando la configuración**Sistema | Interfaces no seguras | Usar credenciales de usuario del servicio**. por defectoes Las cuentas que pueden usar System Monitor de esta manera se refieren aUsuarios administrativos predeterminados y grupos de derechos 24.
2. Los métodos de conexión heredados UDP y TCP deben deshabilitarse a través de la configuración de seguridad del Administrador **Sistema | Interfaces no seguras | DevLink**.
   - **Nota:**Si los métodos de conexión heredados no están deshabilitados, el intercambio de contraseñas entre System Monitor e IP Office no es seguro.
3. Seleccione los métodos de conexión correctos en el Monitor del sistema**Archivo | Seleccionar Unidad**pestaña. Si se utiliza HTTPS, se solicita un certificado de identidad (certificado más clave privada). Esto es utilizado por Systmi m Monitor para identificarse. Para obtener más información sobre certificados y PKI, consulteCertificados y Fideicomiso 38.
4. Para garantizar que solo se utilice HTTPS, la configuración de seguridad del administrador**Servicios | HTTP | Nivel de seguridad del servicio** debe configurarse para deshabilitar HTTP.
   - **Nota:**Muchos componentes utilizan el servicio HTTP de IP Office, incluidos los teléfonos H323, las líneas de IP Office, SoftConsole, Voicemail Pro y one-X Portal for IP Office.
5. Cualquier otra instancia de System Monitor puede leer cualquier archivo de registro guardado por System Monitor sin autorización. Este archivo puede incluir configuración y otra información confidencial y, por lo tanto, se debe controlar el acceso a estos archivos.

Traducido del inglés al español - www.onlinedoctranslator.com

8.16.6 Protección de Voicemail Pro

1. Con el cliente Voicemail Pro, la contraseña de la cuenta de administración predeterminada 'Administrador' debe cambiarse a una contraseña 'segura' de 8 o más caracteres. Cualquier cuenta no utilizada debe ser eliminada.

   - **Nota:**
     Para Voicemail Pro R9.0 y versiones posteriores en Server Edition, Unified Communications Module y Linux Application Server, toda la autenticación se refiere a la IP Office 'local'; la cuenta de administración predeterminada solo se usa en condiciones de falla. Para Unified Communications Module y Linux Application Server, el localyo P Office es una instancia de gestión que se ejecuta en el propio servidor. VerCuentas de usuario y derechos de acceso 22para más información.

2. Mediante el cliente Voicemail Pro, configure la contraseña utilizada para acceder a IP Office en**Administración | Preferencias | generales | Contraseña del correo de voz**. Esta contraseña debe coincidir con la contraseña ingresada en la configuración del Administrador**Seguridad | Sistema | Interfaces no seguras | Contraseña del correo de voz**. La contraseña debe tener 31 caracteres.

   - Para los sistemas nuevos, se genera automáticamente una contraseña adecuada de 31 caracteres y se usa en la primera conexión entre los servicios de IP Office y Voicemail Pro.
   - Los sistemas existentes actualizados a IP Office R11.1 FP1 pueden continuar usando su contraseña actual más corta, pero se ven obligados a usar una contraseña de 31 caracteres en cualquier cambio.

3. La opción de configuración de IP Office**Sistema | Correo de voz | Dirección IP del correo de voz**no se debe dejar en 255.255.255.255, pero configurado en la dirección IP del servidor de Voicemail Pro.

4. Solo los usuarios y grupos que tienen derecho a usar el correo de voz deben tener su casilla de correo activada. Todos los demás deben deshabilitarse mediante la función de deshabilitar buzón de correo del cliente de Voicemail Pro.

   - **Nota:**
     Deshabilitar el buzón también deshabilitará las integraciones de IMAP, MAPI, correo electrónico y correo de voz web para ese usuario.

5. Todos los buzones deben estar protegidos por contraseña/Código de acceso al correo de voz, excepto cuando se conectan desde extensiones confiables (mediante el uso del**Usuario | Números de origen**campo). El mínimo recomendado es de 4 dígitos para uso interno, 9 cuando se puede acceder al buzón desde el exterior.

6. La política de contraseña del buzón/código de correo de voz se debe aplicar configurando la interfaz de telefonía predeterminada del correo de voz en Intuity en el cliente de Voicemail Pro y la longitud mínima del PIN en 4 o 9 mediante la configuración del administrador. **Sistema | Correo de voz | Complejidad del código de correo de voz**.

   - **Nota:**Si se utiliza la TUI de correo de voz de IP Office, los usuarios no están obligados a establecer una nueva contraseña/código de correo de voz en el acceso inicial al buzón.

7. Para evitar el fraude de llamadas a través de la función de marcación externa, se puede desactivar en la configuración de IP Office**Sistema | Mensaje de voz**pestañaen Gerente de IP Office. Cuando se requieren llamadas externas, los pasos de restricción de llamadas dePrevención de llamadas no deseadas 84debe ser usado.

8. Para evitar el fraude de llamadas a través de flujos de llamadas, todos los flujos de llamadas deben tener una protección adecuada contra la marcación un / A números autorizados. Cuando se requiere una llamada externa, los pasos de restricción de llamadas dePrevención de llamadas no deseadas 84debe ser usado.

9. Cuando un teléfono se encuentre en un área no controlada, se debe eliminar el número de fuente confiable predeterminado para el acceso al correo de voz, de modo que todo acceso al correo de voz de IP Office requiera ingresar el código de acceso al correo de voz, incluso desde la extensión de la casa del usuario.

10. Deshabilite todos los servicios no utilizados, como SMTP y MAPI.

11. Si se usa la función de envío SMTP, se debe usar la autenticación. TLS siempre se aplica.

12. Si se usa la función de servidor IMAP4, se debe usar TLS.

13. Si el sistema operativo del servidor host es Microsoft Windows, consulte las pautas de seguridad del sistema operativo de Microsoft correspondientes, que se pueden encontrar enhttps://technet.microsoft.com/en-us/library/windows-serversecurity.aspx . Se puede encontrar más información general enhttps://technet.microsoft.com/enus/security/default.aspx

14. Si la aplicación no se usa, debe deshabilitarse usando Web Control**Configuración | Sistema | Servicios | Inicio automático**ajuste.

8.16.7 Proteger el correo de voz incorporado

1. Solo los usuarios y grupos que tienen derecho a usar el correo de voz deben tener su buzón activado.
2. Todos los buzones deben estar protegidos por contraseña/Código de acceso al correo de voz, excepto cuando se conectan desde extensiones confiables (mediante el uso del**Usuario | Números de origen**campo). El mínimo recomendado es de 4 dígitos para uso interno, 9 cuando se puede acceder al buzón desde el exterior.
3. La política de contraseña de buzón/código de correo de voz debe aplicarse configurando el**Sistema | Correo de voz | Modo de correo de voz**a ***Modo intuitivo***, y la longitud mínima del PIN a 4 o 9 usando la configuración del Administrador**Sistema | Correo de voz | Complejidad del código de correo de voz**.
   - **Nota:**
     Si se utiliza la TUI de correo de voz de IP Office, los usuarios no están obligados a establecer una nueva contraseña/código de correo de voz en el acceso inicial al buzón.
4. Cuando un teléfono se encuentre en un área no controlada, se debe eliminar el número de origen confiable predeterminado para el acceso al correo de voz, de modo que todo acceso al correo de voz de IP Office requiera ingresar el código de acceso al correo de voz, incluso desde la extensión de la casa del usuario.

8.16.8 Protección de la grabadora de contactos

- Contact Recorder otorga plenos derechos de administrador para el primer acceso a la página de administración web, por lo que es importante configurar el nombre y la contraseña lo antes posible. Consulte la sección Configuración general > Grabadora en "*Administración de Avaya IP Office ™ Platform Contact Recorder*".
- Todas las contraseñas deben ser 'fuertes' y de 8 o más caracteres (verGestión de contraseñas y PIN 32).Cualquier cuenta no utilizada debe ser eliminada.
- La interfaz administrativa no segura (HTTP) debe deshabilitarse mediante la interfaz de administración web y configurarse **Sistema | Administrar usuarios | Permitir sin cifrar (http)**el acceso a los***No***. Consulte la sección “Configuración general > Grabadora” en *"Administración de Avaya IP Office ™ Platform Contact Recorder"*.
- Se debe revisar la sección Seguridad avanzada de la documentación de Contact Store; sin embargo, no se recomienda cambiar los puertos de Contact Recorder.
  - **Nota:**
    Contact Recorder no admite la autenticación referida; las cuentas de usuario locales se utilizan en todo momento.
- Si la aplicación no se usa, debe deshabilitarse usando Web Control**Configuración | Sistema | Servicios | Inicio automático**ajuste.

8.16.9 Proteger one-X Portal para IP Office

1. Inicie sesión en la cuenta de administrador predeterminada de one-X Portal for IP Office y cambie la contraseña a una contraseña segura de 8 o más caracteres.

   - **Nota:**
     one-X Portal utiliza esta cuenta paraIP Office si el servicio de autenticación de IP Office no está disponible, consulte Cuentas de usuario y derechos de acceso 22para más información.

2. Para la administración posterior de contraseñas, vaya a one-X Portal for IP Office**Configuración | Usuarios**página. Todas las cuentas de administrador no utilizadas deben eliminarse.

3. En la página de administración de one-X Portal for IP Office, vaya a**Configuración | Proveedores | Proveedor CSTA | Editar**y configure la contraseña utilizada para acceder a IP Office. La contraseña debe coincidir con la contraseña configurada para el ID de usuario de IP Office Manager EnhTcpaService.

4. Si uno-X Po tal para los clientes de IP Office se van a utilizar externamente, sigaEndurecimiento para la operación de trabajadores remotos 82.

5. Si es externovo Los clientes one-X Portal for IP Office están configurados para admitir llamadas VoIP, sigaLimitación de la exposición de la red IP 95.

6. one-X Portal for IP Office ofrece una interfaz HTTP (8080 + 8069) y HTTPS (8443/9443 + 8063) para clientes web. Se debe utilizar HTTPS para el acceso externo. Los puertos HTTP se pueden deshabilitar usando la configuración **Seguridad | Protocolo | Conexión segura (HTTPS)**.

7. Administrarejem un certificado de identidad para las interfaces HTTPS en un servidor basado en Linux, consulteActualizar certificados 80.

8. Para administrar un certificado de identidad para las interfaces HTTPS de servidores basados en Windows, use la página web de administración de one-X Portal for IP Office e importe el archivo de certificado con formato PKCS#12 usando la configuración **Configuración | Certificado | Importar**. Tenga en cuenta que este certificado es específico para las interfaces HTTPS de one-X Portal for IP Office y no forma parte del almacén de certificados del sistema operativo Windows y debe incluir todos los certificados intermedios.

9. Inicie sesión en la cuenta de copia de seguridad y restauración de superusuario predeterminada y cambie la contraseña a una contraseña segura de 8 o más caracteres. Para la administración posterior de contraseñas, vaya a la página AFA de one-X Portal for IP Office **Configuración | Editar**página.

10. Si el sistema operativo del servidor host es Microsoft Windows, consulte las pautas de seguridad del sistema operativo de Microsoft correspondientes, que se pueden encontrar enhttps://technet.microsoft.com/en-us/library/windows-serversecurity.aspx . Se puede encontrar más información general enhttps://technet.microsoft.com/enus/security/default.aspx

11. La consola Openfire no debe activarse en condiciones normales de uso, si en circunstancias excepcionales, y solo bajo la dirección de Avaya, está activada, la consola debe desactivarse tan pronto como sea posible. El comando para deshabilitar está en:
    http://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/oneXportaladmin/diabling_openfire_admin_consol.htm

12. Si no se usa la aplicación, se debe deshabilitar usando el**Configuración de control web | Sistema | Servicios | Inicio automático**ajuste.

¿Comentarios sobre este documento? infodev@avaya.com

8.16.10 Protección de la puerta de enlace WebRTC

1. Si la aplicación no se usa, debe deshabilitarse usando la configuración de Control web**Sistema | Servicios | Inicio automático**ajuste.

8.16.11 Protección del Administrador de medios

1. Si no se usa la aplicación, debe deshabilitarse usando la configuración de Control web**Sistema | Servicios | Inicio automático**ajuste.
2. Si se utilizan correos electrónicos SMTP para alarmas y eventos, seleccione la opción Conexión segura mediante la configuración de IP Office Web Manager.**Aplicaciones | Gerente de Medios | Configuración**.

8.16.12 Asegurar el Reporte de llamadas integrado

1. Si no se usa la aplicación, debe deshabilitarse usando la configuración de Control web**Sistema | Servicios | Inicio automático**ajuste.

8.16.13 Protección de las aplicaciones del centro de contacto de Avaya

1. Cada vez que IP Office Contact Center (IPOCC) y Avaya Contact Center Select (ACCS) se implementan con IP Office, elC El enlace de TI entre IP Office y la aplicación debe protegerse de acuerdo conProtección de las interfaces CTI 84.

2. Consulte la documentación de la aplicación correspondiente para conocer todos los demás aspectos de seguridad:

   - Avaya IP Office Contact Center Característica Descripción
   - Descripción de la solución Avaya Contact Center Select

8.17 Configuración y otros datos confidenciales

Las configuraciones de seguridad de IP Office se cifran y bloquean automáticamente para el IP Office individual y no se pueden exportar, pero la configuración y otros datos de IP Office, Voicemail Pro y one-X Portal for IP Office contienen información no cifrada que puede representar una amenaza para la seguridad o la privacidad. tema.

- Cualquier almacén de datos de copia de seguridad (por ejemplo, un servidor de archivos utilizado para la copia de seguridad/restauración, copias de tarjetas SD) debe estar protegido contra el acceso no autorizado.
- Cualquier mecanismo de respaldo/restauración debe ser seguro; IP Office, Voicemail Pro y one-X Portal for IP Office admiten opciones seguras de respaldo/restauración como HTTPS y SFTP
- Se debe controlar el acceso a las grabaciones de llamadas que se guardan como archivos en el servidor de Voicemail Pro o Contact Recorder.
- Los archivos de configuración fuera de línea y exportados, los registros de System Monitor y los registros del servidor Linux deben controlarse mediante, por ejemplo, cifrado con protección de contraseña. Esto debe incluir cualquier configuración u otros datos confidenciales enviados fuera de la organización.

8.18 Limitación de la exposición de la red IP

Es fundamental controlar el acceso a la red IP de IP Office para reducir la exposición a ataques. La integración de la seguridad de la red está fuera del alcance de este documento; sin embargo, la siguiente sección cubre algunos elementos que deben revisarse como parte del fortalecimiento de la seguridad de la red.

Si usa cualquier nivel de acceso IP externo, IP Office debe**solamente**estar conectado a través de un Firewall correctamente configurado u otro mecanismo de seguridad de la red (por ejemplo, VPN, MPLS). Debería**nunca**estar conectado directamente.

Si no se requiere acceso IP externo, IP Office debe aislarse mediante un firewall u otro mecanismo.

Con Manager, la tabla de rutas IP de IP Office debe inspeccionarse en busca de rutas de puerta de enlace que puedan haberse adquirido sin querer a través de DHCP. Estos deben eliminarse si no son necesarios y la configuración de DCHP debe modificarse para evitar que vuelva a ocurrir.

8.18.1 Cortafuegos

Cualquier Firewall utilizado debe ser seleccionado, implementado, probado y administrado por personal competente para satisfacer las necesidades de la implementación de IP Office.

La publicación especial (SP) 800-41 del NIST, Directrices sobre cortafuegos y política de cortafuegos: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf proporciona información básica, incluidos otros recursos útiles.

Solo se debe abrir el mínimo absoluto de puertos y protocolos de Firewall para su uso con IP Office. Por ejemplo, establezca solo la dirección del puerto y el protocolo necesarios.

Se debe usar la matriz de puertos de IP Office correspondiente para cada versión. Un enlace al documento de matriz de puertos se encuentra en la página Seguridad de productos de Avaya enhttps://support.avaya.com/security .

Directrices de cortafuegos:

- Si una dirección IP remota es estática, por ejemplo, un enlace troncal SIP ITSP, la dirección de origen debe configurarse para restringir aún más el acceso.
- Los puertos/protocolos no seguros de IP Office nunca deben exponerse a Internet.
- Si utiliza un Firewall con estado, H.323 y la inspección SIP deben desactivarse, ya que esto interferirá con el funcionamiento de IP Office.

8.18.2 Controlador de borde de sesión

Se recomienda que Avaya SBCE se ubique detrás del firewall de la empresa y sirva como un dispositivo de seguridad y demarcación entre el IP-PBX y la instalación del operador. Avaya también admite una implementación de Avaya SBCE paralela al firewall, aunque es mejor, como se recomienda para las mejores prácticas de seguridad, colocarlo detrás del firewall como parte de una estrategia de defensa en capas. El SBCE de Avaya realiza NAT transversal, ancla de forma segura la señalización y los medios, y puede normalizar las diferencias de implementación del protocolo SIP entre las implementaciones SIP del operador y de la empresa.

- **Nota:**
  Si se implementa una puerta de enlace de nivel de aplicación (ALG) SBC o SIP, algunas de las medidas de seguridad de IP Office deben trasladarse de IP Office a SBC/ALG; la lista negra de direcciones IP de origen de IP Office debe deshabilitarse con el número de origen sin usuario 'B_DISABLE_SIP_IPADDR'. La lista blanca/negra de SBC/ALG debe estar activada para compensar.

8.18.3 Acceso de mantenimiento remoto

El acceso de System Status Application y System Monitor a IP Office se puede asegurar y los eventos/alarmas se pueden enviar a los servidores syslog (incluido el servidor primario de IP Office) mediante el protocolo TLS.

IP Office SNMP no debe utilizarse sin medidas de seguridad adicionales, como una red privada virtual (VPN).

Todos los sistemas de IP Office admiten conectividad SSLVPN segura y de alta integridad, y Avaya ofrece servicios de soporte de IP Office (IPOSS) basados en esta tecnología. Para obtener más información, consulte Implementación de los servicios VPN SSL de IP Office ™ Platform.

Para la implementación de IP Office en un entorno empresarial o de sucursal, se puede utilizar la puerta de enlace Secure Access Link (SAL) de Avaya.

8.19 Interfaces de mantenimiento seguras

Los eventos y las alarmas se pueden enviar de forma segura a los servidores syslog (incluido el servidor primario de IP Office) mediante el protocolo TLS. Esto se puede habilitar usando la configuración del Administrador**Sistema | Eventos del sistema | Alarmas | registro del sistema | Protocolo**.

Ambos estados del sistemas Monitor de aplicaciones y sistemasa Se puede asegurar el acceso a IP Office. VerProtección de la aplicación de estado del sistema 90yMonitoreo del sistema de seguridad 90.

No se debe usar SNMP ya que no es seguro.

- **Nota:**
  Habilitar la seguridad en estas interfaces aumentará el procesamiento del software de IP Office y no será adecuado para los casos en los que se espera un alto tráfico. En este caso monitoreo localgramo a través de interfaces no seguras o se requiere una solución segura externa. VerLimitación de la exposición de la red IP 95.

Los módems no seguros no deben dejarse conectados a los puertos serie o analógicos.

8.20 Restricción del acceso físico

Cualquier acceso físico no autorizado al sistema podría presentar a los atacantes la oportunidad de restablecer la configuración y los ajustes de seguridad, modificar el BIOS, acceder al puerto serie no seguro, instalar o modificar el software a través de la tarjeta SD u otros mecanismos.

Es esencial asegurar el acceso físico a la plataforma IP Office; mecanismos de control de dicho acceso fuera del alcance de este documento.

8.21 Protección de servidores Server Edition

1. Es importante entender la información y recomendaciones deCertificados y Fideicomiso 38para determinar los requisitos de certificado y confianza del servidor a medida que se ofrecen opciones durante el proceso de encendido inicial.
2. El proceso de encendido impondrá un cambio en el administrador y las contraseñas de seguridad. También actualiza las cuentas de respaldo para one-X Portal para IP Office, Voicemail Pro y Web Control (la interfaz web de administración local de Linux).
3. Todas las contraseñas de las cuentas de administrador de seguridad de todos los demás sistemas de la solución Server Edition deben ser las mismas. Esto se puede hacer usando IP Office Manager**Seguridad | generales | General**para cambiar la configuración individual.
4. Todas las credenciales de la cuenta de usuario del servicio utilizadas para la administración central de todos los sistemas deben ser las mismas. Esto se puede hacer usando IP Office Web Manager Security Manager**Usuarios del servicio | Sincronizar usuario de servicio y contraseña del sistema**.
5. Aplique una política de contraseñas a la aplicación Web Control usando IP Office Web Manager Platform**Configuración | Sistema | Configuración de reglas de contraseña**.
6. Habilite la configuración IP Office Web Manager Platform**Configuración | Sistema | Autenticación | Habilitar autenticación referida**. Esto remitirá todos los inicios de sesión de Web Control a la IP Office local. Las credenciales de la cuenta de administrador de Linux local solo se utilizan en condiciones de error.
7. Deshabilite el servidor de respaldo/restauración HTTP usando la configuración de IP Office Web Manager**Vista de la plataforma | Configuración | Sistema | Servidor HTTP**. A partir de R9.1, un servidor de copia de seguridad/restauración HTTPS siempre está activo para este propósito.
8. Habilite el firewall del servidor interno para aplicar filtros de ataque DoS y DDos usando la configuración de IP Office Web Manager **Vista de la plataforma | Configuración | Sistema | Configuración del cortafuegos | Activar**.
   - Nota: El soporte de firewall en Server Edition nore colocar la necesidad de un firewall externo. Para más información verLimitación de la exposición de la red IP 95.
9. Deshabilite todos los puertos TCP o UDP no seguros que no se utilicen mediante la configuración de IP Office Web Manager**Vista de la plataforma | Configuración | Sistema | Configuración del cortafuegos | Habilitar puertos TCP/UDP**. Esto aplicará el filtrado a todo el tráfico LAN 1 y LAN 2, independientemente del origen o el destino.
10. Si los puertos de entrada utilizados por todas las operaciones de IP Office se ajustan a la siguiente tabla, la configuración**Vista de la plataforma | Configuración | Sistema | Configuración del cortafuegos | Habilitar filtro**se puede activar:

Protocolo	Puertos
TCP	22, 25, 37, 143, 389, 411, 443, 445, 514, 993, 1433, 1434, 1718:1720, 4097, 4560, 5060:5061, 5222, 5269, 5443, 5800:5899, 70514: 7071, 7443, 8005, 8063, 8084, 8087, 8135, 8411, 8444, 8666, 8443, 8805, 9092, 9094, 9095, 9443, 9444, 9888, 32768:65280
UDP	37, 53, 67, 68, 123, 161, 162, 389, 500, 514, 520, 1024:65535

    Para obtener más información sobre el uso de puertos/protocolos de IP Office, consulte la matriz de puertos de IP Office correspondiente que se puede encontrar enhttps://support.avaya.com/security .
11. Si no es necesario, deshabilite el receptor syslog en el**Configuración principal | General**pestaña.
12. Si no es necesario, elimine el cliente syslog en el sistema secundario y en cada sistema de expansión mediante la configuración del administrador.**Sistema | Eventos del sistema | Alarmas | Registro del sistema de destino**.
    - **Nota:**
      Eliminar el destino de syslog detendrá el seguimiento de auditoría y los eventos de seguridad que se envían al servidor primario.
13. Si no es necesario, deshabilite la compatibilidad con Enhanced Access Security Gateway (EASG) mediante la configuración de IP Office Web Manager**Vista de la plataforma | Configuración | Configuración de EASG | Estado**.
14. Si es necesario, administre un nuevo certificado de identidad del servidor mediante IP Office Web Manager:

    una. El nuevo certificado de identidad debe estar en un archivo 'p12' o 'pfx'.

    b. Establecer**Plataforma | Configuración | generales | Certificados | Renovar automáticamente**activo.

    C. Idealmente, todos los certificados utilizados para firmar el nuevo certificado de identidad deberían estar en el mismo archivo.

    d. Si los certificados de firma están en archivos separados, use Security Manager | Certificados | +Añadir Certificado para subir cada uno.

    mi. Establecer**Gerente de Seguridad | Certificados | Editar | Cadena de certificados de ID de oferta**activo.

    F. Usar**Gerente de Seguridad | Certificados | Editar | Establecer**para cargar el archivo del certificado de identidad.

    gramo. El certificado de identidad se propagará automáticamente a todas las interfaces TLS/HTTPS del servidor, todos los certificados de firma se colocarán en el almacén de certificados de confianza (TCS).

    - Para más información, verCertificados y confianza en la página 33 38.

¿Comentarios sobre este documento? infodev@avaya.com

15. SeguirProtección de la solución de la plataforma IP Office 74.

una. Si Voicemail Pro está instalado, sigaProtección de Voicemail Pro 91

b. Si one-X Portal for IP Office está instalado, sigaProtección de one-X Portal para IP Office 93

C. Todas las aplicaciones que no se utilicen deben deshabilitarse mediante el control web.**Configuración | Sistema | Servicios | Inicio automático**ajuste. Tenga en cuenta que IP Office y Management Services nunca deben deshabilitarse.

16. No active la interfaz de administración de plataforma inteligente (IPMI) del servidor; esto otorga acceso físico al servidor.

8.22 Protección del servidor de aplicaciones Linux/módulo de comunicaciones unificadas

El servidor de aplicaciones Linux y el módulo de comunicaciones unificadas (Módulo de comunicaciones unificadas) ejecutan una instancia de IP Office de 'Administración'. Un IP Office de administración es una instalación única de funciones seleccionadas de IP Office que se ejecutan en Linux con los servicios de administración y mantenimiento habilitados. Todas las funciones de telefonía están deshabilitadas y no se requiere licencia.

1. Es importante entender la información y recomendaciones deCertificados y Fideicomiso 38para determinar los requisitos de certificado y confianza del servidor a medida que se ofrecen opciones durante el proceso de encendido inicial.
2. El proceso de encendido impondrá un cambio en el administrador y las contraseñas de seguridad. También actualiza las cuentas de respaldo para one-X Portal para IP Office, Voicemail Pro y Web Control (la interfaz web de administración local de Linux).
3. Aplique una política de contraseñas a la aplicación Web Control usando**Configuración | Sistema | Configuración de reglas de contraseña**.
4. Habilite la configuración**Configuración | Sistema | Autenticación | Habilitar autenticación referida**. Esto remitirá todos los inicios de sesión de Web Control a IP Office de administración. Las credenciales de la cuenta de administrador de Linux local solo se utilizan en condiciones de error.
5. Use IP Office Manager para cargar la configuración de seguridad del IP Office Shell Server que reside en el servidor de aplicaciones Linux/Módulo de comunicaciones unificadas en la misma dirección IP.
   - **Nota:**Esta no es la dirección IP500 V2 del host de Unified Communications Module.
6. SeguirProtección de la solución de la plataforma IP Office 74.
7. Deshabilite el servidor de respaldo/restauración HTTP usando**Configuración | Sistema | Servidor HTTP**. A partir de R9.1, un servidor de copia de seguridad/restauración HTTPS siempre está activo para este propósito.
8. Deshabilite todos los puertos/protocolos no seguros no utilizados mediante**Configuración | Sistema | Configuración del cortafuegos**. Esto aplicará el filtrado a todo el tráfico LAN 1 y LAN 2, independientemente del origen o el destino.
   - **Nota:**
     El soporte de firewall en el servidor de aplicaciones Linux do no reemplaza las necesidades de un firewall externo. Para más información verLimitación de la exposición de la red IP 95.
9. Si no es necesario, desactive la compatibilidad con Enhanced Access Security Gateway (EASG) mediante la configuración de IP Office Web Manager.**Vista de la plataforma | Configuración | Configuración de EASG | Estado**.
10. Si es necesario, administre un nuevo certificado de identidad del servidor en IP Office Shell Server utilizando IP Office Manager **Sistema | Certificados | Certificado de Identidad | Establecer**; este certificado de identidad se propagará automáticamente a todas las interfaces TLS/HTTPS del servidor. Alternativamente, si el sistema es un servidor de aplicaciones Linux, Web Control **Configuración | generales |C certificados | Certificados de Identidad**se pueden utilizar los ajustes. Para más información, ver Certificados y Fideicomiso 38.
11. Si es necesario, administre un nuevo certificado de identidad del servidor en IP Office Shell Server utilizando IP Office Manager **Sistema | Certificados | Certificado de Identidad | Establecer**; este certificado de identidad será automáticotic ally se propaga a todas las interfaces TLS/HTTPS del servidor. Para más información, verCertificados y Fideicomiso 38.
12. Si Voicemail Pro está instalado, sigaProtección de Voicemail Pro 91.
13. Si está instalado Contact Recorder, sigaRegistrador de contactos de seguridad 92.
14. Si está instalado one-X Portal for IP Office, sigaProteger el portal one-X 93.
15. Todas las aplicaciones que no se utilicen deben deshabilitarse mediante la configuración de Control web**Sistema | Servicios | Inicio automático**ajuste. Tenga en cuenta que IP Office y Management Services nunca deben deshabilitarse.
16. No active la interfaz de administración de plataforma inteligente (IPMI) del servidor; esto otorga acceso físico al servidor.

Capítulo 9.

Supervisión de la plataforma IP Office

9. Supervisión de la plataforma IP Office

El monitoreo constante y consistente garantiza que cualquier amenaza pueda identificarse temprano y reaccionar ante ella. Además del monitoreo de amenazas, las instalaciones existentes deben revisarse en busca de cambios en los requisitos de seguridad que puedan ser causados por las necesidades, la tecnología o la regulación del cliente.

- Active todos los informes necesarios. VerActivación de informes 106.
- Supervise todas las alarmas y registros, especialmente para inicios de sesión fallidos repetidos u otra evidencia de ataque
- Detectar otra actividad inusual, por ejemplo:
- Nuevas extensiones VoIP
  - Conjunto de reenvío
  - Teléfonos marcando inesperadamente
  - No se pueden hacer llamadas salientes
  - Destinos de llamadas inusuales
  - Volúmenes de llamadas inusuales o hora del día/semana
  - Factura de teléfono alta
  - No se puede iniciar sesión en teléfonos o aplicaciones
  - No se puede usar el correo de voz
  - La cadena 'Prohibido' en los informes SMDR
  - La etiqueta de syslog de 'IPTables-Rejected' en los eventos de syslog del servidor Linux.
- Revise los avisos de seguridad de Avaya
- Revise las notas de aplicación, los boletines técnicos y los consejos de Avaya IP Office
- Asegúrese de que se apliquen los últimos paquetes de servicio de IP Office
- Supervisar las comunicaciones del proveedor de telefonía
- Llevar a cabo una reevaluación periódica de la seguridad

9.1 Comprobaciones y pruebas

Se deben realizar verificaciones y pruebas exhaustivas para garantizar que la implementación sea segura y que ningún ataque anterior haya comprometido el sistema:

- **Nota:**
  Se debe tener cuidado de no exponer inadvertidamente datos confidenciales como un subproducto de las actividades de prueba.
- Verifique que LAN1/LAN2 no tengan direcciones IP públicas, es decir, directamente accesibles desde Internet.
- Verifique IP Office en busca de Internet no seguro o acceso IP entrante al identificar la dirección IP pública del Firewall (por ejemplo, al usarhttp://whatismyipaddress.com) e intentar acceder a los puertos de IP Office definidos por el documento Port Matrix. La siguiente tabla contiene algunos puertos de ejemplo que deben probarse.

Nota: Esta lista de puertos no es exhaustiva y puede variar de una versión a otra. Un enlace al documento de matriz de puertos se encuentra enhttps://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/general/port_matrix/index.htm .

Puerto	Protocolo	Usar	Posible herramienta de prueba	notas
22	TCP	SSH	SSH, Nmap u otro escáner de puertos	Solo servidores Linux
69	UDP	TFTP	Nmap u otro escáner de puertos	Se puede usar un RRQ TFTP de 'nasystem/who_is'
80	TCP	HTTP	Navegador, Nmap u otro escáner de puertos	Se puede utilizar http://[Dirección IP]
143	TCP	IMAP	Nmap u otro escáner de puertos	Correo de voz Pro solamente
161	UDP	SNMP	Herramienta de prueba SNMP, Nmap u otro escáner de puertos	
411	TCP	HTTP	Nmap u otro escáner de puertos	
443	TCP	HTTPS	Navegador, Nmap u otro escáner de puertos	Se puede usar https://[Dirección IP]
993	TCP	IMAP-TLS	Nmap u otro escáner de puertos	Correo de voz Pro solamente
1300	TCP	H323-TLS	Nmap u otro escáner de puertos	
1720	TCP	H323	Nmap u otro escáner de puertos	
5060	UDP	SORBO	Nmap u otro escáner de puertos	
5061	TCP	SORBO	Nmap u otro escáner de puertos	
5443	TCP	HTTPS	Nmap u otro escáner de puertos	Solo servidores Linux
7070	TCP	HTTPS	Navegador, Nmap u otro escáner de puertos	Solo servidores Linux Se puede usar https://[Dirección IP]:7070
7071	TCP	HTTPS	Navegador, Nmap u otro escáner de puertos	Solo servidores Linux Se puede usar https://[Dirección IP]:7071
8000	TCP	HTTP	Nmap u otro escáner de puertos	Solo servidores Linux
8069	TCP	HTTP	Nmap u otro escáner de puertos	Portal one-X para IP Office solamente
8080	TCP	HTTP	Navegador, Nmap u otro escáner de puertos	https://[IP Dirección]:8080/onexportaladmin.html se puede utilizar
8086	TCP	HTTP	Nmap u otro escáner de puertos	Portal one-X para IP Office solamente
8411	TCP	HTTPS	Nmap u otro escáner de puertos	
8443	TCP	HTTPS	Nmap u otro escáner de puertos	
9443	TCP	HTTPS	Nmap u otro escáner de puertos	Portal one-X para IP Office solamente
50791	TCP		Cliente VMPro, Nmap u otro escáner de puertos	
50792	UDP		Nmap u otro escáner de puertos	
50793	TCP		Nmap u otro escáner de puertos	Solo IP500 V2
50794	UDP+TCP	SysMonito	SysMonitor, Nmap u otro escáner de puertos	
50796	TCP	TLS	Nmap u otro escáner de puertos	
50804	TCP		IP Office Manager, Nmap u otro escáner de puertos	
50805	TCP	TLS	IP Office Manager, Nmap u otro escáner de puertos	
50808	TCP		SSA, Nmap u otro escáner de puertos	

Página1767 de 3226.

Puerto	Protocolo	Usar	Posible herramienta de prueba	notas
50809	TCP	TLS	SSA, Nmap u otro escáner de puertos	
50812	TCP		IP Office Manager, Nmap u otro escáner de puertos	
50813	TCP	TLS	IP Office Manager, Nmap u otro escáner de puertos	
50814	TCP		Nmap u otro escáner de puertos	

Tabla 24: Puertos de ejemplo

Si el acceso es exitoso, puede indicar un Firewall mal configurado u otro sistema de protección de red.

- Intente iniciar sesión en los servidores utilizando el conjunto de cuentas y contraseñas de administrador predeterminadas en la siguiente tabla.
  - Nota: Las cuentas predeterminadas de versiones anteriores no se eliminan en la actualización.

Cuenta predeterminada Nombre	Dominio	Posible herramienta de prueba	notas
seguridad **Administrador** **Gerente** **Operador** **Socio de negocios** **mantenedor** **Servicio IPDECT** **SMGRB5800Administrador** **Administrador de sucursal**	Oficina de PI	Web de IP Office Gerente Gerente de IP Office	Todos los servidores, incluidos IP500 V2 y Comunicaciones Unificadas Módulo
Administrador	Buzón de voz profesional	cliente VM Pro	Correo de voz Pro solamente
Administrador	Portal one-X para IP Office	Navegador	Portal one-X para IP Office solamente
Administrador	control web	Navegador	Solo servidores Linux
raíz	linux	Interfaz de consola	Solo servidores Linux

Si el acceso es exitoso,t Se deben cambiar las credenciales de la cuenta o eliminar la cuenta. VerEliminar cuentas innecesarias 76para obtener más información sobre la eliminación de cuentas

- Utilice IP Office Manager para cargar la configuración y revisar todos los errores y advertencias con especial referencia a las contraseñas. Ninguno debe estar presente.
- Comprobar extensiones y usuarios inesperados
- Verifique la configuración de todos los usuarios para destinos de reenvío inusuales
- Asegúrese de que todas las extensiones SIP**Extensión | Ext. | Forzar autorización**la configuración no ha sido deshabilitada.
- Marque el usuario especial de IP Office 'NoUser'**Número de origen**campo; cualquier entrada inesperada debe aclararse con el personal de soporte. Los números de origen de NoUser a veces se usan para habilitar funciones o comportamientos específicos.
- Verifique que el símbolo del candado se muestre en la parte inferior derecha de la pantalla, lo que indica una conexión segura a IP Office.
- Use IP Office Manager para cargar la configuración de seguridad y revisar todas las advertencias; ninguno debe estar presente.
- Nuevamente, verifique que el símbolo del candado se muestre en la parte inferior derecha de la pantalla, lo que indica una conexión segura a IP Office.
- Inicie sesión en la página de administración de one-X Portal for IP Office, si aparece una advertencia "Cambiar la contraseña predeterminada del administrador", la cuenta del administrador es la predeterminada.
- Para R9.0+, si el inicio de sesión en Web Control, one-X Portal for IP Office o Voicemail Pro falla inesperadamente, verifique la configuración de seguridad de IP Office para la cuenta que se está utilizando; debe tener asignado un grupo de derechos que contenga los derechos 'Externos' correctos.
- Verifique que los inicios de sesión exitosos y fallidos produzcan los informes y resultados esperados.
- Pruebe la restricción de llamadas, las llamadas de emergencia, los códigos de autorización, las llamadas externas de Voicemail Pro y los flujos de llamadas. Las pruebas de llamadas de emergencia se deben coordinar con anticipación con PCSP/Servicios de emergencia para evitar perjudicar una respuesta de emergencia genuina.
- Revise los informes de Firewall, SBC y registrador de llamadas.

Página1768 de 3226.

9.2 Activación de informes

Para garantizar la indicación oportuna de cualquier actividad adversa en cualquier componente, se deben habilitar varios mecanismos de informes. Es importante asegurarse de que los propios mecanismos de denuncia sean fiables y seguros.

- Informes de IP Office 106
- Informes de Voicemail Pro 106
- Informes de la grabadora de contacto 106
- Portal one-X para informes de IP Office 107
- Informes de servidores basados en Linux 107
- Informes de otros componentes 107

9.2.1 Informes de IP Office

Los siguientes eventos y funciones de registro están disponibles para IP Office.

- Eventos del sistema para inicios de sesión fallidos, direcciones IP en la lista negra y fallas de SSL/TLS, lo que podría indicar intentos de obtener acceso no autorizado al sistema. Disponible como syslog, SMTP (correo electrónico), trampas SNMP y visualizable en SSA. Para más información, ver:
  - "Alarmas de servicio" en Uso de la aplicación de estado del sistema de Avaya IP Office™ Platform.
  - La descripción de la**Sistema | Eventos del sistema**en la pestaña Administración de Avaya IP Office™ Platform con Manager.
  - El archivo 'IP_Office_Alarms_N_N_N.xlsx' contenido en el DVD de administración de IP Office.
- Seguimiento de auditoría de inicios de sesión administrativos, su origen y resultado. Disponible como eventos de syslog, también se puede visualizar en SSA y Manager. TENGA EN CUENTA que los cambios basados en el usuario/teléfono no se capturan actualmente. Para más información, ver:
  - "Auditoría de la unidad de control" en Uso*Aplicación de estado del sistema Avaya IP Office™ Platform*.
  - **Archivo | Avanzado | Pista de auditoría**en Administración de la plataforma Avaya IP Office™ con Manager.
- Pista de auditoría detallada de todos los cambios administrativos, incluida la configuración de seguridad. Disponible solo como eventos de syslog.
- Para Server Edition, todos los eventos están activos y se envían a través de syslog al servidor principal.
- Informes de todas las llamadas disponibles como mensaje de informes detallados de mensajes de estación (SMDR) que se pueden enviar a registradores de llamadas de terceros. Para obtener información, consulte la sección SMDR en Administración de Avaya IP Office™ Platform con Manager

9.2.2 Informes de Voicemail Pro

Los siguientes eventos y funciones de registro están disponibles para el servidor Voicemail Pro:

- Pista de auditoría de inicios de sesión administrativos. Disponible solo como eventos de syslog. Para obtener más información, consulte: "Voicemail Pro Syslog" en Administración de Avaya IP Office™ Platform Voicemail Pro. De forma predeterminada para Server Edition, todos los eventos están activos y se envían a través de syslog al principal.
- Las fallas de inicio de sesión en el buzón de correo de voz se informan a través de las alarmas de inicio de sesión fallido de IP Office, consulte más arriba.

9.2.3 Informes del registrador de contactos

Los detalles de la pista de auditoría de los inicios de sesión administrativos están disponibles como eventos de syslog y se muestran en la página de administración web. Para obtener información, consulte**Sistema | Pista de auditoría**en la administración de Avaya IP Office Platform Contact Recorder.

9.2.4 Portal one-X para informes de IP Office

Los siguientes eventos y funciones de registro están disponibles para el servidor one-X Portal for IP Office:

- Pista de auditoría de inicios de sesión administrativos. Disponible solo como eventos de syslog. De forma predeterminada para Server Edition, todos los eventos están activos y se envían a través de syslog al principal.
- Las fallas de inicio de sesión del cliente one-X se informan a través de las alarmas de inicio de sesión fallido de IP Office; consulte la sección de IP Office anterior.

9.2.5 Informes del servidor basado en Linux

Los servidores Server Edition, Linux Application Server y Unified Communications Module generan registros de seguridad y auditoría a través de syslog, ya sea guardados internamente o enviados a un servidor remoto.

- Para habilitar la seguridad del sistema operativo Linux y el registro de auditoría, se deben habilitar las siguientes configuraciones en el**Control web | Configuración | General**pestaña.
  - Privilegios de autenticación y autorización
  - Información almacenada por el demonio de auditoría de Linux (auditd)
  - Servidor web Apache access_log y error_log
- De forma predeterminada para Server Edition, todos los eventos están activos y se envían a través de syslog al principal, donde se pueden almacenar, ver y reenviar a servidores syslog externos. Para más información, ver**Registros | Visor de eventos Syslog**y **Configuración | generales | registro del sistema**en la aplicación Control web.

9.2.6 Informes de otros componentes

- La detección de intrusiones de cortafuegos y los informes deben estar activados.
- La detección e informe de intrusiones de SBC debe estar activada.
- Se debe activar la detección y el informe de actividades de llamadas inusuales del registrador de llamadas.

9.3 Avisos de seguridad de Avaya y actualizaciones de IP Office

1. Regístrese en Avaya Security AdvYo asi ry notificaciones mediante el uso de los procedimientos de suscripción de E-Notificación. Ver Soporte de seguridad de productos de Avaya 111.
2. Regístrese para recibir noticias de la base de conocimientos de IP Office, que incluye actualizaciones sobre boletines técnicos, notas de aplicación y consejos técnicos utilizando las opciones disponibles en:https://ipofficekb.avaya.com/ .

9.4 Respuesta a Incidentes

La contención, erradicación y recuperación es el proceso recomendado a seguir si se detecta un incidente de seguridad:

- Los sistemas atacados/comprometidos deben aislarse o protegerse lo antes posible.
- Los clientes de Avaya con información sobre cualquier problema de seguridad descubierto con los productos de Avaya deben crear una solicitud de servicio utilizando el enlace de autoservicio en https://support.avaya.com, o comunicándose con el número de teléfono de Atención al cliente en el enlace de Soporte de mantenimiento (1-800 -242-2121 para clientes nacionales de EE. UU.). Clientes que no son de Avaya que desean informar un hallazgo de seguridad con Avaya productos deben enviar esta información a securityalerts@avaya.com. VerSoporte de seguridad de productos de Avaya 111para mayor información.
- Avaya proporciona un documento para ayudar a los clientes con las solicitudes de seguridad, consulte https://downloads.avaya.com/css/P8/documents/100161515 .
- Si el ataque se basa en IP, es posible rastrear la dirección IP de origen hasta el ISP en el que está registrado e informarlo. Además, el cortafuegos puede bloquear la dirección IP o la subred.
- La Publicación especial (SP) 800-61 del NIST, Guía de manejo de incidentes de seguridad informática, proporciona una guía general para el manejo de incidentes.http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf .

¿Comentarios sobre este documento? infodev@avaya.com

Capítulo 10.
Apéndices

¿Comentarios sobre este documento? infodev@avaya.com

10. Apéndices

- Apéndice A: soporte de seguridad de productos de Avaya 111
  - oAcceso a los avisos de seguridad de Avaya 111
  - oInterpretación de un aviso de seguridad de Avaya 111
- Apéndice B - Certificados de confianza predeterminados 112
  - oSymantec Class 3 Secure Server CA - G4 en formato PEM 113
  - oAutoridad de Certificación Entrust - L1K en formato PEM 113
  - oGTS Root R1 en formato PEM 114
  - oGTS Root R2 en formato PEM 114
  - oGlobalSign Root CA - R2 en formato PEM 115
  - oISRG Raíz X1 en formato PEM 115
  - oDigiCert Global Root CA en formato PEM 116
  - oDigiCert SHA2 Secure Server CA en formato PEM 116
  - oLet's Encrypt Authority X3 en formato PEM 117
  - oEliminación de un certificado de confianza predeterminado 117
- Apéndice C: administración de certificados de Windows 118
  - oOrganización del almacén de certificados de Windows 118
  - oImportación del almacén de certificados 119
  - oExportación del almacén de certificados 119
  - oConsola de certificados 120
- Apéndice D - Solución de problemas de SRTP 121
  - oHerramientas de resolución de problemas 121
  - oConsejos para solucionar problemas 121
- Apéndice E: Compatibilidad con certificados de interfaz de IP Office 123
- Apéndice F - Seguridad de terminales VoIP de IP Office 127
- Apéndice G: uso de la autoridad de certificación de IP Office 131
  - oGeneración del propio certificado de identidad del servidor CA 131
  - oGeneración de certificados de identidad para otros dispositivos 132
  - oExportación del certificado de firma 132
  - oRenovación/reemplazo del certificado de firma 133
- Apéndice H - Solicitudes de firma de certificados 134
  - oCreación de una CSR mediante el complemento de certificados de Microsoft MMC 135
  - oCreación de una CSR utilizando el paquete OpenSSL 138
  - oCreación de una CSR mediante la línea de comandos del servidor Linux 140
  - oConversión de archivos de certificado 141
- Apéndice I: Aprovisionamiento seguro de teléfonos H.323 de la serie 9600 142
  - oProceso de Estadificación Recomendado 142
  - oProceso automatizado 143
  - oCambio de un certificado de CA raíz 143
- Apéndice J - Dependencias de seguridad de aplicación/cliente 144

10.1 Apéndice A: soporte de seguridad de productos de Avaya

El Equipo de soporte de seguridad de productos de Avaya (PSST) realiza las siguientes funciones:

- Administra las vulnerabilidades y amenazas de los productos de Avaya.
- Mantiene la información publicada enhttp://support.avaya.com/security .
- Realiza pruebas de seguridad y auditorías de los productos principales de Avaya.
- Resuelve problemas de campo relacionados con la seguridad en apoyo de Avaya Global Services.
- Administra la seguridad en el buzón securityalerts@avaya.com .

Como resultado, el PSST monitorea activamente los problemas de seguridad relacionados con los siguientes temas:

- Productos Avaya
- Productos que se incorporan a los productos de Avaya
- Telecomunicaciones y redes de datos generales, según lo identificado por las agencias gubernamentales

Antes de ponerse en contacto con Avaya por un asunto de seguridad, consulte el Flujo de soporte de seguridad del producto, que se puede encontrar enhttps://downloads.avaya.com/css/P8/documents/100161515 . Hay un enlace a este documento en el sitio de soporte de seguridad de Avaya en http://support.avaya.com/security.

Cuando se identifica una vulnerabilidad de seguridad, el PSST determina la susceptibilidad de los productos de Avaya a esas vulnerabilidades y sigue un proceso de acuerdo con la Política de respuesta de vulnerabilidad de seguridad de productos de Avaya definida enhttps://downloads.avaya.com/css/P8/documents/100045520 . Según la categoría de riesgo, el PSST crea un aviso de seguridad de Avaya para notificar a los clientes sobre la vulnerabilidad.

10.1.1 Acceso a los avisos de seguridad de Avaya

Los avisos de seguridad de Avaya se publican en el sitio web de soporte de seguridad enhttp://support.avaya.com/security . Los clientes pueden registrarse en el sitio web de soporte de Avaya para recibir notificaciones por correo electrónico de los avisos de seguridad de Avaya.

10.1.2 Interpretación de un aviso de seguridad de Avaya

Las definiciones precisas que sigue PSST para clasificar las vulnerabilidades en relación con su amenaza potencial para los productos de Avaya están disponibles en la Política de respuesta a vulnerabilidades de seguridad de productos de Avaya en https://downloads.avaya.com/css/P8/documents/100045520 .

10.2 Apéndice B - Certificados de confianza predeterminados

IP Office no confía en todas las autoridades de certificación de manera predeterminada; solo se incluyen los mínimos requeridos para la operación inicial. Hay tres certificados en los que IP Office confía y están presentes en el restablecimiento inicial predeterminado y de configuración de seguridad:

Nombre	Duración	Miniatura	Uso
Symantec Clase 3 Servidor Seguro CA - G4	30 octubre 2023 23:59:59	ff67367c5cd4de 4ae18bcce1d70fdabd7c866135	Una autoridad de certificación intermedia de Symantec propiedad de Avaya. Confía en el servidor SSLVPN de Avaya y en los archivos integrados que se utilizan para los Servicios de soporte de IP Office de Avaya (IPOSS). Requerido para el registro de IP Office y la conexión a IPOSS.
Encomendar la certificación Autoridad - L1K	Inicio (aammddhhmmss): 201510051913562 Fin (aammddhhmmss): 203012051943562		Requerido para soporte de notificaciones push de Apple y SSO de Avaya Spaces
Raíz GTS R1	Inicio (aammddhhmmss): 201606220000002 Fin (aammddhhmmss): 203606220000002		Requerido para soporte de notificaciones push de Apple y SSO de Avaya Spaces
Raíz GTS R2	Inicio (aammddhhmmss): 201606220000002 Fin (aammddhhmmss): 203606220000002		Requerido para soporte de notificaciones push de Apple y SSO de Avaya Spaces
CA raíz de GlobalSign - R2	Inicio (aammddhhmmss): 200612150800002 Fin (aammddhhmmss): 202112150800002		Requerido para soporte de notificaciones push de Apple y SSO de Avaya Spaces
Raíz ISRG X1	Inicio (aammddhhmmss): 201506041104382 Fin (aammddhhmmss): 203506041104382		Requerido para confiar en certificados emitidos por Let's Encrypt, utilizados por IP Office Containerized
CA raíz global de DigiCert	Inicio (aammddhhmmss): 200611100000002 Fin (aammddhhmmss): 203111100000002		Requerido para soporte de notificaciones push de Apple y SSO de Avaya Spaces
Seguro DigiCert SHA2 CA del servidor	Inicio (aammddhhmmss): 201303081200002 Fin (aammddhhmmss): 202303081200002		Requerido para soporte de notificaciones push de Apple y SSO de Avaya Spaces
Vamos a cifrar la autoridad X3	Inicio (aammddhhmmss): 201603171640462 Fin (aammddhhmmss): 202103171640462		Requerido para confiar en certificados emitidos por Let's Encrypt, utilizados por IP Office Containerized

10.2.1 Symantec Class 3 Secure Server CA - G4 en formato PEM

- - - - - BEGIN CERTIFICATE----- MIIFODCCBCCgAwIBAgIQUT+5dDhwtzRAQY0wkwaZ/
zANBgkqhkiG9w0BAQsFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMTMxMDMxMDAwMDAwWhcNMjMxMDMwMjM1OTU5WjB+MQsw
CQYDVQQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24xHzAdBgNV
BAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxLzAtBgNVBAMTJlN5bWFudGVjIENs
YXNzIDMgU2VjdXJlIFNlcnZlciBDQSAtIEc0MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAstgFyhx0LbUXVjnFSlIJluhL2AzxaJ+aQihiw6UwU35VEYJb
A3oNL+F5BMm0lncZgQGUWfm893qZJ4Itt4PdWid/sgN6nFMl6UgfRk/InSn4vnlW
9vf92Tpo2otLgjNBEsPIPMzWlnqEIRoiBAMnF4scaGGTDw5RgDMdtLXO637QYqzus3sBdO9pNevK1T2p7peYyo2qRA4lmUoVlqTObQJUHypqJuI
L9ba4cYY9Z/JJV3zADreJk20KQnNDz0jbxZKgRb78oMQw7jW2FUyPfG9D72MUpVK
Fpd6UiFjdS8W+cRmvvW1Cdj/JwDNRHxvSz+w9wIDAQABo4IBYzCCAV8wEgYDVR0T
AQH/BAgwBgEB/wIBADAwBgNVHR8EKTAnMCWgI6Ahhh9odHRwOi8vczEuc3ltY2Iu
Y29tL3BjYTMtZzUuY3JsMA4GA1UdDwEB/wQEAwIBBjAvBggrBgEFBQcBAQQjMCEw
HwYIKwYBBQUHMAGGE2h0dHA6Ly9zMi5zeW1jYi5jb20wawYDVR0gBGQwYjBgBgpg
hkgBhvhFAQc2MFIwJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cuc3ltYXV0aC5jb20v
Y3BzMCgGCCsGAQUFBwICMBwaGmh0dHA6Ly93d3cuc3ltYXV0aC5jb20vcnBhMCkG
A1UdEQQiMCCkHjAcMRowGAYDVQQDExFTeW1hbnRlY1BLSS0xLTUzNDAdBgNVHQ4E
FgQUX2DPYZBV34RDFIpgKrL1evRDGO8wHwYDVR0jBBgwFoAUf9Nlp8Ld7LvwMAnz
Qzn6Aq8zMTMwDQYJKoZIhvcNAQELBQADggEBAF6UVkndji1l9cE2UbYD49qecxny
H1mrWH5sJgUs+oHXXCMXIiw3k/eG7IXmsKP9H+IyqEVv4dn7ua/ScKAyQmW/hP4W
Ko8/xabWo5N9Q+l0IZE1KPRj6S7t9/
Vcf0uatSDpCr3gRRAMFJSaXaXjS5HoJtGQGX0InLNmfiIEfXzf+YzguaoxX7+0AjiJVgIcWjmzaLmFN5OUiQt/
eV5E1PnXi8t TRttQBVSK/
eHiXgSgW7ZTaoteNTCLD0IX4eRnh8OsN4wUmSGiaqdZpwOdgyA8nTY
Kvi4Os7X1g8RvmurFPW9QaAiY4nxug9vKWNmLT+sjHLF+8fk1A/yO0+MKcc=
- - - - - FINALIZAR CERTIFICADO-----

10.2.2 Autoridad de Certificación Entrust - L1K en formato PEM

- - - - - BEGIN CERTIFICATE----- MIIFDjCCA/
agAwIBAgIMDulMwwAAAABR03eFMA0GCSqGSIb3DQEBCwUAMIG+MQsw
CQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2Vl
IHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMDkg
RW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIwMAYDVQQD
EylFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjAeFw0x
NTEwMDUxOTEzNTZaFw0zMDEyMDUxOTQzNTZaMIG6MQswCQYDVQQGEwJVUzEWMBQG
A1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5lbnRydXN0Lm5l
dC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAt
IGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IC0gTDFLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmqAJqOV38pa9vH4SEkqjrQ
jUcj0u1yFvCRIdJdt7hLqIOPt5EyaM/
OJZMssn2XyP7BtBe6CZ4DkJN7fEmDImiKm95HwzGYei59QAvS7z7Tsoyqj0ip/
wDoKVgG97aTWpRzJiatWA7lQrjV6nN5ZGhT
JbiEz5R6rgZFDKNrTdDGvuoYpDbwkrK6HIiPOlJ/915tgxyd8B/lw9bdpXiSPbBt
LOrJz5RBGXFEaLpHPATpXbo+8DX3Fbae8i4VHj9HyMg4p3NFXU2wO7GOFyk36t0F
ASK7lDYqjVs1/lMZLwhGwSqzGmIdTivZGwIDAQABo4IBDDCCAQgwDgYDVR0PAQH/
BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwMwYIKwYBBQUHAQEEJzAlMCMGCCsG
AQUFBzABhhdodHRwOi8vb2NzcC5lbnRydXN0Lm5ldDAwBgNVHR8EKTAnMCWgI6Ah
hh9odHRwOi8vY3JsLmVudHJ1c3QubmV0L2cyY2EuY3JsMDsGA1UdIAQ0MDIwMAYE
VR0gADAoMCYGCCsGAQUFBwIBFhpodHRwOi8vd3d3LmVudHJ1c3QubmV0L3JwYTAd
BgNVHQ4EFgQUgqJwdN28Uz/Pe9T3zX+nYMYKTL8wHwYDVR0jBBgwFoAUanImetAe
733nO2lR1GyNn5ASZqswDQYJKoZIhvcNAQELBQADggEBADnVjpiDYcgsY9NwHRkw y/
YJrMxp1cncN0HyMg/vdMNY9ngnCTQIlZIv19+4o/0OgemknNM/TWgrFTEKFcxS
BJPok1DD2bHi4Wi3Ogl08TRYCj93mEC45mj/XeTIRsXsgdfJghhcg85x2Ly/rJkC
k9uUmITSnKa1/
ly78EqvIazCP0kkZ9Yujs+szGQVGHLlbHfTUqi53Y2sAEo1GdRvc6N172tkw+CNgxKhiucOhk3YtCAbvmqljEtoZuMrx1gL+1YQ1JH7HdMxWBCMRON1
exCdtTix9qrKgWRs6PLigVWXUX/hwidQosk8WwBD9lu51aX8/wdQQGcHsFXwt35u Lcw=
- - - - - FINALIZAR CERTIFICADO-----

10.2.3 GTS Root R1 en formato PEM

- - - - - BEGIN CERTIFICATE-----
MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
QzEUMBIGA1UEAxMLR1RTIFJvb3QgUjEwHhcNMTYwNjIyMDAwMDAwWhcNMzYwNjIy
MDAwMDAwWjBHMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNl
cnZpY2VzIExMQzEUMBIGA1UEAxMLR1RTIFJvb3QgUjEwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQC2EQKLHuOhd5s73L+UPreVp0A8of2C+X0yBoJx9vaM f/
vo27xqLpeXo4xL+Sv2sfnOhB2x+cWX3u+58qPpvBKJXqeqUqv4IyfLpLGcY9vX
mX7wCl7raKb0xlpHDU0QM+NOsROjyBhsS+z8CZDfnWQpJSMHobTSPS5g4M/SCYe7
zUjwTcLCeoiKu7rPWRnWr4+wB7CeMfGCwcDfLqZtbBkOtdh+JhpFAz2weaSUKK0P
fyblqAj+lug8aJRT7oM6iCsVlgmy4HqMLnXWnOunVmSPlk9orj2XwoSPwLxAwAtc
vfaHszVsrBhQf4TgTM2S0yDpM7xSma8ytSmzJSq0SPly4cpk9+aCEI3oncKKiPo4 Zor8Y /
kB+Xj9e1x3+naH+uzfsQ55lVe0vSbv1gHR6xYKu44LtcXFilWr06zqkUspzBmkMiVOKvFlRNACzqrOSbTqn3yDsEB750Orp2yjj32JgfpMpf/
VjsPOS+C12LOO Rc92wO1AK/1TD7Cn1TsNsYqiA94xrcx36m97PtbfkSIS5r762DL8EGMUUXLeXdYW
k70paDPvOmbsB4om3xPXV2V4J95eSRQAogB/mqghtqmxlbCluQ0WEdrHbEg8QOB+
DVrNVjzRlwW5y0vtOUucxD/SVRNuJLDWcfr0wbrM7Rv1/oFB2ACYPTrIrnqYNxgF
lQIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNV
HQ4EFgQU5K8rJnEaK0gnhS9SZizv8IkTcT4wDQYJKoZIhvcNAQEMBQADggIBADiW Cu49tJYeX+
+dnAsznyvgyv3SjgofQXSlfKqE1OXyHuY3UjKcC9FhHb8owbZEKTV1
d5iyfNm9dKyKaOOpMQkpAWBz40d8U6iQSifvS9efk+eCNs6aaAyC58/UEBZvXw6Z
XPYfcX3v73svfuo21pdwCxXu11xWajOl40k4DLh9+42FpLFZXvRq4d2h9mREruZR
gyFmxhE+885H7pwoHyXa/6xmld01D1zvICxi/ZG6qcz8WpyTgYMpl0p8WnK0OdC3 d8t5/
Wk6kjftbjhlRn7pYL15iJdfOBL07q9bgsiG1eGZbYwE8na6SfZu6W0eX6Dv
J4J2QPim01hcDyxC2kLGe4g0x8HYRZvBPsVhHdljUEn2NIVq4BjFbkerQUIpm/Zg DdIx02OYI5NaAIFItO/
Nis3Jz5nu2Z6qNuFoS3FJFDYoOj0dzpqPJeaAcWErtXvMDdIx02OYI5NaAIFIto/
Nis3Jz5nu2Z6qNuFoS3FJFDYoOj0dzpqPJeaAcWErtXvM
+ SUWgeExX6GjfhaknBZqlxi9dnKlC54dNuYvoS++cJEPqOba+MSSQGwlfnuzCdyy
F62ARPBopY+Udf90WuioAnwMCeKpSwughQtiue+hMZL77/ZRBIls6Kl0obsXs7X9
SQ98POyDGCBDTtWTurQ0sR8WNh8M5mQ5Fkzc4P4dyKliPUDqysU0ArSuiYgzNdws
E3PYJ/HQcu51OyLemGhmW/HGY0dVHLqlCFF1pkgl
- - - - - FINALIZAR CERTIFICADO-----

10.2.4 GTS Root R2 en formato PEM

- - - - - BEGIN CERTIFICATE----- MIIFWjCCA0KgAwIBAgIQbkepxlqz5yDFMJo/
aFLybzANBgkqhkiG9w0BAQwFADBH
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
QzEUMBIGA1UEAxMLR1RTIFJvb3QgUjIwHhcNMTYwNjIyMDAwMDAwWhcNMzYwNjIy
MDAwMDAwWjBHMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNl
cnZpY2VzIExMQzEUMBIGA1UEAxMLR1RTIFJvb3QgUjIwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDO3v2m++zsFDQ8BwZabFn3GTXd98GdVarTzTukk3Lv
CvptnfbwhYBboUhSnznFt+4orO/LdmgUud+tAWyZH8QiHZ/+cnfgLFuv5AS/T3Kg
GjSY6Dlo7JUle3ah5mm5hRm9iYz+re026nO8/4Piy33B0s5Ks40FnotJk9/BW9Bu
XvAuMC6C/Pq8tBcKSOWIm8Wba96wyrQD8Nr0kLhlZPdcTK3ofmZemde4wj7I0BOd
re7kRXuJVfeKH2JShBKzwkCX44ofR5GmdFrS+LFjKBC4swm4VndAoiaYecb+3yXu
PuWgf9RhD1FLPD+M2uFwdNjCaKH5wQzpoeJ/u1U8dgbuak7MkogwTZq9TwtImos1
mKPV+3PBV2HdKFZ1E66HjucMUQkQdYhMvI35ezzUIkgfKtzra7tEscszcTJGr61K8YzodDqs5xoic4DSMPclQsciOzsSrZYuxsN2B6ogtzVJV+mSSeh
x5RWIr9qS34BIbIjMt/kmkRtWVtd9QCgHJvGeJeNkP+byKq0rxFROV7Z+2et1VsR
nTKaG73VululycslaVNVJ1zgyjbLiGH7HrfQy+4W+9OmTN6SpdTi3/UGVN4unUu0
kzCqgc7dGtxRcw1PcOnlthYhGXmy5okLdWTK1au8CcEYof/UVKGFPP0UJAOyh9Ok
twIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/
zAdBgNV HQ4EFgQUu//
KjiOfT5nK2+JopqUVJxce2Q4wDQYJKoZIhvcNAQEMBQADggIBALZp 8KZ3/
p7uC4Gt4cCpx/k1HUCCq+YEtN/L9x0Pg/B+E02NjO7jMyLDOfxA325BS0JT
vhaI8dI4XsRomRyYUpOM52jtG2pzegVATX9lO9ZY8c6DR2Dj/5epnGB3GFW1fgiT
z9D2PGcDFWEJ+YF59exTpJ /JjwGLc8R3dtyDovUMSRqodt6Sm2T4syzFJ9MHwAiA
pJiS4wGWAqoC7o87xdFtCjMwc3i5T1QWvwsHoaRc5svJXISPD+AVdyx+Jn7axEvb
pxZ3B7DNdehyQtaVhJ2Gg/LkkM0JR9SLA3DaWsYDQvTtN6LwG1BUSw7YhN4ZKJmB
R64JGz9I0cNv4rBgF/XuIwKl2gBbbZCr7qLpGzvpx0QnRY5rn/WkhLx3+WuXrD5R
RaIRpsyF7gpo8j5QOHokYh4XIDdtak23CZvJ/
KRY9bb7nE4Yu5UC56GtmwfuNmsk0jmGwZODUNKBRqhfYlcsu2xkiAhu7xNUX90txGdj08+JN7+dIPT7eoOboB6BAFDC
5AwiWVIQ7UNWhwD4FFKnHYuTjKJNRn8nxnGbJN7k2oaLDX5rIMHAnuFl2GqjpuiF
izoHCBy69Y9Vmhh1fuXsgWbRIXOhNUQLgD1bnF5vKheW0YMjiGZt5obicDIvUiLn
yOd/xCxgXS/Dr55FBcOEArf9LAhST4Ldo/DUhgkC
- - - - - FINALIZAR CERTIFICADO-----

10.2.5 GlobalSign Root CA - R2 en formato PEM

- - - - - BEGIN CERTIFICATE----- MIIDujCCAqKgAwIBAgILBAAAAAABD4Ym5g0wDQYJKoZIhvcNAQEFBQAwTDEgMB4G
A1UECxMXR2xvYmFsU2lnbiBSb290IENBIC0gUjIxEzARBgNVBAoTCkdsb2JhbFNp
Z24xEzARBgNVBAMTCkdsb2JhbFNpZ24wHhcNMDYxMjE1MDgwMDAwWhcNMjExMjE1
MDgwMDAwWjBMMSAwHgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEG
A1UEChMKR2xvYmFsU2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAKbPJA6+Lm8omUVCxKs+IVSbC9N/hHD6ErPL
v4dfxn+G07IwXNb9rfF73OX4YJYJkhD10FPe+3t+c4isUoh7SqbKSaZeqKeMWhG8 eoLrvozps6yWJQeXSpkqBy+0Hne/
ig+1AnwblrjFuTosvNYSuetZfeLQBoZfXklq tTleiDTsvHgMCJiEbKjNS7SgfQx5TfC4LcshytVsW33hoCmEofnTlEnLJGKRILzd
C9XZzPnqJworc5HGnRusyMvo4KD0L5CLTfuwNhv2GXqF4G3yYROIXJ/gkwpRl4pa
zq+r1feqCapgvdzZX99yqWATXgABByUr6P6TqBwMhAo6CygPCm48CAwEAAaOBnDCB mTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/
BAUwAwEB/zAdBgNVHQ4EFgQUm +IHV2ccHsBqBt5ZtJot39wZhi4wNgYDVR0fBC8wLTAroCmgJ4YlaHR0cDovL2NybC5n
bG9iYWxzaWduLm5ldC9yb290LXIyLmNybDAfBgNVHSMEGDAWgBSb4gdXZxwewGoG
3lm0mi3f3BmGLjANBgkqhkiG9w0BAQUFAAOCAQEAmYFThxxol4aR7OBKuEQLq4Gs J0/
WwbgcQ3izDJr86iw8bmEbTUsp9Z8FHSbBuOmDAGJFtqkIk7mpM0sYmsL4h4hO
291xNBrBVNpGP+DTKqttVCL1OmLNIG+6KYnX3ZHu01yiPqFbQfXf5WRDLenVOavS ot+3i9DAgBkcRcAtjOj4LaR0VknFBbVPFd5uRHg5h6h+u/
N5GJG79G+dwfCMNYxd AfvDbbnvRG15RjF+Cv6pgsH/76tuIMRQyV+dTZsXjAzlAcmgQWpzU/qlULRuJQ/7 TBj0/
VLZjmmx6BEP3ojY+x1J96relc8geMJgEtslQIxq/H5COEBkEveegeGTLg==ot+3i9DAgBkcRcAtjOj4LaR0VknFBbVPFd5uRHg5h6h+u/
N5GJG79G+dwfCMNYxd AfvDbbnvRG15RjF+Cv6pgsH/76tuIMRQyV+dTZsXjAzlAcmgQWpzU/qlULRuJQ/7 TBj0/
VLZjmmx6BEP3ojY+x1J96relc8geMJgEtslQIxq/H5COEBkEveegeGTLg==ot+3i9DAgBkcRcAtjOj4LaR0VknFBbVPFd5uRHg5h6h+u/
N5GJG79G+dwfCMNYxd AfvDbbnvRG15RjF+Cv6pgsH/76tuIMRQyV+dTZsXjAzlAcmgQWpzU/qlULRuJQ/7 TBj0/
VLZjmmx6BEP3ojY+x1J96relc8geMJgEtslQIxq/H5COEBkEveegeGTLg==
- - - - - FINALIZAR CERTIFICADO-----

10.2.6 Raíz ISRG X1 en formato PEM

- - - - - BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIRAIIQz7DSQONZRGPgu2OCiwAwDQYJKoZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQQDEwxJU1JHIFJvb3QgWDEwHhcNMTUwNjA0MTEwNDM4
WhcNMzUwNjA0MTEwNDM4WjBPMQswCQYDVQQGEwJVUzEpMCcGA1UEChMgSW50ZXJu
ZXQgU2VjdXJpdHkgUmVzZWFyY2ggR3JvdXAxFTATBgNVBAMTDElTUkcgUm9vdCBY
MTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK3oJHP0FDfzm54rVygc
h77ct984kIxuPOZXoHj3dcKi/vVqbvYATyjb3miGbESTtrFj/RQSa78f0uoxmyF+
0TM8ukj13Xnfs7j/EvEhmkvBioZxaUpmZmyPfjxwv60pIgbz5MDmgK7iS4+3mX6U A5/
TR5d8mUgjU+g4rk8Kb4Mu0UlXjIB0ttov0DiNewNwIRt18jA8+o+u3dpjq+sW
T8KOEUt+zwvo/7V3LvSye0rgTBIlDHCNAymg4VMk7BPZ7hm/ELNKjD+Jo2FR3qyH
B5T0Y3HsLuJvW5iB4YlcNHlsdu87kGJ55tukmi8mxdAQ4Q7e2RCOFvu396j3x+ UC
B5iPNgiV5+I3lg02dZ77DnKxHZu8A/
lJBdiB3QW0KtZB6awBdpUKD9jf1b0SHzUvKBds0pjBqAlkd25HN7rOrFleaJ1/
ctaJxQZBKT5ZPt0m9STJEadao0xAH0ahmbWn
OlFuhjuefXKnEgV4We0+UXgVCwOPjdAvBbI+e0ocS3MFEvzG6uBQE3xDk3SzynTn
jh8BCNAw1FtxNrQHusEwMFxIt4I7mKZ9YIqioymCzLq9gwQbooMDQaHWBfEbwrbw
qHyGO0aoSCqI3Haadr8faqU9GY/rOPNk3sgrDQoo//fb4hVC1CLQJ13hef4Y53CI
rU7m2Ys6xt0nUW7/vGT1M0NPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBR5tFnme7bl5AFzgAiIyBpY9umbbjANBgkq
hkiG9w0BAQsFAAOCAgEAVR9YqbyyqFDQDLHYGmkgJykIrGF1XIpu+ILlaS/V9lZL
ubhzEFnTIZd+50xx+7LSYK05qAvqFyFWhfFQDlnrzuBZ6brJFe+GnY+EgPbk6ZGQ
3BebYhtF8GaV0nxvwuo77x/Py9auJ/GpsMiu/X1+mvoiBOv/2X/qkSsisRcOj /KK
NFtY2PwByVS5uCbMiogziUwthDyC3+6WVwW6LLv3xLfHTjuCvjHIInNzktHCgKQ5
ORAzI4JMPJ+GslWYHb4phowim57iaztXOoJwTdwJx4nLCgdNbOhdjsnvzqvHu7Ur
TkXWStAmzOVyyghqpZXjFaH3pO3JLF+l+/+sKAIuvtd7u+Nxe5AW0wdeRlN8NwdC
jNPElpzVmbUq4JUagEiuTDkHzsxHpFKVK7q4+63SM1N95R1NbdWhscdCb+ZAJzVcoyi3B43njTOQ5yOf+1CceWxG1bQVs5ZufpsMljq4Ui0/1lvh+wjChP4k
4RgqsahDYVvTH9w7jXbyLeiNdd8XM2w9U/t7y0Ff/9yi0GE44Za4rF2LN9d11TPA
mRGunUHBcnWEvgJBQl9nJEiU0Zsnvgc/ubhPgXRR4Xq37Z0j4r7g1SgEEzwxA57d
emyPxgcYxn/eR44/KJ4EBs+lVDR3veyJm+kXQ99b21/+jh5Xos1AnX5iItreGCc=
- - - - - FINALIZAR CERTIFICADO-----

10.2.7 CA raíz global de DigiCert en formato PEM

- - - - - BEGIN CERTIFICATE----- MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh

MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3

d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD

QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT

MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j

b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG

9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB CSDMAZOnTjC3U/

dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97 nh6Vfe63SKMI2tavegw5BmV/

Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt 43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P

T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4 gdW7jVg/

tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/

zAdBgNVHQ4EFgQUA95QNVbR TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw

DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr hMAtudXH/

vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg 06O/

nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF

PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls

YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk

CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk

CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk

CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=

- - - - - FINALIZAR CERTIFICADO-----

10.2.8 DigiCert SHA2 Secure Server CA en formato PEM

- - - - - BEGIN CERTIFICATE----- MIIEIDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3

d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT

MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB ANyuWJBNwcQwFZA1W248ghX1LFy949v/

cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83 nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f /

ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikjTvOX6+guqw9ypzAO+sf0 /RR3w6RbKFfCs/mC /

bdFWJsCAwEAAaOCAVowggFWMBIGA1UdewEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY

aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6 Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1

oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh

d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl 5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1IGA

CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl 5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1IGA 8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC 2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit

8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC 2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0 j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLzaHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6 Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1

oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh

QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl 5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/

sELfeNqzqPlt/yGFUzZgTHbO7Djc1IGA 8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC 2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit

c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0 j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLzoDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBY

- - - - - FINALIZAR CERTIFICADO-----

10.2.9 Let's Encrypt Authority X3 en formato PEM

- - - - - BEGIN CERTIFICATE----- MIIEkjCCA3qgAwIBAgIQCgFBQgAAAVOFc2oLheynCDANBgkqhkiG9w0BAQsFADA/ MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT

DkRTVCBSb290IENBIFgzMB4XDTE2MDMxNzE2NDA0NloXDTIxMDMxNzE2NDA0Nlow SjELMAkGA1UEBhMCVVMxFjAUBgNVBAoTDUxldCdzIEVuY3JScHQxIzAhBgNVBAMT

GkxldCdzIEVuY3JScHQgQXV0aG9yaXRSIFgzMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAnNMM8FrlLke3cl03g7NoYzDq1zUmGSXhvb418XCSL7e4S0EF

q6meNQhY7LEqxGiHC6PjdeTm86dicbp5gWAf15Gan/PQeGdxyGkOlZHP/uaZ6WA8 SMx+yk13EiSdRxta67nsHjcAHJyse6cF6s5K671B5TaYucv9bTyWaN8jKkKQDIZ0 Z8h/

pZq4UmEUEz9l6YKHy9v6Dlb2honzhT+Xhq+w3Brvaw2VFn3EK6BlspkENnWA a6xK8xuQSXgvopZPKiAlKQTGdMDQMc2PMTiVFrqoM7hD8bEfwzB/onkxEz0tNvjj /

PIzark5McWvxI0NHWQWM6r6hCm21AvA2H3DkwIDAQABo4IBfTCCAXkwEgYDVR0T AQH/BAgwBgEB/

wIBADAOBgNVHQ8BAf8EBAMCAYYwfwYIKwYBBQUHAQEEczBxMDIGCCsGAQUFBzABhiZodHRwOi8vaXNyZy50cnVzdGlkLm9jc3AuaWRlbnRydXN0LmNv

bTA7BggrBgEFBQcwAoYvaHR0cDovL2FwcHMuaWRlbnRydXN0LmNvbS9yb290cy9yb290LWNyb3NzLTIuY2VydDAfBgNVHSMEGDAWgBTEp7Gkeyxx

VAYDVR0gBE0wSzAIBgZngQwBAgEwPwYLKwYBBAGC3xMBAQEwMDAuBggrBgEFBQcC ARYiaHR0cDovL2Nwcy5yb290LXgxLmxldHNlbmNyeXB0Lm9yZzA8BgNVHR8ENTAz

MDGgL6AthitodHRwOi8vY3JsLmlkZW50cnVzdC5jb20vRFNUUk9PVENBWDNDUkwu Y3JsMB0GA1UdDgQWBBSoSmpjBH3duubRObemRWXv86jsoTANBgkqhkiG9w0BAQsF

AAOCAQEA3TPXEfNjWDjdGBX7CVW+dla5cEilaUcne8IkCJLxWh9KEik3JHRRHGJo uM2VcGfl96S8TihRzZvoroed6ti6WqEBmtzw3Wodatg+VyOeph4EYpr/1wXKtx8/

wApIvJSwtmVi4MFU5aMqrSDE6ea73Mj2tcMyo5jMd6jmeWUHK8so/joWUoHOUgwu X4Po1QYz+3dszkDqMp4fklxBwXRsW10KXzPMTZ+sOPAveyxindmjkW8lGy+QsRlG

PfZ+G6Z6h7mjem0Y+iWlkYcV4PIWL1iwBi8saCbGS5jN2p8M+X+Q7UNKEkROb3N6 KOqkqm57TH2H3eDJAkSnh6/

DNFu0Qg==bTA7BggrBgEFBQcwAoYvaHR0cDovL2FwcHMuaWRlbnRydXN0LmNvbS9yb290cy9k c3Ryb290Y2F4My5wN2MwHwYDVR0jBBgwFoAUxKexpHsscfrb4UuQdf/EFWCFiRAw

VAYDVR0gBE0wSzAIBgZngQwBAgEwPwYLKwYBBAGC3xMBAQEwMDAuBggrBgEFBQcC ARYiaHR0cDovL2Nwcy5yb290LXgxLmxldHNlbmNyeXB0Lm9yZzA8BgNVHR8ENTAz

MDGgL6AthitodHRwOi8vY3JsLmlkZW50cnVzdC5jb20vRFNUUk9PVENBWDNDUkwu Y3JsMB0GA1UdDgQWBBSoSmpjBH3duubRObemRWXv86jsoTANBgkqhkiG9w0BAQsF

AAOCAQEA3TPXEfNjWDjdGBX7CVW+dla5cEilaUcne8IkCJLxWh9KEik3JHRRHGJo uM2VcGfl96S8TihRzZvoroed6ti6WqEBmtzw3Wodatg+VyOeph4EYpr/1wXKtx8/

wApIvJSwtmVi4MFU5aMqrSDE6ea73Mj2tcMyo5jMd6jmeWUHK8so/joWUoHOUgwu X4Po1QYz+3dszkDqMp4fklxBwXRsW10KXzPMTZ+sOPAveyxindmjkW8lGy+QsRlG

PfZ+G6Z6h7mjem0Y+iWlkYcV4PIWL1iwBi8saCbGS5jN2p8M+X+Q7UNKEkROb3N6 KOqkqm57TH2H3eDJAkSnh6/

DNFu0Qg==VAYDVR0gBE0wSzAIBgZngQwBAgEwPwYLKwYBBAGC3xMBAQEwMDAuBggrBgEFBQcC ARYiaHR0cDovL2Nwcy5yb290LXgxLmxldHNlbmNyeXB0Lm9yZzA8BgNVHR8ENTAz MDGgL6AthitodHRwOi8vY3JsLmlkZW50cnVzdC5jb20vRFNUUk9PVENBWDNDUkwu Y3JsMB0GA1UdDgQWBBSoSmpjBH3duubRObemRWXv86jsoTANBgkqhk

- - - - - FINALIZAR CERTIFICADO-----

10.2.10 Eliminación de un certificado de confianza predeterminado

Para eliminar la confianza predeterminada con la que se puede usar un archivo, use la función de eliminación del almacén de certificados confiables de IP Office:

- Cree un archivo de texto con una extensión '.pem', abra y copie los datos PEM anteriores, incluidas las líneas 'BEGIN CERTIFICATE' y 'END CERTIFICATE'. La terminación de línea puede ser Windows o Linux.
- Un archivo .pem por certificado
- Con la función Administrador de archivos de IP Office o IP Office Web Manager, copie el archivo en el ***sistema/primario/certificados/tcs/eliminar***directorio
- Reinicie IP Office

Para agregar un certificado de confianza predeterminado, se pueden seguir los pasos anteriores, pero copie el archivo en el ***sistema/primario/certificados/tcs/añadir***directorio

La función de certificado predeterminado también admite el formato DER binario; verCertificados y Fideicomiso 38para obtener más información sobre los formatos de archivo de certificado.

10.3 Apéndice C: administración de certificados de Windows

El almacén de certificados que utilizan varias aplicaciones de Avaya para guardar y recuperar certificados X509 es el predeterminado que proporciona el sistema operativo Windows. El almacén de certificados de Windows es relevante para las muchas aplicaciones que se ejecutan en Windows que usan certificados para seguridad, ya sea TLS o HTTPS, que incluyen:

- Gerente de IP Office
- Comunicador de Avaya
- Navegador Google Chrome
- Navegador Safari
- Microsoft Internet Explorer
- Microsoft IIS (utilizado por Windows Voicemail Pro)

Hay algunas aplicaciones que actualmente no utilizan el almacén de certificados de Windows:

- IP Office SoftConsole: utiliza un archivo de certificado local
- Navegador Firefox: utiliza su propio almacén de certificados interno
- Entorno Java Runtime 1.6, 1.7 y 1.8: utiliza su propio almacén de certificados interno
- one-X Portal en el servidor de Windows: utiliza un archivo de certificado local.

- **Advertencia:**
  Avaya no acepta ninguna responsabilidad por los cambios realizados por los usuarios en el sistema operativo Windows. Los usuarios son responsables de asegurarse de haber leído toda la documentación relevante y de estar suficientemente capacitados para la tarea que se está realizando.

10.3.1 Organización del almacén de certificados de Windows

De forma predeterminada, los certificados se almacenan en la siguiente estructura:

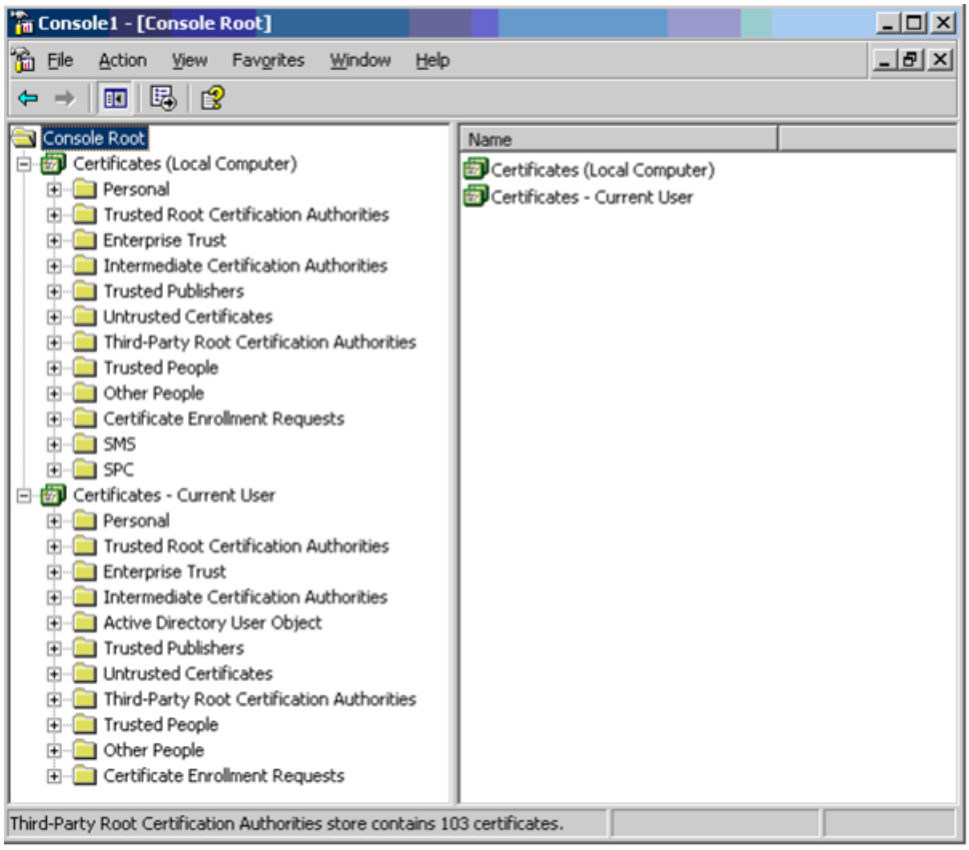


Figura 11: Estructura de almacenamiento de certificados predeterminada

Cada una de las subcarpetas tiene un uso diferente. El área Certificados - Usuario actual cambia con el usuario de Windows conectado actualmente. El área Certificado (Computadora local) no cambia con el usuario de Windows actualmente conectado.

IP Office Manager y otras aplicaciones de Windows solo acceden a algunas de las subcarpetas de certificados:

Página1782 de 3226.

Certificados (locales Computadora) Carpeta	Uso
personales | Certificados	Carpeta buscada por Manager y algunos navegadores web Primero para un certificado para enviar a IP Office cuando se solicite. Certificado que coincide con el nombre del sujeto contenido en Archivo | Preferencias | Seguridad | Certificado ofrecido al sistema. Carpeta a la que se accede cada vez que se utiliza el "almacén de certificados de la máquina local" para la configuración de seguridad. Carpeta buscada por Manager para el certificado coincidente cuando se recibió el certificado del sistema y Archivo | Preferencias | Seguridad | Comprobaciones de certificado de administrador = Medio o Alto.
Raíz de confianza Certificación Autoridades | Certificados	Manager buscó en la carpeta un certificado de CA raíz coincidente cuando se recibió un certificado no autofirmado de IP Office y Archivo | Preferencias | Seguridad | Comprobaciones de certificado de administrador = Medio o Alto. Carpeta buscada por algunos navegadores y otras aplicaciones para que coincida con el certificado de CA raíz cuando se recibió un certificado de IP Office.

Certificados - Carpeta de usuario actual	Uso
personales | Certificados	Manager 2nd buscó en la carpeta un certificado para enviar a IP Office cuando se solicite. Certificado que coincide con el nombre del sujeto contenido en Archivo | Preferencias | Seguridad | Certificado ofrecido al sistema. Carpeta a la que se accede cada vez que se utiliza "Almacén de certificados de usuario actual" para la configuración de seguridad. Manager buscó en la carpeta un certificado coincidente cuando recibió el certificado de IP Office y Archivo | Preferencias | Seguridad | Comprobaciones de certificado de administrador = Medio o Alto.
Raíz de confianza Certificación Autoridades | Certificados	Carpeta buscada por Manager para los certificados principales coincidentes cuando se recibió un certificado no autofirmado del sistema y Archivo | Preferencias | Seguridad | Comprobaciones de certificado de administrador = Medio o Alto. Esta carpeta no la usan aplicaciones que no son de Microsoft, como los navegadores Chrome o Safari; se usa la carpeta Equipo local correspondiente.
Otras personas | Certificados	Carpeta buscada por Manager para los certificados principales coincidentes cuando se recibió un certificado no autofirmado del sistema y Archivo | Preferencias | Seguridad | Comprobaciones de certificado de administrador = Medio o Alto. Esta carpeta no la usan aplicaciones que no son de Microsoft, como los navegadores Chrome o Safari; se usa la carpeta Equipo local correspondiente.

10.3.2 Importación del almacén de certificados

Para usar certificados, ya sea para la configuración de seguridad o para la operación del administrador, deben estar presentes en el almacén de certificados de Windows. El asistente de importación de certificados puede colocar los certificados en el almacén. El Asistente de importación de certificados se puede utilizar cada vez que se visualiza un certificado. Para que el Administrador acceda posteriormente a este certificado, se debe seleccionar la opción Colocar todo el certificado en la siguiente tienda:

- Si el certificado importado es para confiar en IP Office, se debe usar la carpeta Autoridades de certificación raíz confiables y el certificado importado debe ser el certificado de CA raíz.
- Si el certificado va a identificar posteriormente al Administrador, se debe utilizar la carpeta Personal y guardar también la clave privada asociada.

10.3.3 Exportación del almacén de certificados

Cualquier certificado requerido fuera de la PC con Windows debe guardarse primero en el almacén de certificados y luego exportarse. Si el certificado se utilizará para verificar la identidad (es decir, para verificar la entidad remota de un enlace), el certificado por sí solo es suficiente y debe guardarse en formato PEM o DER.

Si el certificado se va a utilizar para la identificación (es decir, para identificar el extremo cercano de un enlace), se requiere el certificado y la clave privada, y se deben guardar en formato PKCS#12, junto con una contraseña "fuerte" para acceder al resultante archivo pfx.

10.3.4 Consola de Certificados

La Consola de certificados de Windows es un complemento de Microsoft Management Console (MMC) que se puede usar para administrar el almacén de certificados de Windows, incluidas la visualización, importación y exportación.

Para obtener más información sobre la Consola de Certificados, consulte http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx

10.4 Apéndice D - Solución de problemas de SRTP

Esta sección proporciona notas para la solución de problemas de SRTP.

10.4.1 Herramientas de resolución de problemas

Aplicación de estado del sistema

- Active Calls muestra si la llamada es segura, directa o retransmitida, si SRTP se realiza mediante VCM o CPU en IP500 V2. Los servidores Linux siempre usan CPU.

Monitoreo del sistema

- Para capturar seguimientos SRTP, establezca filtros en las opciones de seguimiento predeterminadas más:
  - **sorbo | Sorbo + Verboso**
  - **Medios | Eventos de medios | Manejadores de medios**
  - **Medios | Eventos VoIP | VoIP + detallado**
  - **Medios | Eventos VoIP | Primitivo + Verboso**
- Durante las llamadas, en**Estado | [S]Sesiones RTP**ventana, la columna segura describe si se usa SRTP en esa llamada y si lo hace VCM o CPU en IP500 V2. Usar**Mostrar SRTP**botón para mostrar más detalles sobre las sesiones SRTP.

10.4.2 Consejos para la resolución de problemas

El primer paso en la resolución de problemas es verificar si el sistema y todos los dispositivos participantes están configurados correctamente. Algunos puntos finales deben registrarse mediante TLS para tener SRTP disponible.

- Asegúrese de que el sistema esté utilizando la configuración predeterminada para las opciones avanzadas. Si ese no es el caso, verifique que sea intencional.
- Si se utilizan dispositivos SIP y Best Effort está configurado, verifique con SSA/System Monitor cómo se negocia SRTP y si el dispositivo admite cap neg (se puede verificar haciendo una llamada al dispositivo con SRTP y RTP y luego verificando si responde con SRTP o RTP: si es SRTP, se admite cap neg). De lo contrario, anule la configuración de seguridad de los medios del dispositivo y configure***Hacer cumplir***o***Desactivado***, según sea apropiado.
- Las líneas de IP Office con Best Effort configurado y ambas suites criptográficas están habilitadas pueden generar mensajes de inicio de llamada grandes en las líneas de IP Office, ~ 5000 bytes. Si el enlace es lento y/o la tasa de llamadas es alta, puede tener un impacto negativo. Considere usar solo una suite criptográfica o las líneas**Configuración VoIP | Seguridad de los medios**ajuste a***Hacer cumplir***o***Desactivado***.
- Algunos teléfonos no admiten RTCP (SRTCP); verificar el funcionamiento con SRTCP deshabilitado.

10.5 Apéndice E: Compatibilidad con certificados de interfaz de IP Office

La siguiente tabla proporciona una descripción general de la compatibilidad con certificados para las interfaces IP de la plataforma IP Office.

- **Nota:**Se debe consultar la documentación del punto final o del servidor correspondiente, ya que las características admitidas pueden variar según la versión.

Para obtener una lista completa de puertos, consulte la matriz de puertos de IP Office correspondiente que se puede encontrar enhttps://support.avaya.com/security .

Enlace	Protocolo	Soporte de certificado	Certificado de identificación Ofrecido[1]	Certificado de confianza cheques[2]	Comprobación de certificado Control[3]	notas
Oficina de PI						
Línea SIP	SIP-TLS	✓	Teléfono	Bi	✓	
Línea SM	SIP-TLS	✓	Teléfono	Bi	✓	
Extensión SIP	SIP-TLS	✓	Teléfono	Cliente	✗	VerSeguridad de punto final VoIP de IP Office 127para más detalles.
Extensión H323 – señalización	H323-TLS	✓	Hombre	Cliente	n / A	Opción TLS desde R10.0 en adelante VerSeguridad de punto final VoIP de IP Office 127para más detalles.
Extensión H323 – aprovisionamiento	HTTPS	✓	Hombre	Bi	✓	VerSeguridad de punto final VoIP de IP Office 127para más detalles.
Aprovisionamiento DECT R4	HTTPS	✓	Hombre	Bi	✓	VerSeguridad de punto final VoIP de IP Office 127para más detalles.
Aprovisionamiento D100	HTTP	✗	n / A	n / A	n / A	
Línea IP Office	HTTPS	✓	Hombre	Bi	✓	WebSocket
Administrador de IP Office - Seguridad	TLS	✓	Hombre	Bi	✓	Gerente y Gerente SE
Administrador de IP Office - Configuración	TLS	✓	Hombre	Bi	✓	Gerente y Gerente SE
SoftConsole	HTTPS	✓	Hombre	oferta pública inicial	✓	WebSocket
SSA	TLS	✓	Hombre	oferta pública inicial	✗	
Administrador web de IP Office (único)	HTTPS	✓	Hombre	Bi	✓	Administración de instancia única de IP Office Web Manager a través del puerto 8443
Administrador web de IP Office (solución)	HTTPS	✓	Hombre	Cliente	✗	Administración de IP Office Web Manager Server Edition a través del puerto 7070
Directorio del sistema	HTTPS	✓	Hombre	Bi	✓	Función de directorio externo central
Portal one-X para IP Office CTI	TCP	✗	n / A	n / A	n / A	
CTI del IPOCC	TLS	✓	Hombre	Servidor	✓	IP Office es el servidor
ACCS CTI	TLS	✓	Hombre	Servidor	✓	IP Office es el servidor

Enlace	Protocolo	Soporte de certificado	Certificado de identificación Ofrecido[1]	Certificado de confianza cheques[2]	Comprobación de certificado Control[3]	notas
Directorio one-X Portal para IP Office	HTTPS	✓	Hombre	Servidor	✓	IP Office es el servidor
Buzón de voz profesional	HTTPS	✓	Hombre	Servidor	✓	IP Office es el servidor
Cliente de copia de seguridad/restauración	HTTPS	✓	Hombre	Cliente	✓	
Monitoreo del sistema	HTTPS	✓	Hombre	Servidor	✓	IP Office es el servidor
Buzón de voz profesional						
Estado de one-X Portal para IP Office	TCP	✗	n / A	n / A	n / A	Estado del mensaje
one-X Portal para reproducción de máquinas virtuales de IP Office	HTTPS	✓	Hombre	✗	✗	
Cliente de Exchange WS	HTTPS	✓	Hombre	Servidor	n / A	
Cliente SFTP	SSHv2	✓				Exportación de correo de voz y datos de grabación
Portal one-X para IP Office						
Navegador one-XP/Llamada Asistente	HTTPS	✓	Hombre[4]	Cliente	✗	
Complemento de Outlook, SalesForce, Lync	HTTPS	✓	Hombre[4]	Cliente	✗	
one-X Móvil Android	HTTPS	✓	Hombre[4]	Cliente	✗	VerSeguridad de punto final VoIP de IP Office 127para más detalles.
iOS móvil one-X	XMPP-TLS	✓	Hombre[4]	Cliente	✗	VerSeguridad de punto final VoIP de IP Office 127para más detalles.
Ventanas del comunicador	HTTPS	✓	Hombre[4]	Cliente	✗	VerSeguridad de punto final VoIP de IP Office 127para más detalles.
Comunicador iOS	XMPP-TLS	✓	Hombre[4]	Cliente	✗	VerSeguridad de punto final VoIP de IP Office 127para más detalles.
Servidor Linux						
Servidor de copia de seguridad/restauración	HTTPS	✓	Hombre	Cliente	✗	
control web	HTTPS	✓	Hombre	Cliente	✗	
Servidor SSH	SSHv2	✓				
Servidor SFTP	SSHv2	✓				
Servidor WebLM						
Administrador web	HTTPS	✓	Hombre	Cliente	✗	WebLM es el servidor
Registrador de contactos						
Administrador web	HTTPS	✓	Hombre	Cliente	✗	Contact Recorder es el servidor

Tabla 25: Compatibilidad con certificados de aplicaciones de IP Office

Notas:

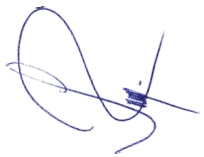
1. Tipo de certificado de identidad presentado:
   - **Teléfono**–Telefonía o Gestión (configurable).
   - **Hombre**–Certificado de gestión.

2. Soporte y dirección de controles de confianza de certificados:
   - **Bi**–Se pueden habilitar comprobaciones de certificados mutuos.
   - **Servidor**–Solo el servidor puede comprobar los certificados.
   - **Cliente**–Solo el cliente puede comprobar los certificados.

3. El color indica la agrupación de los controles de verificación de certificados en el componente del servidor de IP Office:

Color	Control	notas
✓	Gerente de Seguridad:**Sistema | Certificados | Comprobaciones de certificados recibidos (Telefonía)**	Cualquier ajuste que no sea Ninguno solicitará un certificado de cliente Consulte Controles de comprobación de certificados 52para mayor información.
✓	Gerente de Seguridad:**Sistema | Servicios | HTTP | Nivel de seguridad del servicio** Gerente de Seguridad:**Sistema | Certificados | Comprobaciones de certificados recibidos (Gestión)**	VerControles de comprobación de certificados 52para mayor información.
✓	Configuración del administrador:**Línea | Línea | Seguridad**	La configuración del nivel de seguridad del servicio HTTP se aplica primero. Esto permite que el servidor HTTPS general tenga deshabilitadas las verificaciones de certificados, pero aún retenga la verificación de las líneas de IP Office.
✓	Gerente de Seguridad:**Sistema | Servicios | Administración de Seguridad | Nivel de seguridad del servicio** Gerente de Seguridad:**Sistema | Certificados | Comprobaciones de certificados recibidos (Gestión)**	VerControles de comprobación de certificados 52para mayor información.
✓	Gerente de Seguridad:**Sistema | Servicios | Configuración | Nivel de seguridad del servicio** Gerente de Seguridad:**Sistema | Certificados | Comprobaciones de certificados recibidos (Gestión)**	VerControles de comprobación de certificados 52para mayor información.
✓	Gerente de Seguridad:**Sistema | Servicios | Servicios web | Nivel de seguridad del servicio** Gerente de Seguridad:**Sistema | Certificados | Comprobaciones de certificados recibidos (Gestión)**	VerControles de comprobación de certificados 52para mayor información.
✓	Gerente de Seguridad:**Sistema | Certificados | Comprobaciones de certificados recibidos (Gestión)**	Los clientes HTTP de IP Office verificarán el certificado del servidor con el TCS para obtener una configuración de Medio o Alto Consulte Controles de comprobación de certificados 52para mayor información.
✓	Gerente de Seguridad:**Sistema | Interfaces no seguras | TAPI = sin marcar**	IP Office verificará el certificado del servidor ACCS o IPOCC con el TCS según una configuración de Medio VerControles de comprobación de certificados 52para mayor información.

4. Portal one-X para IP Office en el servidor de Windows utiliza un certificado de identificación administrado por separado.



10.6 Apéndice F - Seguridad de extremos VoIP de IP Office

La siguiente tabla proporciona una descripción general de los diversos aspectos de seguridad de los terminales de Avaya con respecto a IP Office.

- Nota: Se debe consultar la documentación relevante del punto final o del servidor, ya que las funciones admitidas pueden variar según la versión.

Oficina IP VoIP punto final	Seguro Medios de comunicación	Seguro Señalización[13]	Seguro Remoto Ajustes[1]	Oficina de PI Generación automática Ajustes	SORBO Apoyo	Validar ¿Certificado de servidor?	ID de oferta ¿Certificado?[7]	¿Se requiere el nombre alternativo del sujeto de IP Office?[8]
Extremo Avaya H.323								
9608, 9611, 9621 y 9641	✓	✓ o parcial[2]	✓	✓[10]	n / A	✓	✓	DNS.1: FQDN de IP Office IP.1: Dirección IP de IP Office LAN1 IP.2: Dirección IP de IP Office LAN2 IP.3: Dirección IP pública si es remota.[14]
Otros 9600 Los telefonos	✗	✗	✓	✓	n / A	✓	✓	✗
Serie 1600	✗	✗	✗	✓	n / A	✓	✓	✗
DECT R4	✗	✗	✓	✓	n / A	✓	✓	✗
Oficina de PI[3]	✓	✓	✓	n / A	n / A	✓	✓	✗
Buzón de voz profesional[4]	✗	✗	✓	n / A	n / A	✗	✗	✗
Terminal SIP de Avaya								
9608, 9611, 9621, 9641[5]	✓	✓	✓	✗	✓	✓	✓	✗
1100/1200 Serie[9]	✓[11]	✓	✓	✓	✗	✓	✓	IP.1: dirección IP de IP Office LAN1 IP.2: dirección IP de IP Office LAN2 IP.3: dirección IP pública si es remota
B179	✓[11]	✓	✓	✓	✓	✓	✓	✗
E129	✓	✓	✓	✓	✓	✓	✓	DNS.1: FQDN de IP Office DNS.2: dirección IP de IP Office si el teléfono está configurado para conectarse al servidor SIP usando la dirección IP en lugar de FQDN[14] SIP URI: dirección IP de IP Office
E159	✗	✗	✗	✓	✗	✗	✗	✗
E169	✗	✗	✗	✓	✗	✗	✗	✗
H175	✓[11]	✓	✓	✓[11]	✓	✓	✓	DNS: nombre de dominio SIP
J129[9]	✓	✓	✓	✓	✓	✓	✓	IP.1: dirección IP de IP Office LAN1[14] IP.2: dirección IP de IP Office LAN2[14] IP.3: Dirección IP pública si es remota[14] URI.1: 'sip': SIP FQDN[14]

Oficina IP VoIP punto final	Seguro Medios de comunicación	Seguro Señalización[13]	Seguro Remoto Ajustes[1]	Oficina de PI Generación automática Ajustes	SORBO Apoyo	Validar ¿Certificado de servidor?	ID de oferta ¿Certificado?[7]	¿Se requiere el nombre alternativo del sujeto de IP Office?[8]
J139, J159, J169, J179	✓	✓	✓	✓	✓	✓	✓	DNS.1: FQDN de IP Office IP.1: dirección IP de IP Office LAN1[14] IP.2: dirección IP de IP Office LAN2[14] IP.3: Dirección IP pública si es remota[14] URI.1: 'sip': SIP FQDN[14]
K155, K165, K175 (Ventaja)	✓	✓	✓	✓	✓	✓	✓	DNS.1: FQDN de IP Office IP.1: dirección IP de IP Office LAN1[14] IP.2: dirección IP de IP Office LAN2[14] IP.3: Dirección IP pública si es remota[14]
Serie Scopia XT	✓	✓	n / A	✗	✓[6]	✓	✓	DNS.1: FQDN de IP Office IP.1: dirección IP de IP Office LAN1[14] IP.2: dirección IP de IP Office LAN2[14] IP.3: Dirección IP pública si es remota.[14]
Comunicador iPad[12]	✓	✓	n / A	✗	✓[6]	✓	✗	✗
Comunicador ventanas[12]	✓	✓	n / A	✗	✓[6]	✓	✗	✗
iOS móvil one-X	✓	✓	n / A	✗	✓[6]	✓	✗	✗
one-x móvil Androide	✓	✓	n / A	✗	✗	✓	✗	DNS.1: FQDN de IP Office IP.1: dirección IP de IP Office LAN1[14] IP.2: dirección IP de IP Office LAN2[14] IP.3: dirección IP pública de IP Office si es remota[14]
DECT SIP D100	✗	✗	✗	✓	✗	✗	✗	✗
Lugar de trabajo	✓	✓	✓	✓	✓	✓	✓	DNS.1: FQDN de IP Office IP.1: dirección IP de IP Office LAN1[14] IP.2: dirección IP de IP Office LAN2[14] IP.3: Dirección IP pública si es remota.[14]
Extremo Avaya WebRTC								
Web de IP Office Cliente	✓	✓	n / A	✗	n / A	✓	✗	DNS.1: FQDN de IP Office IP.1: dirección IP de IP Office LAN1[14] IP.2: dirección IP de IP Office LAN2[14] IP.3: Dirección IP pública si es remota.[14]

Tabla 26: Seguridad de terminales de VoIP

Notas:

1. Capacidad para que el teléfono descargue ajustes y configuraciones de manera remota y segura, generalmente a través de HTTPS.

2. Cuando no se utiliza H323-TLS, la señalización no está totalmente protegida, pero sí el registro, el intercambio de claves SRTP y los dígitos marcados.

3. Línea IP Office con WebSocket y seguridad activa.

4. Enlace entre Voicemail Pro y su IP Office anfitrión. Para Server Edition y Unified Communications Module, este es un enlace interno.

5. Los teléfonos SIP 9608, 9611, 9621 y 9641 solo se admiten como usuarios centralizados en una implementación de sucursal.

6. SIPS siempre activo cuando se selecciona Señalización segura.

7. IP Office no solicita certificados de clientes SIP para el SIPAGS- Sesión TLS en la actualidad. Puede solicitar un certificado para cualquier transferencia HTTPS de acuerdo con la **Autenticacion mutua**ajuste; verControles de comprobación de certificados 52para mayor información..

8. Esta columna indica si el cliente requiere la compatibilidad con el nombre alternativo del sujeto dentro del certificado de identidad recibido de IP Office.
   Por lo general, si se usa DNS, el terminal de VoIP solo requiere el FQDN de IP Office en la SAN y ninguna dirección IP. Las direcciones IP y los nombres de dominio privados no son compatibles con las autoridades de certificación públicas.

9. Los teléfonos de las series 1100/1200 y J129 no admiten FQDN y, por lo tanto, no se pueden usar con certificados proporcionados por autoridades de certificación públicas.

10. IP Office puede aprovisionar el certificado CA raíz de IP Office al teléfono automáticamente mediante el archivo de configuración generado automáticamente. Consulte el capítulo Configuración de terminales de Implementación de OnAvaya™ y Powered by Avaya IP Office e IP Office Contact Center para socios comerciales para obtener más información.

11. Los medios directos están deshabilitados cuando SRTP está habilitado.

12. El cliente no es totalmente compatible con TLSv1.2; cuando la configuración de administración de one-X Portal for IP Office 'TLS v1.2 clients only' está activa, Communicator para Windows no se conectará, Communicator para iPad funcionará, pero sin la presencia de XMPP.

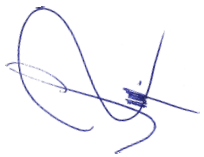
13. Cuando la resiliencia de puntos finales de VoIP está activa con señalización segura o aprovisionamiento seguro, el certificado de CA raíz para el servidor principal y el de respaldo debe ser el mismo.

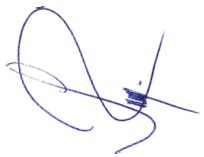
14. Las entradas de la dirección IP del certificado solo se requieren si están configuradas para conectarse al servidor de señalización mediante la dirección IP. A menos que se trate de una implementación privada y cerrada que utilice la CA principal, no se recomiendan las direcciones IP.

15. El teléfono no es compatible con RTCP seguro (SRTCP).

16. 16. Si se deben usar entradas de dirección IP para el dispositivo con CA públicas que no pueden tener entradas de nombre de dirección IP, algunos archivos de configuración del teléfono se pueden mejorar para usar la entrada FQDN_IP_MAP. Esto asigna entradas de direcciones IP a FQDN. Consulte la documentación del teléfono correspondiente para obtener soporte de esta función. Si se utiliza la función de archivo de configuración de generación automática de IP Office, la entrada FQDN_IP_MAP se puede agregar a un archivo '46xxspecials.txt' en la misma ruta donde se pueden encontrar los archivos binarios del teléfono. Por ejemplo, para asignar direcciones IP a FQDN solo para teléfonos 9608, 9611, 9621 y 9641:

```
IF $MODEL4 SEQ 9608 GOTO 96X1SETTINGS IF
$MODEL4 SEQ 9611 GOTO 96X1SETTINGS IF
$MODEL4 SEQ 9621 GOTO 96X1SETTINGS IF
$MODEL4 SEQ 9641 GOTO 96X1SETTINGS GOTO
END
#96X1AJUSTES
ESTABLECER FQDN_IP_MAP "ipol.ca.avaya.com=10.136.100.70,ipol2.ca.avaya.com=10.136.100.74"
# FINAL
```





10.7 Apéndice G: uso de la autoridad de certificación de IP Office

La función de autoridad de certificación (CA) de Linux Application Server y Server Edition Primary se puede utilizar para:

- Genere un certificado de identidad para el propio servidor.
- Genere certificados de identidad para otros dispositivos, incluidos los sistemas, teléfonos y servidores de IP Office.
- Importe un nuevo certificado de firma.
- Actualice el certificado de firma existente.

Se puede acceder a la función CA a través de IP Office Web Manager**Vista de la plataforma | Configuración | Certificados | Certificados de Identidad**.

10.7.1 Generación del Certificado de Identidad Propio del Servidor CA

De forma predeterminada, la CA interna crea y firma automáticamente el propio certificado de identidad de los servidores de aplicaciones Linux o principal. También se vuelve a generar automáticamente si se cambia la dirección IP de LAN1, la dirección IP de LAN2 o el nombre de host. Esto está controlado por la configuración de Administración web**Vista de la plataforma | Configuración | Certificados | Certificados de Identidad | Renovar automáticamente**.

Para crear manualmente un certificado de identidad para el servidor de CA:

1. Desmarque la configuración**Vista de la plataforma | Configuración | Certificados | Certificados de Identidad | Crear certificado para una máquina diferente**.
2. Ingrese un nombre de sujeto único si el valor predeterminado ofrecido no es aceptable. VerContenido del nombre del certificado 50 por más información.
3. Introduzca els Asigne nombres alternativos si el valor predeterminado ofrecido no es aceptable. VerContenido del nombre del certificado 50para más información.
   Se recomienda proporcionar un conjunto completo de nombres alternativos de sujetos para garantizar la compatibilidad con varios clientes y puntos finales de Avaya:

   DNS:<FQDN del servidor>, IP:<dirección IP de LAN1>, IP:<dirección IP de LAN2>, IP:<dirección IP pública>, DNS:<dominio SIP>, URI:sip:<dominio SIP>, URI: <dirección IP LAN1>, URI: <dirección IP LAN2>

   Por ejemplo:

   DNS:ejemplo.com, IP:192.168.0.45, IP:192.168.1.45, IP:203.0.113.30, DNS:ejemplo.sip.com, URI:sip:ejemplo.sip.com, URI:192.168.0.45, URI: 192.168.1.45, URL: sorbo: 192.168.0.45

4. Introduzca el número de días de validez del certificado. La fecha/hora de inicio será la hora UTC actual del servidor. La fecha/hora de finalización será la hora de inicio + el número de días. Los certificados de identidad no deben ser válidos por más de tres años (1095 días). Cuanto más largo sea el período, mayor será el riesgo de compromiso del certificado.
5. Introduzca el algoritmo de clave pública. Este debería ser RSA-2048.
6. Introduzca el algoritmo hash seguro. Esto debería ser SHA-256.
7. Verifique la configuración y luego haga clic en**Generar y Aplicar**. Esto hará que el servidor genere y aplique el nuevo certificado a todas las interfaces durante las cuales se producirá la pérdida del servicio.

10.7.2 Generación de certificados de identidad para otros dispositivos

Para crear manualmente un certificado de identidad para otro dispositivo:

1. Verifique la configuración**Vista de la plataforma | Configuración | Certificados | Certificados de Identidad | Crear certificado para una máquina diferente**.
2. Ingrese la IP de la máquina. Esto se usa para crear el nombre del archivo, pero no el certificado en sí; se debe ingresar una dirección IPv4 de ese dispositivo.
3. Introduzca la contraseña; esto se utiliza para proteger el archivo del certificado de identidad y debe cumplir con los requisitos de complejidad.
4. Ingrese un nombre de sujeto único para el dispositivo. VerContenido del nombre del certificado 50para más información.
5. Ingrese cualquier nombre alternativo de sujeto. VerContenido del nombre del certificado 50para más información.
6. Introduzca el número de días de validez del certificado. La fecha/hora de inicio será la hora UTC actual del servidor. La fecha/hora de finalización será la hora de inicio + el número de días. Los certificados de identidad no deben ser válidos por más de tres años (1095 días). Cuanto más largo sea el período, mayor será el riesgo de compromiso del certificado.
7. Introduzca el algoritmo de clave pública. Debe ser RSA-2048 para todos los dispositivos IP Office. RSA-1024 solo debe usarse para sistemas heredados que no admiten RSA-2048.
8. Introduzca el algoritmo hash seguro. Debe ser SHA-256 para todos los dispositivos de IP Office. SHA-1 solo debe usarse para sistemas heredados que no son compatibles con SHA-256.
9. Verifique la configuración y luego haga clic en Generar. Esto hará que el servidor genere un archivo PKCS#12 que contiene el certificado de identidad, la clave privada y el certificado de firma. El archivo está protegido por la contraseña ingresada y se solicitará cada vez que se abra el archivo.
10. Aparecerá una ventana emergente para guardar el archivo. Guarde el archivo en la máquina local. Una vez que se cierre la ventana emergente, el archivo se eliminará en el servidor de CA.
11. El archivo PKCS#12 ahora puede bmi importado a la implementación de IP Office. VerActualizar certificados 80y Implementación de PKI de IP Office 59para más información.

10.7.3 Exportación del certificado de firma

Si el certificado de firma es un certificado de CA raíz, deberá exportarse en formato PEM y DER para importarlo posteriormente a varios clientes y servidores a fin de confiar en cualquier certificado de identidad creado por esta CA. Esto no exporta la clave privada, solo el certificado.

Para exportar el certificado CA en formato PEM:

1. Seleccione**Vista de la plataforma | Configuración | Certificados | Certificados CA | Descarga (codificación PEM)**.
2. Aparecerá una ventana emergente para guardar el archivo que se llama '***raíz-ca.pem***'. Guarde el archivo en la máquina local para su posterior distribución.

Para exportar el certificado CA en formato DER:

1. Seleccione**Vista de la plataforma | Configuración | Certificados | Certificados CA | Descargar (codificado en DER)**.
2. Aparecerá una ventana emergente para guardar el archivo que se llama '***root-ca.crt***'. Guarde el archivo en la máquina local para su posterior distribución.

10.7.4 Renovación/Reemplazo del Certificado de Firma

Para crear un nuevo certificado de firma:

1. Seleccione**Vista de la plataforma | Configuración | generales | Certificado CA | Crear nuevo**.
2. Esto creará un certificado de CA raíz completamente nuevo y también requerirá nuevos certificados de ID para todas las entidades. El certificado de firma anterior se eliminará.

Para conservar todos los certificados de identificación existentes pero actualizar el certificado de firma:

Se debe tener cuidado de no abusar de la comodidad de esta función, ya que cuanto más tiempo permanezcan sin cambios las claves públicas/privadas, mayor será el riesgo de compromiso.

1. Seleccione**Vista de la plataforma | Configuración | generales | Certificado CA | renovar existente**.
2. Esto creará un nuevo certificado con el mismo contenido y claves públicas/privadas, pero con un número de serie y una fecha de inicio/finalización diferentes.
3. Solo esta nueva CA raíz requiere distribución, los certificados de ID vigentes y firmados por la CA anterior seguirán siendo válidos.

Para reemplazar el certificado de firma existente:

1. Seleccione**Vista de la plataforma | Configuración | generales | Certificado CA | Importar**.
2. El formato debe ser PKCS#12.
3. Esto reemplazará el certificado de firma y puede requerir nuevos certificados de identificación para todas las entidades

Para hacer una copia de seguridad del certificado de firma:

1. Seleccione**Vista de la plataforma | Configuración | generales | Certificado CA | Exportar**.
2. Se solicita una contraseña para asegurar el archivo PKCS#12
3. Aparecerá una ventana emergente para guardar el archivo que se llama '***root-ca-p12***'. Guarde el archivo en la máquina local y agregue un '***.p12***' extensión.

Para restaurar el certificado de firma:

1. Seleccione**Vista de la plataforma | Configuración | generales | Certificado CA | Importar**.

10.8 Apéndice H - Solicitudes de firma de certificado

Se puede utilizar uno de los siguientes métodos para obtener certificados de identidad basados en una solicitud de firma de certificado (CSR) basada en texto a una autoridad de certificación (CA) externa. En todos los casos, el servidor utilizado conservará la clave privada y, por lo tanto, debe protegerse.

- Creación de una CSR mediante el complemento de certificados de Microsoft MMC 135
- Creación de una CSR utilizando el paquete OpenSSL 138
- Creación de una CSR mediante la línea de comandos del servidor Linux 140
- Conversión de archivos de certificado 141

Para el servidor de aplicaciones o Server Edition, se puede usar cualquier método, pero no el paquete OpenSSL del servidor de IP Office; otra PC debe crear el CSR y procesar el certificado recibido.

Esta sección contiene procedimientos para usar cada método. Existen procedimientos para convertir archivos de certificados.

10.8.1 Creación de una CSR con el complemento Certificados de Microsoft MMC

Utilice los siguientes procesos.

- Creación de una CSR utilizando el paquete OpenSSL 138
- Creación de una CSR mediante la línea de comandos del servidor Linux 140
- Conversión de archivos de certificado 141

10.8.1.1 Crear la CSR

1. Si la CA seleccionada proporciona instrucciones o utilidades para generar CSR con las herramientas de Microsoft, se pueden usar con preferencia a los siguientes pasos para proporcionar el formato y el contenido correctos. Cualquier duda sobre formato o contenido deberá ser aclarada con la CA.
2. El siguiente paso cubre el uso del complemento de certificados de Microsoft Management Console para generar una CSR y procesar el certificado de identidad firmado. El certificado de identidad residirá en el almacén de certificados personales de la máquina local y no estará activo en ninguna interfaz de máquina de forma predeterminada.
3. Todos los pasos deben seguirse cuidadosamente para evitar errores.
4. Puede encontrar más información sobre las operaciones de complemento y certificado en: https://technet.microsoft.com/en-us/library/cc771157.aspx
5. Asegúrese de que se haya identificado toda la información de nombres (nombre común, nombres de sujetos alternativos, detalles de la organización, etc.)
6. tudeber iniciar sesión y ejecutar la sesión de consola como administrador.
7. Para abrir Microsoft Management Console (MMC):
   una. Hacer clic**comienzo**.
   b. En el cuadro de búsqueda, escriba***mmc***.
   C. Hacer clic**mmc.exe**.
8. Haga clic en**Archivo > Agregar o quitar complemento**.
9. Haga clic en**Certificados > Agregar > Aceptar**.
10. Seleccione**Cuenta de computadora**y haga clic**próximo**.
11. Seleccione**Computadora local**y haga clic**Finalizar**después**OK**.
12. Ampliar**Certificados (equipo local)**.
13. Haga clic derecho**Personal**, luego haga clic**Seleccione Todas las tareas > Operaciones avanzadas > Crear solicitud personalizada**.
14. Haga clic en**próximo**.
15. Seleccione**Proceder sin política de inscripción**y haga clic**próximo**.
16. Seleccione**(Sin plantilla) Clave heredada**.
17. Seleccione**PKCS #10**y haga clic**próximo**.
18. En la sección Información del certificado, haga clic en el botón de flecha junto a**Detalles**y haga clic**Propiedades**.
19. En el**General**ficha, escriba el nombre de dominio del certificado en el**Nombre amigable**campo.
20. En el**Tema**pestaña, en la**Nombre del tema**campo, ingrese la información a continuación, haciendo clic en**Agregar**después de ingresar cada tipo:

Escribe	Valor	notas
País	Nombre del país (código de 2 letras)	El nombre del país es un código de 2 letras definido por https://www.iso.org/obp/ui/#home ; seleccione Códigos de países y haga clic en buscar por ejemplo, EE. UU.
Estado	Nombre del estado o provincia	no debe ser abreviado
Localidad	Nombre de la localidad	por ejemplo, ciudad
Organización	Nombre de la Organización	por ejemplo, Nombre de la empresa
Unidad de organización	Nombre de la sección/departamento	por ejemplo, TI
Nombre común	FQDN del servidor	por ejemplo, www.ejemplo.com
Correo electrónico	Correo electrónico de contacto	por ejemplo, contacto@ejemplo.com

21. No se deben agregar las entradas no requeridas (por ejemplo, Nombre de la unidad organizativa) o no solicitadas por la CA.

Página1799 de 3226.

22. Si el CSR es para un certificado multidominio/SAN, en el campo Nombre alternativo, ingrese la información a continuación, haciendo clic en **Agregar**después de ingresar cada tipo:

Escribe	Valor	notas
DNS	Entrada DNS SAN	El primer campo de Nombre alternativo debe ser DNS con el mismo valor que el Nombre común. por ejemplo, www.example.com por ejemplo, example.com
dirección IP (v4)	Entrada IP SAN	por ejemplo, 192.168.0.42 por ejemplo, 192.168.0.44
URL	Entrada URI SAN	por ejemplo, sip:example.com por ejemplo, 192.168.0.42

23. En la pestaña Extensión, seleccione**Uso de clave**.

24. Seleccione**no repudio**,**Firma digital**,**Cifrado clave**,**Cifrado de datos**, haciendo clic**Agregar** después de ingresar cada opción.

25. Deseleccionar**Haga que estos usos clave sean críticos**.

26. En la pestaña Extensión, seleccione**Uso extendido de claves**.

27. Seleccionar**Autenticación del servidor**,**Autenticación del cliente**, haciendo clic**Agregar**después de ingresar cada opción.

28. Deseleccionar**Hacer que el uso extendido de claves sea crítico**.

29. En el**Llave privada**pestaña, seleccione**Proveedor de servicios criptográficos**, Seleccione**Proveedor criptográfico fuerte de Microsoft (cifrado)**solamente.

30. En la pestaña Clave privada, seleccione**tipo de clave**, Seleccione**Intercambio**.

31. En la pestaña Clave privada, seleccione**Opciones de clave > Tamaño de clave**y establezca el valor en***2048***.

32. Seleccione**Hacer exportable la clave privada**. Nota: Este paso es importante.

33. Si se presenta, seleccione**Seleccionar algoritmo hash**, Seleccione**Algoritmo hash**y establezca el valor en***sha256***.

34. Revisar todas las entradas; comprobar el**Opciones de clave > Tamaño de clave**, todavía está establecido en el valor de***2048***.

35. Haga clic en**OK**después**próximo**.

36. Ingrese el nombre de archivo (por ejemplo, su dominio) y la ubicación para guardar el CSR. Asegurar**Base 64**es seleccionado. Hacer clic**Finalizar**.

37. Abra el archivo CSR yourdomain.req en un editor de texto y copie todo el texto, incluidas las líneas de inicio y finalización.

38. Vaya a la CA y siga las instrucciones para pegar el CSR completo en el formulario de inscripción SSL de la CA. Si se solicita, el software de servidor utilizado para generar la CSR se puede especificar como Microsoft o Microsoft IIS 7. Si se solicita, se debe seleccionar SHA-256 para el algoritmo hash. No se debe utilizar SHA-1.

10.8.1.2 Descargar e Importar el Certificado de Identidad Firmado

1. Después de la aprobación y generación, reciba/descargue los archivos del certificado de la CA. Debe haber dos o más archivos:

   - El certificado de identidad firmado que debe estar en formato PKCS#7/P7B o PEM
   - Cero, uno o más certificados intermedios en formato PEM

2. El certificado raíz debe descargarse en formato PEM y DER y reservarse para su posterior distribución a los sistemas IP Office.

3. Copie todo en el directorio CSR original.

4. VerNombre y formato del archivo de certificado 42para obtener más información sobre los formatos de archivo de certificado.

5. En el mismo servidor en el que se creó la solicitud de certificado, abra el complemento Certificados de MMC para la cuenta Equipo local.

6. Ampliar**Certificados (equipo local)**.

7. Haga clic derecho**Personal**, luego haga clic**Seleccione Todas las tareas > Importar**.

8. Haga clic en**próximo**.

9. Examine y seleccione el certificado de identidad firmado recibido de la CA, luego haga clic en Abrir.

10. Asegúrese de que estas opciones estén siempre seleccionadas:

    - **Marque la clave privada exportable**

Página1800 de 3226.

- **Importar todas las propiedades extendidas**
- **Importar todos los Certificados en la Cadena**

11. Haga clic en**próximo**.

12. Seleccione**Coloque todos los certificados en la siguiente tienda**. Por debajo**Almacén de certificados**, Cerciorarse**Personal**es seleccionado. y haga clic**próximo**.

13. Complete el Asistente de importación de certificados y haga clic en**Finalizar**.

14. Verifique que haya un ícono de llave en el nuevo certificado, si no, la clave privada no está presente.

15. Repita el proceso de importación para importar los archivos de certificados intermedios; no habrá ningún icono de llave con estos nuevos certificados. Nuevamente, estos deben ir al almacén de certificados personales.

16. Seleccione el certificado de identidad y haga clic en**Abierto**, Seleccione**Detalles**y verifique que el contenido sea el esperado. Seleccione **Ruta de certificación**y verifique que todos los certificados estén presentes en el certificado raíz.

10.8.1.3 Exportar el Certificado de Identidad Firmado

1. El certificado de identidad y su clave privada, certificado(s) raíz e intermedio(s) ahora están almacenados en el almacén de certificados personales de la máquina local. Estos ahora se pueden exportar en un formato apropiado para IP Office.

2. En el mismo servidor en el que se creó la solicitud de certificado, abra el complemento Certificados de MMC para la cuenta Equipo local.

3. Ampliar**Certificados (equipo local)**.

4. Haga clic con el botón derecho en el certificado de identidad (el que tiene el icono de llave), luego haga clic en**Seleccione Todas las tareas > Exportar**, haga clic **próximo**.

5. Seleccione**Sí, exportar la clave privada**, haga clic**próximo**.

6. Seleccione:**Intercambio de información personal - PKCS #12 (.PFX)**,**Exportar todas las propiedades extendidas**, y **Incluya todos los certificados en la ruta de certificación si es posible**.

7. Cuando se le solicite, debe usar una contraseña segura para proteger el archivo. Esta contraseña se solicitará cuando se importe posteriormente a IP Office.

8. Haga clic en**próximo**.

9. Ingrese un nombre de archivo (por ejemplo, su dominio) y luego haga clic en**próximo**, después**Finalizar**. El archivo del certificado de identidad tudominio.pfxdebe ser renombradotudominio.p12.

10. El archivo PKCS#12tudominio.p12ahora tiene el certificado de identidad, la clave privada y todos los certificados intermedios.

11tudominio.p12ahora se puede importar a la implementación de IP Office mediante IP Office o IP Office Web Manager. Consulte la documentación pertinente yImplementación de PKI de IP Office 59para más información.

12. Los archivos de certificado intermedio, raíz y yourdomain.p12 deben conservarse y utilizarse con fines de recuperación.

- **Nota:**Siempre se requerirá una contraseña para abrir el archivo PKCS#12.

10.8.2 Creación de una CSR utilizando el paquete OpenSSL

Utilice los siguientes procesos.

- Creación de una CSR mediante el complemento de certificados de Microsoft MMC 135
- Creación de una CSR mediante la línea de comandos del servidor Linux 140
- Conversión de archivos de certificado 141

10.8.2.1 Crear la CSR

1. El paquete OpenSSL es un producto de terceros y Avaya no puede proporcionar seguridad ni garantía de propósito de ninguna forma.

2. OpenSSL está disponible para máquinas Microsoft Windows y Linux. Verhttps://www.openssl.org/ . Lo siguiente se probó en Windows OpenSSL de 64 bits, versión 1.0.2d.

3. Todos los pasos deben seguirse cuidadosamente para evitar errores.

4. Si la CA seleccionada proporciona instrucciones o utilidades para el uso de OpenSSL, se deben utilizar con preferencia a los siguientes pasos. Cualquier duda sobre formato o contenido deberá ser aclarada con la CA.

5. Asegúrese de que se haya identificado toda la información de nombres (nombre común, nombres de sujetos alternativos, detalles de la organización, etc.)

6. Debe iniciar sesión y ejecutar la sesión de consola como administrador.

7. Cree un directorio para la CSR y la clave y cámbielo.

8. Cree un archivo de texto openssl.cfg con el siguiente contenido, asegúrese de que no haya saltos de línea adicionales:

[requisito]
nombre_distinguido = req_nombre_distinguido
req_extensions = v3_req
aviso = no
[req_nombre_distinguido]
nombre del país =Nombre del país (código de 2 letras) nombre del estado o de la provincia =Nombre del estado o provincia (no abreviado) nombre de la localidad =Nombre de la localidad (por ejemplo, Ciudad) nombre de la organización =Nombre de la organización (por ejemplo, empresa) nombreUnidadOrganizacional =Nombre de la unidad organizativa (por ejemplo, Sección/Departamento) nombrecomún =Nombre común (por ejemplo, www.example.com) dirección de correo electrónico =Dirección de correo electrónico (por ejemplo, contact@example.com) [v3_req]

keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 =www.ejemplo.com
DNS.2 =ejemplo.com
IP.1 =203.0.113.30
IP.2 =203.0.113.40
URI.1 =sip:ejemplo.com URI.2
=203.0.113.30
URI.3 =sorbo: 203.0.113.30

9. Los artículos enrojodebe sustituirse por la información específica del CSR. Asegurarse de que la información solicitada por la CA se suministre con precisión.

10. El nombre del país es un código de 2 letras definido porhttps://www.iso.org/obp/ui/#home ; seleccione Códigos de países y haga clic en Buscar.

11. Cualquier entrada no requerida (por ejemplo, Nombre de la unidad organizativa) o no solicitada por la CA puede eliminarse eliminando la línea completa.

12. Si el certificado es para un solo dominio, elimine todas las líneas desujetoAltName = @alt_namesy en adelante

13. Si el certificado es para varios dominios, la primera entrada de alt_name debe ser DNS.1 y la misma que el nombre común (por ejemplo, www.example.com).

14. Cree la CSR y la clave privada utilizando la línea de comando, asegurándose de que no haya saltos de línea. Los elementos en rojo deben reemplazarse con el nombre de dominio del dispositivo.

openssl req -nuevo -fueraejemplo.csr -nueva clave rsa:2048 -sha256 -keyoutejemplo.key -config abre SSL.cfg

¿Comentarios sobre este documento? infodev@avaya.com

15. Cuando se solicite ('Ingresar frase de contraseña PEM'), se debe ingresar una contraseña segura para el archivo de clave privada. Esto se solicitará más adelante al combinar el certificado firmado.

16. Verifique el CSR con la línea de comando:openssl req -text -noout -verify -inejemplo.csr

17. Verifique que la salida sea la esperada.

18. Abra el archivo CSRejemplo.csr en un editor de texto y copie todo el texto

19. Vaya a la CA y siga las instrucciones para pegar el CSR completo en el formulario de inscripción SSL de la CA. Si se solicita, el software de servidor utilizado para generar la CSR es OpenSSL u 'Otro'. Si se solicita, se debe seleccionar SHA-256 para el algoritmo hash. SHA-1 no debe seleccionarse.

20. Mantenga elejemploArchivo .key para su uso posterior. Tenga en cuenta que siempre se requerirá una contraseña para abrir el archivo clave.

10.8.2.2 Descargar y Combinar el Certificado de Identidad Firmado

1. Después de la aprobación y generación, reciba/descargue los archivos del certificado de la CA. Debe haber dos o más archivos:

- El certificado de identidad firmado que debe estar en formato PEM
- Cero, uno o más certificados intermedios que deben estar en formato PEM

2. Si hay opciones de descarga, seleccionar 'Otro' o 'Apache' debería proporcionar el formato correcto.

3. Copie todo en el directorio CSR original. Cambie el nombre del certificado de identidad al nombre de dominio con una extensión .crt.

4. El certificado raíz debe descargarse en formato PEM y DER y reservarse para su posterior distribución a los sistemas IP Office.

5. Si hay más de un archivo de certificado intermedio: en el directorio CSR original, combine todos los archivos de certificado intermedio en un solo archivo usando la única línea de comando:

   cat intermedio1.crt intermedio2.crt intermedio3.crt > intermedios.crt

6. En el directorio CSR original, una los archivos en un solo archivo PKCS#12 junto con el archivo de certificado intermedio usando la única línea de comando:

   openssl pkcs12 -exportación -in ejemplo.crt -certfile intermedios.crt -inkey ejemplo.key - salida ejemplo.p12

7. Cuando se le solicite ('Ingrese frase de contraseña para ejemplo.clave'), se debe ingresar la contraseña utilizada para proteger el archivo de clave privada al crear el CSR.

8. Cuando se le solicite ('Ingrese la contraseña de exportación'), se debe usar una contraseña segura para proteger el archivo de salida PKCS#12. Esta contraseña se solicitará cuando se importe posteriormente a IP Office.

9. Revise el PKCS#12 con la línea de comando:openssl pkcs12 -info -in ejemplo.p12

10. Deben estar presentes el certificado de identidad, la clave privada y todos los intermediarios.

11. El archivo de certificado de ID ejemplo.p12 e intermedios.crt ahora se pueden importar a la implementación de IP Office usando gramo IP Office o IP Office Web Manager. Consulte la documentación pertinente yImplementación de PKI de IP Office [59]para más información.

12. Los archivos de certificado example.key, example.p12, raíz e intermedio deben conservarse y utilizarse con fines de recuperación.

- **Nota:**Siempre se requerirá una contraseña para abrir el PKCS#12 y el archivo de clave.

10.8.3 Creación de una CSR mediante la línea de comandos del servidor Linux

Utilice los siguientes procesos.

- Creación de una CSR mediante el complemento de certificados de Microsoft MMC 135
- Creación de una CSR utilizando el paquete OpenSSL 138
- Conversión de archivos de certificado 141

10.8.3.1 Crear la CSR

Todos los pasos deben seguirse cuidadosamente para evitar errores.

1. Inicie sesión en la máquina IPOL a través del servicio SSH como administrador, ingrese al menú de certificados en la pestaña de administración
2. Aquí el usuario puede comenzar a crear el CSR llenando los parámetros SN y SAN.
3. Con la ayuda del comando csr_subjectName, el usuario puede/debe especificar los siguientes parámetros: País/Estado/Localidad/ Organización/Unidad de organización/Nombre común/Correo electrónico como se define en la tabla de parámetros de CSR anterior en los campos de nombre de sujeto.
4. No se deben agregar las entradas no requeridas (por ejemplo, Nombre de la unidad organizativa) o no solicitadas por la CA.
5. Si el CSR es para un certificado SAN/multidominio, el usuario tiene la posibilidad de agregar entradas en los campos SAN con la ayuda del comando csr_subjectAltName (agregar). Los valores válidos son DNS (entrada DNS SAN), IP (entrada IPv4 SAN), URI (entrada URI SAN). Podemos especificar múltiples valores para cada entrada, numerándolos como por ejemplo: DNS.1=test1csr.com, DNS.2=test2csr.com.
6. Cuando se hayan completado todos los parámetros de la CSR, el usuario debe verificar la configuración de generación de la CSR con la ayuda del comando csr_view_parameters. El comando mostrará la configuración actual para el CSR. El usuario debería ver algo similar en la pantalla de la consola:

   [requerimiento]
   nombre_distinguido = req_nombre_distinguido
   req_extensions = v3_req
   aviso = no
   [req_distinguished_name] C=US

   ST=Tennessee
   L = Nashville
   O=CSRsPrueba
   OU=CSRsTestDep
   CN=testcsr.com
   dirección de correo electrónico =
   admin@testcsr.com [v3_req]
   basicConstraints = CA: FALSO
   keyUsage = firma digital, no repudio, acuerdo de clave, cifrado de datos, cifrado de clave subjectAltName = @alt_names

   subjectKeyIdentifier = hash
   [alt_names]
   DNS.1=testcsr.com
   IP.1=192.168.42.1
   URI.1=sip:testcsr.com

7. Luego, el usuario debe ejecutar el comando generate_csr que generará la CSR, almacenará la clave privada de la CSR en una ubicación a la que solo puede acceder la raíz y mostrará la CSR generada en la consola.
8. El usuario debe copiar desde la consola el CSR generado (es decir, verlo como texto que comienza con ----- COMENZAR SOLICITUD DE CERTIFICADO----- cadena y termina con -----FINALIZAR SOLICITUD DE CERTIFICADO- ---- cuerda.
9. El CSR se puede pegar en un archivo de texto y se puede firmar en una CA pública o privada, lo que da como resultado un certificado firmado basado en un CSR generado en la máquina IPOL.

10.8.3.2 Descargar y Combinar el Certificado de Identidad Firmado

1. Después de la aprobación y la generación, reciba o descargue los archivos del certificado de la CA.
2. El usuario puede importar un certificado firmado en CLI en el menú admin/certificados con la ayuda del **import_certid** dominio. Este comando no necesita ningún argumento. Después de la invocación, la CLI espera la entrada de un certificado firmado que comienza con la cadena -----BEGIN CERTIFICATE----- y termina con la cadena - - - - - FINALIZAR CERTIFICADO-----. El certificado debe estar en formato pem (texto).
3. Si el certificado es válido (el texto del certificado es válido y también se basa en un CSR generado en la misma máquina ipol), la máquina ipol importará el certificado a la aplicación ipoffice.
4. Tras una operación exitosa, se informará al usuario sobre una operación exitosa.
5. El usuario podrá leer y configurar el indicador de distribución de certificados a través del**read_distribution_flag**y **establecer_distribución_bandera**(activado/desactivado), por lo que el certificado seguirá siendo el predeterminado solo para la aplicación ipoffice (indicador de distribución desactivado) o se distribuirá para todas las aplicaciones en la máquina (indicador de distribución activado).

10.8.4 Conversión de archivos de certificado

El archivo intermedio.crt puede estar en formato PEM o DER; es formato PEM si se puede ver con un editor de texto.

Si se requieren otros formatos, se puede usar OpenSSL:

Para convertir PEM a DER:
openssl x509 -outform der -in intermedio.crt -out intermedio.der

Para convertir DER a PEM:
openssl x509 -inform der -in intermedio.crt -out intermedio.pem

Para convertir PKCS#7 a PEM:
openssl pkcs7 –print_certs -certificado de entrada.pb7 -certificado de salida.pem

Para convertir PKCS#7 y clave privada a PKCS#12:
openssl pkcs7 –print_certs -certificado de entrada.pb7 -certificado de salida.pem
openssl pkcs12 -exportar -in certificado.pem -inkey llave privada.clave -certificado.pfx - archivo de certificado CAcert.cer

Se le pedirá una clave de cifrado para el archivo PKCS#12 resultante.

Para convertir el certificado PEM y la clave privada a PKCS#12:
openssl pkcs12 -exportación -in certificado.pem -inkey clave privada.pem - certificado.pfx

Se le pedirá una clave de cifrado para el archivo PKCS#12 resultante. También se le puede pedir la contraseña de la clave privada.

VerNombre y formato del archivo de certificado 42para más información.

10.9 Apéndice I: Aprovisionamiento seguro de teléfonos H.323 de la serie 9600

Puede configurar puntos finales 9608, 9611, 9621 y 9641 H.323 con o sin preparación. El proceso de puesta en escena es el más seguro.

En la alternativa menos segura sin preparación, el teléfono no autentica el servidor con la conexión HTTPS inicial. Si la conexión telefónica inicial a HTTPS es secuestrada en el servidor de archivos de un atacante, el teléfono puede confiar en el servidor de archivos fraudulento.

En implementaciones con requisitos de seguridad más estrictos donde este riesgo no es aceptable, los teléfonos deben instalarse en un entorno controlado.

10.9.1 Proceso de Estadificación Recomendado

Prepare el servidor de archivos en el centro de ensayo. Puede ser una IP Office que actúe como servidor de archivos y posiblemente también como servidor DHCP, o puede ser otro servidor de archivos HTTP. Los siguientes pasos enumeran los archivos que deben colocarse en el servidor de archivos de ensayo:

1. Coloque el archivo de actualización de teléfonos y los archivos de firmware en el servidor de archivos de ensayo.
2. Coloque el certificado de la CA raíz que firmó el certificado de identidad de IP Office en la nube (o la CA raíz que firmó la CA intermedia superior en la cadena de certificados del certificado de identidad de IP Office) en el servidor de archivos provisional.
3. Edite el archivo de configuración de teléfonos por cliente para que contenga la siguiente configuración y colóquelo en el servidor de archivos de prueba:
4. **NVTLSSRVR**, **NVHTTPSRVR** y **NVMCIPADD** -las tres configuraciones deben especificar el nombre DNS (FQDN) de la instancia de IP Office en la nube. Este FQDN será resuelto por DNS a la dirección IP pública de la instancia de IP Office en la nube. Tenga en cuenta que la instancia de IP Office en la nube para cada cliente tendrá un FQDN y una dirección IP pública diferentes, por lo tanto, el archivo de configuración debe editarse para los teléfonos provisionales de cada cliente.
5. Como alternativa a lo anterior, la dirección IP del servidor HTTPS, la dirección IP del servidor HTTP y la dirección IP del servidor de llamadas se pueden configurar manualmente en cada teléfono mediante la interfaz de usuario de CRAFT. Pero dado que programar teléfonos manualmente a través de CRAFT UI puede llevar mucho tiempo, el método preferido es configurar los parámetros usando el archivo de configuración de preparación según la viñeta anterior.
6. **ESTABLECER CERTIFICADOS DE CONFIANZA** <nombre de archivo del certificado CA raíz>
7. **ESTABLECER TLSSRVRVERIFYID 1** -Este es un parámetro nuevo en los teléfonos 9608, 9611, 9621 y 9641 H.323 R6.5. Cuando se establece en 1, el teléfono verificará la identidad del servidor en las conexiones TLS, lo cual se recomienda por seguridad. El teléfono verificará que el nombre DNS del servidor TLS (como se establece en **NVTLSSRVR**) coincide con el nombre común o subjectAltName en el certificado del servidor.
8. Conecte el teléfono a la red del centro de ensayo y proporcione la dirección IP del servidor de archivos de ensayo, desde DHCP o desde la interfaz de usuario del teléfono.
9. El teléfono se comunicará con el servidor de archivos de prueba a través de HTTP y descargará los archivos de actualización y configuración, el certificado de CA raíz de confianza y los archivos de firmware, si es necesario.
10. Después de la preparación, el teléfono se envía al sitio del cliente.
11. El teléfono está conectado a la LAN en el sitio del cliente y encendido.
12. El teléfono se comunica con IP Office en la nube a través de HTTPS sobre TLS, utilizando la dirección IP de NVTLSSRVR que obtuvo previamente del archivo de configuración provisional y utilizando el puerto 411 (el valor predeterminado del teléfono es TLSPORT). El puerto 411 debe estar abierto en el firewall de la nube y en IP Office. Se establecerá una conexión TLS autenticada, ya que el teléfono verificará el certificado de identidad (o la cadena de certificados de identidad) que IP Office en la nube ofrece en la conexión TLS, cotejándolo con el certificado de CA raíz confiable que obtuvo el teléfono durante la preparación.
13. El teléfono obtendrá el *96x1Hupgrade.txt* archivo y el generado automáticamente *46xxconfiguraciones.txt* archivo desde la nube de IP Office a través de la conexión HTTPS/TLS. El teléfono también obtendrá los archivos de idioma de IP Office en la nube a través de HTTPS.
14. El 46xxsettings.txt generado automáticamente especificará **PUERTO HTTP 8411**. El número de puerto 8411 debe estar abierto en el firewall de la nube, mientras que el puerto 80 probablemente estará cerrado.
15. Esto se basa en una mejora en IP Office. El puerto 8411 está codificado en Linux IP Office y está abierto para acceso HTTP restringido, lo que permite que solo los teléfonos IP de Avaya obtengan solo archivos de firmware.
16. IP Office incluye la configuración **PUERTO HTTP 8411** en el archivo 46xxsettings.txt generado automáticamente que se envía a un teléfono si y solo si la solicitud del archivo de configuración vino en HTTPS (no HTTP) e IP Office determina que el teléfono se está conectando desde Internet. IP Office toma esta determinación si la dirección IP de origen de la solicitud no es una dirección privada RFC 1918 y no está en la red privada del cliente, como se puede especificar opcionalmente en **NUSN "DIRECCIÓN_PRIVADA"**.
17. Si el nuevo firmware del teléfono está disponible en IP Office en la nube, como se indica en el archivo de actualización, el teléfono lo obtendrá de IP Office en la nube a través de HTTP en el puerto 8411 según lo especificado por HTTPPORT en el 46xxsettings.txt generado automáticamente.
18. Garantizar durante el aprovisionamiento inicial el impacto de una gran cantidad de conjuntos que realizan descargas de firmware.

Página1806 de 3226.

10.9.2 Proceso automatizado

1. Asegúrese de que el certificado de CA raíz, que se utilizó para firmar el certificado de identidad de IP Office, esté instalado en el almacén de certificados de confianza de IP Office.
2. Si la política de confianza seleccionada para IP Office utiliza una CA pública conocida, descargue el certificado de CA raíz con codificación PEM del sitio web de la CA e instálelo en el almacén de certificados de confianza de IP Office mediante IP Office. Modo de seguridad del administrador**Sistema | Certificados | Almacén de certificados de confianza | Agregar**.
3. Si la política de confianza seleccionada para IP Office utiliza su propia CA interna, entonces el certificado de CA raíz ya estará en el almacén de certificados de confianza de IP Office.
4. Asegúrese de que el certificado de identidad de IP Office incluya un campo Nombre alternativo del sujeto que contenga la dirección IP pública de IP Office.
5. Esto es necesario para que los teléfonos puedan verificar la identidad del servidor, cuando los teléfonos están configurados para conectarse a la dirección IP pública de IP Office. No es necesario cuando los teléfonos se configuran mediante preparación para conectarse al FQDN de IP Office.
6. Si IP Office utiliza un certificado de identidad generado por su propia CA interna, entonces debe generar un nuevo certificado de identidad con la dirección IP pública en Nombre alternativo del sujeto. Precaución: Vuelva a generar solo el certificado de identidad y no desactivenorte volver a generar necesariamente el certificado de CA raíz, lo que puede ser perjudicial (consulte Cambio de un certificado de CA raíz 143).
7. Configure en cada teléfono los siguientes parámetros a través del menú CRAFT del teléfono: Dirección IP del servidor HTTPS, Dirección IP del servidor HTTP y Dirección IP del servidor de llamadas. Los tres parámetros deben establecerse en la dirección IP de IP Office.

8. El teléfono se reinicia, se pone en contacto con IP Office y obtiene e instala automáticamente el certificado de CA raíz de IP Office.

10.9.3 Cambio de un certificado de CA raíz

Precaución: Cambiar la CA raíz que firmó el certificado de identidad de IP Office puede bloquear los teléfonos instalados que se aprovisionaron previamente para confiar solo en la CA raíz anterior. Evite hacer esto innecesariamente. Si se va a instalar un certificado de identidad firmado por una CA externa en IP Office, esto debe hacerse antes de instalar los teléfonos si es posible.

Si es necesario cambiar la CA raíz, debe hacerse con precaución y requerirá un esfuerzo administrativo:

Una opción es realizar un paso de preparación antes de cambiar el certificado de identidad de IP Office; coloque un archivo de configuración editado manualmente en IP Office con TRUSTCERTS especificando tanto la CA raíz actual como el nuevo archivo de CA raíz, y coloque ambos archivos de CA raíz en la tarjeta/disco SD. Luego reinicie todos los teléfonos. Los teléfonos se conectarán con éxito a IP Office, obtendrán el nuevo archivo de configuración y obtendrán e instalarán la nueva CA raíz de confianza. Luego, cambie el certificado de identidad de IP Office y elimine el archivo de configuración editado manualmente. La próxima vez que los teléfonos se conecten, confiarán en el nuevo certificado de identidad.

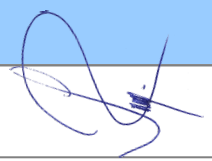
Otra opción es borrar la configuración del teléfono usando CRAFT en todos los teléfonos 96x1 y luego repetir la configuración de la dirección del servidor en cada teléfono.

No se requiere ningún esfuerzo si el teléfono usa HTTP y no HTTPS para obtener el archivo de configuración (lo que puede no ser posible en todos los entornos). La próxima vez que el teléfono se reinicie, obtendrá automáticamente un nuevo archivo de configuración (con el nuevo nombre de TRUSCERT) y buscará la nueva CA raíz.

10.10 Apéndice J - Dependencias de seguridad de aplicación/cliente

Las siguientes tablas brindan una descripción general de los componentes de IP Office y sus dependencias en varias configuraciones de seguridad de IP Office.

Aplicaciones

Componente de IP Office	Controles de interfaz	Iniciar sesión Cuenta	Certificado de IP Office Usar	Otros controles	notas
Gerente de IP Office	Servicio IP Office: - Configuración (segura) - Administración de seguridad (segura) Interfaz heredada: - Código de programa	Usuario del servicio	Sí: - Gestión		Código de programa utilizado solo para la actualización de Manager de IP500 V2
Gestión Web	Servicio IP Office: - Servicios web	Usuario del servicio	Sí: - Gestión		
control web	Servicio IP Office: - Externo	Usuario del servicio	Sí: - Gestión		
Buzón de voz profesional	Servicio IP Office: - HTTP (seguro)	Mensaje de voz clave	Sí: - Gestión		
Portal one-X para IP Office	Servicio IP Office: - EnhTSPI Interfaz heredada: - Lectura del directorio HTTP - Escritura de directorio HTTP	Usuario del servicio	No		
SSA	Servicio IP Office: - Aplicación de estado del sistema	Usuario del servicio	Sí: - Gestión		
SoftConsole	Servicio IP Office: -HTTP	Usuario de IP Office	Sí: - Gestión		
Monitoreo del sistema	Servicio IP Office: -HTTP Interfaz heredada: -DevLink	Usuario del servicio o Monitor clave	Sí: - Gestión	System Monitor usará un usuario de servicio cuando el **Seguridad | Sistema | Interfaces no seguras | Usar credenciales de usuario del servicio**está activo	
TAPI	Interfaz heredada: -TAPI	Sistema clave	No		El instalador TAPI requiere el servicio TAPI de IP Office habilitado
DevLink	Interfaz heredada: -DevLink	Monitor clave	No		El instalador de DevLink requiere que el servicio DevLink de IP Office esté habilitado (?)
Registrador de contactos	Ninguna	Interno a Contacto Grabadora		Desactivar servicio en Web Control	

Componente de IP Office	Controles de interfaz	Iniciar sesión Cuenta	Certificado de IP Office Usar	Otros controles	notas
Cliente WebRTC	Servicio IP Office: - Externo	Usuario del servicio			Ver el cliente WebRTC a continuación
Estación base maestra DECT R4	Servicio IP Office: - HTTP (seguro) Interfaz heredada: - Lectura del directorio TFTP	Usuario del servicio	Sí: - Gestión		Consulte la extensión DECT R4 a continuación
ACC		Interno a ACCS			Consulte la documentación de ACCS
IPOCC		Interno a IPOCC			Ver documentación de IPOCC
WebLM	Deshabilitar servicio	Interno a WebLM			Consulte la documentación de WebLM

Líneas

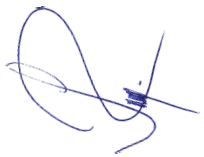
Componente de IP Office	Controles de interfaz	Iniciar sesión Cuenta	Certificado de IP Office Usar	Otros controles	notas
Línea IP Office	Servicio IP Office: -HTTP	Línea IP Office clave	Sí: - Gestión		
Línea SIP	Eliminar línea SIP	Línea SIP	Sí: - Gestión - Telefonía		
Analógico/Digital	Quitar línea	No	No		Las líneas analógicas/ digitales no se pueden eliminar

Clientes UC

Componente de IP Office	Controles de interfaz	Iniciar sesión Cuenta	Certificado de IP Office Usar	Otros controles	notas
Comunicador de Avaya	Servicio one-X Portal para IP Office	Usuario de IP Office	Sí: - Gestión	HTTPS solo se puede habilitar mediante la configuración Protocolo | Seguro Conexión (HTTPS)	
one-x móvil	Servicio one-X Portal para IP Office	Usuario de IP Office	Sí: - Gestión		Solo se puede habilitar HTTPS
Navegador one-XP/Llamada Asistente	Servicio one-X Portal para IP Office	Usuario de IP Office	Sí: - Gestión		Solo se puede habilitar HTTPS
Complemento de Outlook, SalesForce, Lync	Servicio one-X Portal para IP Office	Usuario de IP Office	Sí: - Gestión		Solo se puede habilitar HTTPS
Colaboración web	Servicio one-X Portal para IP Office	Usuario de IP Office	Sí: - Gestión		Solo se puede habilitar HTTPS
WebRTC	Servicio WebRTC Registrador SIP	Usuario de IP Office	Sí: - Gestión		**Página1809 de 3226.**

Extensión

Componente de IP Office	Controles de interfaz	Iniciar sesión Cuenta	Certificado de IP Office Usar	Otros controles	notas
DECT R4	Línea IP DECT	Usuario de IP Office, SARI/ PARQUE	No	DECT de creación automática extensión	
H.323	Registrador H323	Usuario de IP Office O Extensión clave	Sí: - Gestión	Crear automáticamente H323 extensión	Solo se puede habilitar TLS
SORBO	Registrador SIP	Usuario de IP Office	Sí: - Gestión	SIP de creación automática extensión	
Analógico/Digital	No	Usuario de IP Office	No		Analógico/Digital las extensiones no pueden ser remoto



Capítulo 11.

Historia del documento

11. Historial del documento

Fecha	Tema	Resumen de cambios
23 de septiembre de 2020	05a	Actualizaciones para R11.1 SP1. Alinear con ADMS168370 Versión 13.
28 de octubre de 2020	05b	Eliminar enlace externo obsoleto.
5 de marzo de 2021	05c	Aclaración ronda contraseña del servidor de correo de voz en 11.1 FP1 o superior.

© 2021 AVAYA Todos los derechos reservados.

Aviso

Si bien se han realizado esfuerzos razonables para garantizar que la información de este documento sea completa y precisa en el momento de la impresión, Avaya no asume ninguna responsabilidad por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información de este documento sin la obligación de notificar a ninguna persona u organización sobre dichos cambios.

Descargo de responsabilidad de la documentación

"Documentación" hace referencia a la información publicada por Avaya en varios medios que pueden incluir información sobre productos, instrucciones de funcionamiento y especificaciones de rendimiento que Avaya generalmente puede poner a disposición de los usuarios de sus productos y servicios alojados. La documentación no incluye materiales de marketing. Avaya no será responsable de ninguna modificación, adición o eliminación de la versión original publicada de la documentación, a menos que Avaya haya realizado dichas modificaciones, adiciones o eliminaciones. El usuario final acepta indemnizar y eximir de responsabilidad a Avaya, a los agentes, servidores y empleados de Avaya frente a todos los reclamos, juicios, demandas y sentencias que surjan de, o en relación con, modificaciones, adiciones o eliminaciones posteriores a esta documentación, en la medida en que sean realizadas por Usuario final.

Descargo de responsabilidad del enlace

Avaya no es responsable del contenido o la confiabilidad de los sitios web vinculados a los que se hace referencia en este sitio o la documentación proporcionada por Avaya. Avaya no es responsable de la precisión de la información, declaración o contenido proporcionado en estos sitios y no respalda necesariamente los productos, servicios o información descritos u ofrecidos en ellos. Avaya no garantiza que estos enlaces funcionen todo el tiempo y no tiene control sobre la disponibilidad de las páginas enlazadas.

Garantía

Avaya proporciona una garantía limitada para el hardware y el software de Avaya. Consulte su contrato de venta para establecer los términos de la garantía limitada. Además, el lenguaje de la garantía estándar de Avaya, así como la información sobre el soporte para este producto mientras está bajo garantía, está disponible para los clientes de Avaya y otras partes a través del sitio web de Soporte de Avaya: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 en el enlace "Garantía y ciclo de vida del producto" o en el sitio sucesor designado por Avaya. Tenga en cuenta que si adquirió los productos de un socio de canal autorizado de Avaya fuera de los Estados Unidos y Canadá, dicho socio de canal de Avaya le proporciona la garantía y no Avaya.

"Servicio alojado" hace referencia a una suscripción de servicio alojado que adquiere de Avaya o de un socio de canal autorizado de Avaya (según corresponda) y que se describe con más detalle en Hosted SAS u otra documentación de descripción del servicio con respecto al servicio alojado aplicable. Si compra una suscripción al Servicio alojado, es posible que la garantía limitada anterior no se aplique, pero puede tener derecho a servicios de soporte en relación con el Servicio alojado, como se describe más adelante en los documentos de descripción del servicio para el Servicio alojado correspondiente. Comuníquese con Avaya o con el socio de canal de Avaya (según corresponda) para obtener más información.

Servicio alojado

LO SIGUIENTE SE APLICA SI COMPRA UNA SUSCRIPCIÓN AL SERVICIO ALOJADO DE AVAYA O DE UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA), LOS TÉRMINOS DE USO PARA LOS SERVICIOS ALOJADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO BAJO EL ENLACE Los "Términos de uso de Avaya para servicios alojados" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, Y SON APLICABLES A CUALQUIER PERSONA QUE ACCEDA O UTILICE EL SERVICIO ALOJADO. AL ACCEDER O UTILIZAR EL SERVICIO ALOJADO, O AL AUTORIZAR A OTROS A HACERLO, USTED, EN SU NOMBRE Y EN EL DE LA ENTIDAD PARA LA QUE LO ESTÁ HACIENDO (EN ADELANTE DENOMINADO INTERCAMBIABLEMENTE COMO "USTED" Y "USUARIO FINAL"), ACEPTA LOS TÉRMINOS DE USO. SI USTED ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR DICHA ENTIDAD A ESTOS TÉRMINOS DE USO. SI USTED NO TIENE TAL AUTORIDAD, O SI NO DESEA ACEPTAR ESTOS TÉRMINOS DE USO, NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEMPRE QUE PARA CIERTOS SERVICIOS ALOJADOS SI CORRESPONDE, PUEDE TENER LA OPORTUNIDAD DE UTILIZAR LICENCIAS FLEX, QUE SERÁN FACTURADO SEGÚN EL USO REAL POR ENCIMA DEL NIVEL DE LICENCIA DEL CONTRATO. CONTACTE A AVAYA O AL SOCIO DEL CANAL DE AVAYA PARA OBTENER MÁS INFORMACIÓN SOBRE LAS LICENCIAS PARA EL SERVICIO ALOJADO CORRESPONDIENTE, LA DISPONIBILIDAD DE CUALQUIER LICENCIA FLEX (SI CORRESPONDE), PRECIOS E INFORMACIÓN DE FACTURACIÓN, Y OTRA INFORMACIÓN IMPORTANTE RELACIONADA CON EL SERVICIO ALOJADO. NO DEBE ACCEDER O UTILIZAR EL SERVICIO ALOJADO NI AUTORIZAR A NADIE A ACCEDER O UTILIZAR EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEMPRE QUE PARA CIERTOS SERVICIOS ALOJADOS SI CORRESPONDE, PUEDE TENER LA OPORTUNIDAD DE UTILIZAR LICENCIAS FLEX, QUE SERÁN FACTURADO SEGÚN EL USO REAL POR ENCIMA DEL NIVEL DE LICENCIA DEL CONTRATO. CONTACTE A AVAYA O AL SOCIO DEL CANAL DE AVAYA PARA OBTENER MÁS INFORMACIÓN SOBRE LAS LICENCIAS PARA EL SERVICIO ALOJADO CORRESPONDIENTE, LA DISPONIBILIDAD DE CUALQUIER LICENCIA FLEX (SI CORRESPONDE), PRECIOS E INFORMACIÓN DE FACTURACIÓN, Y OTRA INFORMACIÓN IMPORTANTE RELACIONADA CON EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEMPRE QUE PARA CIERTOS SERVICIOS ALOJADOS SI CORRESPONDE, PUEDE TENER LA OPORTUNIDAD DE UTILIZAR LICENCIAS FLEX, QUE SERÁN FACTURADO SEGÚN EL USO REAL POR ENCIMA DEL NIVEL DE LICENCIA DEL CONTRATO. CONTACTE A AVAYA O AL SOCIO DEL CANAL DE AVAYA PARA OBTENER MÁS INFORMACIÓN SOBRE LAS LICENCIAS PARA EL SERVICIO ALOJADO CORRESPONDIENTE, LA DISPONIBILIDAD DE CUALQUIER LICENCIA FLEX (SI CORRESPONDE), PRECIOS E INFORMACIÓN DE FACTURACIÓN, Y OTRA INFORMACIÓN IMPORTANTE RELACIONADA CON EL SERVICIO ALOJADO. SU USO DEL SERVICIO ALOJADO ESTARÁ LIMITADO POR EL NÚMERO Y EL TIPO DE LICENCIAS ADQUIRIDAS BAJO SU CONTRATO PARA EL SERVICIO ALOJADO, SIEMPRE QUE PARA CIERTOS SERVICIOS

Licencias

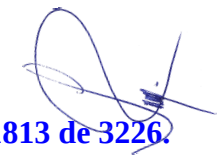
LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, BAJO EL ENLACE "TÉRMINOS DE LICENCIA DE SOFTWARE DE AVAYA (Productos de Avaya)" O EL SITIO SUCESOR SEGÚN LO DESIGNE AVAYA, SON APLICABLES A CUALQUIER PERSONA QUE DESCARGUE , UTILIZA Y/O INSTALA EL SOFTWARE DE AVAYA, COMPRADO DE AVAYA INC., CUALQUIER AFILIADO DE AVAYA O UN SOCIO DE CANAL DE AVAYA (SEGÚN CORRESPONDA) EN VIRTUD DE UN ACUERDO COMERCIAL CON AVAYA O UN SOCIO DE CANAL DE AVAYA. A MENOS QUE AVAYA ACORDE LO CONTRARIO POR ESCRITO, AVAYA NO EXTENDERÁ ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE CUALQUIER PERSONA QUE NO SEA AVAYA, UNA AFILIADA DE AVAYA O UN SOCIO DE CANAL DE AVAYA; AVAYA SE RESERVA EL DERECHO DE TOMAR ACCIONES LEGALES CONTRA USTED Y CUALQUIER OTRA PERSONA QUE UTILICE O VENDA EL SOFTWARE SIN LICENCIA. AL INSTALAR, DESCARGAR O UTILIZAR EL SOFTWARE O AUTORIZAR A OTROS A HACERLO, USTED,

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el cual el alcance de la licencia se detalla a continuación. Cuando la documentación del pedido no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de Sistema Designado. El número aplicable de licencias y unidades de capacidad para las que se otorga la licencia será uno (1), a menos que se especifique un número diferente de licencias o unidades de capacidad en la documentación u otros materiales disponibles para Usted. "Software" hace referencia a los programas informáticos en código objeto, proporcionados por Avaya o un socio de canal de Avaya, ya sea como productos independientes, preinstalados en productos de hardware y cualquier mejora, actualización, parche, corrección de errores o versiones modificadas de los mismos. "Procesador Designado" significa un único dispositivo informático independiente. "Servidor" se refiere a un Procesador designado que alberga una aplicación de software a la que pueden acceder varios usuarios. "Instancia" significa una única copia del Software que se ejecuta en un momento determinado: (i) en una máquina física; o (ii) en una máquina virtual de software implementada ("VM") o implementación similar.

Tipos de licencia

Licencia de sistema(s) designado(s) (DS). El Usuario final puede instalar y usar cada copia o una Instancia del Software solo en una cantidad de Procesadores designados hasta la cantidad indicada en el pedido. Avaya puede solicitar que los Procesadores designados se identifiquen en el pedido por tipo, número de serie, clave de función, Instancia, ubicación u otra designación específica, o que el Usuario final los proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este objetivo.

Licencia de Usuario Concurrente (CU). El Usuario final puede instalar y utilizar el Software en varios Procesadores designados o en uno o más Servidores, siempre que solo el número de Unidades con licencia acceda y utilice el Software en un momento dado. Una "Unidad" significa la unidad en la que Avaya, a su sola discreción, basa el precio de sus licencias y puede ser, sin limitación, un agente, puerto o usuario, una cuenta de correo electrónico o correo de voz a nombre de una persona. o función corporativa (por ejemplo, webmaster o servicio de asistencia), o una entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software. Las Unidades pueden vincularse a un Servidor específico e identificado oa una Instancia del Software.



Licencia de base de datos (DL). El Usuario final puede instalar y utilizar cada copia o una Instancia del Software en un Servidor o en varios Servidores, siempre que cada uno de los Servidores en los que se instala el Software se comunique con no más de una Instancia de la misma base de datos.

Licencia de CPU (CP). El Usuario final puede instalar y utilizar cada copia o Instancia del Software en una cantidad de Servidores hasta la cantidad indicada en el pedido, siempre que la capacidad de rendimiento de los Servidores no exceda la capacidad de rendimiento especificada para el Software. El usuario final no puede volver a instalar ni operar el software en servidores con una mayor capacidad de rendimiento sin el consentimiento previo de Avaya y el pago de una tarifa de actualización.

Licencia de usuario nominal (NU). Usted puede: (i) instalar y usar cada copia o Instancia del Software en un solo Procesador o Servidor Designado por Usuario Designado autorizado (definido a continuación); o (ii) instalar y usar cada copia o Instancia del Software en un Servidor, siempre que solo los Usuarios designados autorizados accedan y usen el Software. “Usuario designado” hace referencia a un usuario o dispositivo que ha sido expresamente autorizado por Avaya para acceder y utilizar el Software. A discreción exclusiva de Avaya, un "Usuario designado" puede ser, entre otros, designado por nombre, función corporativa (por ejemplo, webmaster o servicio de asistencia), una cuenta de correo electrónico o de correo de voz en nombre de una persona o función corporativa, o un entrada de directorio en la base de datos administrativa utilizada por el Software que permite a un usuario interactuar con el Software.

Licencia Shrinkwrap (SR). Puede instalar y utilizar el Software de acuerdo con los términos y condiciones de los acuerdos de licencia aplicables, como la licencia "retractil" o "clickthrough" que acompaña o se aplica al Software ("Licencia Shrinkwrap").

Software de la herencia de Nortel

“Software Heritage Nortel” significa el software que fue adquirido por Avaya como parte de su compra de Nortel Enterprise Solutions Business en diciembre de 2009. El software Heritage Nortel es el software incluido en la lista de productos Heritage Nortel que se encuentra en https://support. .avaya.com/LicenseInfo bajo el enlace "Productos de Heritage Nortel" o el sitio sucesor designado por Avaya. Para el software Heritage Nortel, Avaya otorga al cliente una licencia para usar el software Heritage Nortel proporcionado a continuación únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la Documentación, y únicamente como está integrado, para su ejecución en , o para comunicación con equipos Avaya.

Derechos de autor

Salvo que se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, la documentación, el software, el servicio alojado o el hardware proporcionado por Avaya. Todo el contenido de este sitio, la documentación, el Servicio alojado y el producto proporcionado por Avaya, incluida la selección, disposición y diseño del contenido, es propiedad de Avaya o de sus otorgantes de licencias y está protegido por derechos de autor y otras leyes de propiedad intelectual, incluida la ley sui generis. derechos relativos a la protección de las bases de datos. No puede modificar, copiar, reproducir, volver a publicar, cargar, publicar, transmitir o distribuir de ninguna manera ningún contenido, en su totalidad o en parte, incluido cualquier código y software, a menos que Avaya lo autorice expresamente. La reproducción, transmisión, difusión, almacenamiento o uso no autorizados sin el consentimiento expreso por escrito de Avaya puede ser un delito,

virtualización

Lo siguiente se aplica si el producto se implementa en una máquina virtual. Cada producto tiene su propio código de pedido y tipos de licencia. Tenga en cuenta que cada Instancia de un producto se debe licenciar y pedir por separado. Por ejemplo, si el cliente usuario final o el socio de canal de Avaya desea instalar dos instancias del mismo tipo de productos, entonces se deben pedir dos productos de ese tipo.

Componentes de terceros

"Componentes de terceros" significa que ciertos programas de software o partes de los mismos incluidos en el Software o el Servicio alojado pueden contener software (incluido el software de código abierto) distribuido bajo acuerdos de terceros ("Componentes de terceros"), que contienen términos relacionados con los derechos de uso de ciertos partes del Software ("Términos de terceros"). Según sea necesario, la información sobre el código fuente del sistema operativo Linux distribuido (para aquellos productos que tienen el código fuente del sistema operativo Linux distribuido) y la identificación de los titulares de derechos de autor de los componentes de terceros y los términos de terceros que se aplican está disponible en los productos, la documentación o en el sitio web de Avaya. en: https://support.avaya.com/Copyright o en el sitio sucesor designado por Avaya. Los términos de la licencia de software de código abierto proporcionados como Términos de terceros son consistentes con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del software de código abierto. Los Términos de terceros prevalecerán sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables en la medida en que estos Términos de licencia de software le impongan mayores restricciones que los Términos de terceros aplicables.

Lo siguiente se aplica si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO TIENE LICENCIA BAJO LA LICENCIA DE LA CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS POR LOS QUE NO RECIBE REMUNERACIÓN PARA (i) CODIFICAR VÍDEO EN CUMPLIMIENTO CON EL ESTÁNDAR AVC (“AVC VIDEO”) Y/O (ii) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. SE PUEDE OBTENER INFORMACIÓN ADICIONAL DE MPEG LA, LLC CONSULTE HTTP://WWW.MPEGLA.COM.

Proveedor de servicio

LO SIGUIENTE SE APLICA AL ALOJAMIENTO DE PRODUCTOS O SERVICIOS DE AVAYA POR PARTE DEL SOCIOS DE CANAL DE AVAYA. EL PRODUCTO O EL SERVICIO ALOJADO PUEDE UTILIZAR COMPONENTES DE TERCEROS SUJETOS A TÉRMINOS DE TERCEROS Y REQUIERE QUE UN PROVEEDOR DE SERVICIOS TENGA UNA LICENCIA INDEPENDIENTE DIRECTAMENTE DEL PROVEEDOR DE TERCEROS. EL ALOJAMIENTO DE PRODUCTOS DE AVAYA POR PARTE DE UN SOCIO DE CANAL DE AVAYA DEBE SER AUTORIZADO POR ESCRITO POR AVAYA Y SI DICHOS PRODUCTOS ALOJADOS UTILIZAN O INTEGRAN DETERMINADO SOFTWARE DE TERCEROS, INCLUYENDO, ENTRE OTROS, SOFTWARE O CÓDECS DE MICROSOFT, EL SOCIO DE CANAL DE AVAYA DEBE OBTENER CUALQUIER LICENCIA CORRESPONDIENTE DE FORMA INDEPENDIENTE ACUERDOS, A CARGO DEL SOCIO DE CANAL DE AVAYA, DIRECTAMENTE DEL PROVEEDOR TERCERO CORRESPONDIENTE.

CON RESPECTO A LOS CÓDECS, SI EL SOCIO DE CANAL DE AVAYA ALOJA CUALQUIER PRODUCTO QUE UTILICE O INTEGRA EL CÓDEC G.729, EL CÓDEC H.264 O EL CÓDEC H.265, EL SOCIO DE CANAL DE AVAYA RECONOCE Y ACEPTA QUE EL SOCIO DE CANAL DE AVAYA ES RESPONSABLE DE CUALQUIER Y TODAS LAS TARIFAS Y/O REGALÍAS RELACIONADAS. EL CÓDEC G.729 TIENE LICENCIA DE SIPRO LAB TELECOM INC. CONSULTE WWW.SIPRO.COM/CONTACT.HTML. EL CÓDEC H.264 (AVC) TIENE LICENCIA BAJO LA LICENCIA DE CARTERA DE PATENTES DE AVC PARA EL USO PERSONAL DE UN CONSUMIDOR U OTROS USOS EN LOS QUE NO RECIBE REMUNERACIÓN PARA: (I) CODIFICAR VÍDEO EN CUMPLIMIENTO CON EL ESTÁNDAR AVC (“VIDEO AVC ”) Y/O (II) DECODIFICAR VÍDEO AVC QUE FUE CODIFICADO POR UN CONSUMIDOR INVOLUCRADO EN UNA ACTIVIDAD PERSONAL Y/O FUE OBTENIDO DE UN PROVEEDOR DE VÍDEO CON LICENCIA PARA PROPORCIONAR VÍDEO AVC. NO SE CONCEDE NINGUNA LICENCIA NI SE IMPLÍCITA PARA NINGÚN OTRO USO. INFORMACIÓN ADICIONAL PARA H.

De acuerdo con las leyes

El cliente reconoce y acepta que es responsable de cumplir con las leyes y reglamentaciones aplicables, incluidas, entre otras, las leyes y reglamentaciones relacionadas con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude y los derechos de interpretación musical. , en el país o territorio donde se utiliza el producto Avaya.

Prevención del fraude de llamadas

"Fraude interurbano" es el uso no autorizado de su sistema de telecomunicaciones por parte de una parte no autorizada (por ejemplo, una persona que no es un empleado corporativo, agente, subcontratista o que no trabaja en nombre de su empresa). Tenga en cuenta que puede haber un riesgo de fraude de llamadas asociado con su sistema y que, si ocurre, puede resultar en cargos adicionales sustanciales para sus servicios de telecomunicaciones.

Intervención de fraude de llamadas de Avaya

Si sospecha que está siendo víctima de fraude de llamadas y necesita asistencia o soporte técnico, llame a la línea directa de intervención de fraude de llamadas del Centro de Servicio Técnico al +1-800-643-2353 para los Estados Unidos y Canadá. Para obtener números de teléfono de soporte adicionales, consulte el sitio web de soporte de Avaya: https://support.avaya.com o el sitio sucesor designado por Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de soporte de seguridad de Avaya en la sección Políticas de seguridad y soporte de https://support.avaya.com/security. Las sospechas de vulnerabilidades de seguridad de productos de Avaya se manejan según el Flujo de soporte de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Descarga de Documentación

Para obtener las versiones más recientes de la documentación, consulte el sitio web de soporte de Avaya: https://support.avaya.com, o el sitio sucesor designado por Avaya.

Comuníquese con el soporte de Avaya

Consulte el sitio web de soporte de Avaya: https://support.avaya.com para obtener avisos y artículos sobre productos o servicios alojados, o para informar un problema con su producto o servicio alojado de Avaya. Para obtener una lista de números de teléfono de soporte y direcciones de contacto, vaya al sitio web de Soporte de Avaya: https://support.avaya.com (o el sitio sucesor designado por Avaya), desplácese hasta la parte inferior de la página y seleccione Contacto Soporte Avaya.

Tabla de Figuras

Figura 1: Cifrado simétrico/asimétrico 13
Figura 2: Autenticación de mensajes 14
Figura 3: Marco de autenticación y autorización ..... dieciséis
Figura 4: Asignación de grupos de derechos de servicios 23
Figura 5: Comprobación de clave de aplicación de Avaya 38
Figura 6: Dominio de confianza de PKI 38
Figura 7: Distribución de certificación - Autoridad de certificación externa 53
Figura 8: Distribución de certificados - Autoridad de certificación interna 54
Figura 9: Distribución de certificados - Protocolo simple de inscripción de certificados (SCEP) 54
Figura 10: Distribución de certificados - Autoridad de certificación externa 55
Figura 11: Estructura de almacenamiento de certificados por defecto 118

Mesa de Mesas

Tabla 1: Métodos de seguridad 12
Tabla 2: Algoritmos de cifrado 13
Tabla 3: Autenticación de mensajes 14
Tabla 4: Servicios de IP Office 18
Tabla 5: Niveles de seguridad del servicio 18
Tabla 6: Configuración de seguridad predeterminada 19
Tabla 7: Administrador de seguridad predeterminado 24
Tabla 8: Usuarios de servicio predeterminados 25
Tabla 9: Grupos de derechos predeterminados 26
Tabla 10: Asignaciones de grupos de derechos predeterminados 29
Tabla 11: Contraseñas de usuarios administrativos 35
Tabla 12: Contraseñas de usuario y códigos de inicio de sesión 36
Tabla 13: Formatos de archivo de certificado 42
Tabla 14: Extensiones de nombre de archivo de certificado 42
Tabla 15: Configuración del certificado inicial de IP500 V2 45
Tabla 16: Certificado de CA principal predeterminado 47
Tabla 17: Certificado de identidad principal predeterminado 48
Tabla 18: Certificado Secundario/de Expansión Predeterminado 49
Tabla 19: Opciones de SRTP 69
Tabla 20: Seguridad de Señalización VoIP 70
Tabla 21: Ancho de banda SRTP 71
Tabla 22: Efecto de los Servicios de Inhabilitación 77

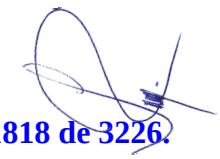
Mesa de Mesas

Tabla 23: Derechos Mínimos de Acceso 78

Tabla 24: Puertos de ejemplo .... .104

Tabla 25: Compatibilidad con certificados de aplicaciones de IP Office 125

Tabla 26: Seguridad de terminales de VoIP 128



Índice

3

3DES 13

A

Acceso
  Físico 96
ACC 94
Administradores
  Clave 34
Avisos 107, 111
AES 13, 68
Algoritmos 13
Software antivirus 17
Servidor de aplicaciones
  Seguro 99
Aplicaciones
  Seguro 88
ASBCE 95
Cifrado asimétrico 13
Audiencia 6
Auditoría 12
Autenticación 12, 14
  Estructura dieciséis
  RTP/RTCP 68
Autorización 12
autorización
  Estructura dieciséis
Cierre de sesión automático 86
Controlador de borde de sesión de Avaya 95

B

Banda ancha
  SRTP 71
Restricción de llamadas 84
  Reenvío 87
  Usuario 85
Mejor esfuerzo 68
Controlador de fronteras 95
Administrador de sucursal 25
Socio comercial 25

C

CA 39
Restricción de llamadas 84
  Reenvío 87
  Usuario 85
Llamar a Seguridad 68
Capacidad
  SRTP 71
CCPA 15
CER 42
Certificado 39
  Comprobaciones de solicitudes de firma de certificados 41 134
  Convertir 141
  Certificados predeterminados 112
  Configuración por defecto 44
  Distribución 53
  Extensión 42
  Nombre del archivo 42
  Formato 42
  Soporte de IP Office 43
  Emisor 40
  Mantenimiento 64
  Nombre Contenido 50
  Llave pública 40
  Renovando 64
  Número de serie 40
  Firma 40
  Nombre alternativo del sujeto 40
  TLS 41
  Política de confianza 56
  Válida desde 40
  Autoridad de certificación de administración de certificados de Windows 39 118
Verificación de identidad de certificado 39
Solicitudes de firma de certificado 134
Certificados 38
  Actualización 80
Cambios 6
Cheques 41
Confidencialidad 12
Confidencial 8
Centro de contacto 94
Registrador de contactos 92
  Informes 106
Convertir
  Archivos de certificado 141
tubo de rayos catódicos 42
RSC 134
CTI 88

D

Integridad de datos 12
Privacidad de datos 15
Defecto
  Configuración del certificado 44
  Certificados 112
  Grupos de Derechos 26
  Administrador de seguridad 24
  Configuraciones de seguridad 19
  Usuarios del servicio 25
valores predeterminados
  cambio 76
DER 42
DES 13
Enlace de desarrollo 19
certificado digital 116
Descargo de responsabilidad 8
Cuotas de disco 17
DNS 50
Cambios en el documento 6
DTL 68

mi

EASG 17
Correo de voz integrado 92
Cifrado 13
  RTP/RTCP 68
TSPI mejorado 18, 19
EnhTcpaService 25
confiar 113
Exportar
  Certificado de Windows 118
Extensión 42
  Cambiar certificado 143
  Seguro 81
  Puesta en escena 142

F

Extensión de nombre de archivo 42
Cortafuegos 17, 95

Página1819 de 3226.

Formato 42
Reenvío 87
FQDN 50

GRAMO

RGPD 15
Global Sign 115
GTS 114

H

Tamaño de hash 14
Escritorio compartido 86
Directorio HTTP 19

yo

RCI 94
Identificación 12
Certificado de Identidad 39
Importación
Certificado de Windows 118
Clasificaciones de información 8
Reportero de llamadas integrado 94
IP 50
Oficina de PI
Certificado 43
Gerente 89
Informes 106
Grupos de derechos 23
Usuarios del servicio 23
Actualizaciones 107
Contraseñas de usuario 36
Administrador web 89
Aplicaciones de IP Office
Seguro 88
Servicios IP Office 18
Servicio IPDECT 25
IPCC 94
ISRG 115
Emisor 40

k

Tamaño de llave 13
Uso clave 40

L

Vamos a cifrar 117
Línea
Seguro 83
Seguridad de la plataforma Linux 17
Teléfono bloqueado 86
Cerrar sesión 86
Código de inicio de sesión 32, 36
Política del sistema 33
Cerrar sesión 86

METRO

Mantenedor 25
Mantenimiento 96
Acceso de mantenimiento 95
gerente 89
MD5 14
Medios de comunicación
Seguro 83
Administrador de medios 94
Seguridad de los medios 68
Autenticación de mensajes 14
Supervisar 90
Monitoreo 102
MPLS 68
Certificado de dominio múltiple 39
Multi-SAN 39
Autenticación mutua 39

norte

NDA 8

O

Portal one-X
Informes 107
Portal one-X para IP Office 93

PAGS

p21 42
Contraseña 32
Contraseñas de administrador 34
Política 79
Política del sistema 33
contraseñas
Usuario 36
pb7 42
PEM 42
Datos Personales 15
pfx 42
Teléfono
Cambiar Certificado 143
Aprovisionamiento 142
Puesta en escena 142
Bloqueo de teléfono 86
Acceso Físico 96
Código PIN 32
Política del sistema 33
PKCS#12 42
PKCS#7 42
Dominio de confianza de PKI
38 Planificación 71
Seguridad de la plataforma 17
Puertos 103
Prevenir
Reenvío 87
Privacidad 15
Propietario 8
Protocolos 103
Público 8
Clave pública 40
Algoritmo de clave pública 40

q

Cuotas 17

R

RC4 13
Acceso de mantenimiento remoto 95
Trabajadores remotos 82
Renovar
Certificados 80
Renovación de Certificados 64
Informes 102
Responsabilidad
Seguridad de IP Office 9
Actualizaciones de seguridad 9
Restringido 8
Grupos de Derechos 23
Predeterminado 26
Asignación predeterminada 27
raíz 17
Certificado raíz CA 39
Certificado raíz 39

Página1820 de 3226.

RTCP 68
RTP 68
S
SAN DNS 50
SBC 95
Seguro
ACC 94
Servidor de aplicaciones 99
Registrador de contactos 92
CTI 88
Correo de voz integrado 92
Extensión 81
Aplicaciones integradas de 94
Call Reporter IP Office 88
Mantenimiento 96
Gerente 89
Medios de comunicación 83
Administrador de medios 94
one-X Portal para el aprovisionamiento de 93
teléfonos de IP Office 142
Servidores Server Edition 97
SSA 90
Monitoreo del sistema 90
Tronco 83
UCM 99
Buzón de voz profesional 91
Administrador web 89
WebLM 89
WebRTC 94
Seguridad
Planificación 71
VoIP 68
Administrador de seguridad 24
Avisos de seguridad 107, 111 Base
de datos de seguridad 14
Servidor
Informes 107
Autenticación del servidor 39
Usuario del servicio 23
Usuarios del servicio
Defecto 25
Remover 76
Grupos de derechos 27
Servicios 18
Defecto 19
Deshabilitar 77
Controlador de borde de sesión 95
SHA-1 14, 68
SHA-2 14
Firma 40
Algoritmo de firma 40
Certificado de dominio único 39
SIP 50
REDCE 87
SRTP 68
Capacidad 71
Solución de problemas 121
SSA 90
Puesta en escena 142
Contraseña segura 32
Sujeto 40
Nombre alternativo del sujeto
40 Symantec 113
Cifrado simétrico 13
Monitoreo del sistema 90
Aplicación de estado del sistema 90
Actualización del sistema 29
T
TAPI 19, 88
TCS 39
Terminología 39
TFTP19
Seguridad de terceros 17
TLS 41
Seguridad de la capa de transporte 41
Resolución de problemas
Certificados 64
SRTP 121
Tronco
Seguro 83
Dominio de confianza 38, 39
Política de confianza 56
Tienda de confianza 39
Certificado de confianza 39
Almacén de certificados de confianza 39
Fuente de confianza 86
tu
UCM
Seguro 99
Certificado de comunicación unificada 39
Actualizar
Certificados 80
Mejora 29
URL 50
Usuario
Código de inicio de sesión 36
contraseñas 36
V
Válido desde 40
Valido Hasta 40
Mensaje de voz
Correo de voz incorporado 92
Informes 106
Fuente de confianza 86
Buzón de voz profesional 91
VoIP 68
Planificación 71
Señalización de Seguridad 70
W
Control web 89
Administrador web 89
Servicios web 19
WebLM 89
Puerta de enlace WebRTC 94
Comodín 50
Certificado comodín 39
Windows
Gestión de certificados 118

Página1821 de 3226.

© 2021 Avaya Inc. Todos los derechos reservados.

Acciones

Navegación: **Administración de llamadas** > **Operadora automática** > **Agregar operadora automática** > **Acciones**

Esta ficha define las acciones que los usuarios que llaman pueden llevar a cabo según la tecla DTMF que presionen. Para cambiar una acción, seleccione la fila correspondiente y haga clic en **Editar**. Cuando la clave esté configurada como se requiere, haga clic en **Aceptar**.

Estos ajustes se pueden editar en línea. Los cambios a estos parámetros no requieren un reinicio del sistema.

Campo	Descripción
Tecla	Las teclas del teclado del teléfono estándar, 0 a 9 más * y #. La opción **Fax** puede utilizarse para una transferencia al destino de fax requerido y luego se activará mediante la detección de tonos de fax. Si se deja **Sin definir**, las llamadas de fax obedecerán la configuración de reserva de las rutas para llamadas entrantes una vez que se haya alcanzado el Tiempo máximo de inactividad de la operadora automática establecido en la ficha Operadora automática | Operadora automática.
Acción Las siguientes acciones pueden asignarse a cada tecla.	
Transferencia de Centrex	Se utiliza para transferir la llamada entrante a un número de teléfono externo definido en el campo **Número de transferencia**. Esta opción es compatible con Embedded Voicemail únicamente.
Marcación por nombre	Se pide a quien realiza la llamada que marque el nombre del usuario que necesita y luego presione #. Luego se reproducen los anuncios de nombre grabado de los usuarios coincidentes para que quien realiza la llamada pueda elegir el que corresponda. La configuración **Marcar por orden de coincidencia de nombres** de la ficha Operadora automática establece el orden de nombres utilizado. Tenga en cuenta que el nombre utilizado es el **Nombre completo del usuario**, si se configuró; de lo contrario, se utilizará el **Nombre de usuario**. No se incluyen los usuarios que no tienen un anuncio de nombre grabado o que estén configurados en **Excluir del directorio**. Para Embedded Voicemail en el modo IP Office, los usuarios pueden grabar su nombre al acceder a su buzón y marcar *05. Para Embedded Voicemail en modo Intuity, se solicita a los usuarios que graben su nombre cuando acceden a su buzón.
Marcación por número	Esta opción permite que quienes llaman con teléfonos DTMF maquen el número de extensión del usuario que requieren. No se establece ningún destino para esta opción. Se debe incluir el aviso para usar esta opción en el saludo con las opciones del menú de la operadora automática. Se requiere un número de extensión con una longitud uniforme para todos los usuarios y los miembros del grupo de búsqueda. La configuración Marcación directa por número de la operadora automática afecta el funcionamiento de esta opción.
Transferencia normal	Se puede utilizar con o sin una configuración de **Destino**. Cuando no existe una configuración de **Destino**, esta acción se comporta como una acción de **Marcación por número**. Cuando hay una configuración de **Destino**, esta acción espera una conexión antes de transferir la llamada. El llamador puede escuchar una música en espera. No se escuchan anuncios.
Sin definir	La tecla correspondiente no tiene ninguna acción.

Página1823 de 3226.

Campo	Descripción
Estacionar y enviar anuncio	La función Estacionar y enviar anuncio se admite cuando la opción **Tipo de correo de voz** del sistema está diseñada como **Embedded Voicemail** o **Voicemail Pro**. La función Estacionar y enviar anuncio también se admite en sistemas en los que la opción **Mensajería modular por SIP** está configurada como el sistema de correo de voz central y **Embedded Voicemail** local proporciona funcionamiento de operadora automática. La función Estacionar y enviar anuncio es una opción en buzón de correo de usuario en donde se configura una tecla con la función Estacionar y enviar anuncio. Cuando el sistema de correo de voz responde una llamada entrante y la persona que llama marca el dígito DTMF en la cual está configurada la función Estacionar y enviar anuncio, la persona que llama escucha el aviso de la función Estacionar y aviso de anuncio. IP Office estaciona la llamada y envía un anuncio a la extensión o grupo de búsqueda designado. Cuando se selecciona la función Estacionar y enviar anuncio en el cuadro desplegable **Acción**, aparecen los siguientes campos: • **Prefijo de posición de estacionamiento:** El número de prefijo de posición de estacionamiento deseado. El máximo es ocho dígitos. Un 0-9 se agregará a este prefijo para formar una Posición de estacionamiento completa. • **Conteo para reintentar:** Número de reintentos de anuncio; el intervalo varía entre 0 y 5. • **Tiempo de espera para reintentar:** Se proporciona en formato M:SS (minuto:segundos). El rango puede ser configurado en incrementos de 15 segundos. La configuración mínima es de 15 segundos y la configuración mínima es de 5 minutos. La configuración predeterminada es de 15 segundos. • **Aviso de anuncio**: Código corto para grabar el aviso de anuncio o cargar la indicación grabada. (La indicación se puede cargar en la tarjeta SD de la misma manera que las indicaciones AA).
Volver a reproducir saludo	Reproducir nuevamente el saludo de la operadora automática.
Transferencia	Transfiere la llamada al destino seleccionado. Se trata de una transferencia no supervisada; si el usuario que llama no obtiene respuesta, la llamada se administra como si fuera una llamada directa a ese número.
Transferencia a una operadora	Esta acción se puede realizar para transferir llamadas a otra operadora automática existente.
Destino	Establece el destino para la acción. El destino puede ser un usuario, un grupo de búsqueda o un código corto. Si el campo de destino se deja en blanco, las personas que llaman pueden marcar el número de extensión del usuario que requieran. Tenga en cuenta que no se proporciona ningún aviso para esta opción; por lo tanto, debe incluirse en el saludo con las opciones del menú de la operadora automática.

Tema principal: Descripciones del campo Agregar operadora automática

©2020 Avaya Inc
All Rights Reserved.

Thu, 23-Jan-2020
(CallMgmtAutoAttendActions.html)

Performance figures, data and operation quoted in this document are typical and must be specifically confirmed in writing by Avaya before they become applicable to any particular order or contract. The company reserves the right to make alterations or amendments at its own discretion. The publication of information in this document does not imply freedom from patent or any other protective rights of Avaya or others.

All trademarks identified by TM or ® are registered trademarks or trademarks respectively are the property of their respective owners.

https://ipofficekb.avaya.com/businesspartner/ipoffice11_0es/mergedProjects/webmanager/CallMgmtAutoAttendActions.html

Operadora automática

Navegación: **Administración de llamadas** > **Operadora automática** > **Agregar operadora automática** > **Operadora automática**

Esta configuración se usa para definir el nombre del servicio de operadora automática y los perfiles horario que deben controlar la reproducción de los saludos de la operadora automática.

Estos ajustes se pueden editar en línea. Los cambios a estos parámetros no requieren un reinicio del sistema.

Campo	Descripción
Nombre	Rango = hasta 12 caracteres Este campo configura el nombre para el servicio de operadora automática. Las llamadas externas pueden dirigirse a la operadora automática ingresando AA:Nombre en el campo de destino de la ruta para una llamada entrante.
Inactividad máxima	Predeterminado = 8 segundos, rango = de 1 a 20 segundos. Este campo define cuánto tiempo debe esperar la operadora automática a que se presione una tecla válida tras la reproducción de los avisos. Si se excede ese tiempo, se desconecta a la persona que llama o se la tranfiere a la extensión alternativa configurada en la Ruta para llamadas entrantes utilizada para la llamada.
Permitir grabación local	Predeterminado = Activado. Cuando está desactivado, se bloquea el uso de los códigos cortos para grabar avisos para la operadora automática. Sin embargo, los códigos cortos sí pueden usarse para reproducir los saludos.
Marcación directa por número	Predeterminado = Desactivado. Esta configuración afecta el funcionamiento de cualquier tecla presionada en el menú de la operadora automática configurada para utilizar la acción **Marcación por número**. Si se lo selecciona, la tecla presionada para la acción se incluye en cualquier dígito siguiente marcado por la persona que llama para la búsqueda de extensiones coincidentes. Por ejemplo, si se configura 2 en las acciones para **Marcación por número**, una persona que llama puede marcar 201 para comunicarse con la extensión 201. Si no se lo selecciona, la tecla presionada para la acción no se incluye en ningún dígito siguiente marcado por la persona que llama para la búsqueda de extensiones del sistema. Por ejemplo, si se configura 2 en las acciones para **Marcación por número**, una persona que llama debe marcar 2 y luego 201 para comunicarse con la extensión 201.
Marcación por orden de coincidencia de nombres	Predeterminado = nombre de pila/apellido. Determina el orden del nombre usado para la función Marcar por nombre de Embedded Voicemail. Las opciones son: • **Primero luego último** • **Último luego primero**

Campo	Descripción
Número AA	Este número es asignado por el sistema y no puede modificarse. Se lo usa junto a los códigos cortos para acceder al servicio de operadora automática o para grabar saludos para la operadora automática.
Mañana/Tarde/Noche/Opciones de menú	Cada operadora automática puede tener tres períodos de tiempo distintos, definidos por los perfiles de hora relacionados. Se puede grabar un saludo para cada período. Las personas que llaman escuchan el saludo correspondiente, seguido por el saludo con las opciones del menú, que debe detallar las acciones disponibles. Las opciones son: • **Perfil de horario** El perfil de horario que define cada período de funcionamiento de la operadora automática. Cuando hay superposiciones o intervalos entre los perfiles de hora, se da prioridad al perfil de la mañana, de la tarde y luego de la noche. • **Código corto** Estos campos indican los códigos de acceso del sistema creados automáticamente para permitir grabar los saludos para los distintos perfiles de horario y el aviso con las opciones del menú. • **Nombre de la grabación**: Predeterminado = En blanco Rango = Hasta 31 caracteres. Este campo aparece al lado del código corto utilizado para grabar manualmente los avisos de la operadora automática. Sólo se lo usa si se utilizan archivos .wav pregrabados como saludo en lugar de grabar manualmente los saludos mediante los códigos cortos indicados. Tenga en cuenta que, si se lo utiliza, este campo distingue mayúsculas y minúsculas y usa el nombre incorporado dentro del archivo .wav en lugar del nombre real del archivo. Este campo puede usarse con todos los sistemas que admiten Embedded Voicemail. La utilidad para convertir archivos .wav en el formato correcta la proporciona Manager y se inicia con las opciones Archivo | Opciones avanzadas | Utilidad de saludos LVM. A continuación, los archivos deben transferirse manualmente a la tarjeta de memoria de Embedded Voicemail. Para obtener información detallada, consulte el Manual de instalación de IP Office Embedded Voicemail.

Tema principal: Descripciones del campo Agregar operadora automática

©2020 Avaya Inc
All Rights Reserved.
Thu, 23-Jan-2020
(CAllMgmtAutoAttendAddAutoAttend.html)

Performance figures, data and operation quoted in this document are typical and must be specifically confirmed in writing by Avaya before they become applicable to any particular order or contract. The company reserves the right to make alterations or amendments at its own discretion. The publication of information in this document does not imply freedom from patent or any other protective rights of Avaya or others.

All trademarks identified by TM or ® are registered trademarks or trademarks respectively are the property of their respective owners.

Traducido del inglés al español - www.onlinedoctranslator.com

Laboratorio de pruebas de soluciones e interoperabilidad de Avaya

Notas de aplicación para Avaya IP Office versión 11.0 y Avaya Session Border Controller for Enterprise versión 8.0.1 con el servicio gratuito de llamadas IP de AT&T mediante IPv6 - Edición 1.0

Resumen

Estas Notas de aplicación describen los pasos para configurar Avaya IP Office 11.0 y Avaya Session Border Controller for Enterprise 8.0.1 con el servicio AT&T IP Toll Free, mediante conexiones de transporte IPv6 y AVPN o MIS/PNT.

El servicio IP Toll Free de AT&T es una solución de comunicaciones de voz sobre IP (VoIP) administrada que brinda servicios gratuitos a través de troncales SIP para clientes comerciales.

Los lectores deben prestar atención a**Sección 2**, en particular el alcance de las pruebas como se describe en **Sección 2.1**así como cualquier observación anotada en**Sección 2.2**, para garantizar que sus propios casos de uso estén adecuadamente cubiertos por este alcance y resultados.

AT&T es miembro del programa de proveedores de servicios Avaya DevConnect. La información en estas Notas de aplicación se obtuvo a través de pruebas de cumplimiento de DevConnect y discusiones técnicas adicionales. Las pruebas se realizaron a través del programa DevConnect en el laboratorio de pruebas de soluciones e interoperabilidad de Avaya.

©2020 Avaya Inc. Todos los derechos reservados.

Tabla de contenido

1. Introducción 4
2. Enfoque general de la prueba y resultados de la prueba 5
   2.1. Pruebas de cumplimiento de interoperabilidad 6
   2.2. Resultados de la prueba 7
   2.3. Apoyo 8
3. Configuración de referencia 9
   3.1. Información ilustrativa de configuración 11
   3.2. Flujos de llamadas 12
      3.2.1. Entrante básico 12
      3.2.2. Cobertura al correo de voz 13
4. Equipos y Software Validados 14
5. Configuración del servidor primario de Avaya IP Office 15
   5.1. Licencia ..... dieciséis
   5.2. Gestión de TLS 17
   5.3. Ajustes del sistema 18
      5.3.1. Pestaña LAN1 18
      5.3.2. Pestaña de correo de voz 21
      5.3.3. Pestaña Telefonía 22
      5.3.4. Pestaña VoIP 23
   5.4. Ruta IP 25
   5.5. Línea SIP 26
      5.5.1. Creación de una línea SIP a partir de una plantilla XML 27
      5.5.2. Línea SIP – Pestaña Línea SIP 28
      5.5.3. Línea SIP - Pestaña Transporte 29
      5.5.4. Línea SIP: pestaña Detalles de la llamada 30
      5.5.5. Línea SIP - pestaña VoIP 31
      5.5.6. Línea SIP – Pestaña Avanzado SIP 32
   5.6. Línea de IP Office 33
   5.7. Usuarios, Extensiones y Grupos de búsqueda 34
      5.7.1. Usuario 34
      5.7.2. Extensión 35
      5.7.3. Grupos de búsqueda 36
   5.8. Ruta de llamadas entrantes 38
      5.8.1. Llamadas a estaciones IP Office y grupos de búsqueda 38
      5.8.2. Llamadas a guiones de Voicemail Pro 40
   5.9. Aprovisionamiento del centro de llamadas en Voicemail Pro 41
   5.10. Guardar la configuración del servidor primario de IP Office 45
6. Configuración del sistema de expansión Avaya IP Office 46
   6.1. Sistema de Expansión - Hardware Físico 46
   6.2. Sistema de expansión: configuración de LAN 47
   6.3. Sistema de Expansión - Ruta IP 47
   6.4. Sistema de Expansión - Línea IP Office 48
   6.5. Guardar la configuración del sistema de expansión de IP Office 49

©2020 Avaya Inc. Todos los derechos reservados.

7. Configurar el controlador de borde de sesión de Avaya para empresas 50
7.1. Administración de dispositivos: estado 51
7.2. Gestión de TLS 53
7.2.1. Verificar certificados TLS: Avaya Session Border Controller para empresas 53
7.2.2. Perfiles de servidor 54
7.2.3. Perfiles de clientes 56
7.3. Administración de redes 58
7.4. Interfaces de medios 59
7.5. Interfaces de señalización 60
7.6. Perfiles de interfuncionamiento del servidor 61
7.6.1. Perfil de interfuncionamiento del servidor: IP Office 61
7.6.2. Perfil de interfuncionamiento del servidor: AT&T 63
7.7. Perfiles de servidores SIP ..... sesenta y cinco
7.7.1. Perfil del servidor SIP: IP Office ..... sesenta y cinco
7.7.2. Perfil de servidor SIP – AT&T 67
7.8. Perfiles de enrutamiento 69
7.8.1. Perfil de enrutamiento: IP Office 69
7.8.2. Perfil de enrutamiento: AT&T 70
7.9. Perfil de ocultación de topología 71
7.10. Reglas de aplicación 72
7.11. Reglas de los medios 72
7.12. Reglas de señalización 74
7.13. Grupos de políticas de punto final 75
7.14. Opciones avanzadas 76
7.15. Flujos de punto final - Flujo de servidor 77
8. Configuración del servicio de llamadas gratuitas IP de AT&T 79
9. Pasos de verificación 79
9.1. Servicio de llamadas gratuitas IP de AT&T 79
9.2. SBCE de Avaya 80
9.2.1. Incidentes 80
9.2.2. El estado del servidor 81
9.2.3. Rastreos de protocolo 82
9.3. Oficina de IP de Avaya 83
9.3.1. Aplicación de estado del sistema 83
9.3.2. Aplicación del monitor del sistema 85
10. Conclusión 86
11. Referencias adicionales 86

©2020 Avaya Inc. Todos los derechos reservados.

1. Introducción

Estas Notas de aplicación describen los pasos para configurar Avaya IP Office versión 11.0 (Avaya IP Office) y Avaya Session Border Controller for Enterprise (Avaya SBCE) versión 8.0.1 con el servicio AT&T IP Toll Free usando Internet Protocol versión 6 (IPv6) y**AVPN**o **MIS/PTN**conexiones de transporte.

Avaya IP Office es una solución de comunicaciones versátil que combina la confiabilidad y facilidad de un sistema de telefonía tradicional con las aplicaciones y ventajas de una solución de telefonía IP. Esta solución de comunicaciones convergentes puede ayudar a las empresas a reducir costos, aumentar la productividad y mejorar el servicio al cliente.

El controlador de borde de sesión de Avaya para empresas es el punto de conexión entre IP Office de Avaya y el servicio IP Toll Free de AT&T y se utiliza no solo para proteger el enlace troncal SIP, sino también para realizar ajustes en la señalización SIP y los medios para la interoperabilidad. El SBCE de Avaya también realiza traducciones de direcciones de red entre la red privada IPv4 de CPE y el enlace troncal IPv6 SIP gratuito de AT&T IP, tanto en la capa IP como en la capa SIP.

El servicio IP Toll Free de AT&T es una solución de comunicaciones de voz sobre IP (VoIP) administrada que brinda servicios gratuitos a través de troncales SIP para clientes comerciales. El servicio gratuito de AT&T utiliza AVPN[1]o MIS/PNT[2]servicios de transporte.

Nota–El servicio IP Toll Free de AT&T se denominará IPTF en el resto de este documento.

[1]AVPN utiliza RTP comprimido (cRTP).
[2]MIS/PNT no es compatible con cRTP.

©2020 Avaya Inc. Todos los derechos reservados.

2. Enfoque general de la prueba y resultados de la prueba

Las pruebas de cumplimiento de DevConnect son realizadas conjuntamente por miembros de Avaya y DevConnect. El plan de prueba definido de forma conjunta se centra en el ejercicio de API y/o interfaces basadas en estándares pertinentes a la interoperabilidad de los productos probados y sus funcionalidades. Las pruebas de cumplimiento de DevConnect no pretenden sustituir el rendimiento completo del producto o las pruebas de funciones realizadas por los miembros de DevConnect, ni deben interpretarse como una aprobación por parte de Avaya de la idoneidad o integridad de la solución de un miembro de DevConnect.

Las pruebas de cumplimiento de interoperabilidad se centraron en verificar los flujos de llamadas entrantes y salientes entre IPTF y el Equipo de las instalaciones del cliente (CPE) que contiene Avaya SBCE y Avaya IP Office (ver**Sección 3.2**para ver ejemplos de flujo de llamadas).

El entorno de prueba descrito en estas Notas de aplicación consistió en:

- Una empresa simulada con Avaya IP Office 11.0, Avaya SBCE 8.0.1, Avaya SIP, H.323, Teléfonos Digitales y Analógicos, así como emuladores de máquinas de fax (Ventafax).
- Versiones de laboratorio del servicio IPTF, al que se conectó la empresa simulada mediante transporte AVPN/MIS.

Avaya recomienda a nuestros clientes que implementen las soluciones de Avaya usando las capacidades de seguridad y encriptación apropiadas habilitadas por nuestros productos. Las pruebas a las que se hace referencia en esta nota de aplicación de DevConnect incluyeron la habilitación de capacidades de cifrado admitidas en los productos de Avaya. Los lectores deben consultar la documentación del producto de Avaya correspondiente para obtener más información sobre las capacidades de seguridad y cifrado admitidas por esos productos de Avaya.

El soporte para estas capacidades de seguridad y encriptación en cualquier componente de la solución que no sea de Avaya es responsabilidad de cada proveedor individual. Los lectores deben consultar la documentación del producto proporcionada por el proveedor correspondiente para obtener más información sobre esos productos.

Para las pruebas asociadas con esta nota de aplicación, la interfaz entre los sistemas de Avaya y el servicio de llamadas gratuitas de AT&T no incluyó el uso de ninguna función de cifrado específica solicitada por AT&T.

El cifrado (TLS/SRTP) se utilizó internamente en la empresa entre los productos de Avaya siempre que fue posible.

©2020 Avaya Inc. Todos los derechos reservados.

2.1. Pruebas de cumplimiento de interoperabilidad

La prueba de cumplimiento se basó en un plan de prueba proporcionado por AT&T, para la funcionalidad requerida para la certificación como una solución compatible con la red IPTF. Las llamadas se realizaron desde la PSTN a través de la red de prueba IPTF, al CPE.

Las pruebas de cumplimiento de interoperabilidad se centraron en verificar los flujos de llamadas entrantes (ver**Sección 3.2**) entre Avaya IP Office, Avaya SBCE y el servicio IPTF.

Las siguientes funciones VoIP de enlace troncal SIP se probaron con el servicio IPTF:

- Llamadas entrantes desde la PSTN, enrutadas por el servicio IPTF, a Avaya SBCE y Avaya IP Office. Estas llamadas se realizan a través de la línea SIP de IP Office de Avaya y pueden ser generadas/respondidas por teléfonos/softphones SIP de Avaya, teléfonos H.323, teléfonos analógicos, teléfonos digitales, máquinas de fax analógicas o mediante grupos de búsqueda. También se utilizaron la cobertura de Voicemail Pro y las aplicaciones de operadora automática de Voicemail Pro.
- Establecimiento de rutas de llamadas y conversaciones bidireccionales entre PSTN y teléfonos/agentes de IP Office a través de IPTF.
- Funciones básicas de telefonía como llamada en espera, retención, transferencia y conferencia.
- Funciones gratuitas de AT&T IP como Legacy Transfer Connect y Alternate Destination Routing
- Fax entrante utilizando T.38 o G.711 y terminales G3 o SG3.
- Desconexión adecuada cuando la persona que llama abandona una llamada antes de responder y cuando la parte de Avaya IP Office o la parte PSTN finaliza una llamada activa.
- OPCIONES SIP monitoreo de la salud del troncal SIP. En la configuración de referencia, Avaya IP Office envió OPCIONES al elemento de frontera del servicio IPTF y AT&T respondió con*405 Método no permitido*(cuál es la respuesta esperada). Esa respuesta es suficiente para que Avaya IP Office considere la conexión.
- Llamadas entrantes usando los códecs G.729A y G.711 ULAW.
- Llamadas de larga duración.
- Transmisión DTMF (RFC 2833) para una navegación exitosa por correo de voz, incluida la navegación de una aplicación de operadora automática simple configurada en Voicemail Pro, así como funciones generadas por IPTF DTMF.

Un terminal de trabajador remoto de Avaya (softphone SIP de Avaya Equinox) fue uno de los terminales de Avaya utilizados en la configuración de referencia. El trabajador remoto reside en el lado público de Avaya SBCE (a través de una conexión TLS) y se registra/comunica con Avaya Session Manager a través de Avaya SBCE, como si fuera un extremo que reside en el espacio de CPE privado. La configuración del entorno del trabajador remoto está más allá del alcance de este documento.

©2020 Avaya Inc. Todos los derechos reservados.

2.2. Resultados de la prueba

Los objetivos de la prueba establecidos en**Sección 2.1**, con las limitaciones que se indican a continuación, fueron verificadas.

1. **Avaya IP Office solo admite un tamaño de paquete (ptime) de 20 milisegundos**–Si bien no se encontraron problemas durante las pruebas, AT&T recomienda que, para lograr la máxima utilización del ancho de banda del cliente, se especifique un valor de ptime de 30.

2. **Función de enrutamiento de destino alternativo (ADR) gratuito de IP basada en la respuesta del código de error SIP**–El servicio IP Toll Free se puede configurar para invocar la función de redirección de llamadas ADR al recibir una respuesta de error del CPE.
    - Las siguientes condiciones de error se produjeron en la configuración de referencia y se probaron con éxito: 480 Temporalmente no disponible, 486 Ocupado aquí, 500 Error interno del servidor y 503 Servicio no disponible.
    - Aunque las siguientes condiciones de error no se produjeron en la configuración de referencia, los códigos de error asociados se simularon durante las pruebas a través de una regla de manipulación de señalización SBCE de Avaya, lo que permitió que la función de Redirección de llamadas ADR asociada se probara con éxito en cada caso: 408 Tiempo de espera de solicitud, 504 Tiempo de espera del servidor y 600 Ocupado en todas partes.

3. **Las llamadas desconectadas no se liberan de IP Office:**Cuando la persona que llama PSTN desconecta la llamada y el usuario de IP Office no cuelga, IP Office no borrará la llamada correctamente. AT&T envía un mensaje BYE con un parámetro "tgrp" en el encabezado del URI de solicitud que incluye direcciones IPv6. IP Office no puede analizar el mensaje BYE debido al contenido del parámetro tgrp. Se usó un perfil de interconexión de servidores en Avaya SBCE para eliminar el parámetro "tgrp". Ver **Sección 7.6.1**. Con el perfil de interfuncionamiento del servidor en su lugar, la llamada se borra correctamente.

4. **Marcas DiffServ –**El encabezado IP en los paquetes de señalización SIP y medios RTP enviados desde Avaya SBCE a AT&T no contienen los valores DSCP de calidad de servicio configurados en las Reglas de medios y señalización en Políticas de dominio (**Secciones 7.11**y**7.12**). Este problema parece estar restringido a las interfaces SBCE de Avaya configuradas con direcciones IPv6, y Avaya lo está investigando actualmente.

5. **IP Office determina la prioridad del códec**–IP Office seguirá la prioridad del códec en función de la Selección de códec en la ficha VoIP de la línea SIP, consulte**Sección 5.5.5**. No seguirá la prioridad del códec establecida por el servicio IPTF.

6. **El códec G.729B no es compatible con el servidor IP Office Server Edition**–No se pudieron ejecutar casos de prueba específicos en el Plan de prueba de AT&T que requieren el uso del códec G.729B en el CPE. El códec G729B no es compatible con troncales SIP que terminan en la plataforma de servidor Avaya IP Office Server Edition Linux, tal como se implementó en la configuración de prueba. El códec G.729B es compatible cuando el enlace troncal SIP termina en un sistema independiente o de expansión IP Office IP500 V2.

©2020 Avaya Inc. Todos los derechos reservados.

7. **Las llamadas de fax G.711 fallan:**El fax G.711 se probó en la configuración de referencia. Después de completar la configuración de voz inicial con el código G.729A, IP Office de Avaya no envía una nueva invitación a AT&T para realizar la transición al fax G.711, a menos que la Cadena personalizada de línea SIP **SLIC_PREFER _EXISTENTE_CODEC**se agrega a la pestaña Ingeniería de la línea SIP. El equipo de desarrollo de Avaya IP Office está investigando este problema. Al usar la cadena anterior, IP Office envió la nueva INVITACIÓN en G.711, pero después de detectar el tono de fax, AT&T envía una nueva INVITACIÓN en T.38 al CPE. Debido a que el Soporte de transporte de fax se configuró en G.711 en la pestaña VoIP de la línea SIP para ejecutar la prueba, IP Office devuelve un "488 No aceptable aquí" y la llamada de fax falla.

   El fax G711 no debe utilizarse en esta solución. El fax T.38 se probó con éxito y es el método recomendado para el fax.

8. **Servicios IP gratuitos IP InfoPack**y**No se pudieron ejecutar los casos de prueba de telefonía fija/movilidad**. El plan de prueba IP Toll Free proporcionado por AT&T especifica casos de prueba para verificar la transmisión entrante de INFOPAK y datos fijos/móviles por el servicio IP Toll Free. Debido a problemas de aprovisionamiento de red y soporte de laboratorio, estos casos de prueba no se pudieron ejecutar.

2.3. Apoyo

Los clientes de AT&T pueden obtener asistencia para el servicio de llamada gratuita IP de AT&T llamando al (800) 325-5555.

Los clientes de Avaya pueden obtener documentación y soporte para los productos de Avaya visitando: http://support.avaya.com. En los Estados Unidos, (866) GO-AVAYA (866-462-8292) brinda acceso a los menús generales de soporte de ventas y servicios. Los clientes también pueden usar números específicos (proporcionados en http://support.avaya.com) para acceder directamente a servicios de consulta y soporte específicos según sus acuerdos de soporte de Avaya.

©2020 Avaya Inc. Todos los derechos reservados.

3. Configuración de referencia

Nota–Los documentos utilizados para aprovisionar el entorno de prueba se enumeran en**Sección 11**. Las referencias a estos documentos se indican mediante la notación**[X]**, dónde*X*es el número de referencia del documento.

La configuración de referencia utilizada en estas Notas de aplicación se muestra en**Figura 1**en la página siguiente y consta de los siguientes componentes:

- Avaya IP Office proporciona los servicios de comunicaciones de voz para un sitio empresarial en particular. En la configuración de referencia, Avaya IP Office se ejecuta en la plataforma Avaya IP Office Server Edition. Tenga en cuenta que esta solución también es extensible a implementaciones que utilizan la plataforma independiente IP500 V2.
- En la configuración de muestra, el servidor principal ejecuta el software Avaya IP Office Server Edition Linux. Avaya Voicemail Pro, ejecutándose como un servicio en el servidor principal, proporcionó las capacidades de mensajería de voz en la configuración de referencia.
- El Sistema de Expansión (V2) se utiliza para admitir estaciones IP digitales, analógicas y adicionales. Consta de un Avaya IP Office 500 V2 con módulos de expansión de extensión analógicos y digitales, así como un VCM64 (Módulo de compresión de voz).
- Los puntos finales de Avaya están representados con un teléfono de escritorio Avaya 9608 H.323, teléfonos de escritorio Avaya J169 SIP, un teléfono de escritorio Avaya 1140E SIP, un teléfono de escritorio digital Avaya 9508, así como un softphone Avaya Equinox para Windows (SIP). Los terminales de fax están representados por PC que ejecutan el software de emulación Ventafax conectados por módem a un puerto analógico Avaya IP Office.
- Avaya SBCE proporciona la funcionalidad SIP Session Border Controller (SBC), incluida la traducción de direcciones y la manipulación de encabezados SIP entre el servicio IPTF y el CPE. En la configuración de referencia, Avaya SBCE se ejecuta en una plataforma VMware. Esta solución también es extensible a otras plataformas de Avaya Session Border Controller para empresas.

Nota–En la configuración de referencia, Avaya SBCE realiza traducciones de direcciones de red entre la red privada IPv4 de CPE y el enlace troncal SIP IPv6 gratuito de IP de AT&T, tanto en la capa IP como en la capa SIP.

- Avaya IP Office y Avaya SBCE se implementaron con la siguiente configuración. o
  - Interfaz IP Office LAN1 conectada a la red privada del CPE. (IPv4)
  - o Interfaz Avaya SBCE A1 conectada a la red privada del CPE. (IPv4)
  - o Interfaz Avaya SBCE B1 conectada a la red de AT&T. (IPv6)
- TLS/5061 es el puerto/protocolo de transporte recomendado para usar en la conexión LAN1 de Avaya IP Office a la interfaz Avaya SBCE A1. Sin embargo, se puede usar TCP/5060 para esta conexión si se desea.
- El transporte UDP a través del puerto 5060 se utilizó entre Avaya SBCE y AT&T.
- El servicio IPTF de AT&T requiere rangos de puertos RTP 16384-32767.
- AT&T proporcionó los números de acceso entrantes y salientes (DID y DNIS) utilizados en la configuración de referencia. Tenga en cuenta que el servicio IPTF puede entregar varias longitudes de dígitos en la URI de solicitud de invitación SIP, según el aprovisionamiento del orden del circuito. En la configuración de referencia, el servicio IPTF entregó 15 dígitos.

©2020 Avaya Inc. Todos los derechos reservados.

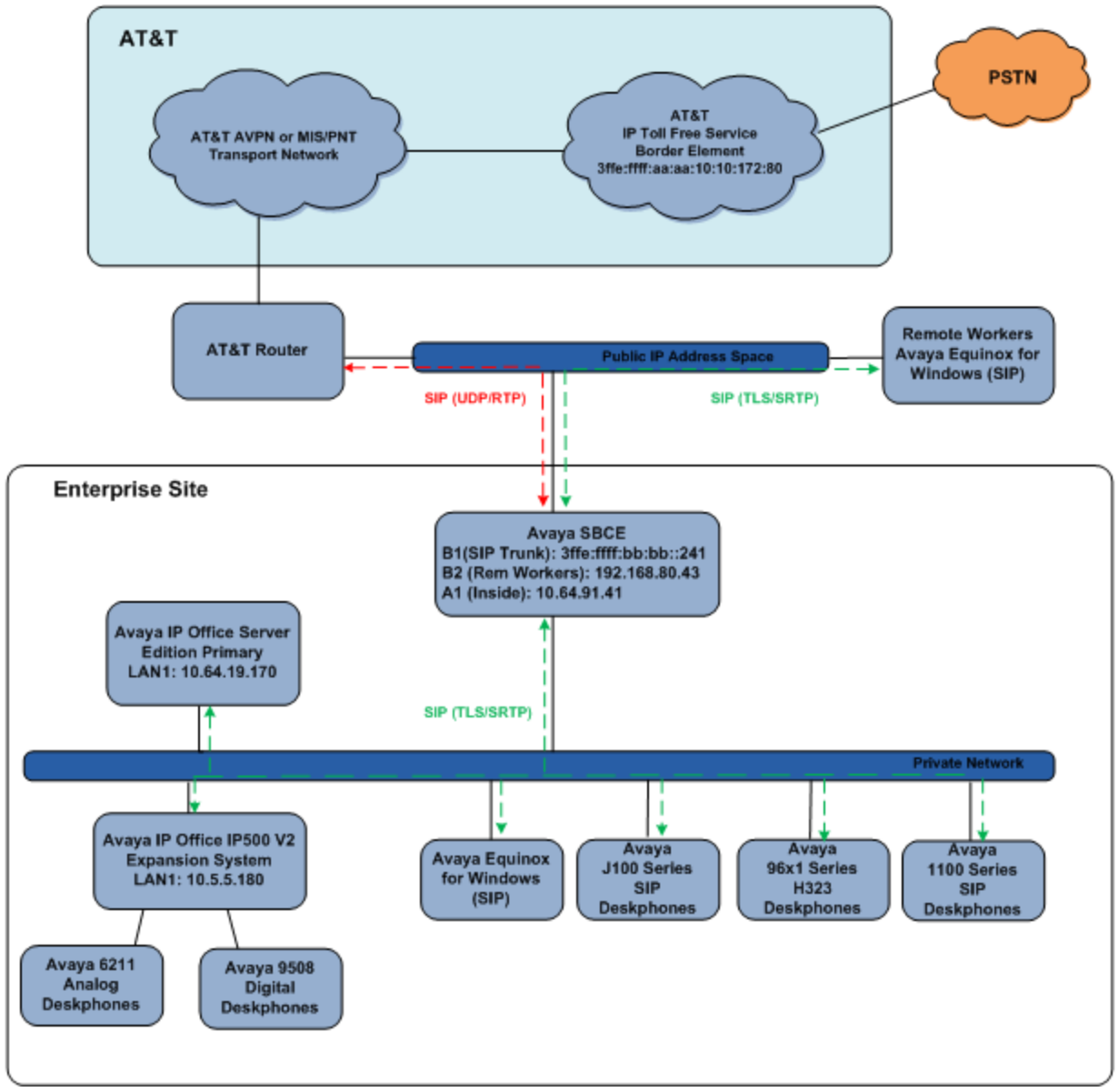


Figura 1: Configuración de prueba

Se utilizó un extremo de Avaya Remote Worker (Avaya Equinox for Windows) en la configuración de referencia. El extremo del trabajador remoto reside en el lado público de un SBCE de Avaya (a través de una conexión TLS) y se registra/se comunica con IP Office como si fuera un extremo que reside en el espacio del CPE privado.

Nota–La configuración del entorno del trabajador remoto está más allá del alcance de este documento. Referirse a[7] en el **Referencias adicionales**sección para obtener información sobre las implementaciones de trabajadores remotos.

©2020 Avaya Inc. Todos los derechos reservados.

3.1. Información de configuración ilustrativa

Los valores específicos enumerados en**tabla 1**a continuación y en las secciones subsiguientes se utilizan en la configuración de referencia descrita en estas Notas de aplicación y solo tienen fines ilustrativos. Los clientes deben obtener y utilizar los valores en función de sus propias configuraciones específicas.

Nota–La interfaz Avaya SBCE "B1" se comunica con AT&T Border Element (BE) ubicado en la red AT&T IPTF. Por motivos de seguridad, las direcciones IP públicas de Avaya SBCE y AT&T BE no se incluyen en este documento. Sin embargo, como marcadores de posición en las siguientes secciones de configuración, las direcciones IPv6**3ffe:ffff:bb:bb::241**(Avaya SBCE "B1"), y**3ffe:ffff:aa:aa:10:10:172:80**(dirección de AT&T BE), se especifican. Además, los números DID/DNIS de AT&T que se muestran en este documento también son ejemplos. El servicio de atención al cliente de AT&T proporcionará las direcciones IP de elementos fronterizos y los números DID/DNIS reales como parte del proceso de aprovisionamiento de IPTF.

Componente	Valor ilustrativo en estas aplicaciones notas norte
Oficina IP de Avaya	
Servidor primario, interfaz LAN1	10.64.19.170
Sistema de expansión, interfaz LAN1	10.5.5.180
Avaya SBCE	
"Interfaz interior", A1	10.64.91.41
Interfaz "Exterior", B1	3ffe:ffff:bb:bb::241
Servicio IPTF de AT&T	
Dirección IP del elemento de borde	3ffe:ffff:aa:aa:10:10:172:80

Tabla 1: Valores ilustrativos utilizados en estas notas de aplicación

©2020 Avaya Inc. Todos los derechos reservados.

3.2. Flujos de llamadas

Para comprender cómo Avaya IP Office maneja las llamadas entrantes y salientes del servicio IPTF de AT&T, en esta sección se describen dos flujos básicos de llamadas.

3.2.1. Entrada básica

El primer escenario de llamada ilustrado en la figura a continuación es una llamada de servicio AT&T IPTF entrante que llega a Avaya IP Office, que a su vez enruta la llamada a un grupo de búsqueda, teléfono o terminal de fax.

1. Un teléfono PSTN origina una llamada a un número de servicio IPTF.
2. La PSTN enruta la llamada a la red de servicio AT&T IPTF.
3. El servicio IPTF de AT&T enruta la llamada al SBCE de Avaya.
4. Avaya SBCE realiza la traducción de direcciones de red (NAT) SIP y cualquier modificación de encabezado SIP especificada, y enruta la llamada a Avaya IP Office.
5. Avaya IP Office aplica las manipulaciones de dígitos necesarias según el DID y enruta la llamada a un grupo de búsqueda, teléfono o terminal de fax.

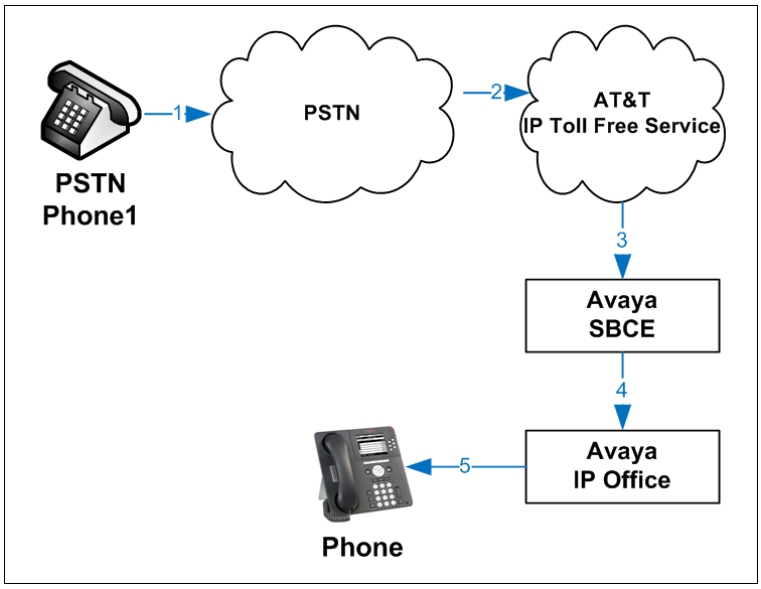


Figura 2: Llamada IPTF de AT&T entrante

©2020 Avaya Inc. Todos los derechos reservados.

3.2.2. Cobertura al correo de voz

El escenario de llamada que se ilustra en la siguiente figura es una llamada entrante que está cubierta para el correo de voz. En la configuración de referencia, el sistema de correo de voz utilizado es Voicemail Pro, que se ejecuta en el servidor de aplicaciones.

1. Igual que el escenario de la primera llamada en**Sección 3.2.1**.
2. El teléfono de Avaya IP Office no responde la llamada y la llamada cubre la aplicación externa Avaya IP Office Voicemail Pro.

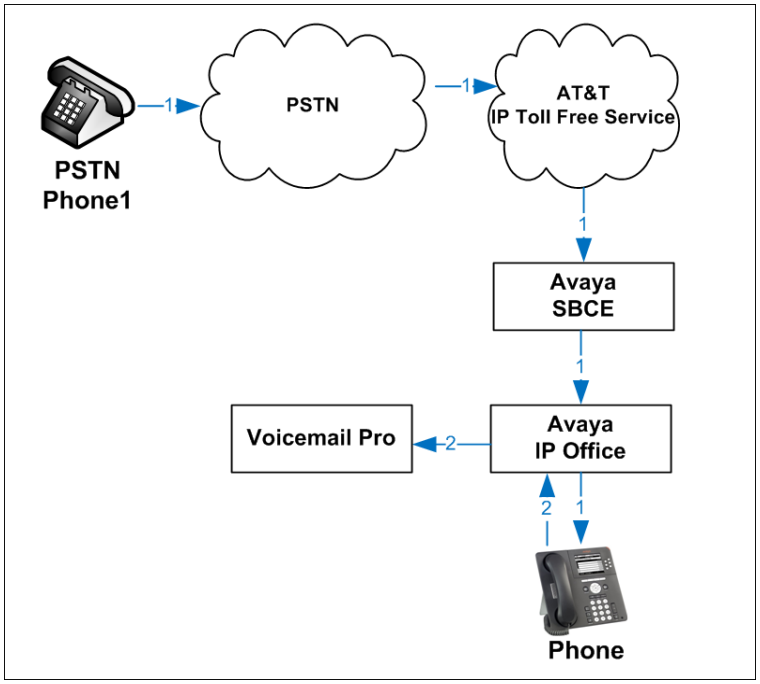


Figura 3: Cobertura al correo de voz (Voicemail Pro)

©2020 Avaya Inc. Todos los derechos reservados.

4. Equipos y Software Validados

Se utilizaron los siguientes equipos y software para la configuración de muestra proporcionada:

Equipo/Software	Versión de lanzamiento
Avaya	
Edición de servidor Avaya IP Office Avaya IP Office Voicemail Pro	Versión 11.0.4.1.0 Compilación 11 Versión 11.0.4.1.0 Compilación 2
Sistema de expansión Avaya IP Office 500 V2	Versión 11.0.4.1.0 Compilación 11
Administrador de IP Office de Avaya	Versión 11.0.4.1.0 Compilación 11
Controlador de borde de sesión de Avaya para empresas	Versión 8.0.1.0-10-17555
Teléfono de escritorio IP serie 96x1 de Avaya (H.323)	Versión 6.8002
Teléfono de escritorio IP Avaya 1140E (SIP)	Lanzamiento 04.04.23.00
Teléfono de escritorio IP Avaya J169 (SIP)	Versión 4.0.3.0.10
Teléfono de escritorio digital Avaya 9508	Liberar 0.60
Avaya Equinox para Windows	Versión 3.6.4.31.2
Dispositivo de fax de Avaya	Ventafax 7.10

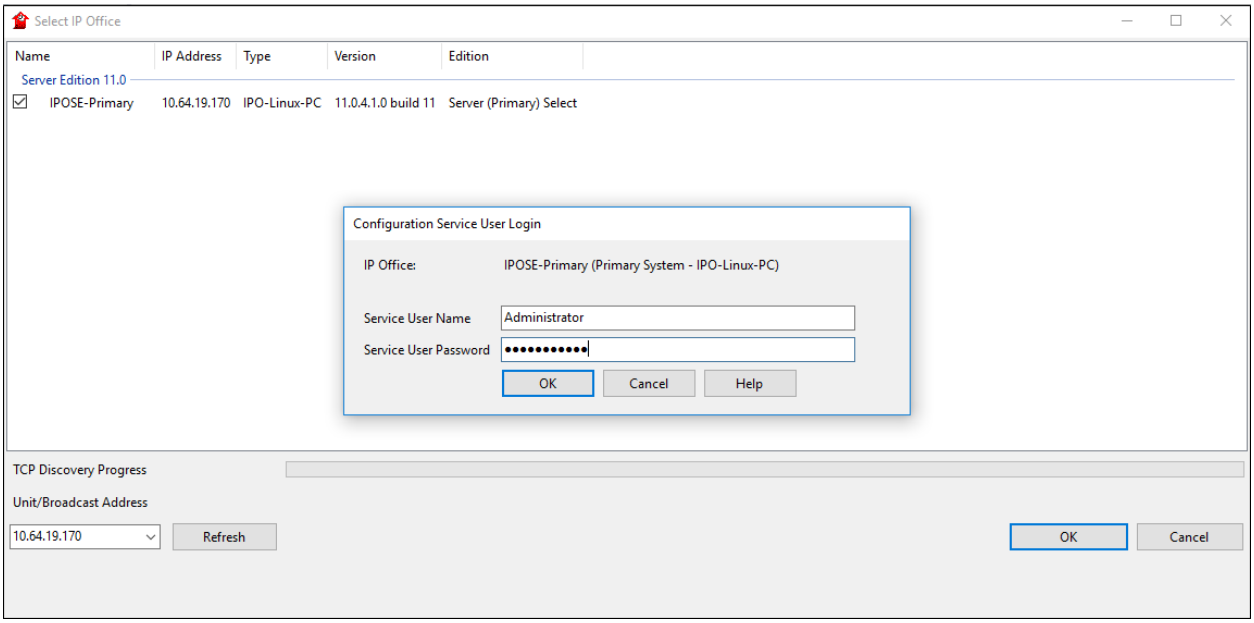
Tabla 1: Versiones de equipos y software

Nota -Las pruebas de cumplimiento se aplican cuando la solución probada se implementa con un IP Office 500 V2 independiente y también cuando se implementa con todas las configuraciones de IP Office Server Edition. IP Office Server Edition requiere una expansión IP Office 500 V2 para admitir puntos finales o troncales analógicos o digitales.

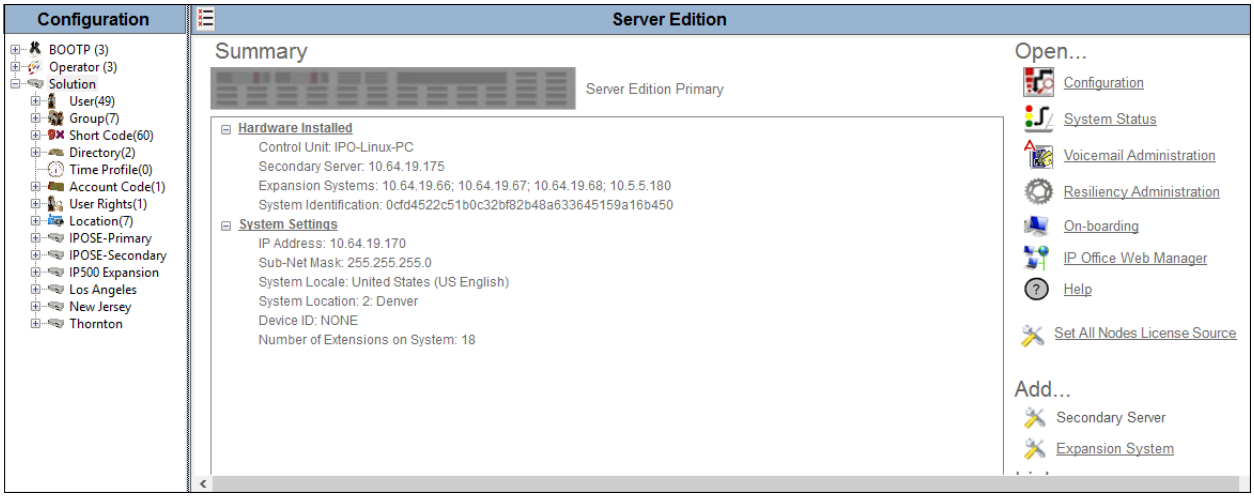
©2020 Avaya Inc. Todos los derechos reservados.

5. Configuración del servidor primario de Avaya IP Office

Avaya IP Office se configura a través de la aplicación Avaya IP Office Manager. Desde la PC que ejecuta la aplicación IP Office Manager, seleccione**comienzo→Programas→Oficina de PI→Gerente** para iniciar la aplicación Administrador. Inicie sesión con las credenciales adecuadas.



En los sistemas Server Edition, aparecerá la pantalla Solution View, similar a la que se muestra a continuación. Todos los componentes configurables de Avaya IP Office se muestran en el panel izquierdo, conocido como Panel de navegación. Al hacer clic en el signo "más" junto al nombre del sistema del servidor principal, por ejemplo, **IPOSE-Primario**, en el panel de navegación se expandirá el menú en este servidor.



©2020 Avaya Inc. Todos los derechos reservados.

En las pantallas presentadas en las siguientes secciones, el menú Ver se configuró para mostrar el panel de navegación en el lado izquierdo, el panel de grupo en el centro y el panel de detalles en el lado derecho. Se hará referencia a estos paneles en el resto de este documento.

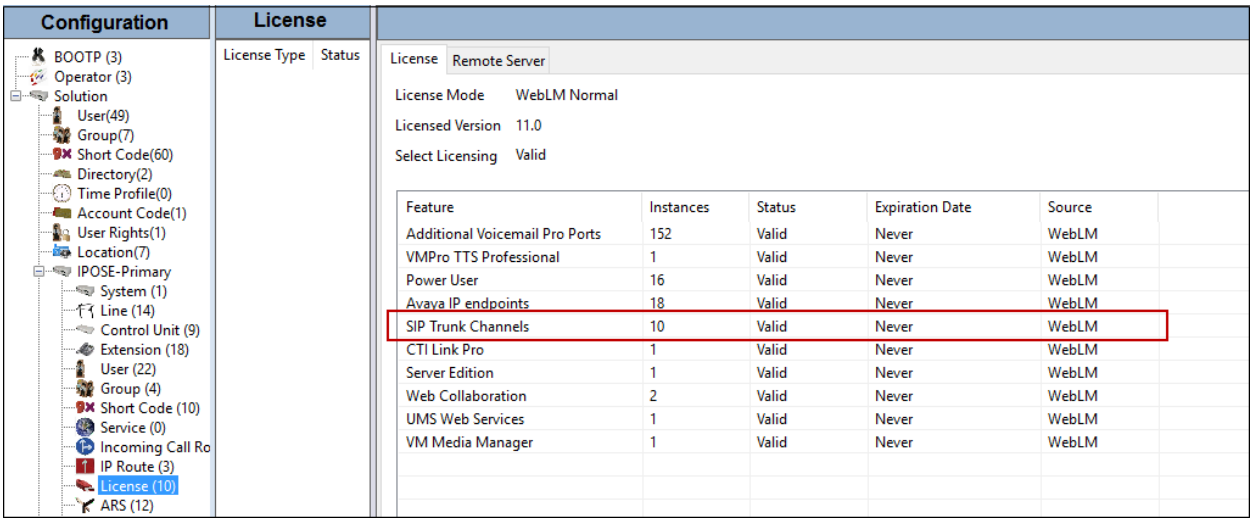
Se supone que las configuraciones de características estándar que no están directamente relacionadas con la interfaz con el proveedor de servicios ya están implementadas y no forman parte de estas Notas de aplicación.

5.1. Licencia

La configuración y las funciones descritas en estas Notas de aplicación requieren que el sistema IP Office tenga la licencia correspondiente. Si una función deseada no está habilitada o no hay capacidad suficiente, comuníquese con un representante de ventas autorizado de Avaya.

En la configuración de referencia,**IPOSE-Primario**se usó como el nombre del sistema del servidor primario y**Expansión IP500**se usó como el nombre del sistema del sistema de expansión. Toda la navegación descrita en las siguientes secciones (p. ej.,**Licencia**) aparece como submenús debajo del nombre del sistema en el panel de navegación.

Navegar a**Licencia**en el panel de navegación. En el Panel de detalles verifique que el**Estado de la licencia** por**Canales troncales SIP**es válido y que el número de**Instancias**es suficiente para admitir la cantidad de canales aprovisionados para el troncal SIP.



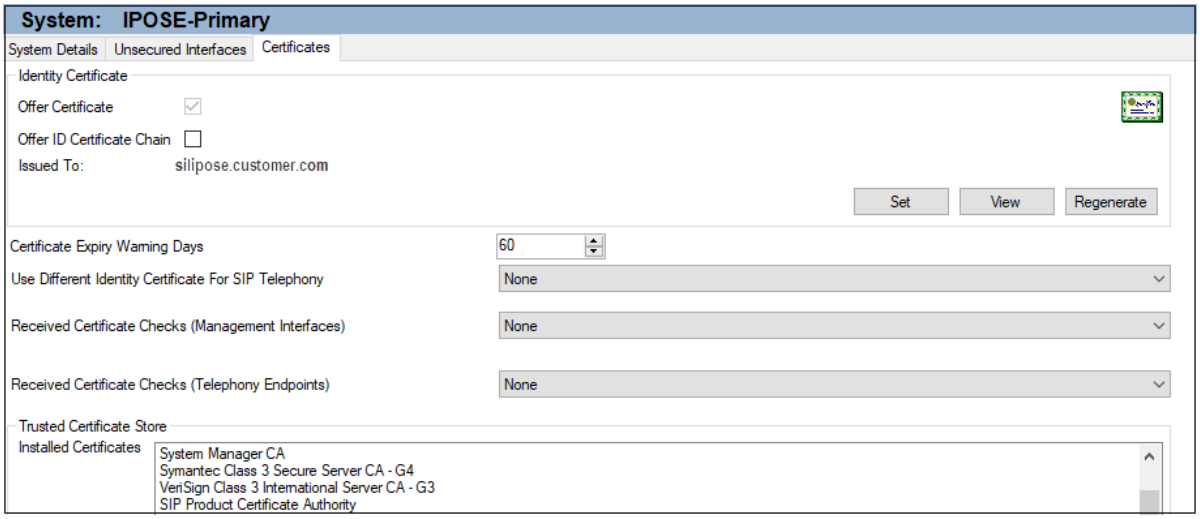
©2020 Avaya Inc. Todos los derechos reservados.

5.2. Gestión TLS

Para la prueba de cumplimiento, la señalización en el enlace troncal SIP entre IP Office y Avaya SBCE se aseguró mediante TLS. Las pruebas se realizaron utilizando certificados de identidad firmados por una autoridad de certificación local**SystemManager CA**. La generación e instalación de estos certificados están fuera del alcance de estas Notas de aplicación. Sin embargo, una vez que los certificados están disponibles, se pueden ver en IP Office de la siguiente manera.

Para ver los certificados actualmente instalados en IP Office, vaya a**Expediente→Avanzado→ Configuraciones de seguridad**. Inicie sesión con las credenciales de seguridad adecuadas (no se muestran). En la ventana Configuración de seguridad, navegue hasta**Seguridad→Sistema**y seleccione el**Certificados**pestaña.

Para verificar el certificado de identidad, busque el**Certificado de Identidad**sección y haga clic**Vista**para ver los detalles del certificado.



©2020 Avaya Inc. Todos los derechos reservados.

5.3. Ajustes del sistema

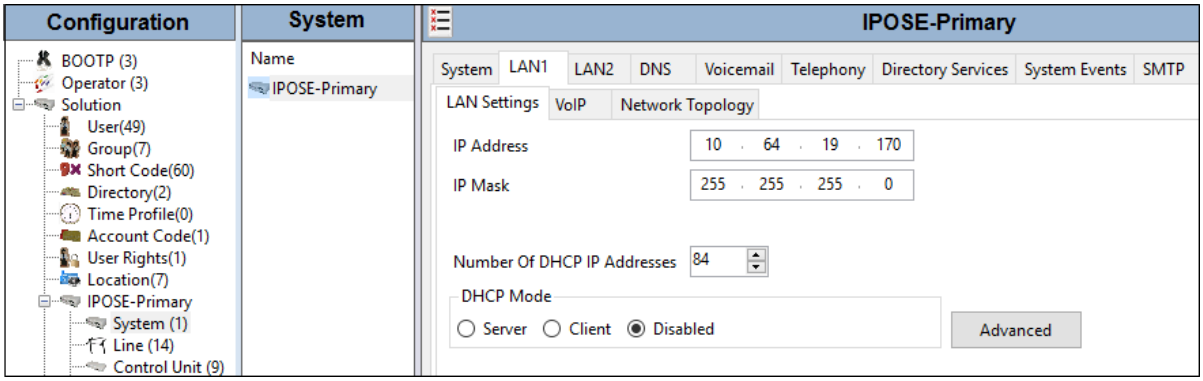
Esta sección ilustra la configuración de los ajustes del sistema. Seleccione**Sistema**en el panel de navegación para configurar estos ajustes. El orden de las subsecciones corresponde a una navegación de izquierda a derecha de las pestañas en el panel Detalles para la configuración del sistema. Para todas las siguientes secciones de configuración, el **OK**(no se muestra) debe seleccionarse para que se guarden los cambios.

5.3.1. Pestaña LAN1

En la configuración de muestra, LAN1 se usa para conectar el servidor primario a la red privada de la empresa.

Para ver o configurar la dirección IP y la máscara de subred de LAN 1, seleccione la**LAN1→Configuración de LAN** e ingrese la información según sea necesario, de acuerdo con los requisitos específicos del cliente:

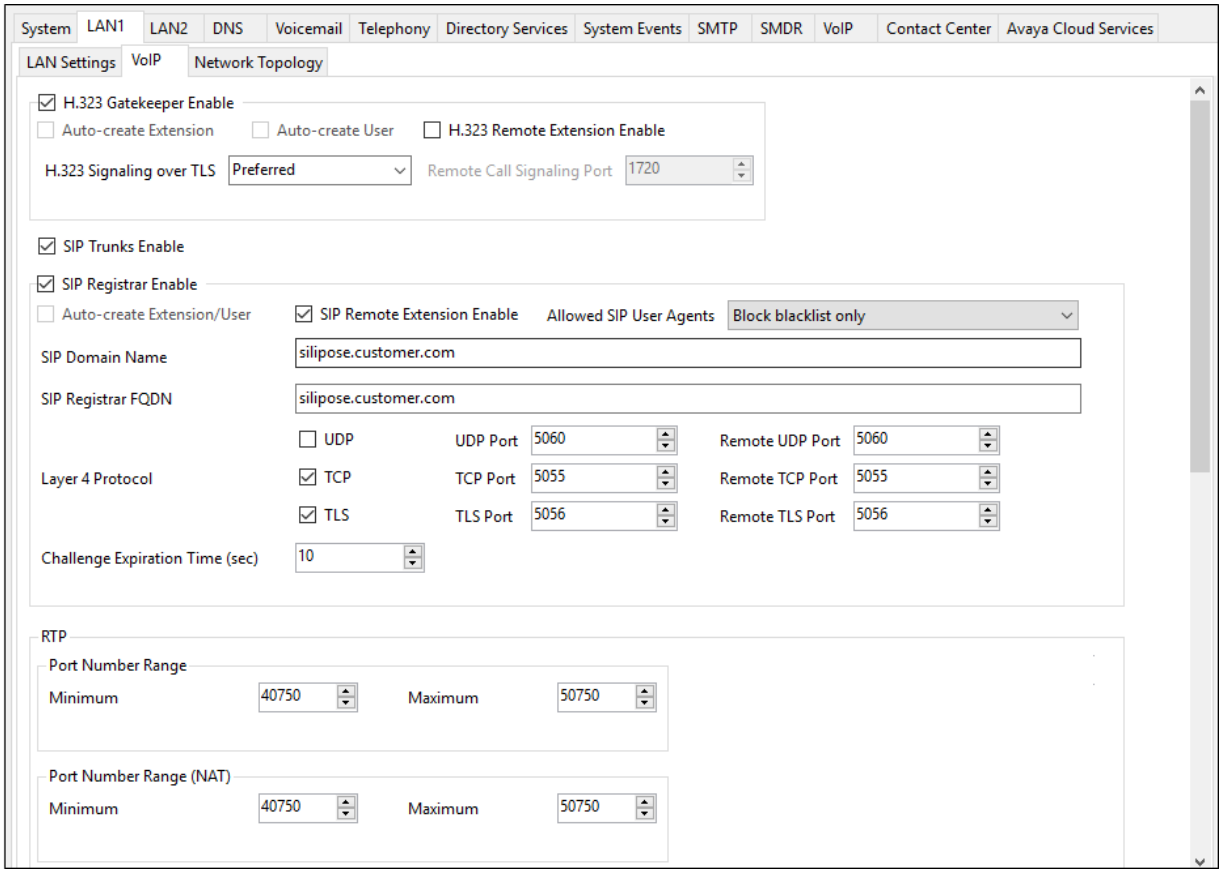
- **Dirección IP**:**10.64.19.170**se utilizó en la configuración de referencia.
- **Máscara IP**:**255.255.255.0**se utilizó en la configuración de referencia.
- Haga clic en el**OK**botón (no se muestra).



©2020 Avaya Inc. Todos los derechos reservados.

Selecciona el**LAN1→VoIP**pestaña como se muestra en la siguiente pantalla. Los siguientes ajustes se utilizaron en la configuración de referencia:

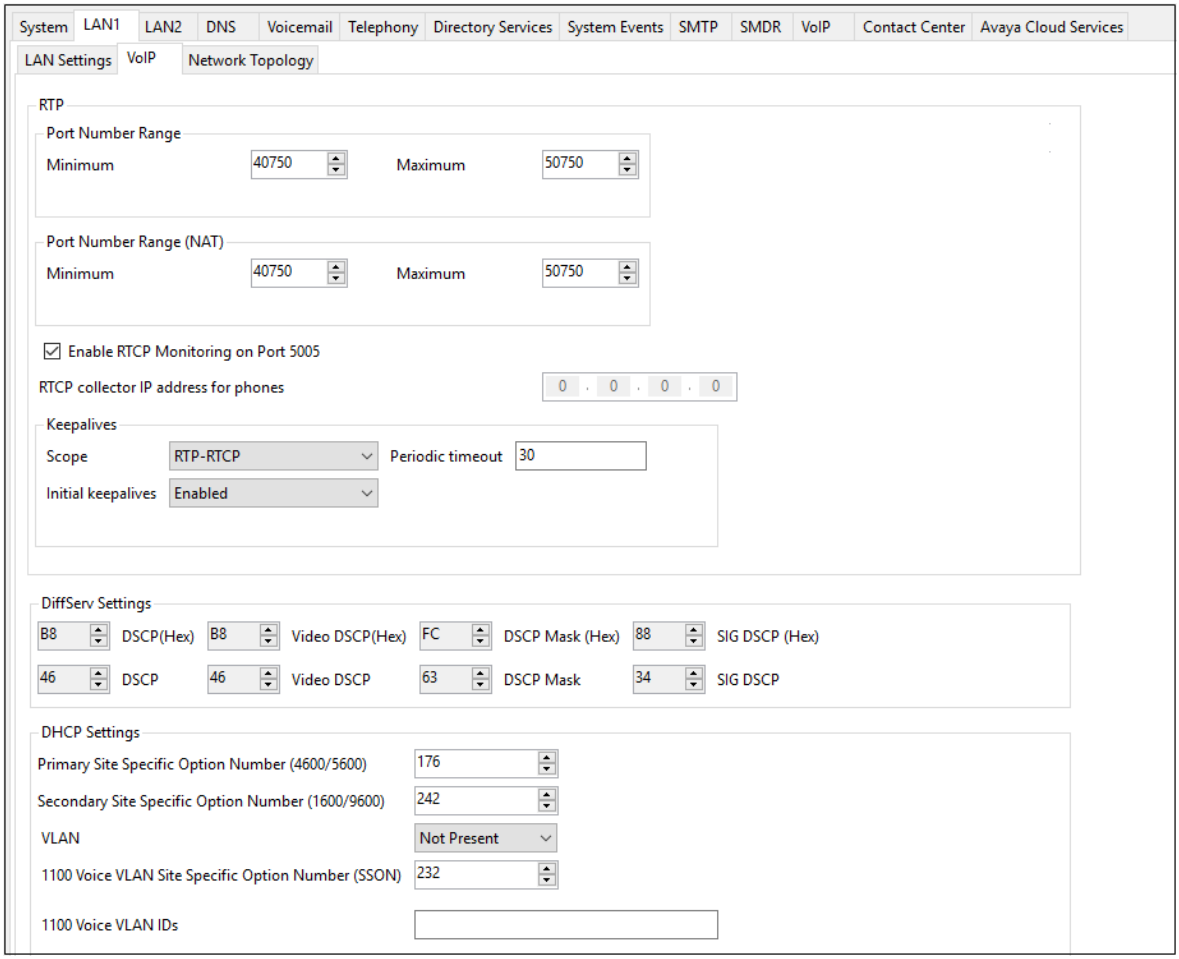
- los**H323 Gatekeeper Habilitar**La casilla está marcada para permitir el uso de teléfonos IP de Avaya con el protocolo H.323, como los teléfonos de escritorio de la serie 96x1 de Avaya utilizados en la configuración de referencia.
- La señalización H.323 sobre TLS debe configurarse según las necesidades del cliente. En la configuración de referencia se estableció en**Privilegiado**.
- los**Activación de troncales SIP**Se debe marcar el parámetro para habilitar la configuración de troncales SIP para AT&T.
- los**Habilitar registrador SIP**Se marcó la casilla para permitir el uso de Avaya J100-Series Deskphones, Avaya 1100-Series Deskphones y Avaya Equinox.
- los**Nombre de dominio**y**Registrador SIP FQDN**puede configurarse de acuerdo con los requisitos del cliente. Se muestran los valores utilizados en la configuración de referencia.
- Selecciona el**Protocolo de capa 4**sección en función de las necesidades del cliente. En la configuración de referencia **TCP/5055**y**TLS/5056**fueron configurados.



©2020 Avaya Inc. Todos los derechos reservados.

Desplácese hacia abajo en la página:

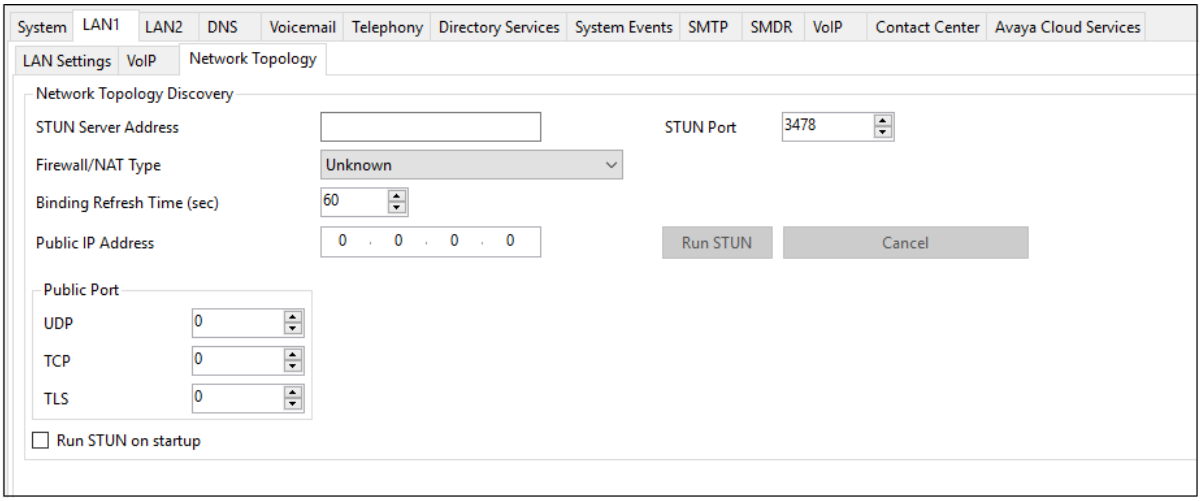
- Verifique el**Rango de número de puerto RTP**. Según esta configuración, Avaya IP Office solicitará que se envíen medios RTP a un puerto UDP en el rango configurable para llamadas que usan LAN1. los**Mínimo**y **Máximo**los números de puerto se mantuvieron en sus valores predeterminados en la configuración de referencia.
- En el**Keepalives**sección, configure el**Alcance**a**RTP-RTCP**. Selecciona el**Tiempo de espera periódico**a**30** y el**Keepalives iniciales**parámetro a**Activado**. Esto se hace para evitar posibles problemas con los cortafuegos de la red que cierran los canales RTP inactivos.
- En el**Configuración de DiffServ**IP Office se puede configurar para marcar el punto de código de servicios diferenciados (DSCP) en el encabezado de IP con valores específicos para admitir políticas de calidad de servicios (QoS) tanto para señalización como para medios. los**DSCP**campo es el valor utilizado para los medios, mientras que el**SIG DSCP**es el valor utilizado para la señalización. Esta configuración debe establecerse de acuerdo con las políticas de QoS del cliente vigentes. Se muestran los valores predeterminados utilizados durante la prueba de conformidad.
- Hacer clic**OK**para cometer (no se muestra).



©2020 Avaya Inc. Todos los derechos reservados.

Selecciona el**LAN1→Topología de la red**como se muestra en la siguiente pantalla, e ingrese lo siguiente:

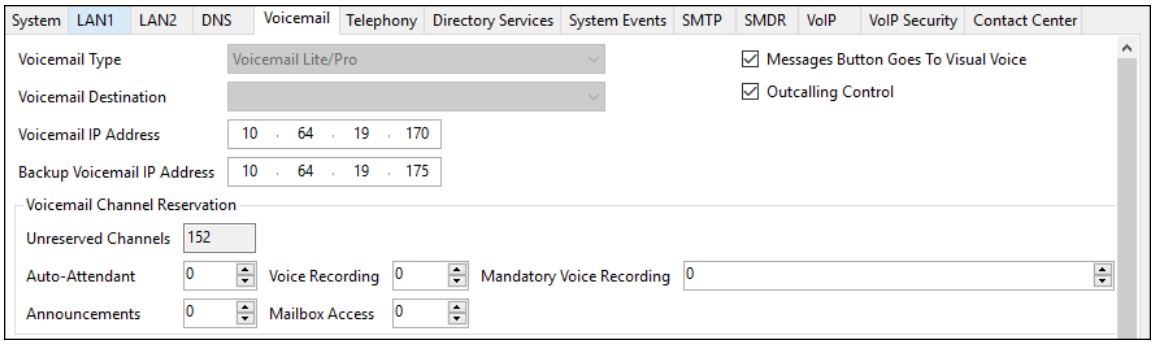
- **Cortafuegos/Tipo de NAT**se fijó en**Desconocido**en la configuración de referencia.
- los**Dirección IP pública**y**Puerto Público**Las secciones no se utilizan para la conexión del servicio troncal SIP IPTF de AT&T.
- Haga clic en el**OK**botón (no se muestra).



5.3.2. Pestaña de correo de voz

Como se describe en**Seccion 3**, se utilizó Voicemail Pro en la configuración de referencia.

- Establecer**Tipo de correo de voz**a**Correo de voz Lite/Pro**.
- Establecer**Dirección IP del correo de voz**a la dirección IP del servidor que aloja el correo de voz. En la configuración de referencia, este es el servidor primario,**10.64.19.170**.
- Otros parámetros en esta pantalla son los predeterminados. Haga clic en el**OK**botón (no se muestra).



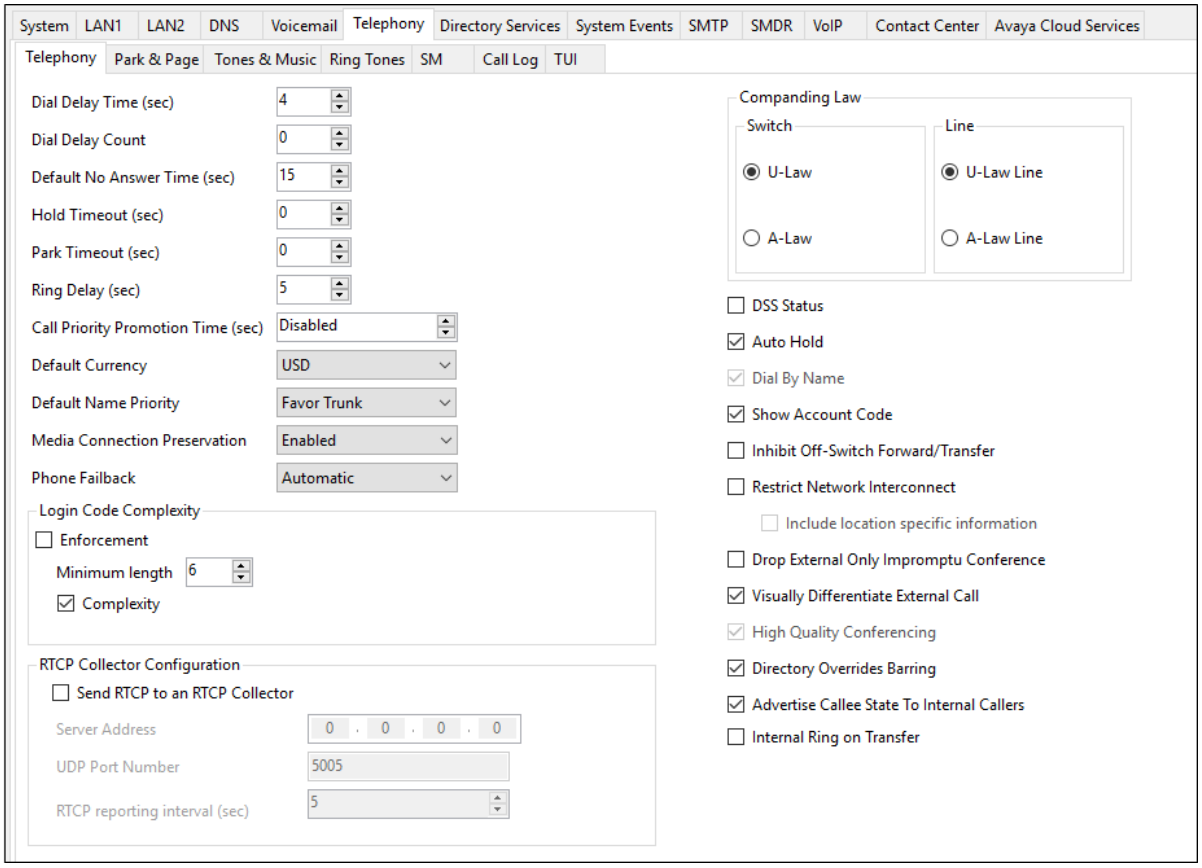
©2020 Avaya Inc. Todos los derechos reservados.

5.3.3. Ficha Telefonía

Para ver o cambiar la configuración de telefonía, seleccione la**Telefonía**pestaña y**Telefonía**subpestaña como se muestra en la siguiente pantalla. Los ajustes presentados aquí simplemente ilustran los valores utilizados en la configuración de referencia y no pretenden ser prescriptivos.

- Desmarque la**Inhibir Desactivar Reenviar/Transferir**casilla para permitir el desvío de llamadas y transferencias de llamadas a la PSTN a través del troncal SIP al proveedor de servicios. Si por razones de seguridad no se debe permitir que las llamadas entrantes se transfieran de nuevo a la PSTN, deje esta configuración marcada.

- Selecciona el**Ley de Compansión**parámetros a**Ley U**como es típico en América del Norte.
- Los valores predeterminados se utilizan en los otros campos.
- Haga clic en el**OK**botón (no se muestra).



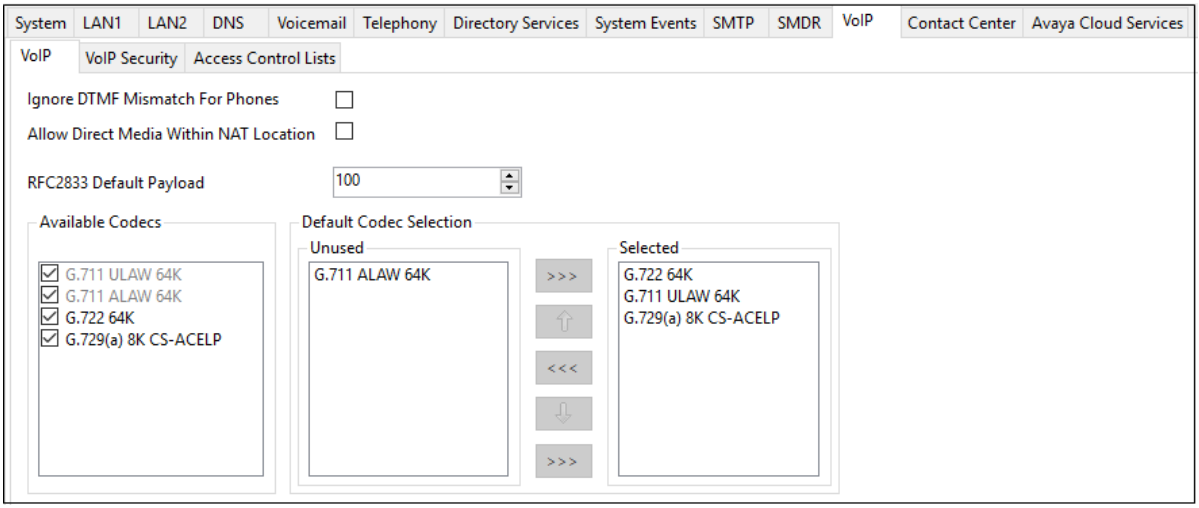
©2020 Avaya Inc. Todos los derechos reservados.

5.3.4. Pestaña VoIP

Navegar a la**VoIP**en el panel Detalles para ver o cambiar los códecs del sistema y la configuración de seguridad de VoIP.

Selecciona el**VoIP→VoIP**pestaña. Configure los siguientes parámetros:

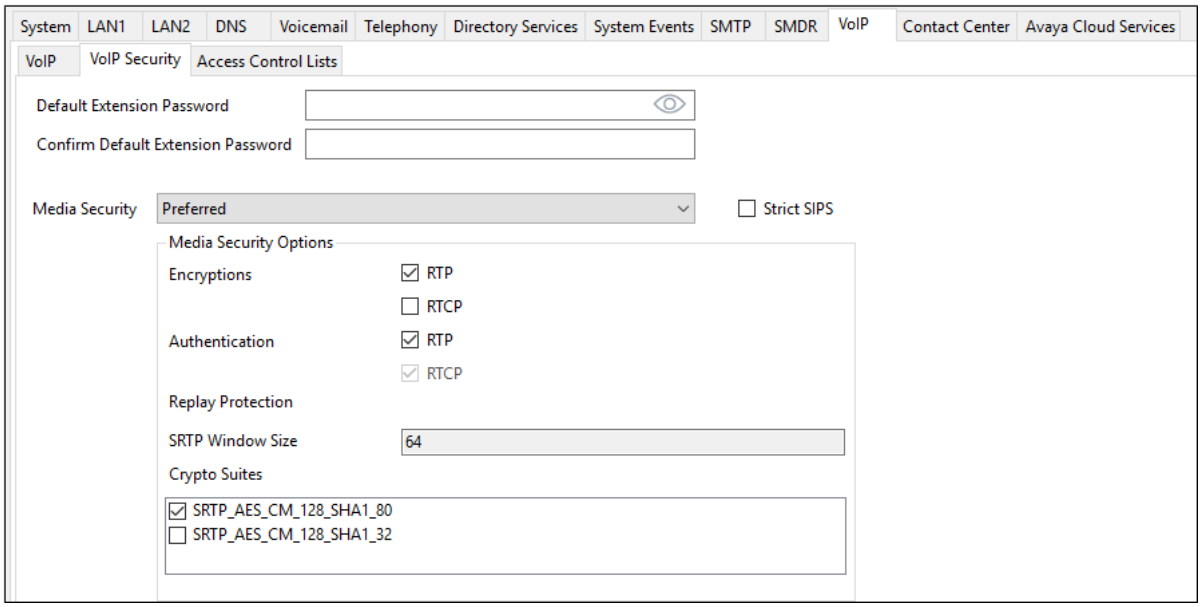
- los**RFC2833 Carga útil predeterminada**El campo permite la configuración manual del tipo de carga útil utilizada en las llamadas SIP iniciadas por IP Office. Durante la prueba de cumplimiento, esto se configuró en**100**, el valor preferido por AT&T.
- Para la selección de códecs, seleccione los códecs y el orden de preferencia de los códecs a la derecha, debajo del **Seleccionado**columna. los**Selección de códec predeterminado**El área permite configurar el orden de preferencia de los códecs en todo el sistema. Los botones entre las dos listas se pueden usar para mover códecs entre las**No usado**y**Seleccionado**y para cambiar el orden de los códecs en el**Seleccionado**lista de códecs. De forma predeterminada, todas las líneas y teléfonos IP (SIP y H.323) utilizarán la selección de códec predeterminado del sistema que se muestra aquí, a menos que se configure de otra manera para una línea o extensión específica. El siguiente ejemplo muestra los códecs utilizados para teléfonos IP (SIP y H.323), se utilizaron los códecs y el orden predeterminados del sistema.
- Hacer clic**OK**para cometer (no se muestra).



©2020 Avaya Inc. Todos los derechos reservados.

Durante la prueba de cumplimiento, se utilizó SRTP internamente en la empresa siempre que fue posible. Para ver o configurar los ajustes de cifrado de medios, seleccione el**VoIP**→**Seguridad VoIP**ficha en el panel Detalles.

- Selecciona el**Seguridad de los medios**menú desplegable para**Privilegiado**para que IP Office intente usar RTP encriptado para dispositivos que lo admitan y recurra a RTP para dispositivos que no admitan encriptación.
- Por debajo**Opciones de seguridad de medios**, Seleccione**RTP**Para el**Cifrados**y**Autenticación** campos.
- Por debajo**Paquetes criptográficos**, Seleccione**SRTP_AES_CM_128_SHA1_80**.
- Hacer clic**OK**para cometer (no se muestra).



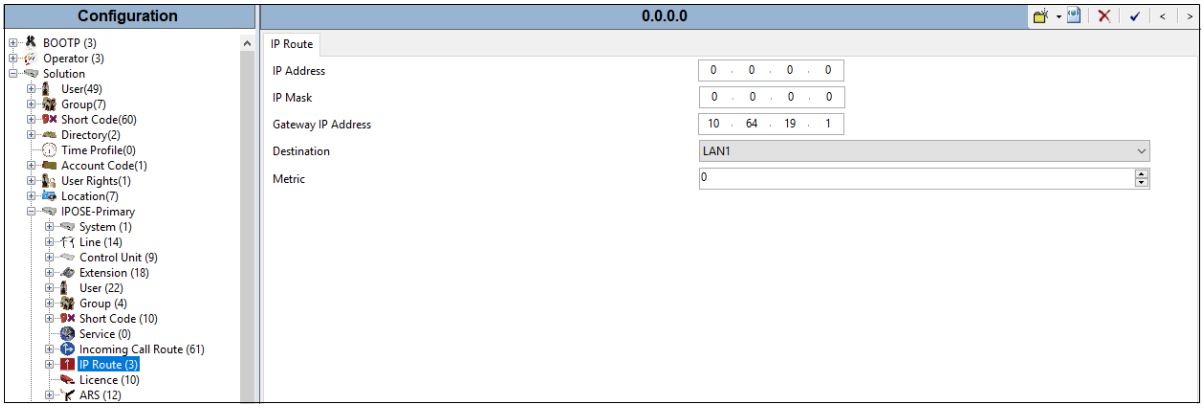
©2020 Avaya Inc. Todos los derechos reservados.

5.4. Ruta IP

En la configuración de muestra, el puerto LAN1 de IP Office está conectado físicamente al conmutador de red de área local en el sitio del cliente de IP Office. Avaya SBCE reside en una subred diferente y requiere una ruta IP para permitir el tráfico SIP entre los dos dispositivos.

Para crear una nueva ruta IP, haga clic derecho en**Ruta IP**en el panel de navegación izquierdo. Seleccione**Nuevo**(no mostrado).

- Selecciona el**Dirección IP**y**Máscara IP**de la subred del lado privado de Avaya SBCE, o ingrese**0.0.0.0**para hacer de esta la ruta predeterminada.
- Establecer**Dirección IP de la puerta de enlace**a la dirección IP del enrutador en la subred de IP Office. La puerta de enlace predeterminada para esta red es**10.64.19.1**.
- Establecer**Destino**a**LAN1**del menú desplegable.
- Hacer clic**OK**para cometer (no se muestra).



©2020 Avaya Inc. Todos los derechos reservados.

Página1853 de 3226.

5.5. Línea SIP

Las siguientes secciones describen la configuración de una línea SIP. La línea SIP termina el extremo CPE de la troncal SIP al servicio AT&T IPTF.

El método recomendado para crear/configurar una Línea SIP es usar la plantilla asociada con el aprovisionamiento descrito en estas Notas de aplicación. La plantilla es un archivo .xml que Avaya IP Office Manager puede usar para crear una nueva línea SIP para troncales SIP con el servicio IPTF de AT&T. Siga los pasos en**Sección 5.5.1**para crear un SIP Trunk a partir de la plantilla.

Algunos elementos relevantes para un entorno de cliente específico no están incluidos en la plantilla o es posible que deban actualizarse después de crear la línea SIP. Los ejemplos incluyen lo siguiente:

- Direcciones IP.
- Credenciales de registro de troncales SIP (si corresponde).
- Entradas SIP URI.
- Ajuste de la**Usar topología de red**Campo de información en la pestaña Transporte.

Por lo tanto, es importante que la configuración de la línea SIP se revise y actualice si es necesario después de crear la línea SIP a través de la plantilla. Los datos de la línea SIP resultantes se pueden verificar con la configuración manual que se muestra en**Secciones 5.5.2**a**5.5.6**.

Además, la siguiente configuración de Línea SIP no es compatible con la Edición básica:

- Línea SIP: número de origen para llamadas desviadas y hermanadas.
- Transporte: segundo servidor DNS explícito.
- Credenciales SIP – Requisito de registro.
- Ingeniería Avanzada SIP.

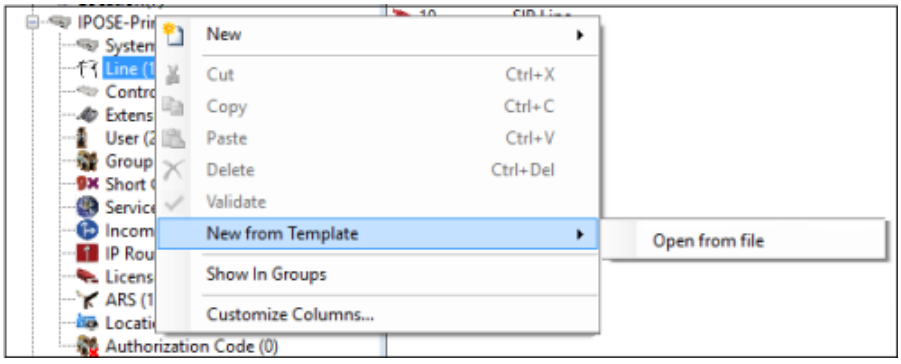
Alternativamente, una línea SIP se puede crear manualmente. Para hacerlo, haga clic derecho en**Línea**en el **Navegación**panel y seleccione**Nuevo→Línea SIP**. Luego, siga los pasos descritos en**Secciones 5.5.2** a**5.5.6**.

©2020 Avaya Inc. Todos los derechos reservados.

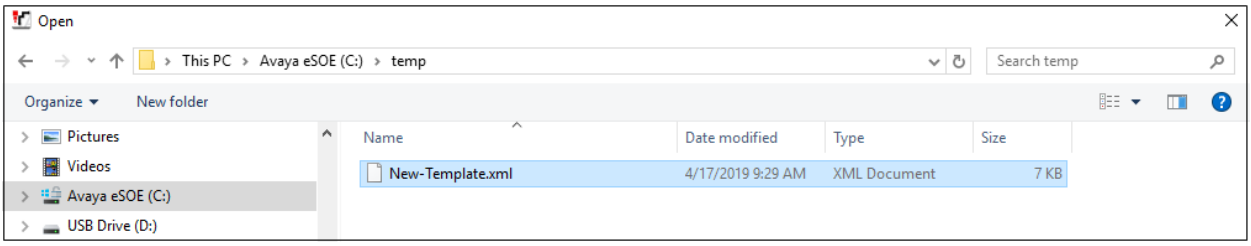
5.5.1. Creación de una línea SIP a partir de una plantilla XML

Nota–Las plantillas de línea SIP generadas por DevConnect siempre se exportan en formato XML. Estas plantillas XML no incluyen información confidencial específica del cliente y, por lo tanto, son adecuadas para su distribución. Las plantillas de formato XML se pueden usar para crear troncales SIP en los sistemas IP Office Standard Edition (IP500 V2) e IP Office Server Edition. Alternativamente, se pueden generar plantillas binarias. Sin embargo, las plantillas binarias incluyen todos los parámetros de configuración del Trunk, incluida la información confidencial específica del cliente. Por lo tanto, las plantillas binarias solo deben usarse para clonar troncales dentro del entorno de un cliente específico.

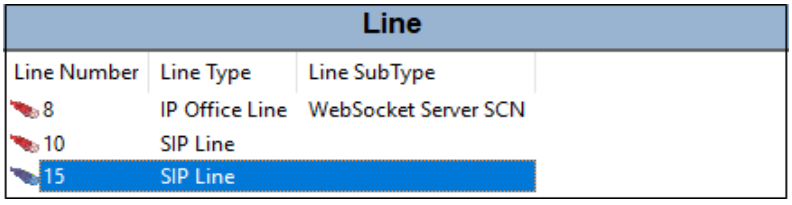
Copie un archivo de plantilla creado previamente en la computadora donde está instalado IP Office Manager. Para crear el Troncal SIP a partir de la plantilla, haga clic derecho en**Línea**en el panel de navegación, luego navegue hasta**Nuevo**→**Nuevo desde plantilla**. Seleccione**Abrir desde archivo.**



Navegue hasta el directorio donde se copió la plantilla en la computadora local (p. ej., l*temperatura*) y selecciónelo. Hacer clic**Abierto**(no mostrado).



Se crea la nueva Línea SIP, y aparecerá en la**Navegación**panel (p. ej., Línea SIP**15**). Los datos de la línea SIP resultantes se pueden verificar con la configuración manual que se muestra en**Secciones 5.5.2** a **5.5.6**.



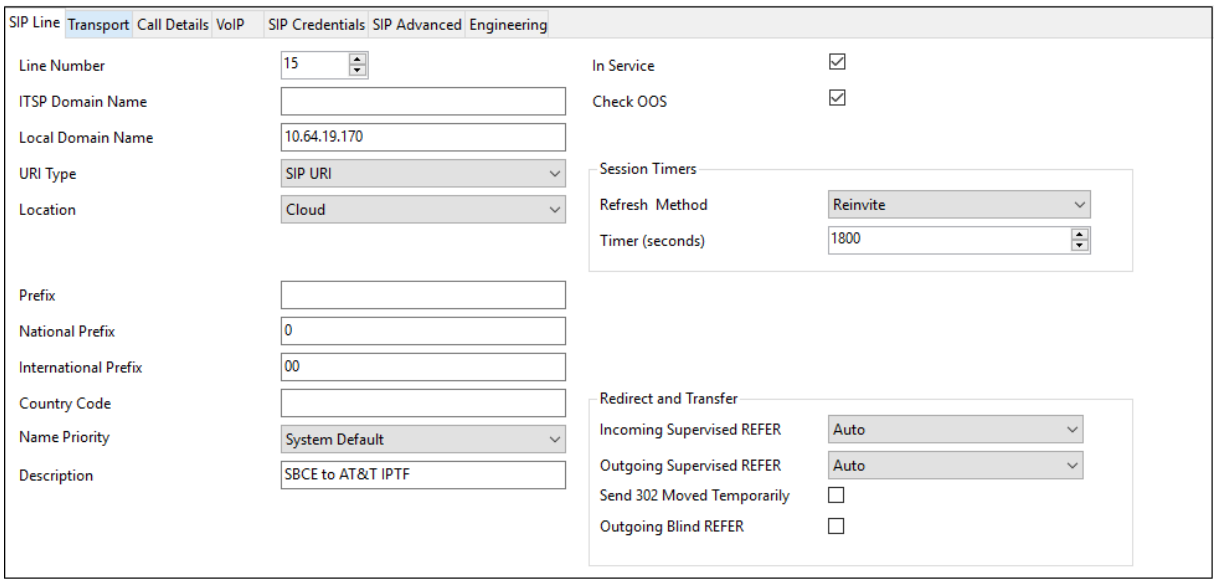
©2020 Avaya Inc. Todos los derechos reservados.

Página1855 de 3226.

5.5.2. Línea SIP: pestaña Línea SIP

Sobre el**Línea SIP**pestaña en el**Detalles**panel, configure o verifique los parámetros como se muestra a continuación:

- **Nombre de dominio de ITSP**: déjelo como predeterminado (en blanco) para que IP Office envíe el**Dirección de proxy de ITSP**como el nombre de dominio. Ver**Sección 5.5.3**.
- **Nombre de dominio local:**Configure la dirección IP pública de la interfaz LAN1 de Avaya IP Office (p. ej.,**10.64.19.170**).
- Comprueba eso**En servicio**casilla está marcada, el valor predeterminado. Esto hace que la troncal esté disponible para llamadas entrantes y salientes.
- Comprueba eso**Comprobar fuera de servicio**casilla está marcada, el valor predeterminado. IP Office utilizará el método SIP OPTIONS para verificar periódicamente la línea SIP.
- **Método de actualización:**Ajustado a**Re invitar**, ya que AT&T no admite ACTUALIZAR
- Establecer**Temporizador (segundos)**a**1800**. Este campo especifica el tiempo de expiración de la sesión. Con este valor, se envía un mensaje de actualización de sesión cada 15 minutos, a la mitad del tiempo de vencimiento.
- **Referencia supervisada entrante**: Establezca este campo en**Auto**(defecto).
- **Referencia supervisada saliente**: Establezca este campo en**Auto**(defecto).
- **Enviar 302 Movido temporalmente**: Verifique que esto no esté marcado (predeterminado).
- **Referencia ciega saliente**: Verifique que esto no esté marcado (predeterminado).
- Utilice los valores predeterminados para los demás campos.
- Hacer clic**OK**(no mostrado).

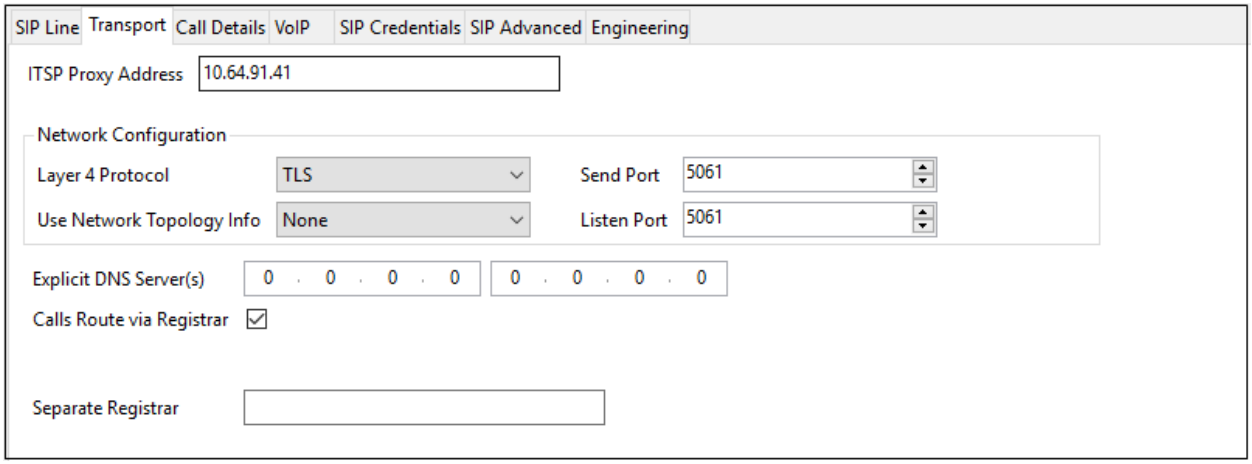


©2020 Avaya Inc. Todos los derechos reservados.

5.5.3. Línea SIP - Ficha Transporte

Selecciona el**Línea SIP**→**Transporte**pestaña y configure lo siguiente:

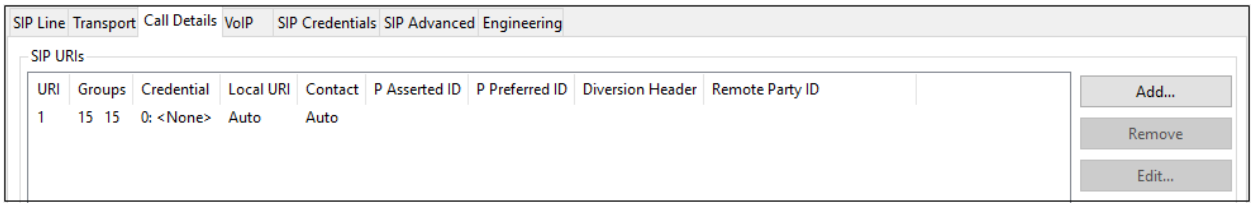
- **Dirección de proxy de ITSP:**Configure la dirección IP de Avaya SBCE A1 (p. ej.,**10.64.91.41**).
- **configuración de la red**→**Protocolo de capa 4**: Ajustado a**TLS**.
- **configuración de la red**→**Puerto de envío**: Ajustado a**5061**.
- **configuración de la red**→**Usar información de topología de red**: Ajustado a**Ninguna**.
- **configuración de la red**→**Puerto de escucha**: Ajustado a**5061**.
- Verificar**Ruta de llamadas vía Registrar:**Habilitado (predeterminado)
- Hacer clic**OK**(no mostrado).



©2020 Avaya Inc. Todos los derechos reservados.

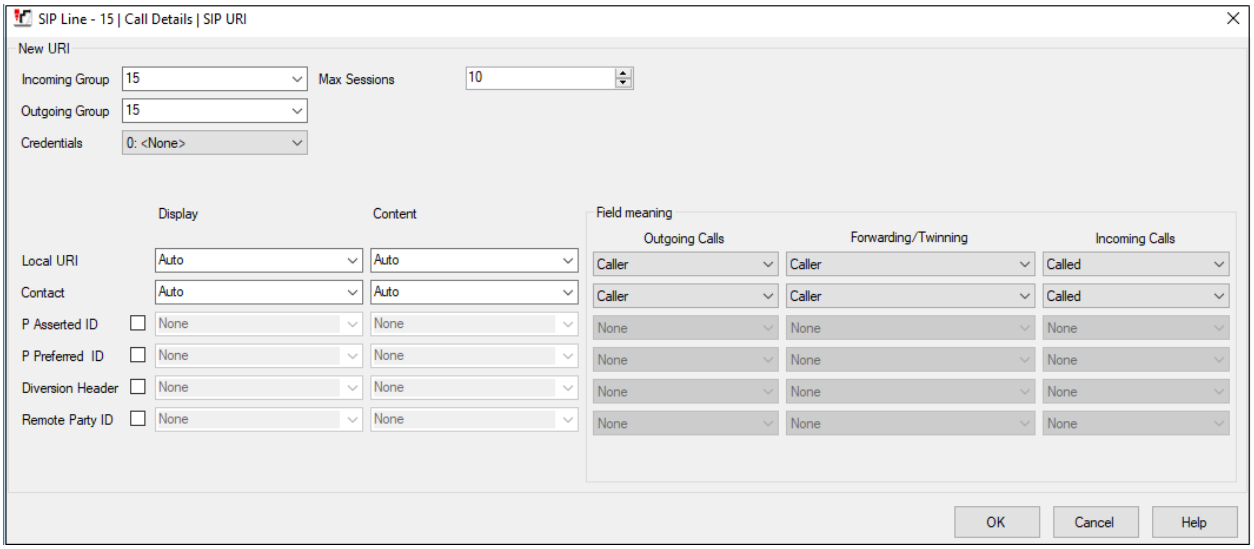
5.5.4. Línea SIP: pestaña Detalles de la llamada

Selecciona el**Detalles de la llamada**pestaña. Para agregar un nuevo SIP URI, haga clic en el**Agregar...**botón. Para revisar un SIP URI existente, selecciónelo y haga clic en el**Editar**botón.



los**URI SIP**se abrirá la ventana. Configure lo siguiente:

- **Grupo entrante:**Establecer en un número de grupo no utilizado, por ejemplo,**15**. Este valor hace referencia a la **ID de grupo de línea**puesto en el**Rutas de llamadas entrantes**en**Sección 5.8**.
- **Sesiones máximas:**En la configuración de referencia, esto se estableció en**10**. Esto establece la cantidad máxima de llamadas simultáneas que pueden usar el URI antes de que Avaya IP Office vuelva a estar ocupado para cualquier otra llamada.
- **Grupo saliente:**Establecer en un número de grupo no utilizado, por ejemplo,**15**.
- Para el**URI local**, y**Contacto**campos, deje las selecciones bajo el**Monitor**y **Contenido** columnas al valor predeterminado**Auto**.
- Sobre el**Significado del campo**sección, configure los valores como se muestra en la siguiente captura de pantalla.
- Hacer clic**OK**.



- Para editar una entrada existente, haga clic en una entrada de la lista y haga clic en el**Editar**botón.
- Cuando se hayan agregado o editado todas las entradas de SIP URI, haga clic en**OK**en la parte inferior de la pantalla (no se muestra).

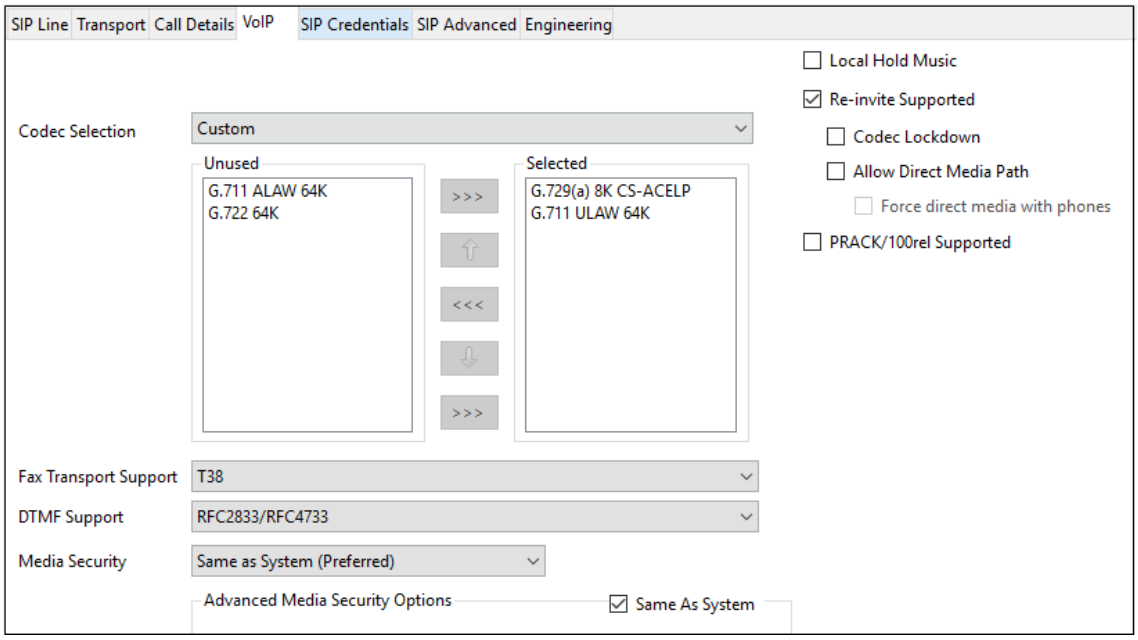
©2020 Avaya Inc. Todos los derechos reservados.

5.5.5. Línea SIP - pestaña VoIP

Selecciona el**Línea SIP→VoIP**pestaña. Establezca los parámetros como se muestra a continuación:

- los**Selección de códec**caja desplegable→**Sistema por defecto**mostrará una lista de todos los códecs disponibles. En la configuración de referencia,**Disfraz**fue seleccionado con**G729(a) 8K CS-ACELP**y **G.711 ULAW 64K**especificado. Esto hace que Avaya IP Office incluya estos códecs en la oferta del Protocolo de descripción de sesión (SDP) y en el orden especificado. Tenga en cuenta que en la configuración de referencia, G.729A se establece como el códec preferido en el enlace troncal SIP a la red IPTF de AT&T.

- El fax T.38 es el método preferido para el fax. Selecciona el**Soporte de transporte de fax**a**T.38**del menú desplegable. Ver**Sección 2.2**,**artículo 7**.
- Selecciona el**Soporte DTMF**campo a**RFC2833/RFC4733**. Esto indica a IP Office que envíe tonos DTMF mediante mensajes de eventos RTP como se define en RFC2833.
- Selecciona el**Seguridad de los medios**menú desplegable para**Igual que el sistema (preferido)**. Verifique que el **Igual que el sistema**se comprueba el parámetro. Esta configuración utilizará el mismo nivel de seguridad de medios para la troncal que se define para el sistema en**Sección 5.3.4**. La seguridad de los medios a nivel del sistema está establecida en**Privilegiado,**especificando que se prefiere SRTP sobre RTP.
- los**Volver a invitar Compatible**El parámetro se puede marcar para permitir la renegociación del códec en los casos en que el destino de una llamada entrante o transferencia no admita el códec negociado originalmente en el enlace troncal.
- Los valores predeterminados se pueden utilizar para todos los demás parámetros.
- Haga clic en el**OK**para cometer (no se muestra).



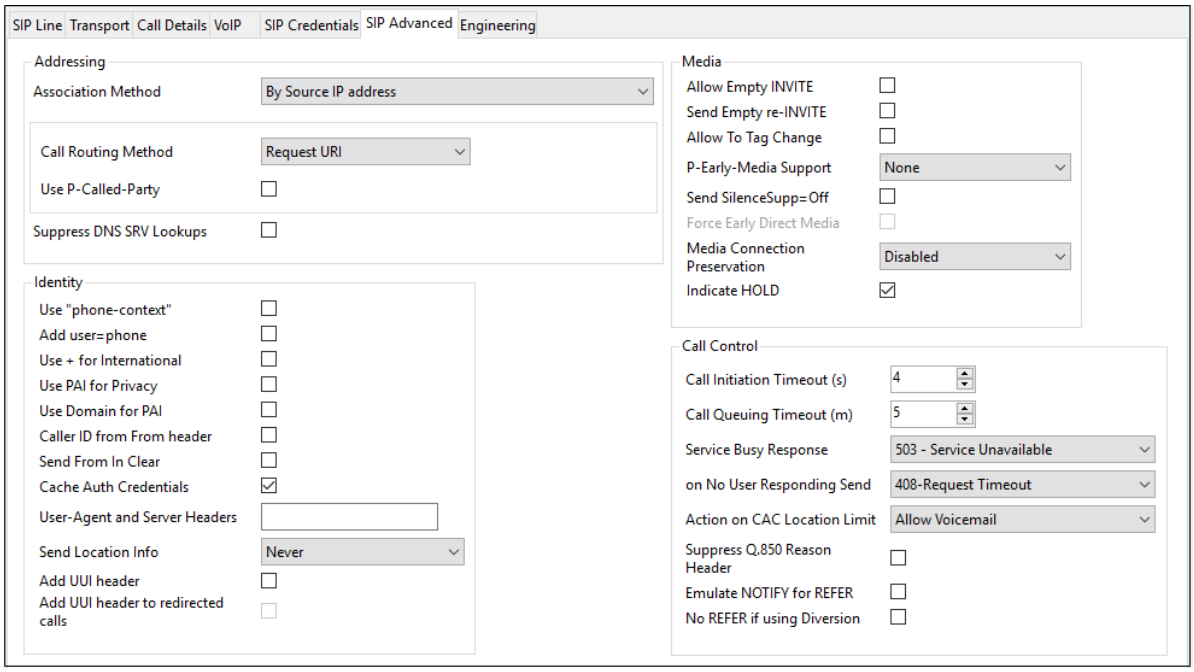
©2020 Avaya Inc. Todos los derechos reservados.

5.5.6. Línea SIP – Pestaña Avanzado SIP

IP Office se puede configurar para señalar cuando una llamada se pone en espera mediante el envío de una INVITACIÓN con el atributo de medios "sendonly". AT&T, a su vez, responderá con el atributo de medios "recvonly" y dejará de enviar medios RTP mientras la llamada esté en espera. Cuando la llamada se suspende, IP Office enviará otra INVITACIÓN con el atributo de medios "sendrecv" que indica a AT&T que comience a enviar RTP nuevamente.

Para que Avaya IP Office envíe una señal a AT&T cuando una llamada se pone en espera o no, seleccione la**Línea SIP** → **SIP Avanzado**pestaña e ingrese lo siguiente:

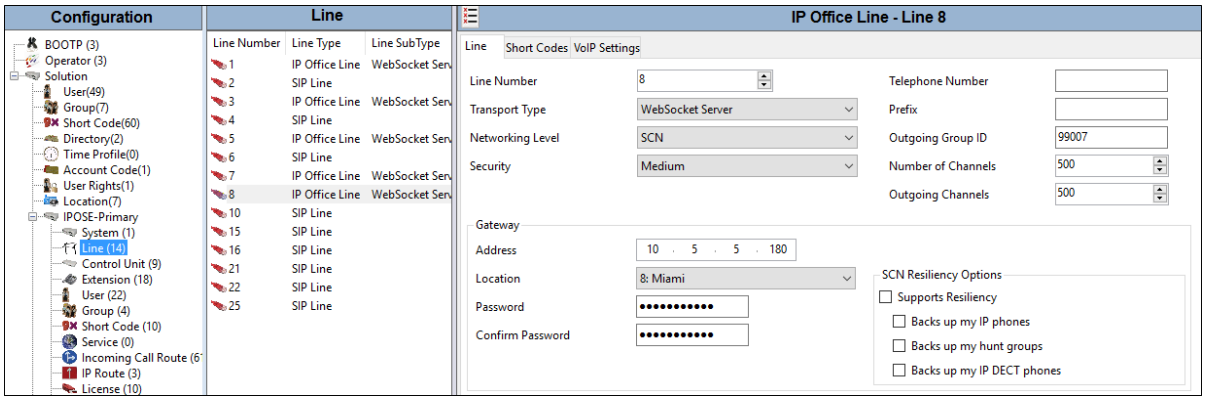
- Seleccione**Indicar ESPERA**en el**Medios de comunicación**sección.
- Hacer clic**OK**para cometer (no se muestra).



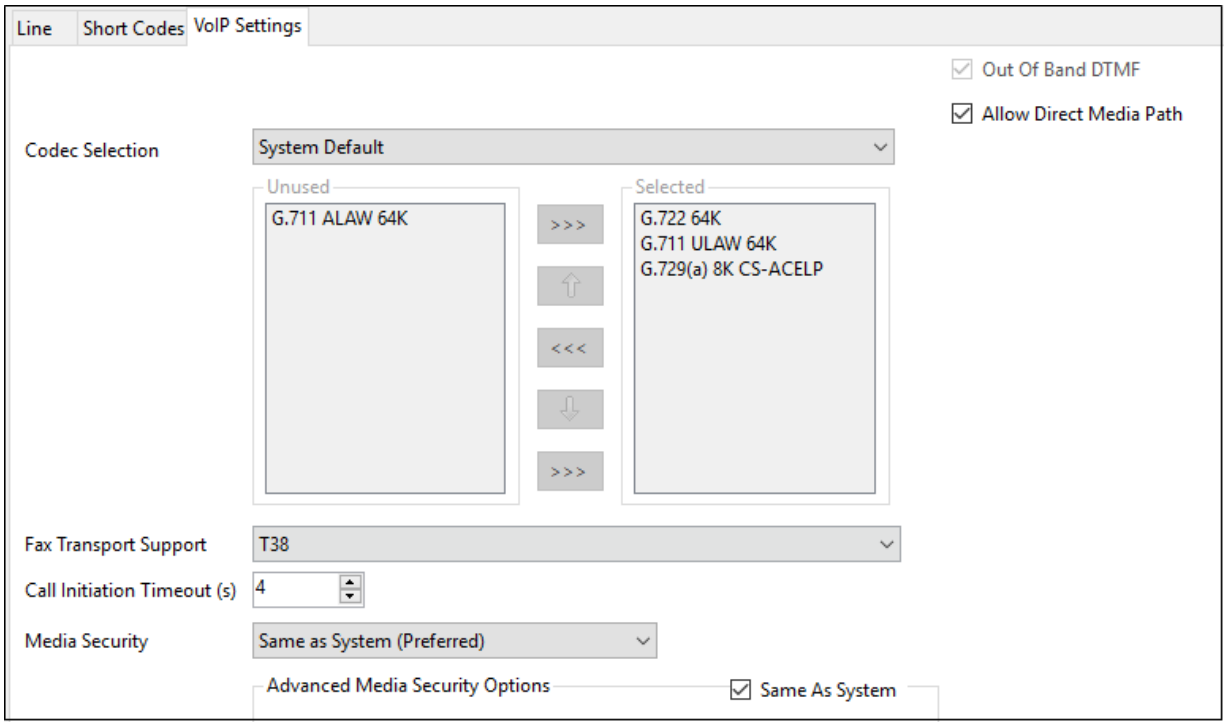
©2020 Avaya Inc. Todos los derechos reservados.

5.6. Línea IP Office

En los sistemas IP Office Server Edition, las líneas de IP Office se crean automáticamente en cada servidor cuando se agrega un servidor secundario o un sistema de expansión a la solución. Para editar una línea de IP Office existente, seleccione**Línea**en el panel de navegación y seleccione la línea adecuada para configurarla en el panel de grupo. La siguiente pantalla muestra la línea de IP Office al sistema de expansión IP500 V2.



La siguiente pantalla muestra la línea de IP Office,**Configuración VoIP**pestaña. En la configuración de referencia, una máquina de fax está conectada a uno de los puertos analógicos del Sistema de expansión.**Soporte de transporte de fax**se establece en**T.38**. Se utilizaron valores predeterminados para todos los demás parámetros.



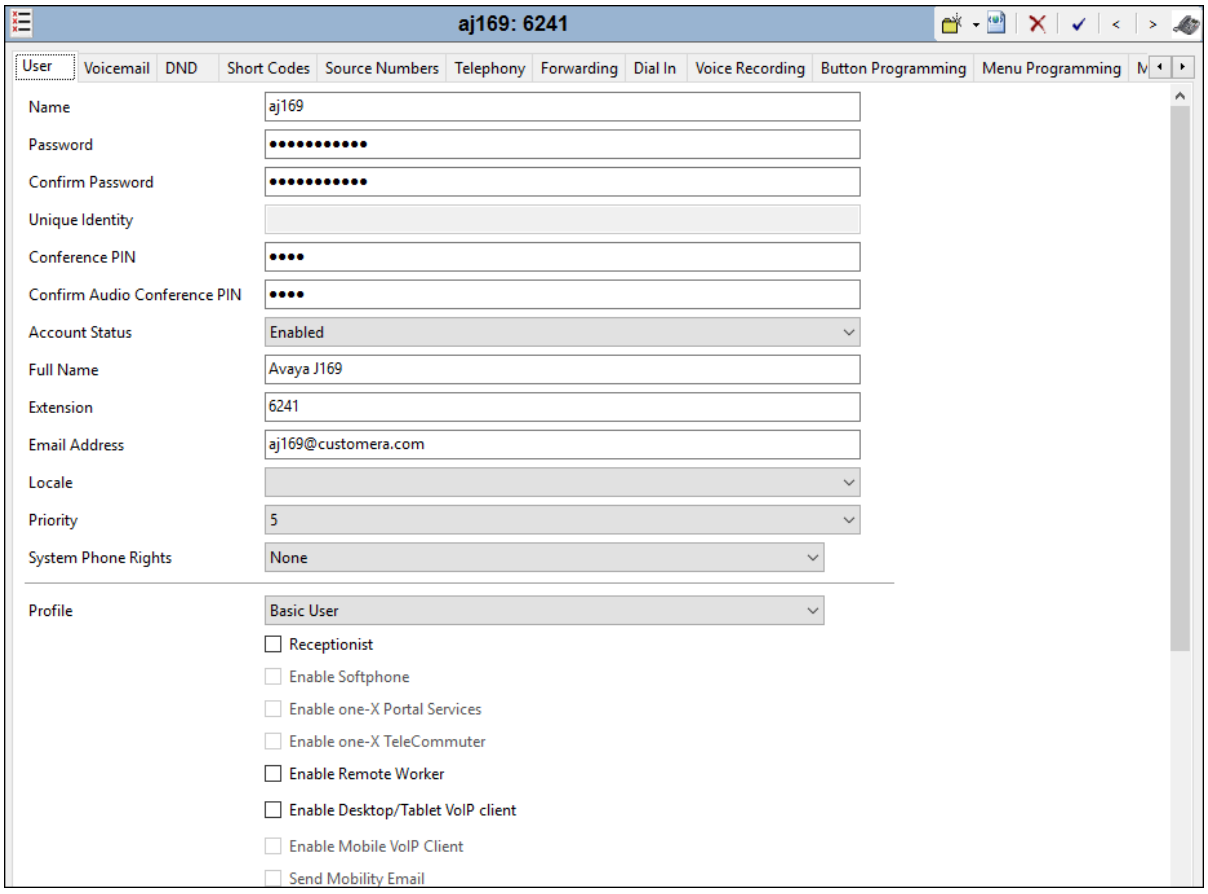
©2020 Avaya Inc. Todos los derechos reservados.

5.7. Usuarios, extensiones y grupos de búsqueda

En esta sección, se ilustrarán ejemplos de usuarios, extensiones y grupos de IP Office. En aras de la brevedad, solo uno de los usuarios y extensiones que se muestran en**Figura 1**será presentado, ya que la configuración es fácilmente extrapolable a otros usuarios. Para agregar un usuario, haga clic derecho en **Usuario**en el **Navegación**panel y seleccione**Nuevo**. Para editar un usuario existente, seleccione**Usuario**en el **Navegación** panel, y seleccione el usuario apropiado para ser configurado en el**Grupo**cristal.

5.7.1. Usuario

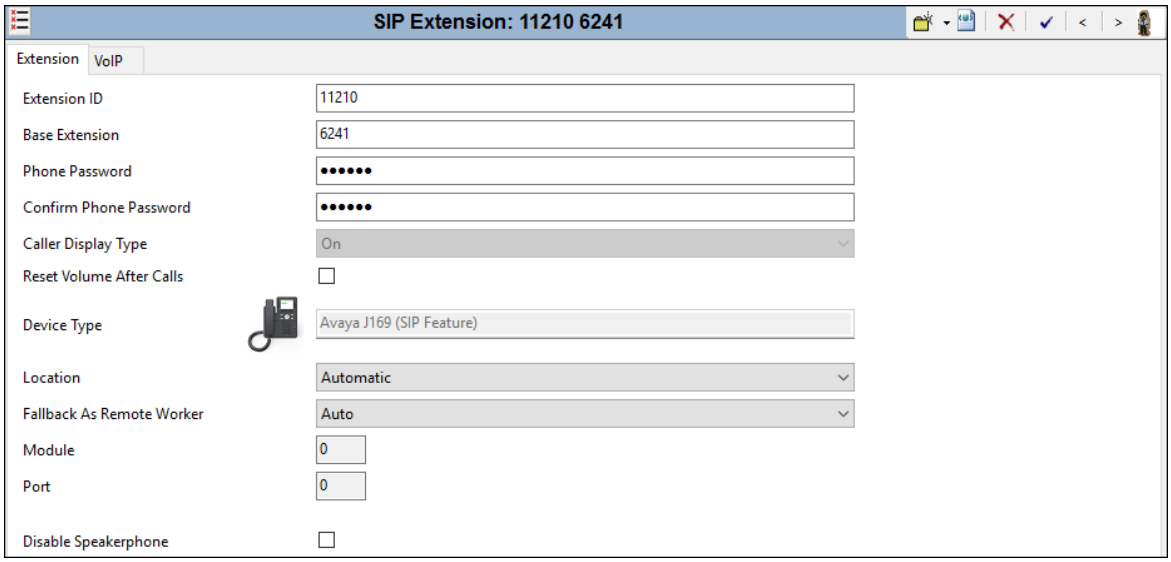
La siguiente pantalla muestra la**Usuario**pestaña para el usuario 6241. Como se muestra en**Figura 1**, este usuario corresponde al terminal SIP Avaya J169.



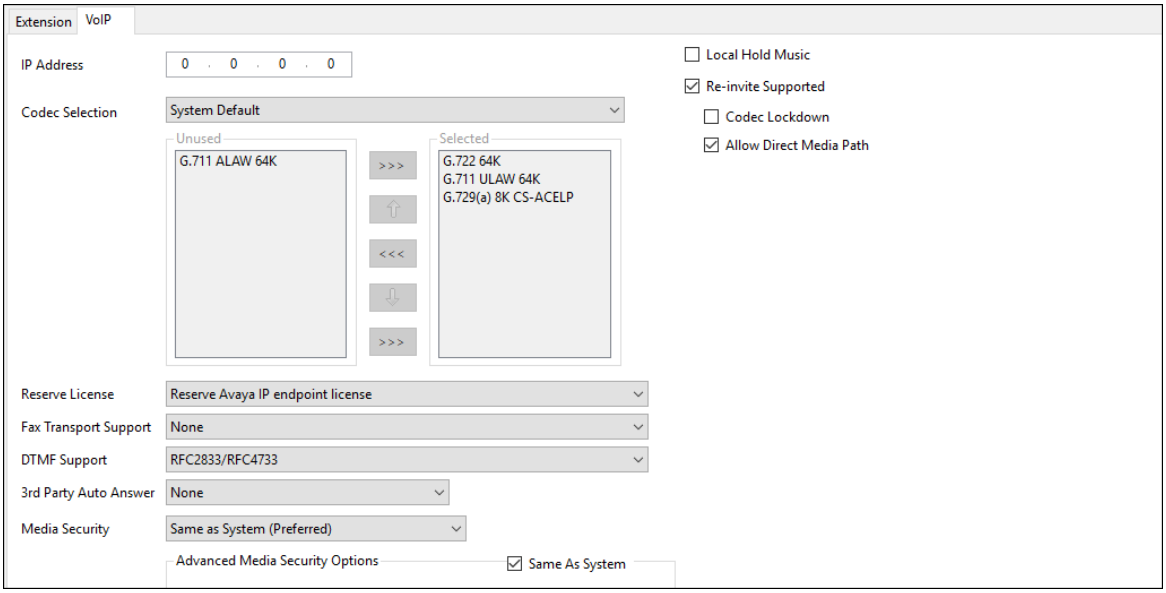
©2020 Avaya Inc. Todos los derechos reservados.

5.7.2. Extensión

La siguiente pantalla muestra la información de la extensión para el usuario 6241 (Avaya J169 SIP). Para ver, seleccione**Extensión**desde el panel de Navegación, y la extensión apropiada desde el panel de Grupo.



La siguiente pantalla muestra la**VoIP**pestaña para la extensión. los**Dirección IP**el campo puede dejarse en blanco. Comprobar el **Reservar la licencia de endpoint IP de Avaya**caja. los**Selección de códec**El parámetro puede conservar la configuración predeterminada "**Sistema por defecto**" para seguir la configuración del sistema que se muestra en**Sección 5.3.4**. El parámetro Media Security también puede conservar la configuración predeterminada "**Igual que el sistema (preferido)**" para seguir la configuración del sistema que se muestra en**Sección 5.3.4**.

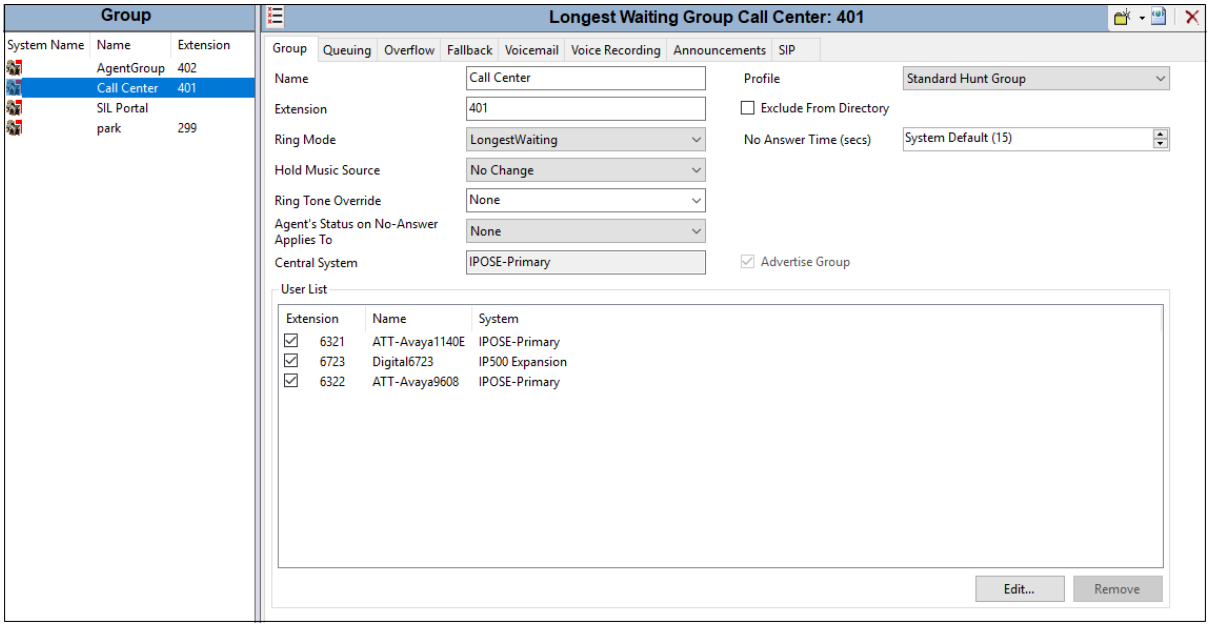


©2020 Avaya Inc. Todos los derechos reservados.

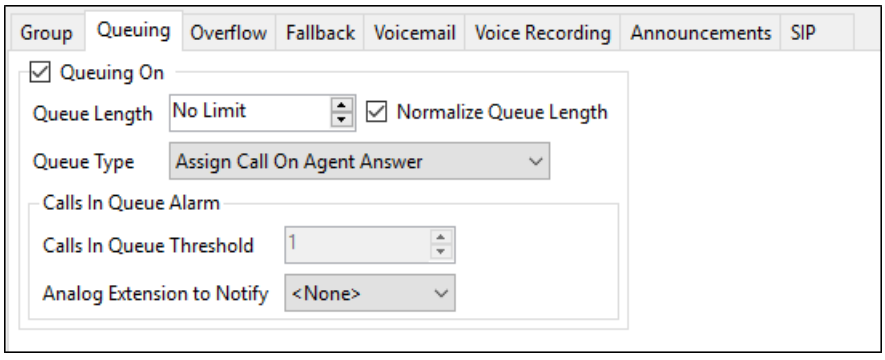
5.7.3. Grupos de búsqueda

Durante la verificación de estas Notas de aplicación, los usuarios también podrían recibir llamadas entrantes como miembros de un grupo de búsqueda. Para configurar un nuevo grupo de búsqueda, haga clic derecho**Grupo**en el panel de navegación y seleccione**Nuevo**. Para ver o editar un grupo de búsqueda existente, seleccione**Grupo**desde el panel de Navegación, y el grupo de búsqueda apropiado desde el panel de Grupo.

La siguiente pantalla muestra la**Grupo**pestaña para el grupo de búsqueda 401. Las extensiones telefónicas en el **Lista de usuarios** se basan en la extensión que no se ha utilizado durante el período más largo, debido a la **Modo de timbre**ajuste "**Espera más larga**" (es decir, "espera más larga", la mayoría de los usuarios inactivos reciben la próxima llamada). Haga clic en el**Editar**botón para cambiar el**Lista de usuarios**.

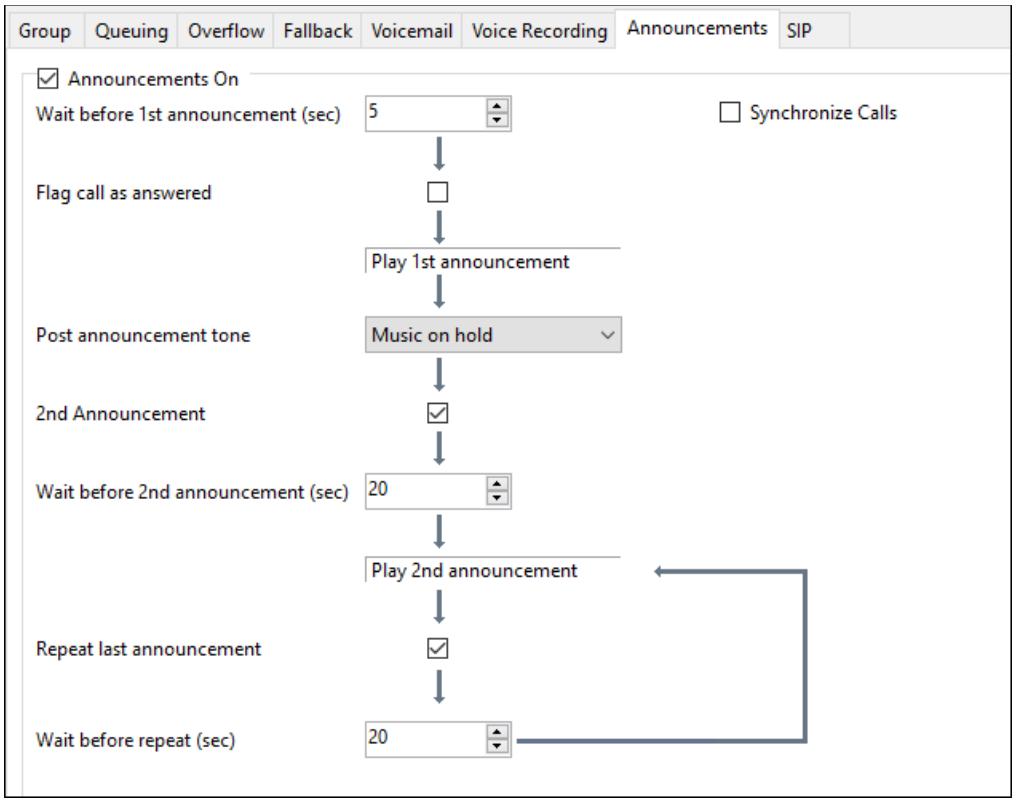


Bajo la**haciendo cola**pestaña, verifique la**Cola activada**cuadro y establecer el**Longitud de la cola**campo a cualquier valor deseable. Utilice los valores predeterminados para todos los demás campos.



©2020 Avaya Inc. Todos los derechos reservados.

Bajo la**Anuncios**pestaña, verifique la**Anuncios en**caja. El tiempo de espera se puede establecer en cualquier valor deseable. los**Sincronizar llamadas**está marcada para reducir en gran medida la cantidad de canales de correo de voz necesarios para reproducir anuncios. Estos anuncios se reproducen si un agente para una habilidad en particular no está disponible.



En la configuración de referencia, estos pasos se usaron para crear el grupo de búsqueda adicional "AgentGroup" (402).

©2020 Avaya Inc. Todos los derechos reservados.

5.8. Ruta de llamada entrante

Nota–Los dígitos definidos y coincidentes en la tabla de ruta de llamadas entrantes son los dígitos DNIS especificados en el URI de solicitud de AT&T, no los dígitos DID marcados por la persona que llama. El servicio IPTF puede entregar varias longitudes de dígitos DNIS en la URI de solicitud de invitación SIP, según el aprovisionamiento del orden del circuito. En la configuración de referencia, el servicio IPTF entregó 15 dígitos.

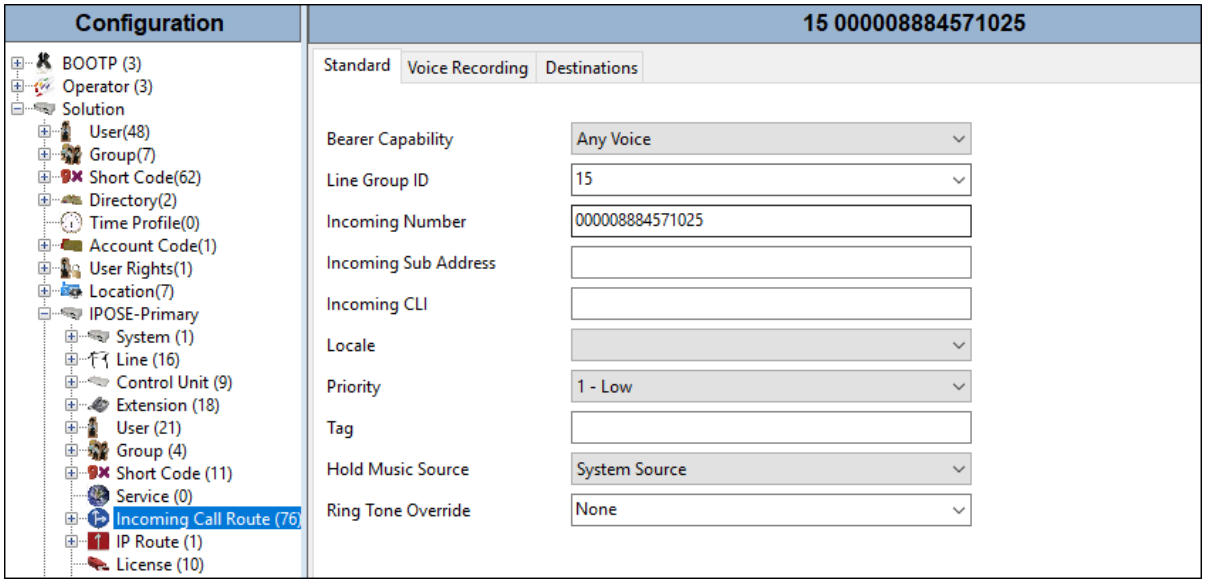
La tabla de rutas de llamadas entrantes asignará números DNIS de AT&T específicos a un usuario de IP Office o grupo de búsqueda, así como a scripts de Voicemail Pro.

Para agregar una ruta de llamada entrante, haga clic derecho en**Ruta de llamada entrante**en el panel de navegación y seleccione**Nuevo**(no mostrado). Para editar una ruta de llamada entrante existente, seleccione una**Ruta de llamada entrante** en el panel de navegación y la información de la ruta de llamada asociada se muestra en el panel de grupo.

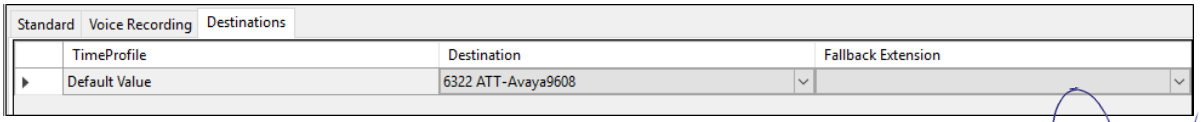
5.8.1. Llamadas a estaciones IP Office y grupos de búsqueda

En el siguiente ejemplo, el número entrante**000008884571025**está dirigido al teléfono H.323 6322. En el **Estándar**pestaña ingrese lo siguiente:

- **ID de grupo de línea**: Introduzca la Línea SIP definida en**Sección 5.5**(p.ej,**15**).
- **Número entrante**: ingrese los dígitos DNIS asociados enviados por AT&T (p. ej., **000008884571025**).
- Utilice valores predeterminados para los campos restantes y haga clic en**OK**(no mostrado).

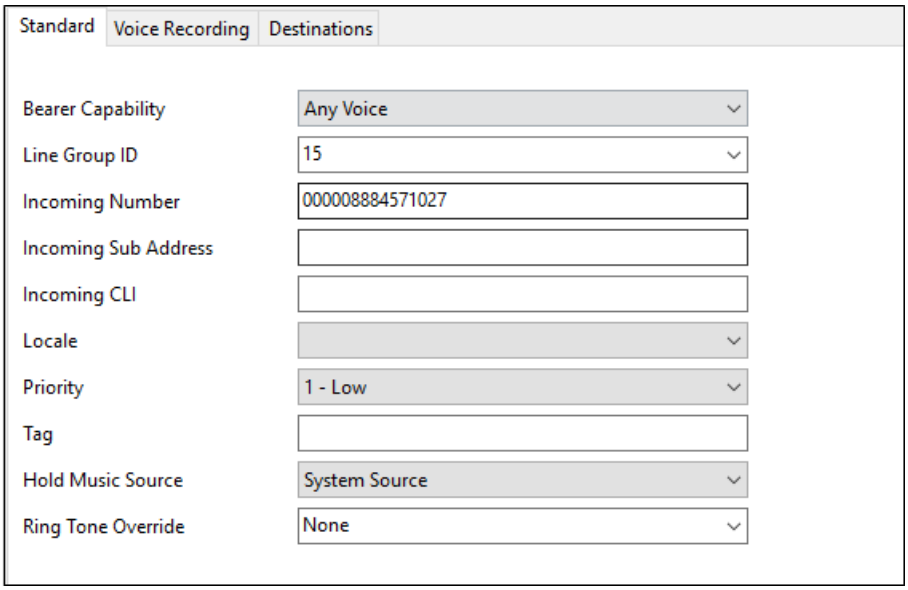


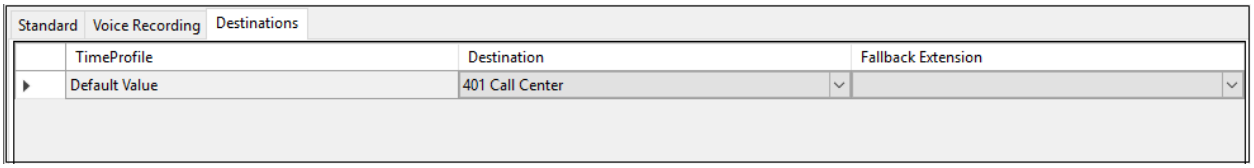
Selecciona el**Destinos**pestaña. Desde el**Destino**menú desplegable, seleccione el terminal asociado con este número, extensión**6322**en este ejemplo.



©2020 Avaya Inc. Todos los derechos reservados.

A continuación se muestra un ejemplo de una llamada para AT&T DNIS**000008884571027**siendo dirigido a Hunt Group **401**(Centro de llamadas).





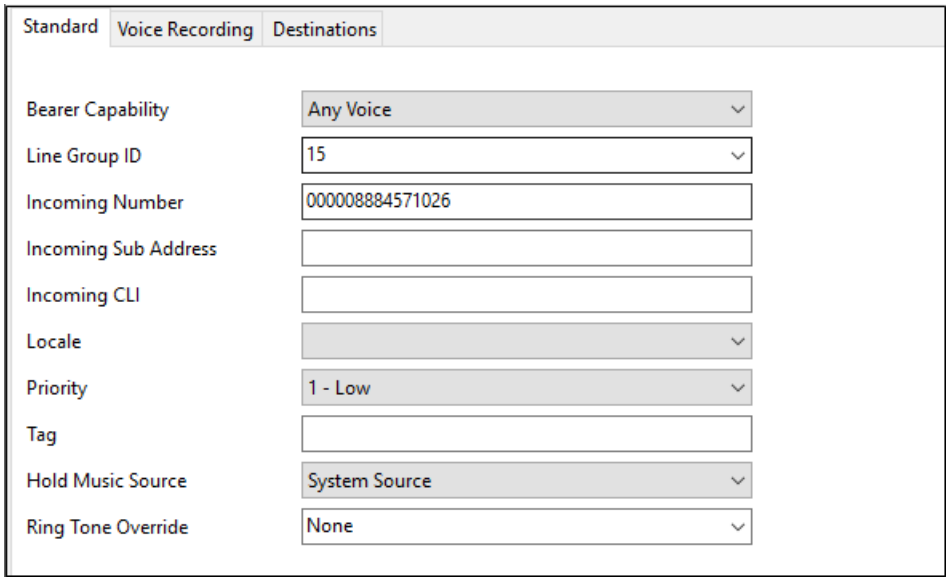
©2020 Avaya Inc. Todos los derechos reservados.

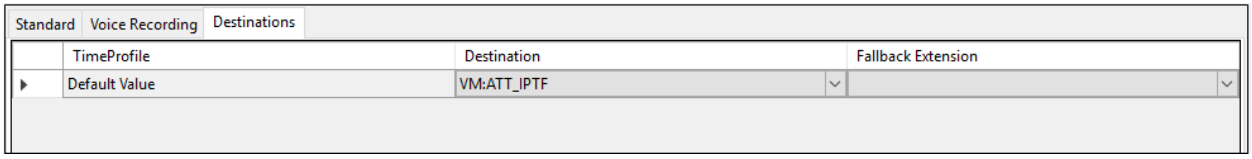
5.8.2. Guiones de llamadas a Voicemail Pro

Como se describe a continuación en**Sección 5.9**, los guiones de Voicemail Pro se definen con nombres específicos. Estos nombres de guiones se especifican como destinos en la tabla de rutas de llamadas entrantes.

En el siguiente ejemplo, el número entrante**000008554571026**se dirige a la secuencia de comandos de la operadora automática de Voicemail Pro**ATT_IPTF**.

1. En el**Estándar**pestaña repetir los pasos en**Sección 5.8.1**, con los siguientes cambios:
   - **Número entrante**: ingrese los dígitos DNIS asociados enviados por AT&T (p. ej., **000008554571026**).
2. En el**Destinos**pestaña ingrese lo siguiente:
   - En el**Destinos**columna, ingrese la cadena**Máquina virtual: ATT_IPTF**en el menú desplegable (tenga en cuenta que si el módulo de correo de voz no aparece en la lista, ingrese el valor manualmente).
   - Utilice valores predeterminados para los campos restantes y haga clic en**OK**(no mostrado).





©2020 Avaya Inc. Todos los derechos reservados.

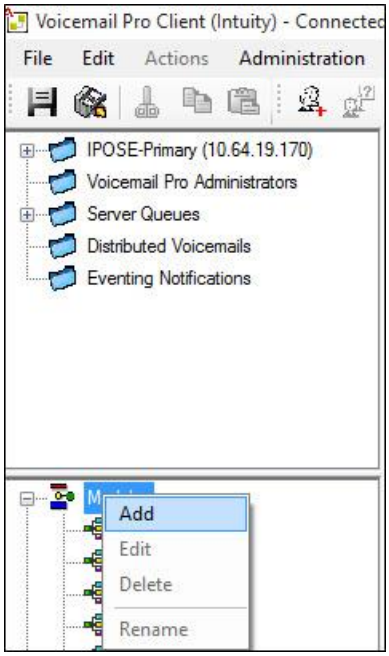
5.9. Aprovisionamiento de centro de llamadas en Voicemail Pro

Nota–Si bien el aprovisionamiento y la programación de Voicemail Pro están fuera del alcance de este documento, a continuación se describe un ejemplo de script de operadora automática.

En la configuración de referencia, Voicemail Pro se usa para el procesamiento de correo de voz y para simular la funcionalidad básica del centro de llamadas.

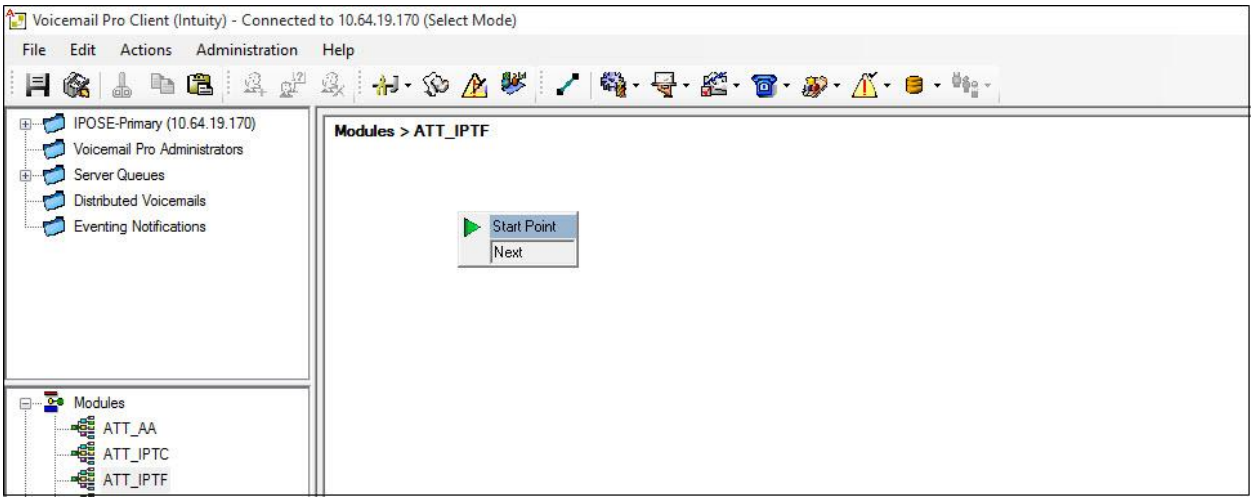
La función de operadora automática se aprovisionó para solicitar a las personas que llaman que seleccionen una opción numérica (1, 2 o 3), que transferiría la llamada a un grupo de búsqueda de IP Office de Avaya asociado (centro de llamadas, grupo de agentes) o a una extensión específica. Esto se logra a través de los siguientes pasos:

1. Grupos de caza**Centro de llamadas**y**Grupo de agentes**se crean en IP Office (**Sección 5.7.3**).
2. El usuario 6241 se crea en IP Office (**Sección 5.7.1**)
3. Ruta de llamadas entrantes para dígitos DNIS**0000088845710 26**se define para el acceso a la secuencia de comandos de la operadora automática (**Sección 5.8.2**).
4. A través de la interfaz GUI de Voicemail Pro:
    - Abre el**Cliente Voicemail Pro**aplicación e inicie sesión en el servidor de Voicemail Pro (no se muestra).
    - Crear un**Punto de partida**haciendo clic derecho en**Módulos**y seleccionando**Agregar**.



- Introduzca un nombre (por ejemplo,**ATT_IPTF**) y haga clic en**OK**(no mostrado). El nuevo script "ATT_IPTF" aparecerá en Módulos y aparecerá un ícono de Punto de inicio en el área de trabajo.

©2020 Avaya Inc. Todos los derechos reservados.



- Haga clic en el**Punto de partida**icono para activar las opciones de script en la parte superior de la pantalla. De las opciones, seleccione el**Acciones básicas**y haga , Selecciona el**Menú**icono , clic en el área de trabajo para colocar el**Menú**icono.

  i. Haga doble clic en el**Punto de partida**icono.

  1. En el**General**pestaña→**Nombre de token**, ingresar**Punto de partida**y haga clic**OK** (no mostrado).

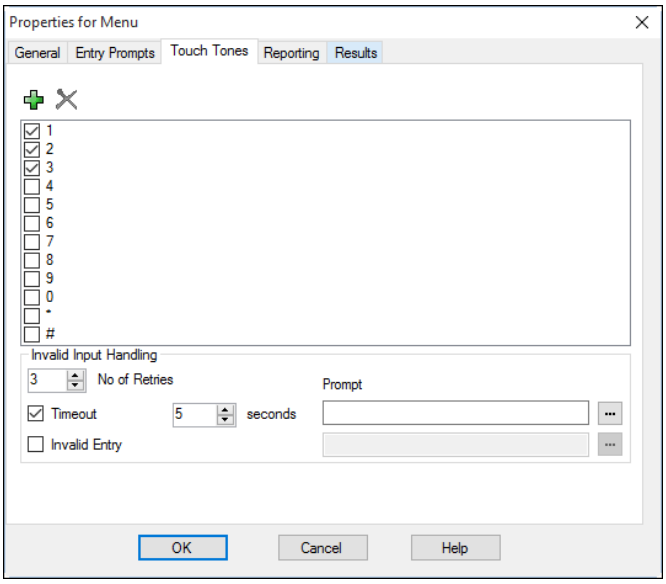
  ii. Haga doble clic en el**Menú**icono.

  1. En el**General**pestaña→**Nombre de token**, ingresar**Menú**(no mostrado).
  2. En el**Indicaciones de entrada**pestaña (no se muestra), seleccione o cree una**Indicación de entrada**que le indicará a la persona que llama qué dígitos debe presionar (p. ej., **menuprincipal.wav**). Para modificar una grabación existente, haga doble clic en el . archivo wav y volver a grabar. Si no existen archivos .wav, haga doble clic en el icono para abrir el editor .wav.
  3. En el**Tono táctil**pestaña:

     una. Seleccione**1, 2,**y**3**como posibles dígitos de entrada.

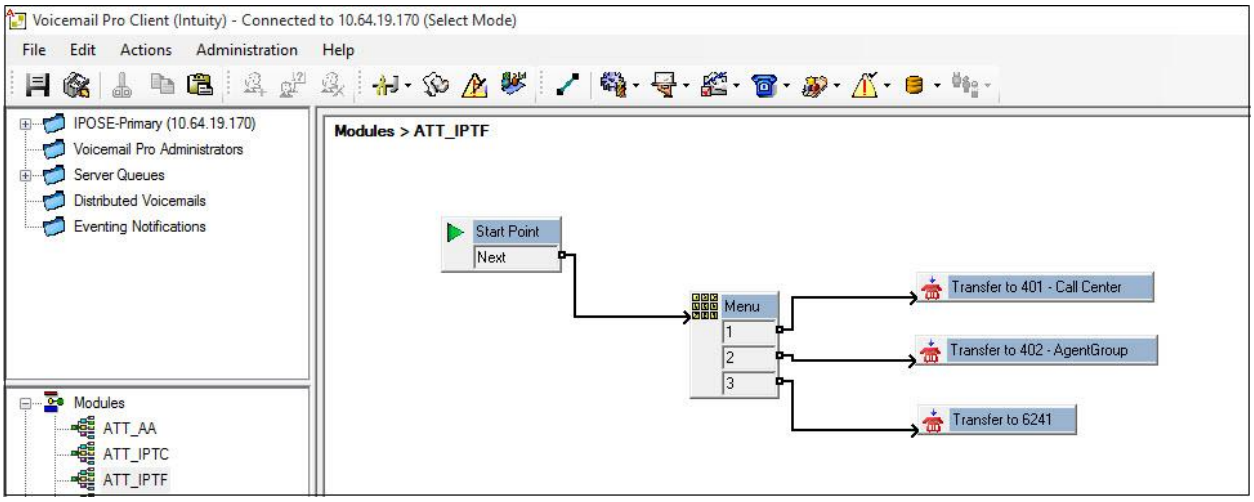
     b. Seleccione**3**por**Número de reintentos**.
  4. Haga clic en**OK**.

©2020 Avaya Inc. Todos los derechos reservados.



- Haga clic en el icono Acciones de telefonía , seleccione el icono Transferir y haga clic en el área de trabajo para colocar el**Transferir**icono en el área de trabajo. Esto se utilizará para el "Centro de llamadas". Seleccione y coloque dos iconos de transferencia más (estos se utilizarán para "Grupo de agentes" y "Usuario 6241").
    i. Haga doble clic en el primero**Transferir**icono.
        1. En el**General**pestaña→**Nombre de token**=**Transferir al 401 - Call Center** (no mostrado).
        2. En el**Específico**pestaña→**Destino = 401**(no mostrado).
    ii. Haga doble clic en el segundo**Transferir**icono.
        1. En el**General**pestaña→**Nombre de token**=**Transferir a 402 - AgentGroup**(no mostrado).
        2. En el**Específico**pestaña→**Destino**=**402**(no mostrado).
    iii. Haga doble clic en el tercero**Transferir**icono.
        1. En el**General**pestaña,**Nombre de token**=**Transferir al 6241**(no mostrado).
        2. En el**Específico**pestaña,**Destino = 6241**(no mostrado).
- En la barra de opciones, seleccione el icono Conector y:
    i. Arrastre una línea de flujo de conexión desde el**Punto de partida**caja a la**Menú**cuadro (vea la captura de pantalla a continuación).
    ii. Arrastre las líneas de flujo de conexión de cada uno de los**Menú**opciones a sus asociados **Transferir** cajas (ver captura de pantalla a continuación).

©2020 Avaya Inc. Todos los derechos reservados.



5. En el menú superior, seleccione**Expediente→Guardar y hacer en vivo**o seleccione el icono.

Cuando se recibe el número DNIS de AT&T asociado (p. ej.,**000008884571026**), IP Office enviará la llamada a Voicemail Pro. A la persona que llama se le pedirá que ingrese 1, 2 o 3 para acceder al Centro de llamadas, al Grupo de agentes o al usuario 6241. La extensión asociada de Avaya IP Office (p. ej., 401, 402 o 6241) luego sonará.

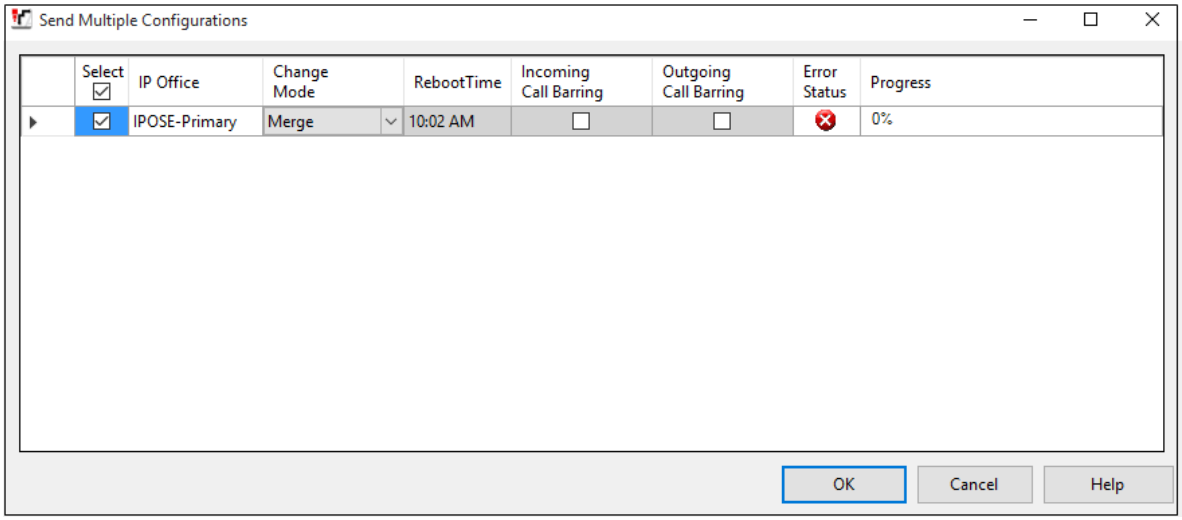
©2020 Avaya Inc. Todos los derechos reservados.

5.10. Guardar la configuración del servidor primario de IP Office

Los cambios de aprovisionamiento realizados en Avaya IP Office Manager deben aplicarse al servidor de Avaya IP Office para que los cambios surtan efecto. En la parte superior de la página de Avaya IP Office Manager, haga clic en**Expediente→Guardar configuración**(si esa opción está atenuada, no hay cambios pendientes).

Aparecerá una pantalla similar a la siguiente, con**Unir**o**Reiniciar**seleccionado automáticamente, en función de la naturaleza de los cambios de configuración. los**Unir**La opción guardará el cambio de configuración sin afectar la operación actual del sistema. los**Reiniciar**La opción guardará la configuración y hará que el servidor Avaya IP Office se reinicie.

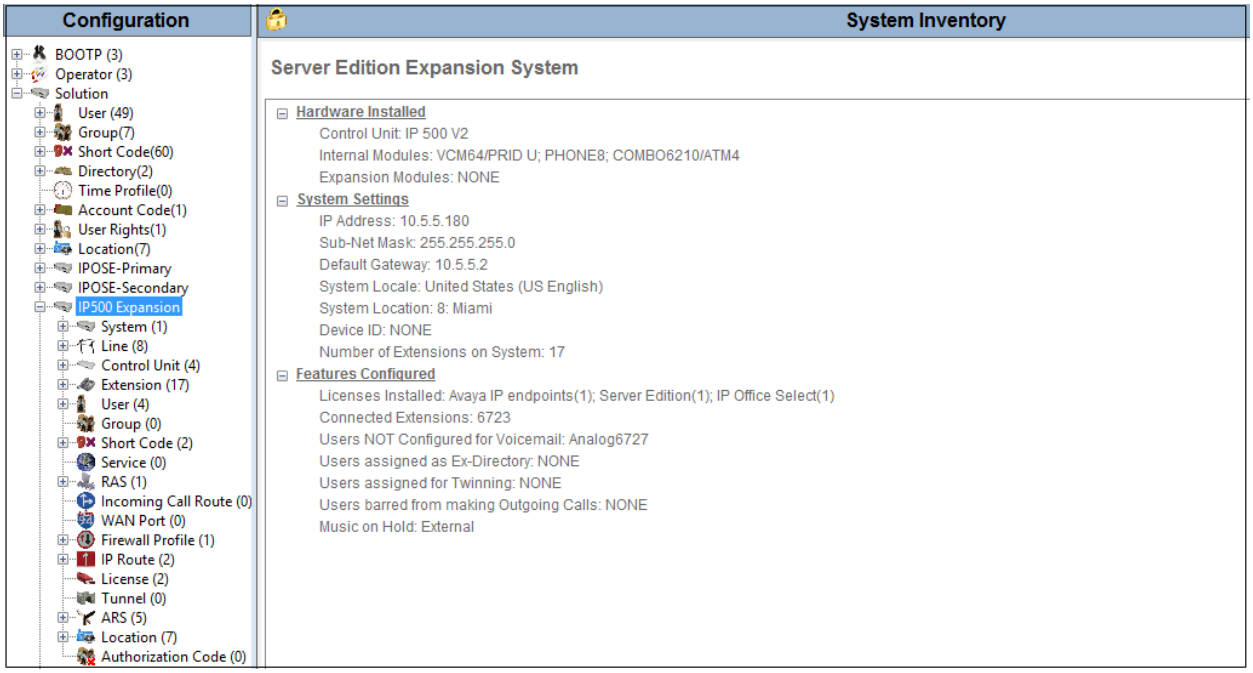
Hacer clic**OK**para ejecutar el guardado.



©2020 Avaya Inc. Todos los derechos reservados.

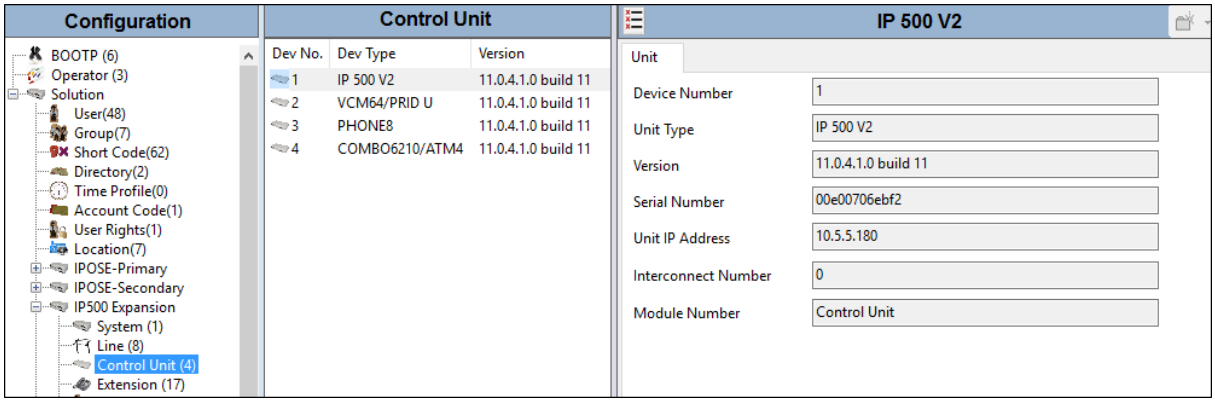
6. Configuración del sistema de expansión Avaya IP Office

Navegar a**Expediente**→**Configuración abierta**(no se muestra), seleccione el sistema Avaya IP Office adecuado en la ventana emergente e inicie sesión con las credenciales adecuadas. Al hacer clic en el signo "más" junto a**Expansión IP500**en el panel de navegación izquierdo se expandirá el menú en este servidor.



6.1. Sistema de expansión: hardware físico

En la configuración de muestra, el Sistema de expansión IP500 V2 contenía una tarjeta analógica PHONE8 y una tarjeta COMBO6210, para admitir estaciones analógicas y digitales. También se incluye un VCM64 (módulo de compresión de voz). Tanto la tarjeta VCM64 como la COMBO6210 proporcionan canales de compresión de voz a la unidad de control. Los canales de compresión de voz son necesarios para admitir llamadas de VoIP, incluidas las extensiones de IP o las troncales de IP.

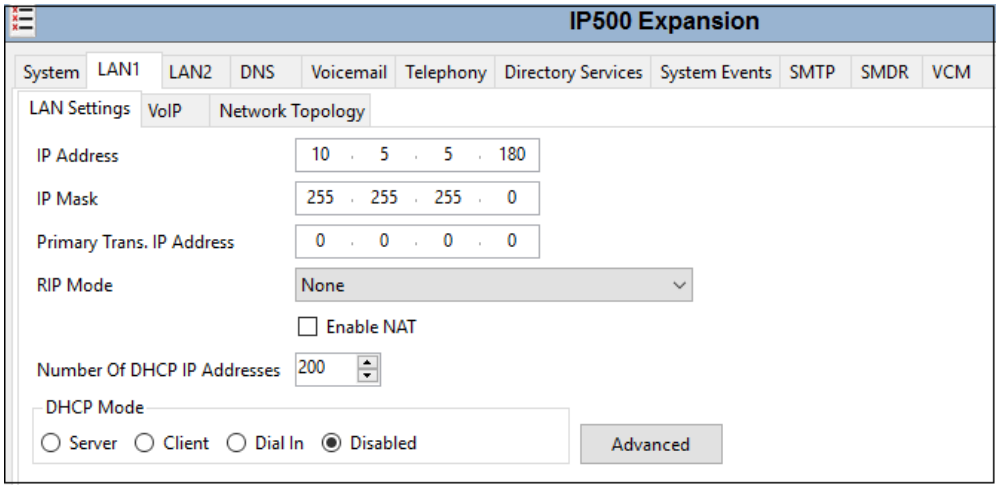


©2020 Avaya Inc. Todos los derechos reservados.

6.2. Sistema de expansión: configuración de LAN

En la configuración de muestra, LAN1 se usa para conectar el Sistema de expansión a la red empresarial. Para ver o configurar la dirección IP de LAN1, seleccione**Sistema**en el panel de navegación. Selecciona el **LAN1→Configuración de LAN**en la pestaña Detalles e ingrese lo siguiente:

- **Dirección IP: 10.5.5.180**se utilizó en la configuración de referencia.
- **Máscara IP: 255.255.255.0**se utilizó en la configuración de referencia
- Haga clic en el**OK**botón (no se muestra).

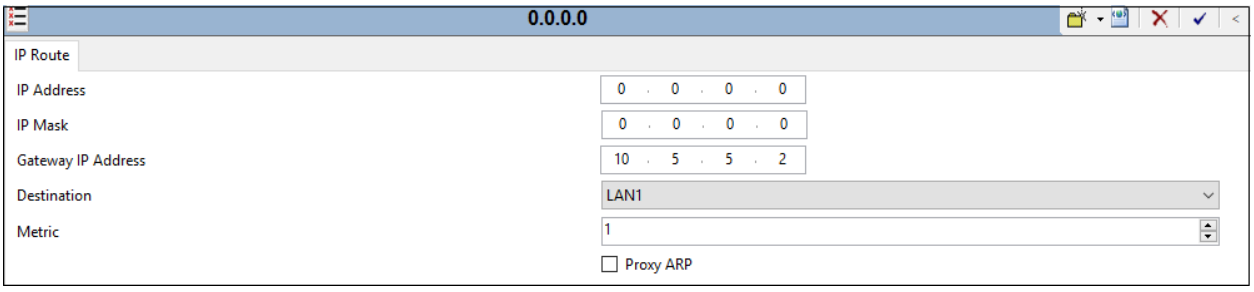


Se utilizaron valores predeterminados en el**VoIP**y**Topología de la red**pestañas (no se muestran).

6.3. Sistema de Expansión - Ruta IP

Para crear una ruta IP para el sistema de Expansión, haga clic derecho en**Ruta IP**en el panel de navegación izquierdo. Seleccione**Nuevo**(no mostrado).

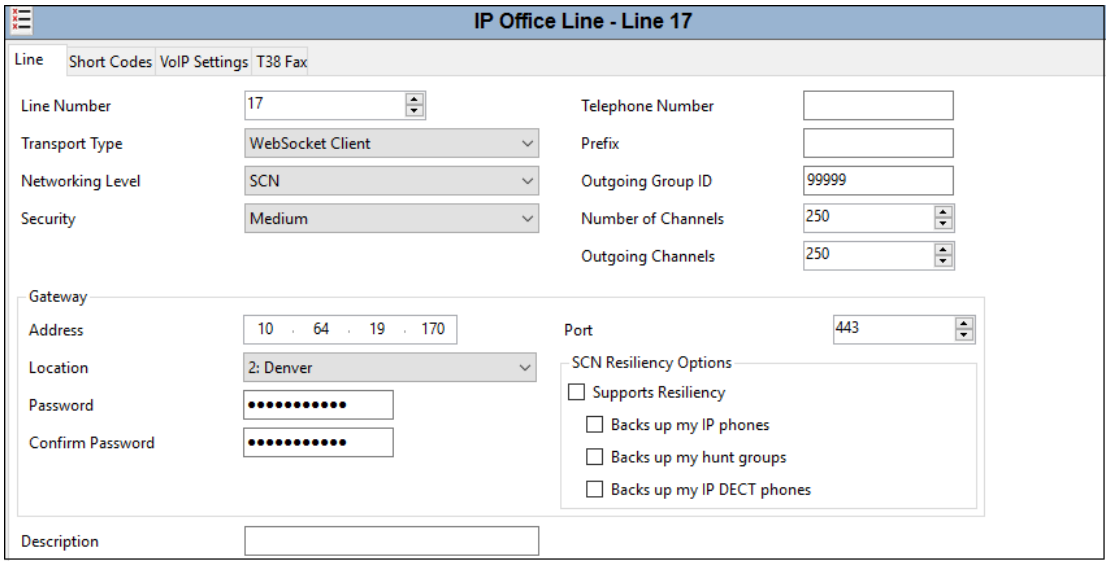
- Ingresar**0.0.0.0**sobre el**Dirección IP**y**Máscara IP**campos para hacer de esta la ruta predeterminada.
- Establecer**Dirección IP de la puerta de enlace**a la dirección IP del enrutador predeterminado en la subred de IP Office. La puerta de enlace predeterminada en la configuración de referencia era**10.5.5.2**
- Establecer**Destino**a**LAN1**del menú desplegable.



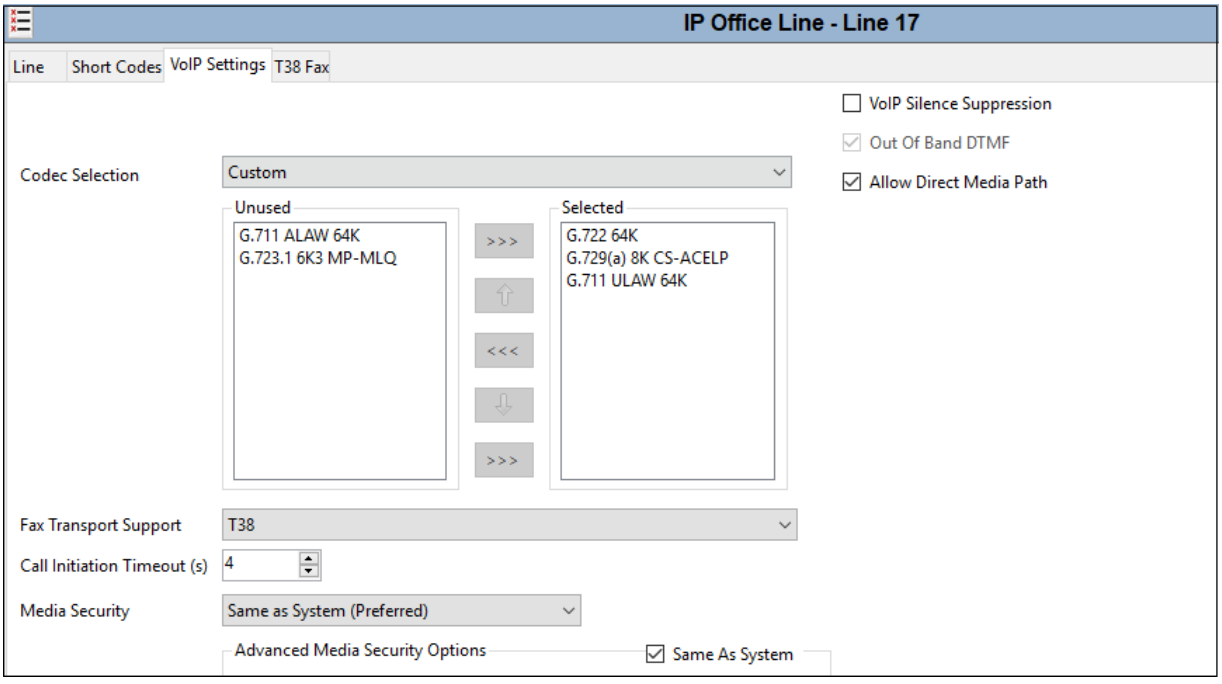
©2020 Avaya Inc. Todos los derechos reservados.

6.4. Sistema de Expansión - Línea IP Office

La Línea de IP Office se creó automáticamente en cada servidor cuando se agregó el Sistema de expansión a la solución. A continuación se muestra la línea de IP Office al servidor principal.

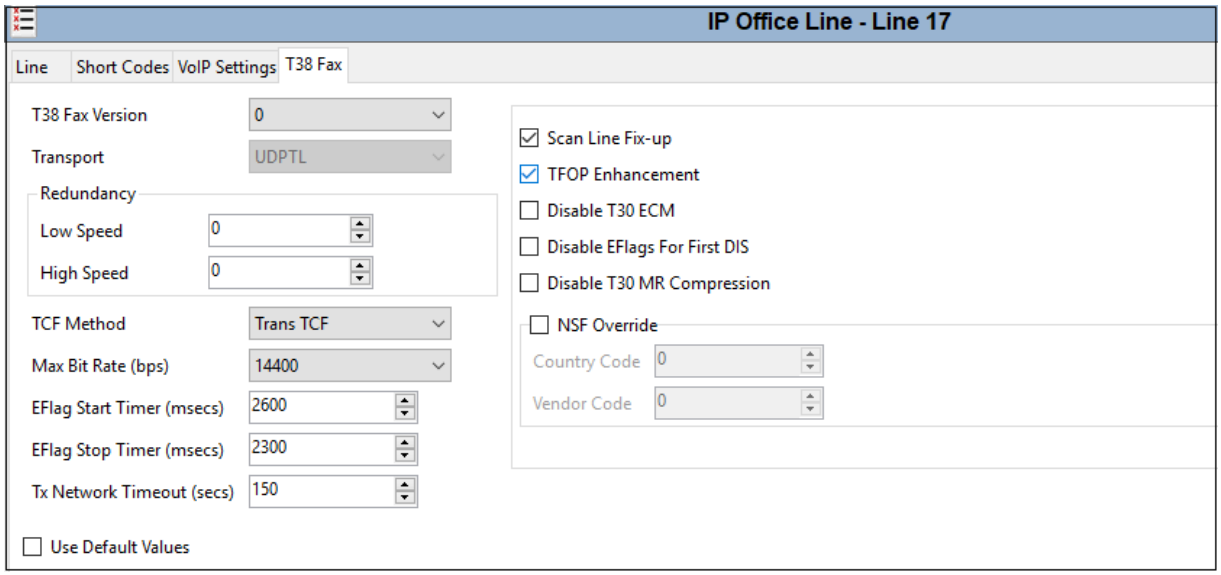


En la configuración de referencia, una máquina de fax está conectada a uno de los puertos analógicos del Sistema de expansión. Para admitir el fax T.38, seleccione el**Configuración VoIP**ficha y establecer**Soporte de transporte de fax**a**T38.**



©2020 Avaya Inc. Todos los derechos reservados.

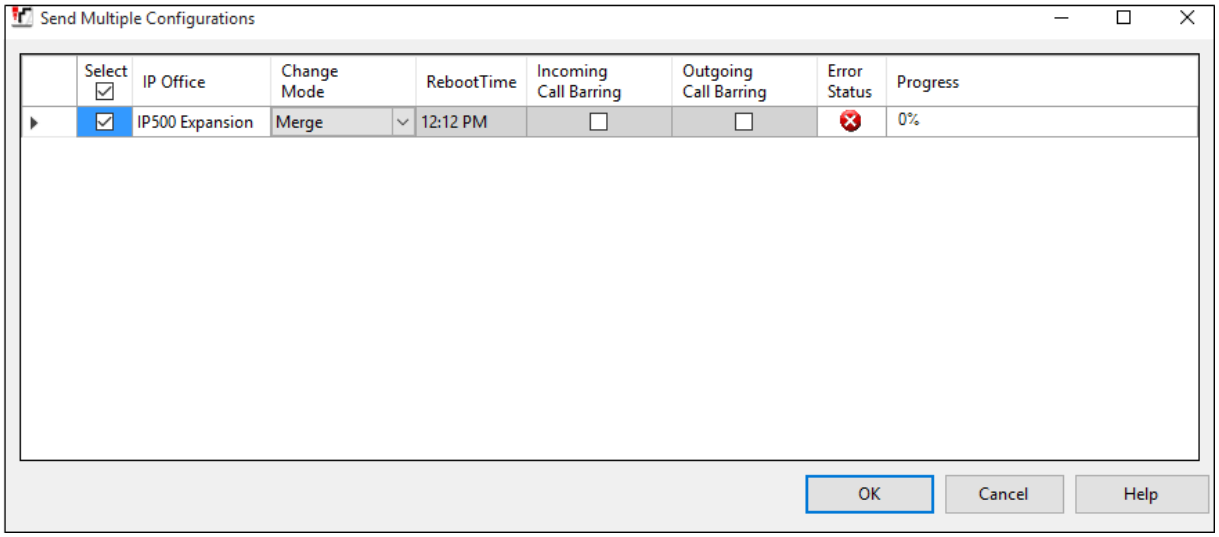
Selecciona el**Fax T38**pestaña. los**Usar valores predeterminados**la casilla está desmarcada y el**Versión de fax T38**se establece en "**0**". Todos los demás valores se dejan por defecto.



6.5. Guardar la configuración del sistema de expansión de IP Office

Navegar a**Expediente→Guardar configuración**en la barra de menú en la parte superior de la pantalla para guardar la configuración realizada en las secciones anteriores

Aparecerá lo siguiente, ya sea con**Uni**o**Reiniciar**seleccionado, en función de la naturaleza de los cambios de configuración realizados desde la última vez que se guardó. Tenga en cuenta que al hacer clic**OK**puede causar una interrupción del servicio. Hacer clic**OK**para proceder.



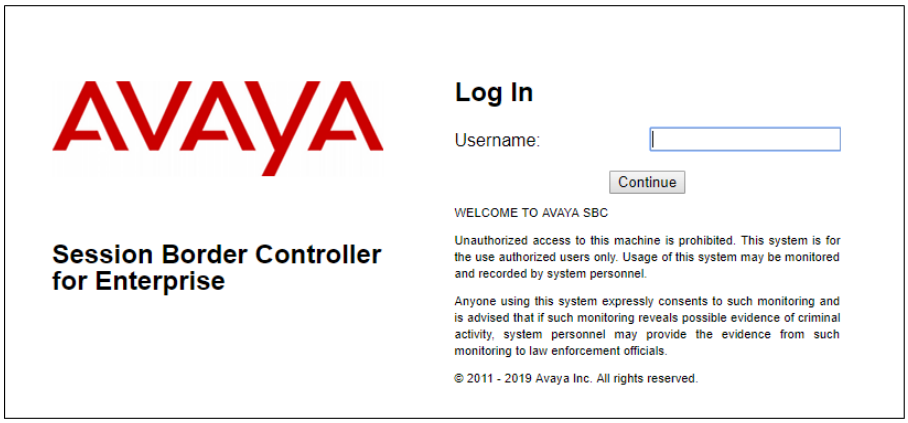
©2020 Avaya Inc. Todos los derechos reservados.

7. Configurar Avaya Session Border Controller para empresas

Esta sección cubre la configuración de Avaya SBCE. Se supone que ya se completó el aprovisionamiento inicial de Avaya SBCE, incluida la asignación de la dirección IP de la interfaz de administración y la instalación de la licencia; por lo tanto, estas tareas no están cubiertas en estas Notas de aplicación. Para obtener más información sobre la instalación y el aprovisionamiento de Avaya SBCE, consulte la documentación de Avaya SBCE en el**Referencias adicionales**sección.

Utilice un navegador WEB para acceder a la interfaz web de Element Management Server (EMS) e ingrese https://*dirección IP*/sbc en el campo de dirección del navegador web, donde*dirección IP*es la dirección IP de LAN de administración de Avaya SBCE.

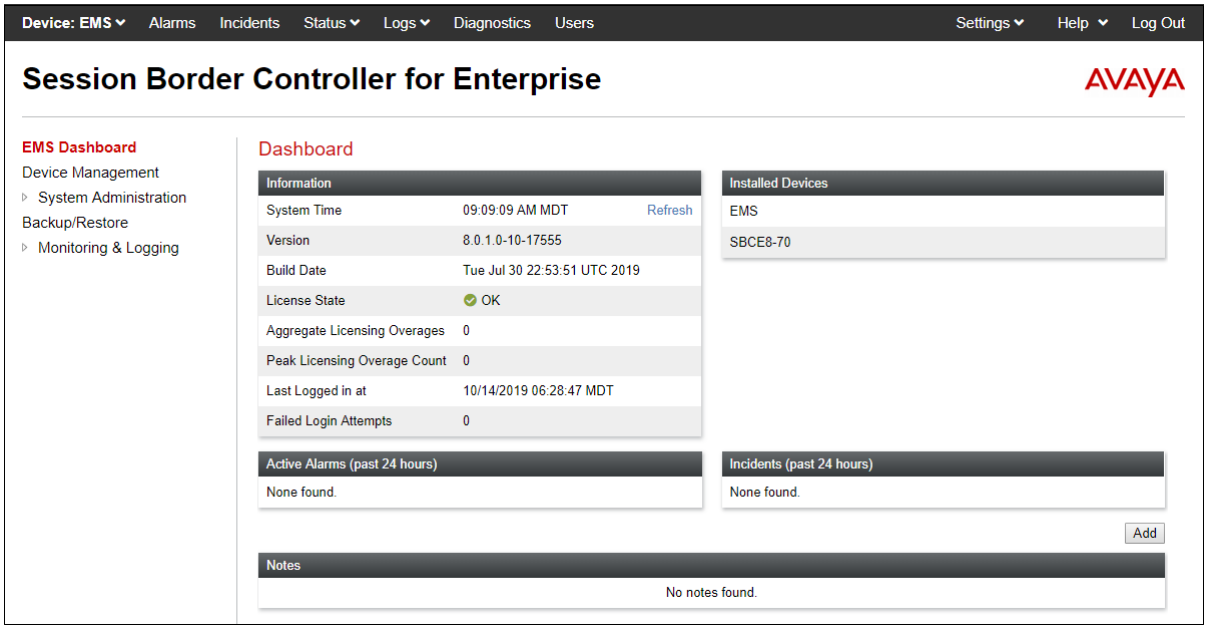
Introducir el**Nombre de usuario**y haga clic en**Continuar**.



Introduzca la contraseña y haga clic en**Iniciar sesión**.

©2020 Avaya Inc. Todos los derechos reservados.

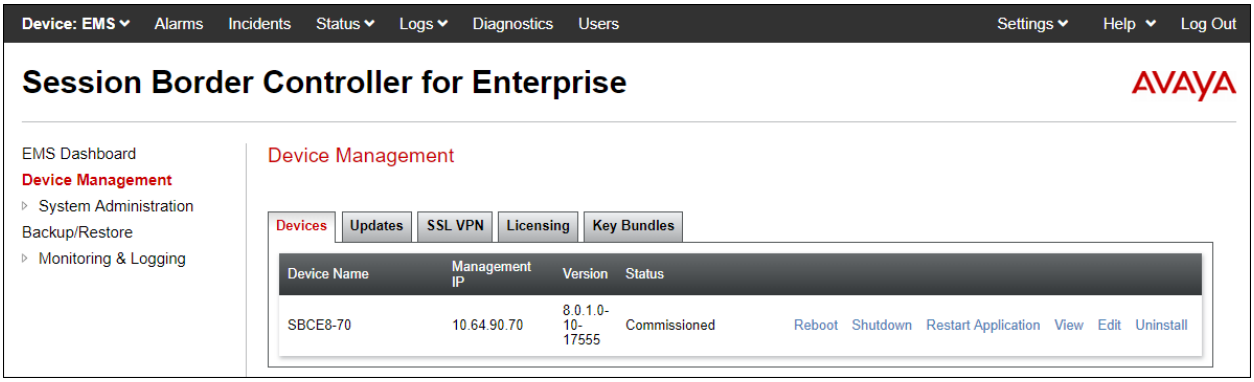
Aparecerá la página Panel EMS de Avaya SBCE. Tenga en cuenta que se muestra la versión del software instalado. Verifique que el**Estado de la licencia**es**OK**. La SBCE solo operará por un corto tiempo sin una licencia válida. Comuníquese con su representante de Avaya para obtener una licencia.



7.1. Gestión de dispositivos: estado

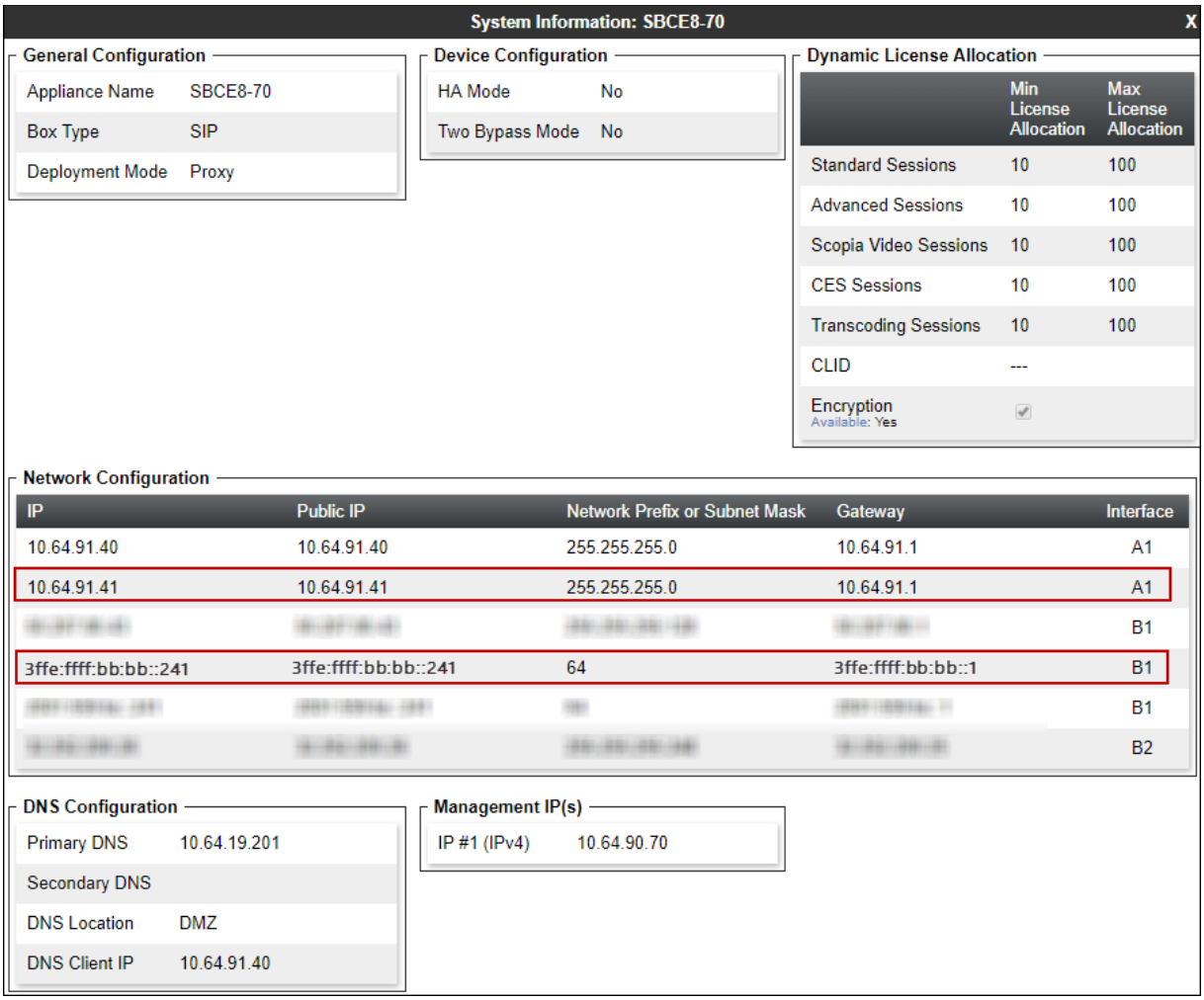
Seleccione**Gestión de dispositivos**en el menú de la izquierda. Se muestra una lista de dispositivos instalados en la **Dispositivos**pestaña en el panel derecho. En el caso de la configuración de muestra, un solo dispositivo llamado **SBCE8-70** se muestra. Verifique que el**Estado**columna muestra**Oficial**. De lo contrario, comuníquese con su representante de Avaya. Para ver la configuración de este dispositivo, haga clic en**Vista**en la pantalla de abajo.

> **Nota**–Ciertos cambios de configuración de Avaya SBCE requieren que se reinicie la aplicación subyacente. Para hacerlo, haga clic en**Reiniciar aplicación**mostrado a continuación.



©2020 Avaya Inc. Todos los derechos reservados.

los**Información del sistema**pantalla muestra el**configuración de la red**,**Configuración DNS**y **IP de administración**información proporcionada durante la instalación y corresponde a**Figura 1**. En el entorno de prueba compartido, el resaltado**A1**y**B1**Las direcciones IP son las relevantes para la configuración de la troncal SIP para AT&T.



©2020 Avaya Inc. Todos los derechos reservados.

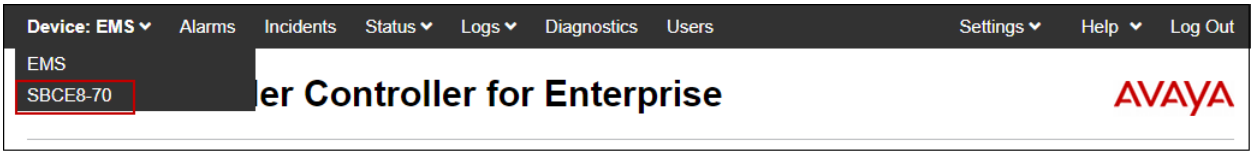
7.2. Gestión TLS

Nota–Las pruebas se realizaron utilizando certificados de identidad firmados por una autoridad de certificación local. El procedimiento para crear y obtener estos certificados está fuera del alcance de estas Notas de aplicación.

En la configuración de referencia, el transporte TLS se usa para la comunicación entre IP Office y Avaya SBCE. Los siguientes procedimientos muestran cómo ver los certificados y configurar los perfiles para admitir la conexión TLS.

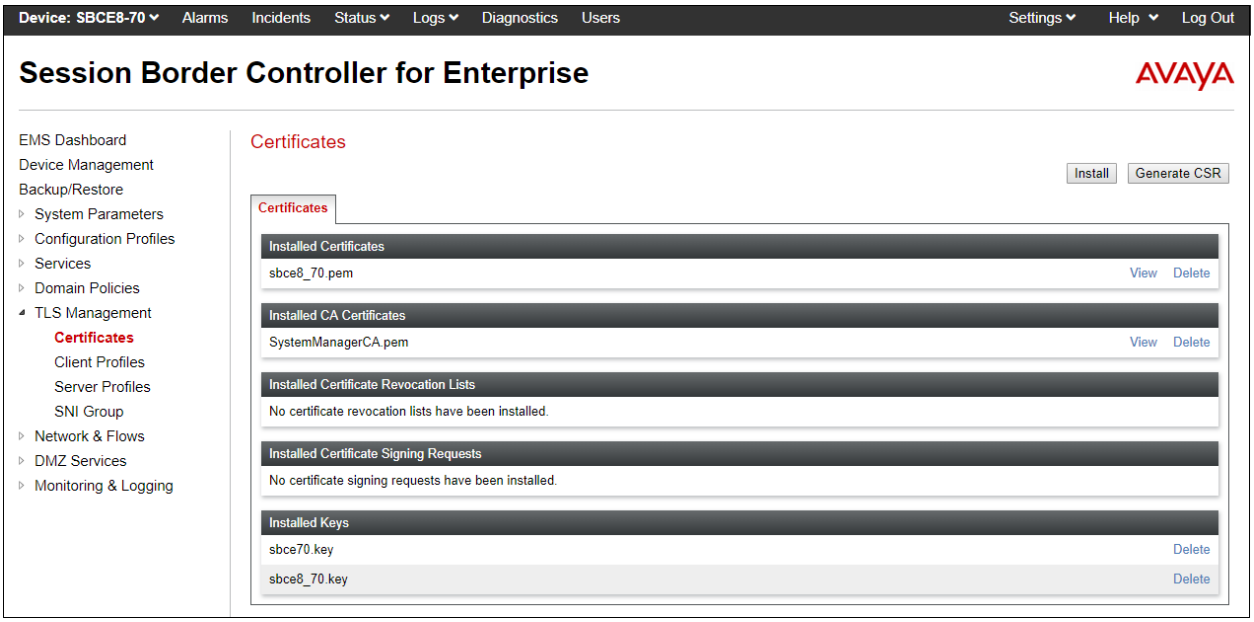
7.2.1. Verificar certificados TLS: Avaya Session Border Controller para empresas

Para acceder a los menús de configuración de SBCE, seleccione el dispositivo SBCE en el menú de navegación superior.



Seleccione**Gestión TLS→Certificados**del menú de la izquierda. Verifique lo siguiente:

- El certificado de CA raíz está presente en el**Certificados CA instalados**área.
- El certificado de identidad firmado está presente en el**Certificados instalados**área.
- La clave privada asociada al certificado de identidad está presente en el**Claves instaladas** área.



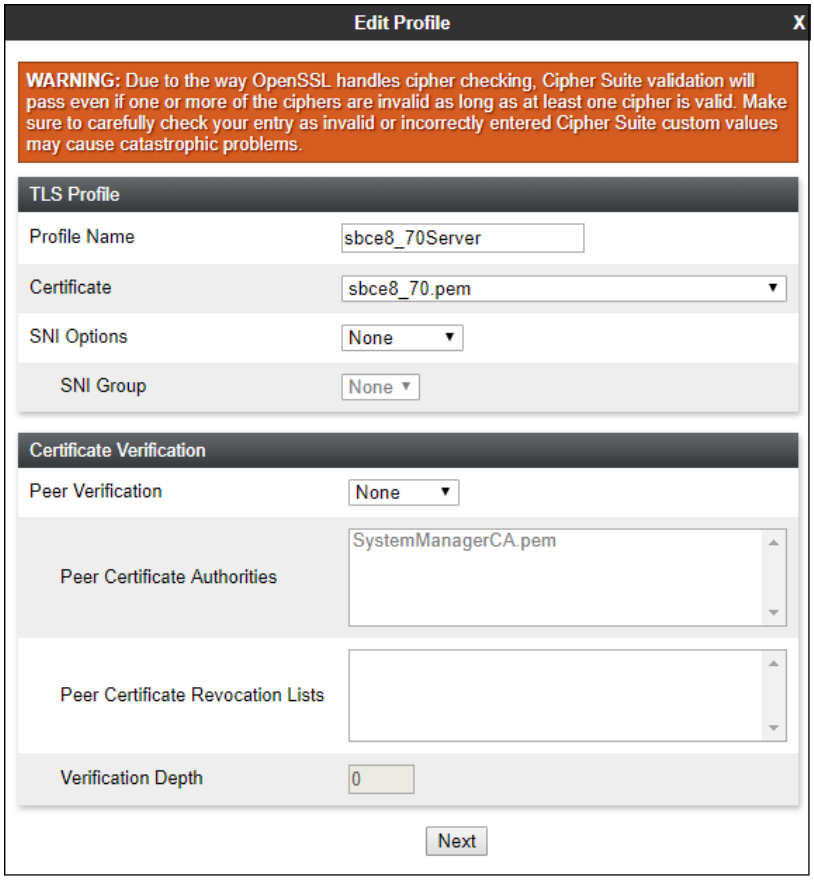
©2020 Avaya Inc. Todos los derechos reservados.

7.2.2. Perfiles de servidor

Paso 1-Seleccione**Gestión TLS→Perfiles de servidor**y haga clic en**Agregar**. Introduzca la siguiente:

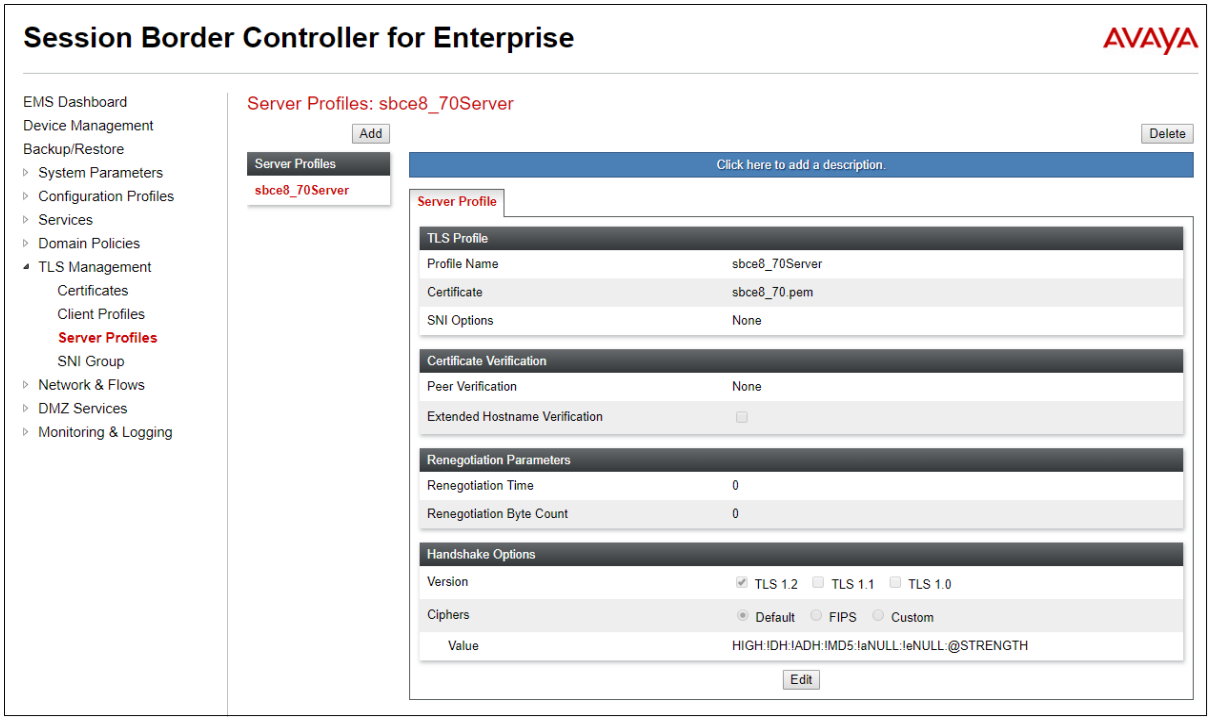
- **Nombre de perfil:**ingrese un nombre descriptivo.
- **Certificado:**seleccione el certificado de identidad, por ejemplo,**sbce8_70.pem**, desde el menú desplegable.
- **Verificación de pares**=**Ninguna**.
- Hacer clic**próximo**.

Paso 2-Acepte los valores predeterminados para la siguiente pantalla (no se muestra) y haga clic en**Finalizar**.



©2020 Avaya Inc. Todos los derechos reservados.

La siguiente pantalla muestra el TLS completado**Perfil del servidor**forma:



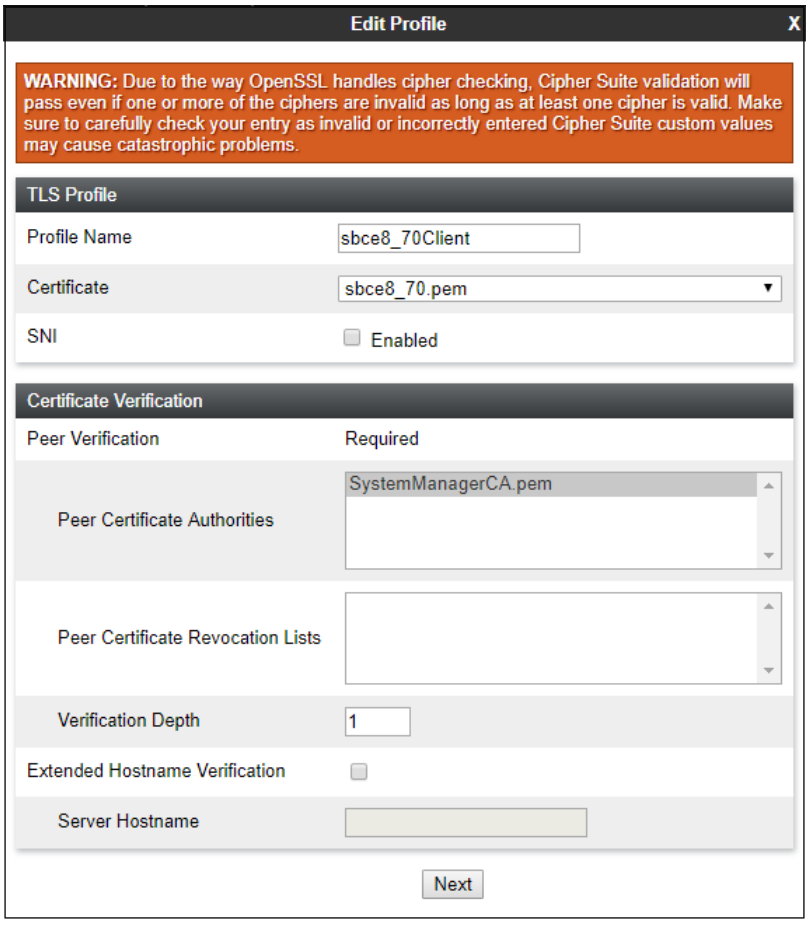
©2020 Avaya Inc. Todos los derechos reservados.

7.2.3. Perfiles de clientes

Paso 1-Seleccione**Gestión TLS→Perfiles de clientes**y haga clic en**Agregar**. Introduzca la siguiente:

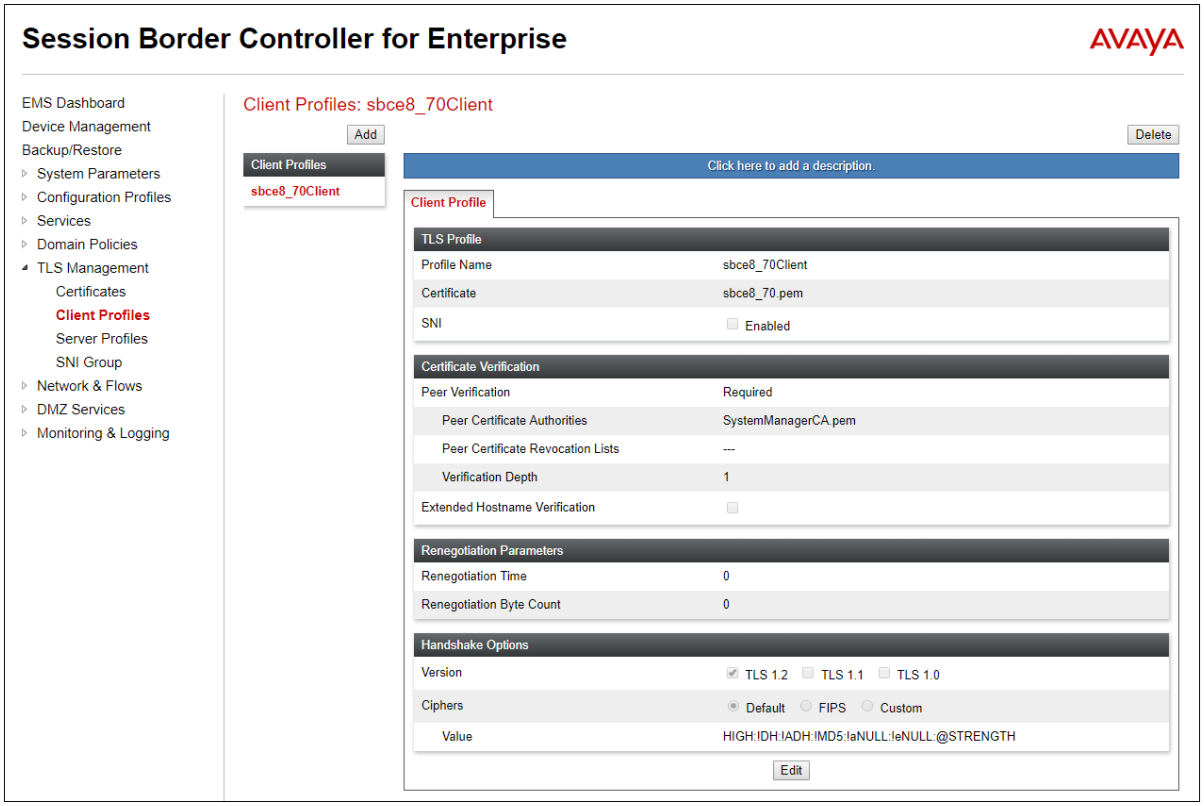
- **Nombre de perfil:**ingrese un nombre descriptivo.
- **Certificado:**seleccione el certificado de identidad, por ejemplo,**sbce8_70.pem**, desde el menú desplegable.
- **Verificación de pares**=**Requerido**.
- **Autoridades de certificación pares:**seleccione el certificado de CA utilizado para verificar el certificado recibido de Session Manager, por ejemplo,**SystemManagerCA.pem**.
- **Profundidad de verificación:**ingresar**1**.
- Hacer clic**próximo**.

Paso 2-Acepte los valores predeterminados para la siguiente pantalla (no se muestra) y haga clic en**Finalizar**.



©2020 Avaya Inc. Todos los derechos reservados.

La siguiente pantalla muestra el TLS completado**Perfil del cliente**forma:



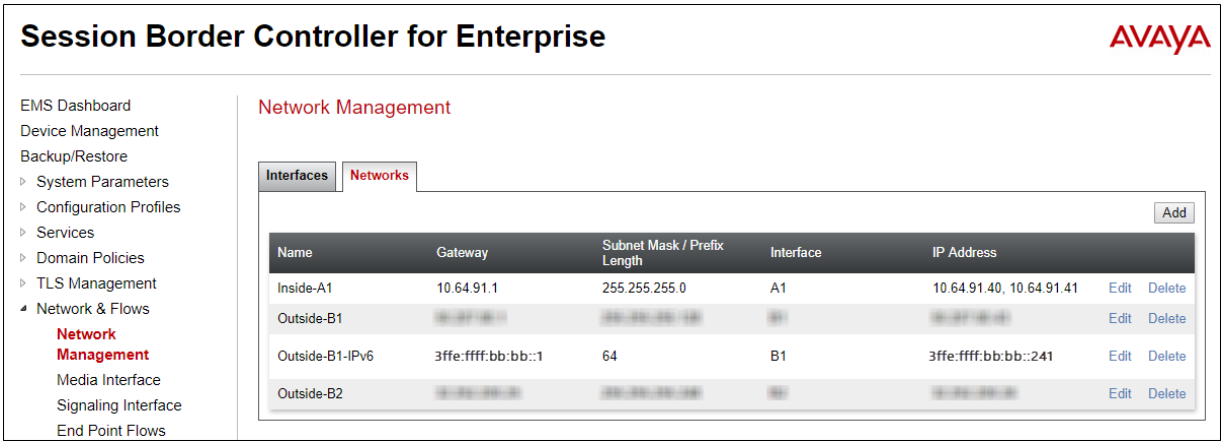
©2020 Avaya Inc. Todos los derechos reservados.

7.3. Administración de redes

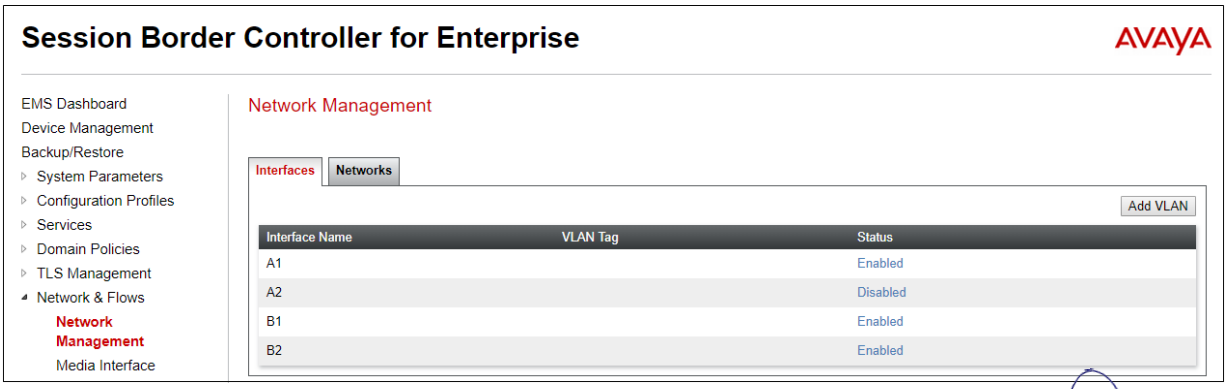
La pantalla Administración de red es donde se configuran y habilitan los ajustes de la interfaz de red. Durante el proceso de instalación de Avaya SBCE, se define cierta información específica de la red, como la(s) dirección(es) IP del dispositivo, la(s) dirección(es) IP pública(s), la máscara de red, la puerta de enlace, etc., para conectar el dispositivo a la red. Es esta información la que llena las diversas pantallas de la pestaña Administración de red, que se puede editar según sea necesario para optimizar el rendimiento del dispositivo y la eficiencia de la red. Navegar a**Redes y flujos→Administración de redes**. Sobre el**Redes**pestaña, verifique las direcciones IP asignadas a las interfaces. La siguiente pantalla muestra que la interfaz empresarial está asignada a**A1**y la interfaz hacia AT&T está asignada a**B1**.

Las siguientes direcciones IP de Avaya SBCE e interfaces asociadas se usaron en la configuración de muestra:

- **A1**:**10.64.91.41**–Dirección IPv4 configurada para AT&T IPTF a IP Office.
- **B1: 3ffe:ffff:bb:bb::241**–Dirección IPv6 configurada para el servicio AT&T IPTF. Esta dirección es conocida por AT&T. Ver**Seccion 3**.



Verifique que las interfaces estén habilitadas en el**Interfaces**pestaña. La siguiente pantalla muestra las interfaces**A1**y**B1**con estado**Activado**. Para habilitar una interfaz, haga clic en el correspondiente **Desactivado**enlace debajo de la columna Estado para cambiarlo a**Activado**.



©2020 Avaya Inc. Todos los derechos reservados.

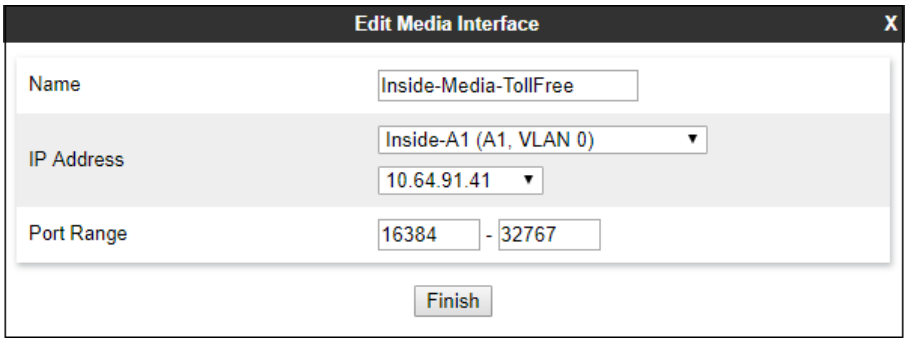
7.4. Interfaces de medios

Las interfaces de medios se crean para especificar la dirección IP y el rango de puertos en los que Avaya SBCE aceptará flujos de medios en cada interfaz. Los paquetes que salen de las interfaces de Avaya SBCE anunciarán esta dirección IP y uno de los puertos en este rango como la dirección IP de escucha y el puerto en el que SBCE aceptará los medios del servidor conectado.

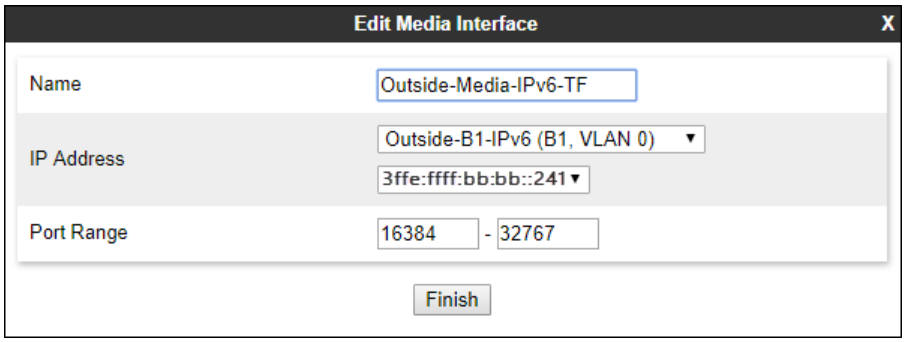
Para crear una nueva interfaz de medios en la dirección empresarial, vaya a**Red y flujos→ Interfaz de medios**en el menú del lado izquierdo y haga clic en**Agregar**(no mostrado). Sobre el**Agregar interfaz de medios**pantalla, ingrese un**Nombre**para la interfaz multimedia. Seleccione la dirección IP privada de Avaya SBCE de la**Dirección IP**Menú desplegable. Tenga en cuenta que el**rango de puertos**fue configurado con los valores requeridos por AT&T (**16384**–**32767**). Hacer clic**Finalizar**.

Algunos puertos en el rango requerido por AT&T ya fueron asignados por Avaya SBCE para uso interno, de manera predeterminada. Ver**Sección 7.14**para conocer los pasos necesarios para reasignar los rangos de puertos utilizados por Avaya SBCE, de modo que se pueda acomodar el rango requerido por AT&T.

La siguiente pantalla muestra la**Inside-Media-TollFree**interfaz multimedia creada en la configuración de referencia.



Se creó una segunda Interfaz de Medios hacia la red de AT&T con el nombre**Medios externos-IPv6-TF**, Como se muestra abajo. La dirección IPv6 externa de Avaya SBCE en la interfaz B1 se seleccionó del menú desplegable. los**rango de puertos**fue configurado con los valores requeridos por AT&T (**16384**–**32767**).

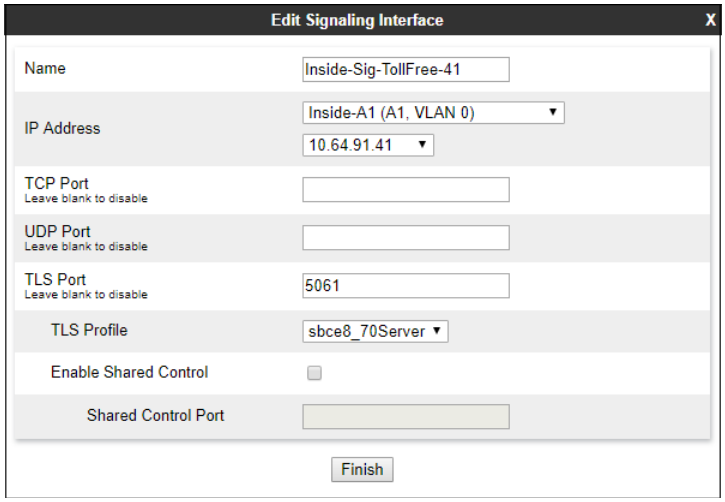


©2020 Avaya Inc. Todos los derechos reservados.

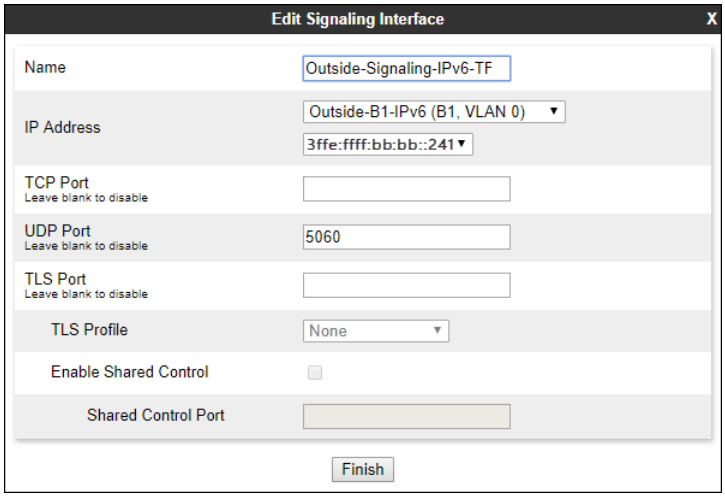
7.5. Interfaces de señalización

La pantalla Signaling Interface es donde se definen los puertos de señalización SIP. Avaya SBCE escuchará las solicitudes SIP en los puertos definidos. Cree una interfaz de señalización para las interfaces IP internas y externas.

Para crear una nueva interfaz de señalización en la dirección empresarial, vaya a**Red y flujos→ Interfaz de señalización**y haga clic**Agregar**. Sobre el**Agregar interfaz de señalización**pantalla, ingrese un**Nombre**para la interfaz. Seleccione la dirección IP privada para Avaya SBCE de la **Dirección IP**Menú desplegable. Dado que TLS se usa en la configuración de muestra para escuchar el tráfico de señalización de IP Office,**5061**se ingresa bajo**Puerto TLS**. El perfil TLS se establece en el perfil del servidor TLS**sbce8_70Servidor**se muestra en**Sección 7.2.2**. Hacer clic**Finalizar**.



Una segunda interfaz de señalización con el nombre**Señalización externa-IPv6-TF**fue creado de manera similar en la dirección de la red. La dirección IPv6 externa de Avaya SBCE en la interfaz B1 se seleccionó del menú desplegable. Por debajo**El puerto UDP,**ingresar**5060**según lo especificado por AT&T. Hacer clic **Finalizar**.



©2020 Avaya Inc. Todos los derechos reservados.

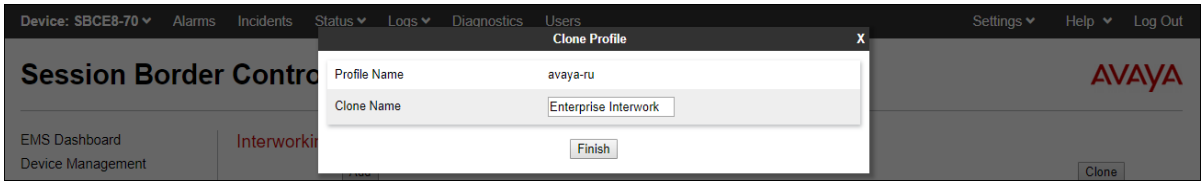
7.6. Perfiles de interfuncionamiento del servidor

El perfil de Internetworking del servidor incluye parámetros para hacer que Avaya SBCE funcione en una red VoIP empresarial utilizando diferentes implementaciones del protocolo SIP. Hay perfiles predeterminados disponibles que se pueden usar tal cual, o se pueden modificar, o se pueden configurar nuevos perfiles como se describe a continuación.

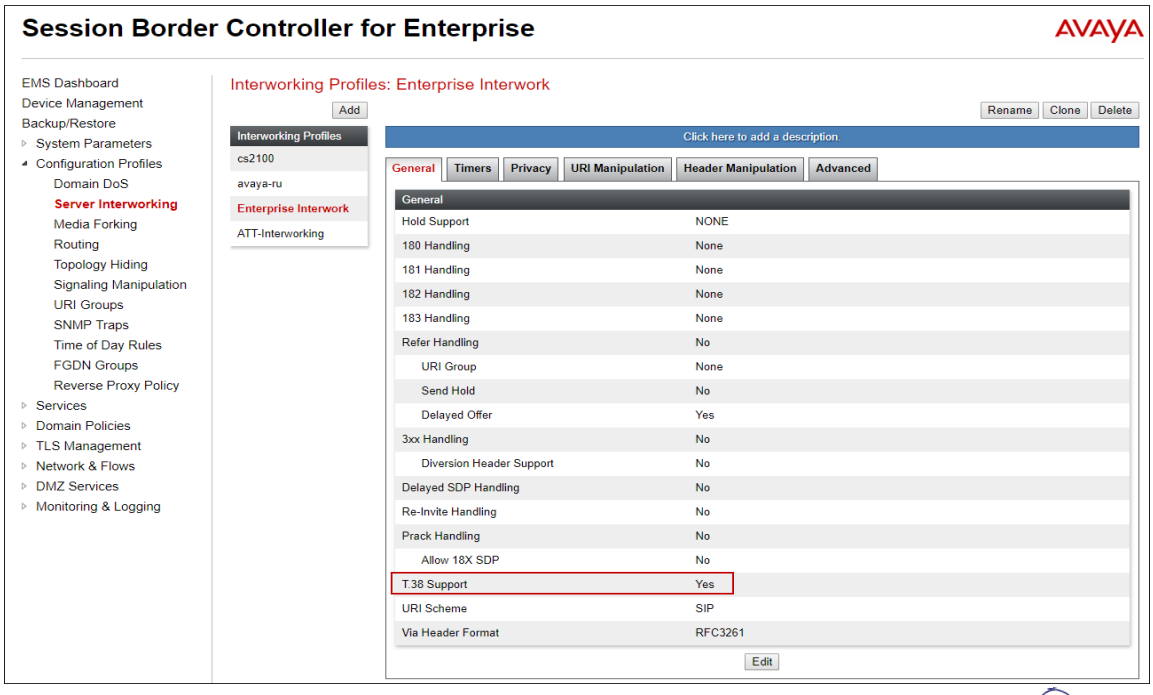
En la configuración de muestra, se crearon perfiles de interconexión de servidores separados para IP Office y el servicio IPTF de AT&T.

7.6.1. Perfil de interfuncionamiento del servidor: IP Office

En la configuración de muestra, el perfil de interfuncionamiento del servidor de IP Office se clonó a partir del perfil predeterminado.**avaya-ru**perfil. Para clonar un perfil de interconexión de servidores para IP Office, vaya a **Perfiles de configuración→Interfuncionamiento de servidores**, Selecciona el**avayu-ru**perfil y haga clic en el **Clon**botón. Entrar a**Nombre del clon**y haga clic**Finalizar**continuar.



La siguiente pantalla muestra la**Interfuncionamiento empresarial**perfil utilizado en la configuración de muestra, con **Soporte T.38**ajustado a**Sí**. Para modificar el perfil, desplácese hacia abajo hasta la parte inferior de la pantalla y haga clic en **Editar**. Selecciona el**Soporte T.38**parámetro y luego haga clic en**próximo**y entonces**Finalizar**(no mostrado).

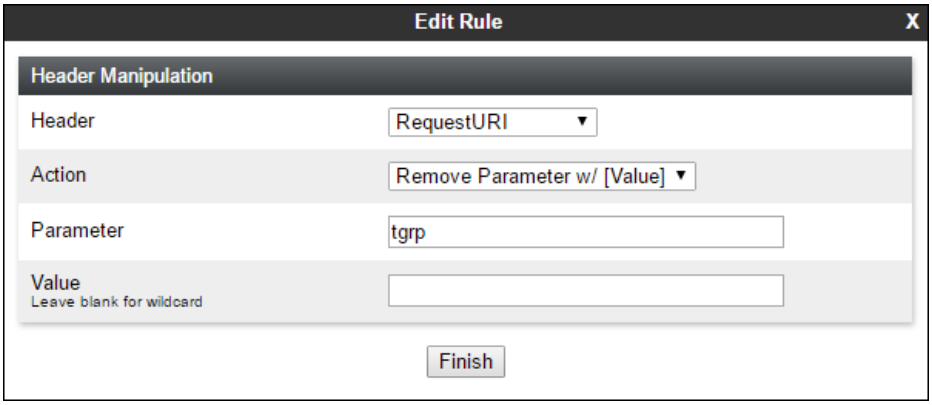


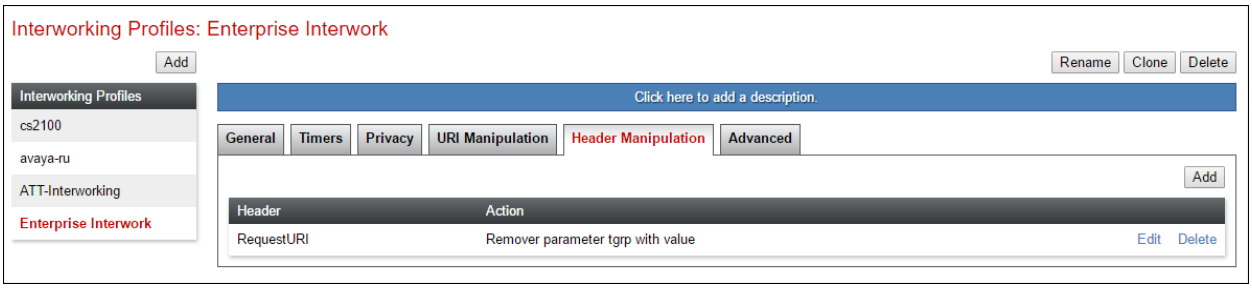
©2020 Avaya Inc. Todos los derechos reservados.

Como se describe en**Sección 2.2**,**elemento 3**, el mensaje BYE recibido de AT&T contenía un parámetro "tgrp" que incluía direcciones IPv6. IP Office no pudo procesar correctamente este mensaje BYE. La siguiente regla de manipulación de encabezados del perfil de Interfuncionamiento de servidores eliminará este parámetro del encabezado URI de solicitud en el mensaje BYE que llega de AT&T.

Selecciona el**Manipulación de encabezado**pestaña. Haga clic en**Agregar**e ingresa lo siguiente:

- **Encabezamiento:**Seleccione**SolicitudURI**del menú desplegable
- **Acción:**Seleccione**Eliminar parámetro con [Valor]**del menú desplegable
- **Parámetro=tgrp**
- **Valor:**dejar en blanco
- Hacer clic**Finalizar**

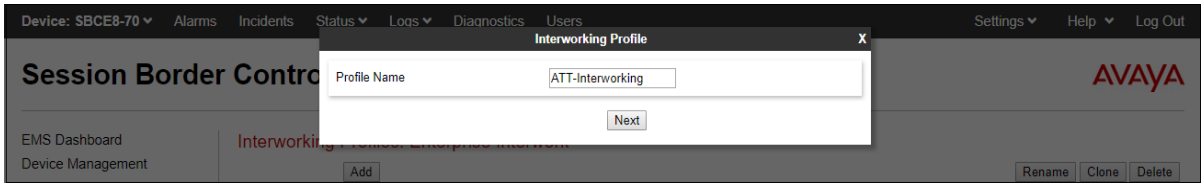




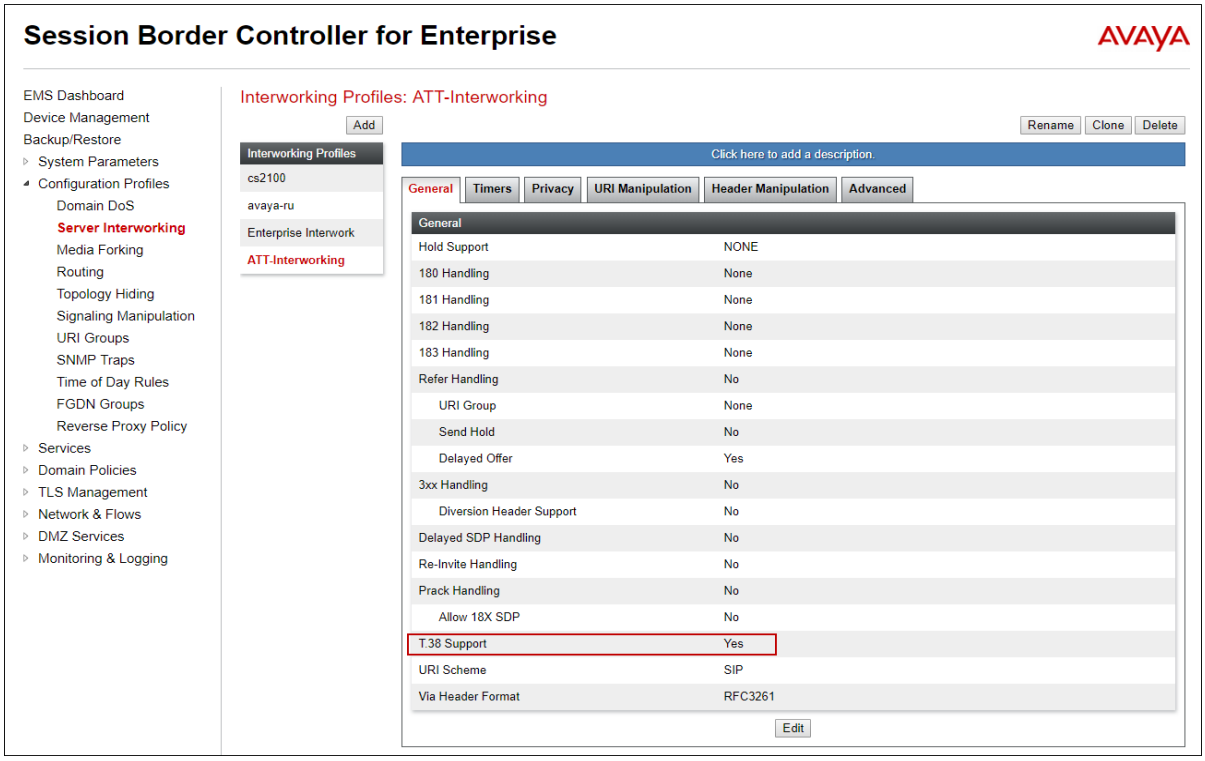
©2020 Avaya Inc. Todos los derechos reservados.

7.6.2. Perfil de interfuncionamiento del servidor: AT&T

Para crear un nuevo perfil de interconexión de servidores para AT&T, vaya a**Perfiles de configuración→ Interfuncionamiento de servidores**y haga clic**Agregar**Como se muestra abajo. Entrar a**Nombre de perfil**y haga clic**próximo**.

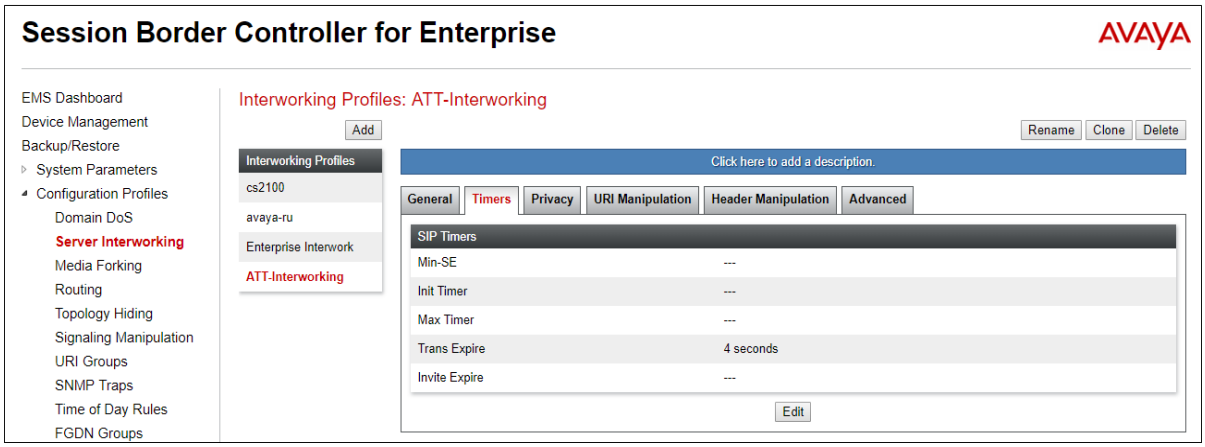


Las siguientes pantallas muestran la**Interfuncionamiento ATT**perfil utilizado en la configuración de muestra. Sobre el **General**pestaña, los valores predeterminados se utilizan con la excepción de**Soporte T.38**ajustado a**Sí**.

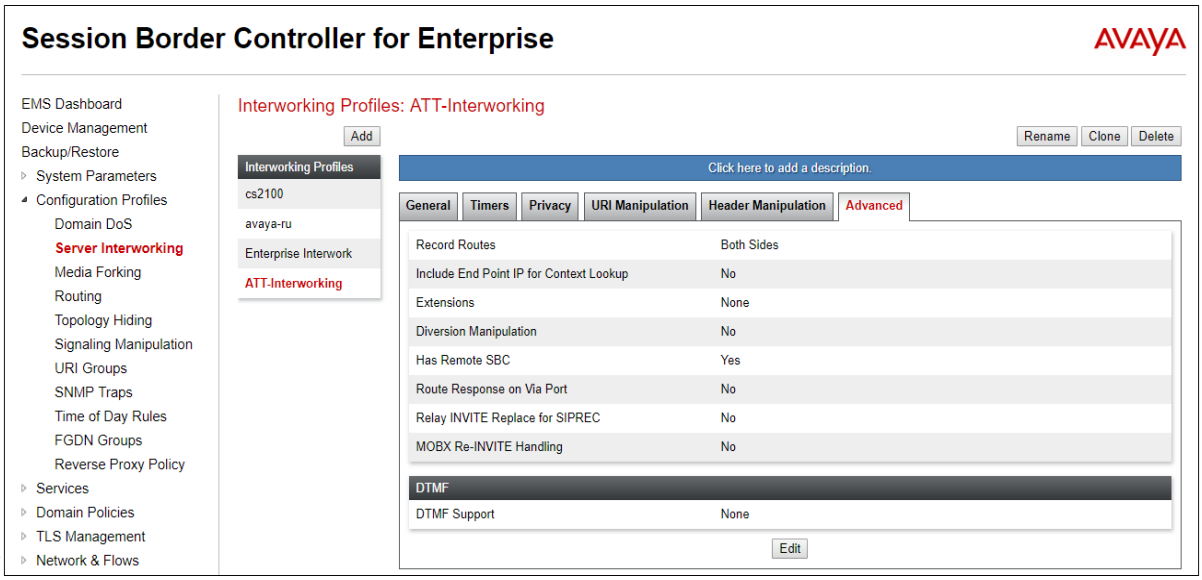


©2020 Avaya Inc. Todos los derechos reservados.

los**Temporizadores**La pestaña muestra los valores utilizados para las pruebas de cumplimiento para el**expiración trans**campo. los **expiración trans**timer establece el tiempo asignado en el que Avaya SBCE probará el primer servidor principal antes de probar el servidor secundario, si existe uno.



Hacer clic**próximo**para aceptar los parámetros predeterminados para el**Privacidad**,**Manipulación de URI**, y**Manipulación de encabezado**pestañas (no se muestran) y avance a la**Avanzado**área.**Grabar Rutas**se establece en **Ambos lados**. Los valores predeterminados se pueden utilizar para todos los demás campos.



©2020 Avaya Inc. Todos los derechos reservados.

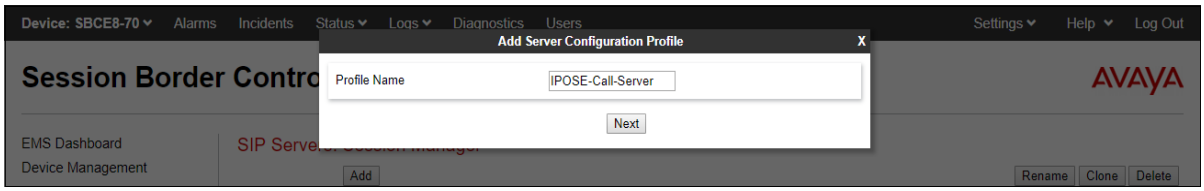
7.7. Perfiles de servidores SIP

los**Perfil del servidor SIP**contiene parámetros para configurar y administrar varios parámetros específicos del servidor de llamadas SIP, como asignaciones de puertos TCP y UDP, parámetros de señalización de latidos, estadísticas de seguridad DoS y dominios confiables.

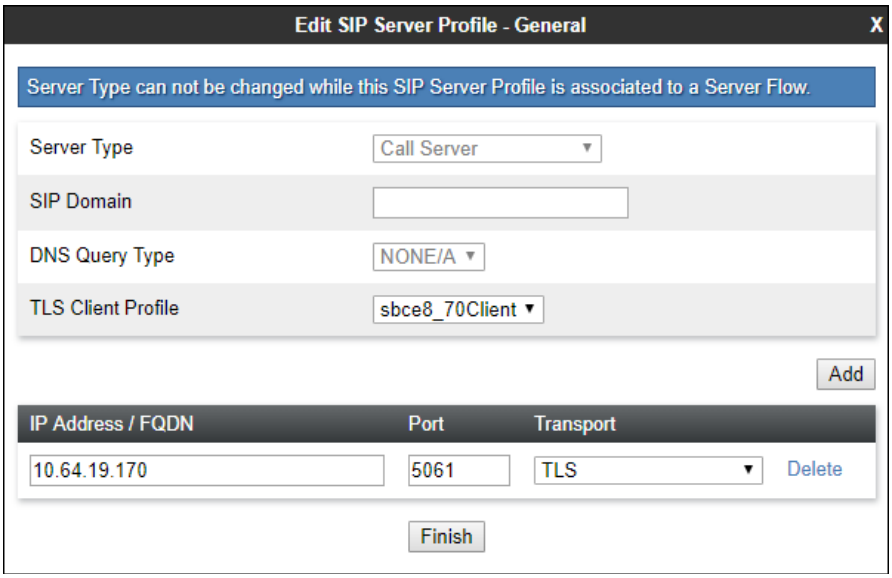
En la configuración de muestra, se crearon perfiles de configuración de servidor separados para IP Office y el servicio IPTF de AT&T.

7.7.1. Perfil del servidor SIP – IP Office

Para agregar un perfil de servidor SIP para IP Office, vaya a**Servicios→Servidores SIP**y haga clic**Agregar**. Introduzca un nombre descriptivo para el nuevo perfil y haga clic en**próximo**.

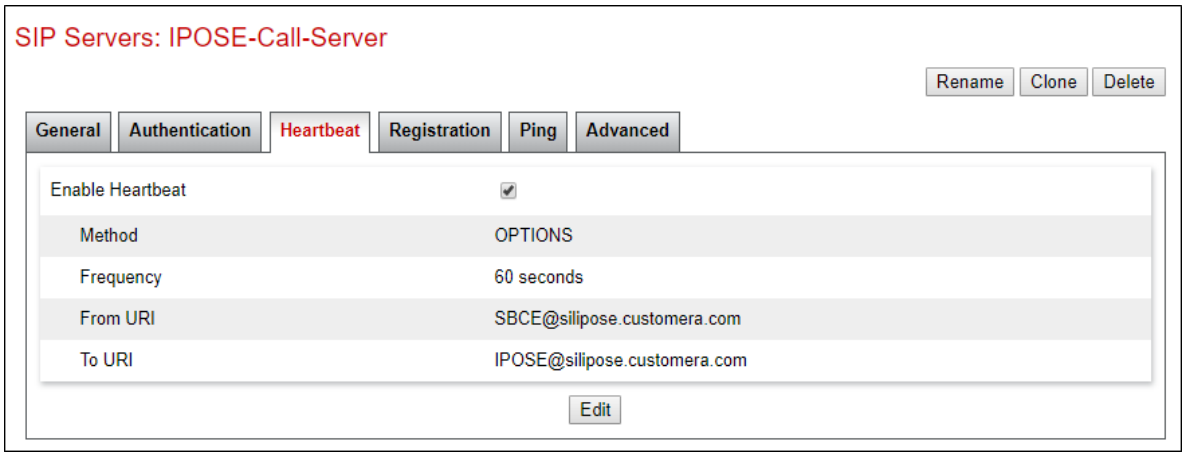


Las siguientes pantallas ilustran el perfil del servidor SIP denominado**Servidor de llamadas IPOSE**. En el **General** parámetros, el**Tipo de servidor**se establece en**Servidor de llamadas**. En el**Dirección IP/FQDN**campo, se ingresa la dirección IP de la interfaz LAN 1 de IP Office en la configuración de muestra. Esta dirección IP es**10.64.19.170**. Por debajo**Puerto**,**5061**se ingresa y el**Transporte**el parámetro se establece en**TLS**. El perfil TLS**sbce8_70Cliente**creado en **Sección 7.2.3**es seleccionado para**Perfil de cliente TLS**. Si agrega el perfil, haga clic en**próximo**(no se muestra) para continuar. Si está editando un perfil existente, haga clic en**Finalizar**.

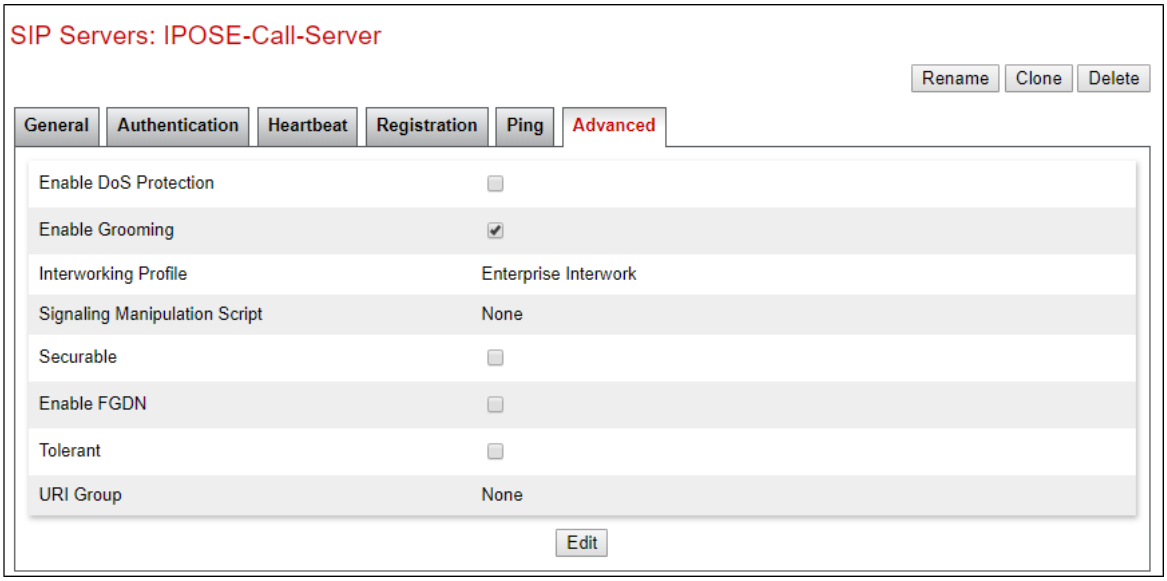


©2020 Avaya Inc. Todos los derechos reservados.

Los valores predeterminados se pueden utilizar en el**Autenticación**pestaña, haga clic**próximo**(no se muestra) para proceder a la **Latido del corazón**pestaña. Avaya SBCE se puede configurar opcionalmente para generar "latidos" en forma de PING u OPCIONES SIP hacia IP Office. Comprobar el**Habilitar latido**cuadro y seleccione **OPCIONES**desde el**Método**Menú desplegable. Seleccione la frecuencia deseada que el SBCE generará OPCIONES hacia IP Office.



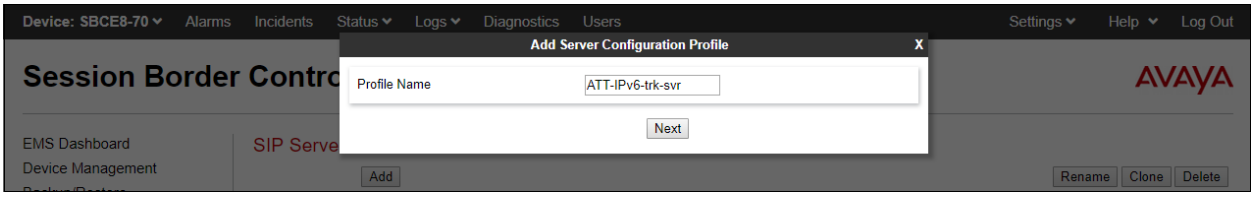
Sobre el**Avanzado**pestaña,**Habilitar preparación**es cheque y el**Perfil de interfuncionamiento**se establece en **Interfuncionamiento empresarial**creado en**Sección 7.6.1**para IP Office.



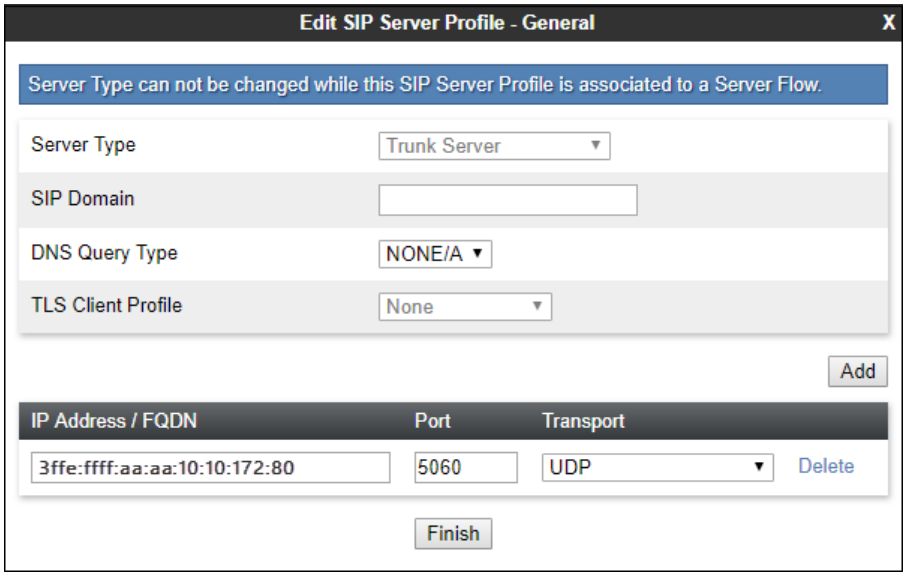
©2020 Avaya Inc. Todos los derechos reservados.

7.7.2. Perfil de servidor SIP - AT&T

Para agregar un perfil de servidor SIP para AT&T, vaya a**Servicios→Servidores SIP**y haga clic**Agregar**. Introduzca un nombre descriptivo para el nuevo perfil y haga clic en**próximo**.



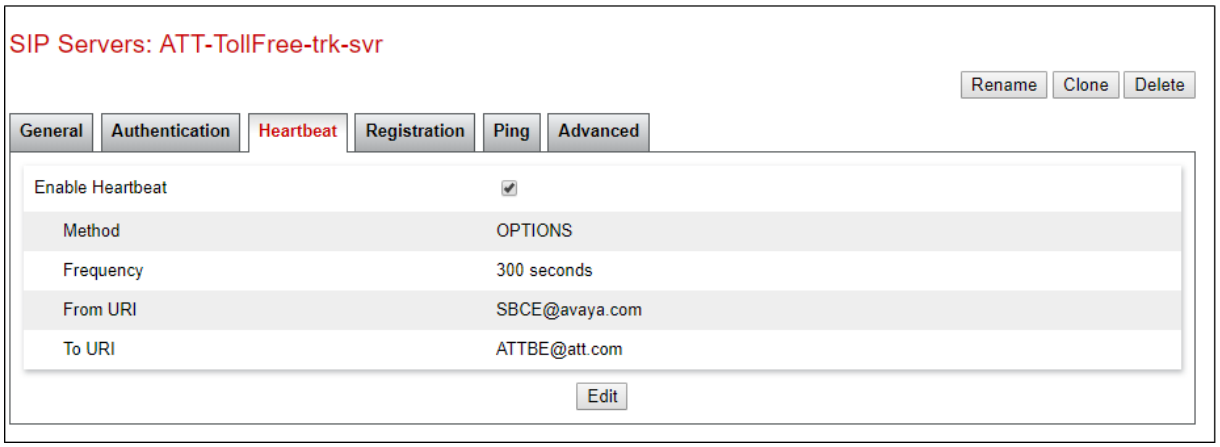
Las siguientes pantallas ilustran el perfil del servidor SIP**ATT-IPv6-trk-svr**. En el**General** parámetros, el**Tipo de servidor**se establece en**Servidor troncal**. En el**Dirección IP/FQDN**campos, se ingresa la dirección IP del elemento de borde proporcionada por AT&T. Esto es**3ffe:ffff:aa:aa:10:10:172:80**. Por debajo**Puerto**,**5060**se ingresa y el **Transporte**el parámetro se establece en**UDP**. Si agrega el perfil, haga clic en**próximo**(no se muestra) para continuar. Si está editando un perfil existente, haga clic en**Finalizar**.



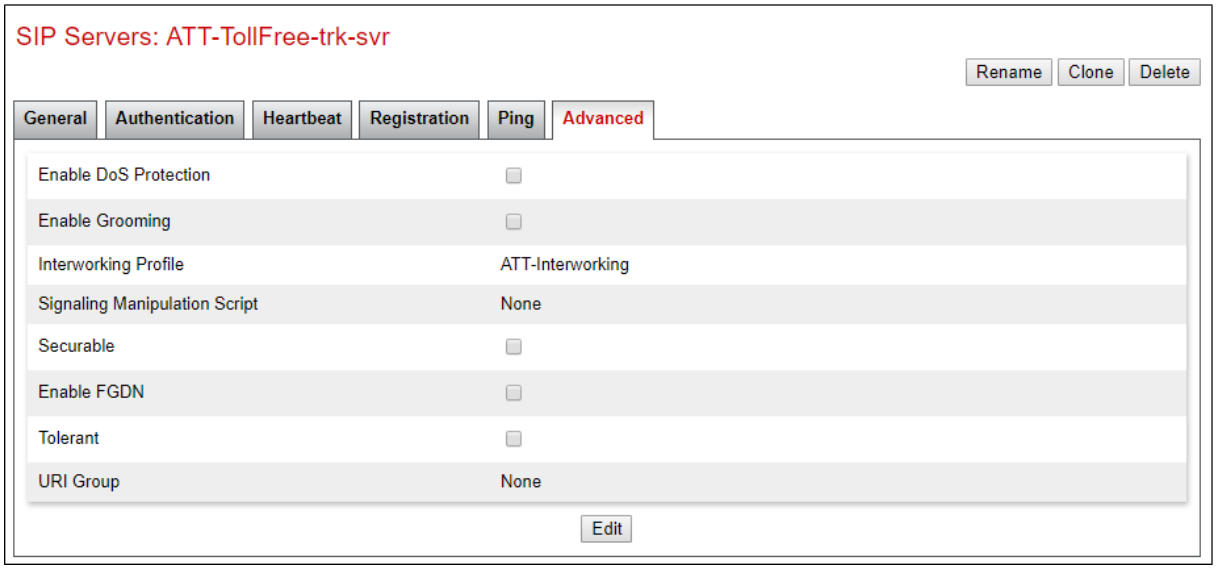
Los valores predeterminados se pueden utilizar en el**Autenticación**pestaña, haga clic**próximo**(no se muestra) para proceder a la **Latidos del corazón**pestaña. Avaya SBCE se puede configurar para generar "latidos" en forma de OPCIONES SIP hacia AT&T. Esta configuración es opcional. Independientemente de si Avaya SBCE está configurado para generar OPCIONES SIP hacia AT&T, AT&T recibirá OPCIONES del sitio de IP Office como resultado de la**Comprobar fuera de servicio**parámetro que se está habilitando en IP Office (consulte **Sección 5.5.2**). Cuando IP Office envía OPCIONES SIP a la dirección IP privada interna de Avaya SBCE, Avaya SBCE enviará OPCIONES SIP a AT&T. Cuando AT&T responda, Avaya SBCE pasará la respuesta a IP Office.

©2020 Avaya Inc. Todos los derechos reservados.

Seleccione**OPCIONES**desde el**Método**Menú desplegable. Seleccione la frecuencia deseada que el SBCE generará OPCIONES. los**Desde URI**y**A URI**se puede completar para configurar URI fácilmente identificables para que aparezcan en OPCIONES SIP proporcionadas por Avaya SBCE. Si agrega un nuevo perfil, haga clic en**próximo**a continuar a la**Avanzado**ajustes.



Sobre el**Avanzado**pestaña,**Habilitar preparación**no se utiliza para conexiones UDP y se deja sin marcar. los**Perfil de interfuncionamiento**se establece en**Interfuncionamiento ATT**creado en**Sección 7.6.2**para AT&T.



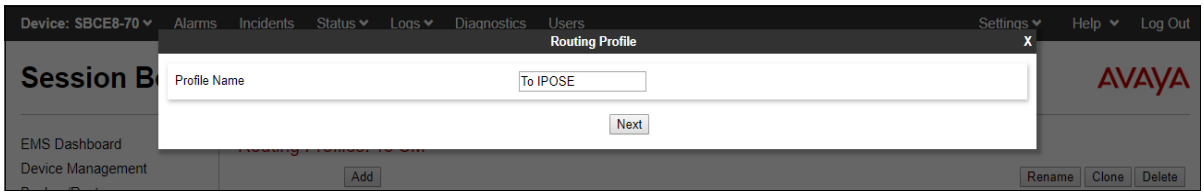
©2020 Avaya Inc. Todos los derechos reservados.

7.8. Perfiles de enrutamiento

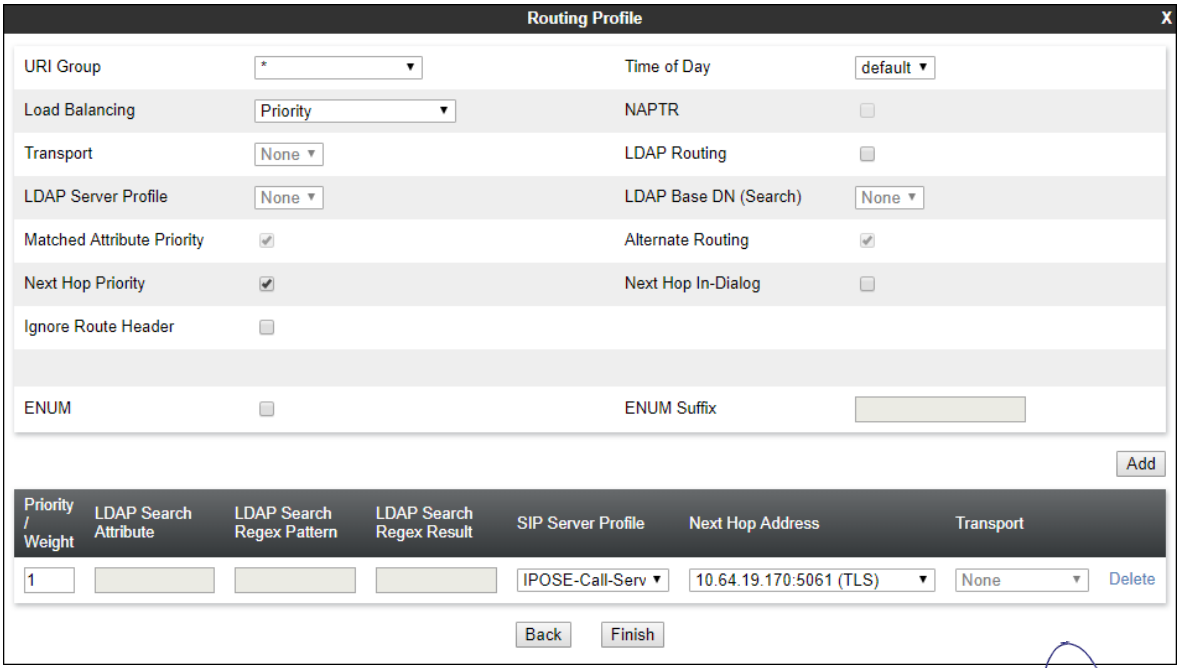
Los perfiles de enrutamiento definen un conjunto específico de criterios de enrutamiento de paquetes que se utilizan junto con otros tipos de políticas de dominio para identificar un flujo de llamadas en particular y, por lo tanto, determinar qué características de seguridad se aplicarán a esos paquetes. Los parámetros definidos por los perfiles de enrutamiento incluyen configuraciones de transporte de paquetes, direcciones de servidores de nombres y métodos de resolución, información de enrutamiento del próximo salto y tipos de transporte de paquetes. Se crearon perfiles de enrutamiento separados en la configuración de referencia para el servicio IP Office y AT&T IPTF.

7.8.1. Perfil de enrutamiento: IP Office

Para agregar el perfil de enrutamiento para IP Office, vaya a**Perfiles de configuración→Enrutamiento**y seleccione **Agregar**. Entrar a**Nombre de perfil**y haga clic**próximo**continuar.



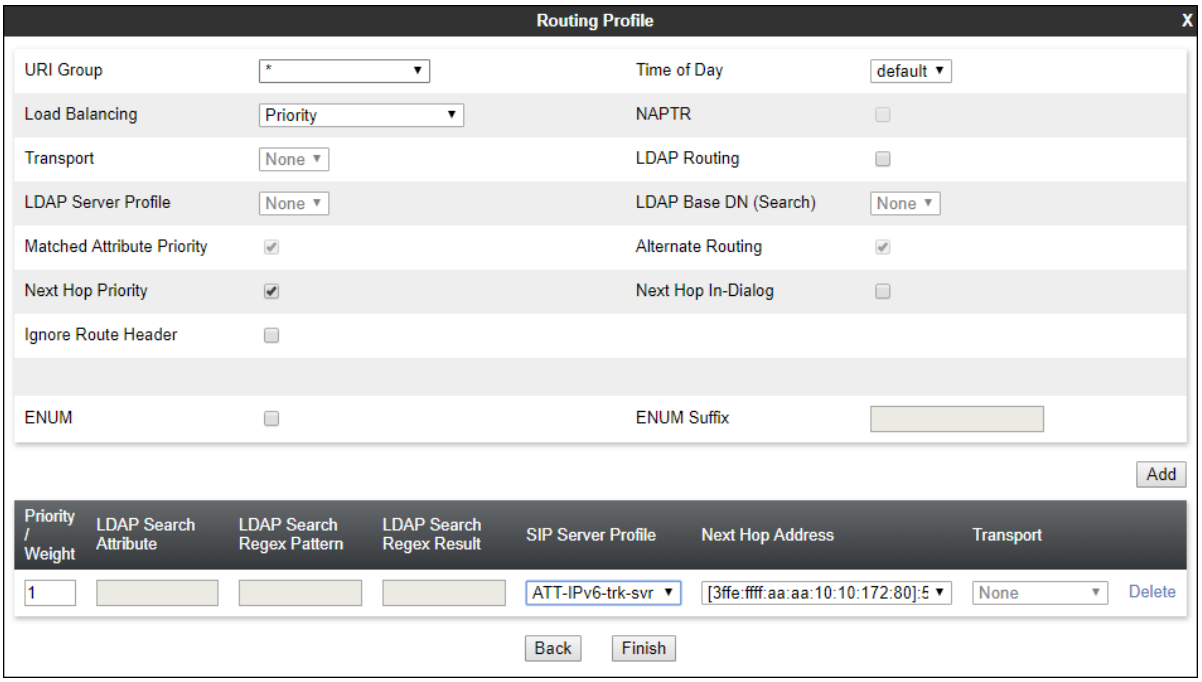
La siguiente pantalla muestra el perfil de enrutamiento**A IPOSE**creado en la configuración de muestra. Los parámetros en la parte superior del perfil se dejan en su configuración predeterminada. Al hacer clic en el**Agregar** El botón en esta pantalla permite ingresar la regla de enrutamiento en la parte inferior del perfil. los**Prioridad / Peso**el parámetro se establece en**1**y la Oficina de PI**Perfil del servidor SIP**, creado en**Sección 7.7.1**, se selecciona en el menú desplegable. los**Dirección del próximo salto**(dirección IP, puerto y transporte) se selecciona automáticamente con los valores del perfil del servidor SIP de IP Office, y**Transporte** se vuelve gris. Hacer clic **Finalizar**.



©2020 Avaya Inc. Todos los derechos reservados.

7.8.2. Perfil de enrutamiento - AT&T

Del mismo modo, agregue un perfil de enrutamiento a AT&T. La siguiente pantalla muestra el perfil de enrutamiento **A ATT IPv6**creado en la configuración de muestra. Los parámetros en la parte superior del perfil se dejan en su configuración predeterminada. los**Prioridad / Peso**el parámetro se establece en**1**y AT&T **Perfil del servidor SIP**, creado en**Sección 7.7.2**, se selecciona en el menú desplegable. los **Dirección del próximo salto**se selecciona automáticamente con los valores del perfil del servidor SIP de AT&T, y**Transporte** se vuelve gris. Hacer clic**Finalizar**.



©2020 Avaya Inc. Todos los derechos reservados.

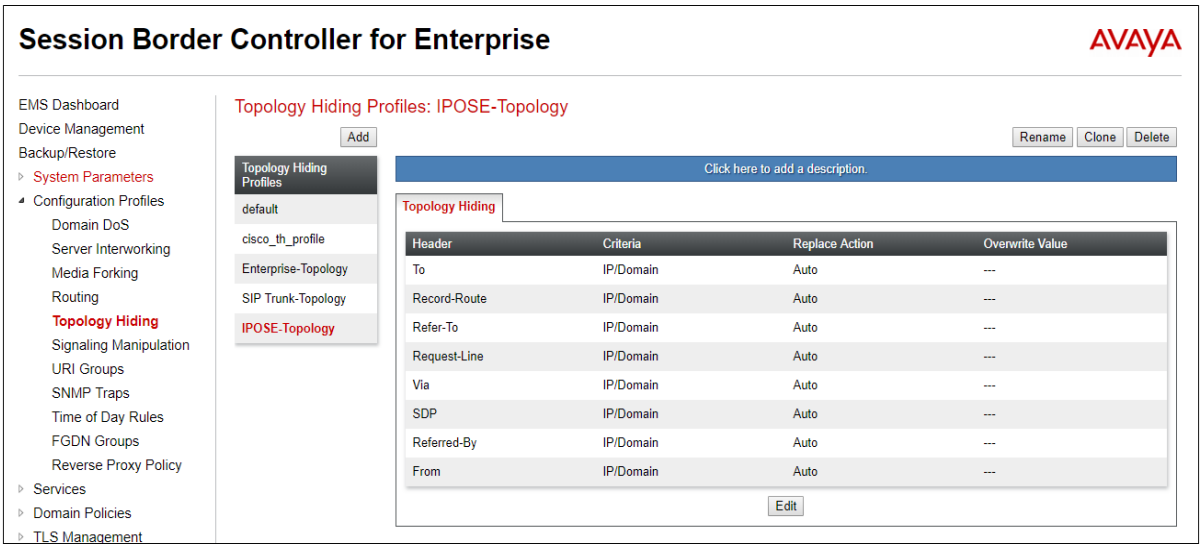
7.9. Perfil de ocultación de topología

El perfil de ocultación de topología administra cómo se sustituye o cambia la información de origen, destino y enrutamiento en los encabezados de mensajes SIP y SDP para mantener la integridad de la red. Oculta la topología de la red empresarial de las redes externas.

Para crear los perfiles de Ocultación de topología para IP Office y AT&T, vaya a**Perfiles de configuración→ Topología**Ocultación. Haga clic en el**Agregar**para agregar un nuevo perfil, o seleccione un perfil oculto de topología existente para editar. En la configuración de ejemplo, el**defecto**el perfil se clonó tanto para IP Office como para AT&T. Posteriormente se aplicarán a los flujos del servidor en**Sección 7.15**.

En el**Reemplazar acción**columna una acción de**Auto**reemplazará el campo de encabezado con la dirección IP de la interfaz Avaya SBCE y el**Sobrescribir**utilizará el valor en el**Sobrescribir valor**.

En el ejemplo mostrado,**IPOSE-Topología**fue clonado desde el valor predeterminado. Un segundo perfil,**Topología troncal SIP**(no se muestra) se clonó de manera similar desde el valor predeterminado.

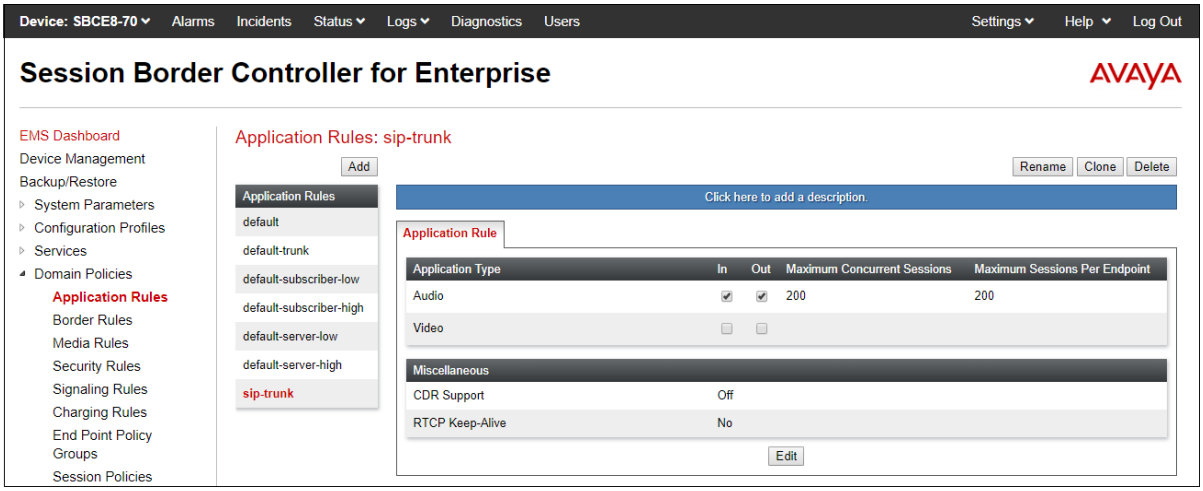


©2020 Avaya Inc. Todos los derechos reservados.

7.10. Reglas de aplicación

Las reglas de aplicación definen qué tipos de aplicaciones de comunicaciones unificadas (UC) basadas en SIP protegerá el dispositivo de seguridad Avaya SBCE: voz, video y/o mensajería instantánea (IM). Además, puede determinar la cantidad máxima de sesiones simultáneas de voz y video que procesará la red para evitar el agotamiento de los recursos.

Seleccione**Políticas de dominio→Reglas de aplicación**en el menú del lado izquierdo como se muestra a continuación. Haga clic en el**Agregar**para agregar un nuevo perfil, o seleccione una regla de aplicación existente para editar. En la configuración de ejemplo, el**sorbete**se creó la regla para IP Office y AT&T. En una instalación de cliente real, configure el**Máximo de sesiones simultáneas**Para el**Audio**y**Video**aplicaciones a un valor ligeramente mayor que las sesiones con licencia. Por ejemplo, si tiene licencia para 150 sesiones, establezca los valores en**200**. los**Sesión máxima por punto final**debe coincidir con el**Máximo de sesiones simultáneas**.



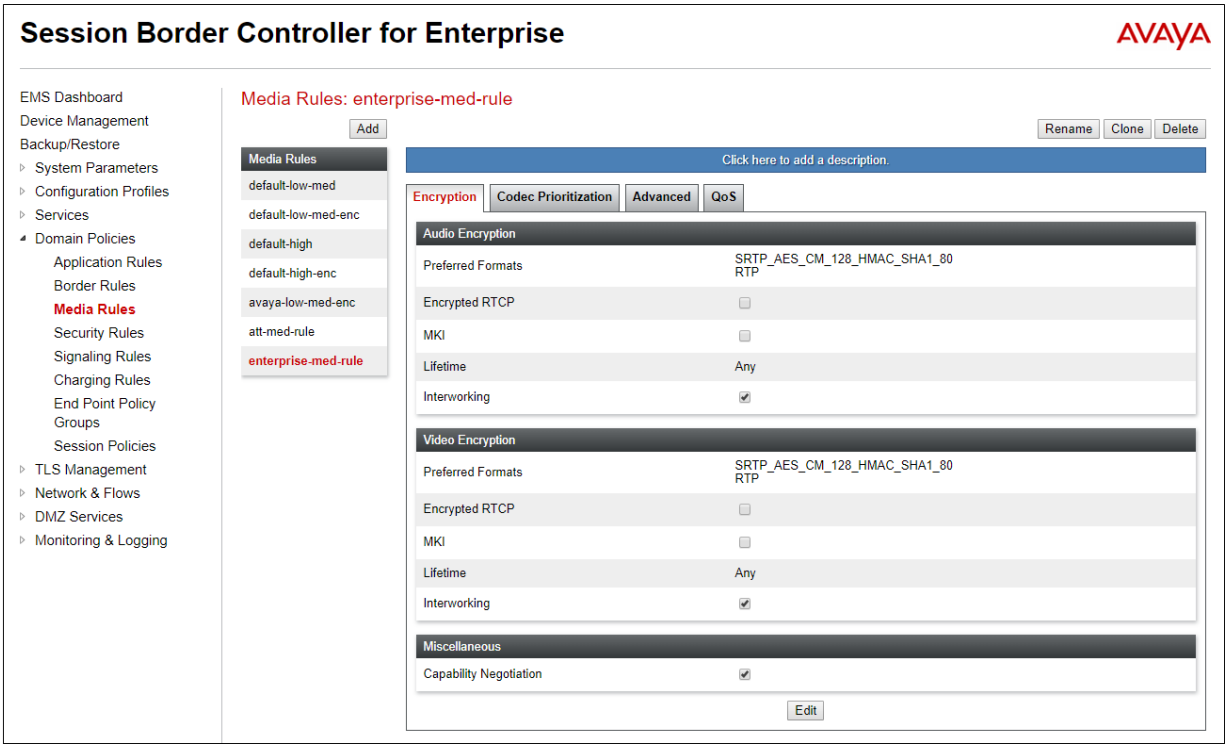
7.11. Reglas de medios

Las reglas de medios definen los parámetros de los paquetes de medios RTP, como la priorización de las técnicas de cifrado y las técnicas de cifrado de paquetes. Juntos, estos parámetros relacionados con los medios definen un perfil estricto que está asociado con otras políticas específicas de SIP para determinar cómo el producto de seguridad Avaya SBCE manejará los paquetes de medios que coincidan con estos criterios.

Para crear una regla de medios para IP Office, seleccione**Políticas de dominio→Reglas de medios**del menú del lado izquierdo. En la configuración de ejemplo, el valor predeterminado**avaya-low-med-enc**La regla se clonó para IP Office y luego se modificó como se muestra en la pantalla a continuación. Con el**avaya-low-med-enc**regla elegida, haga clic en**Clon** . Introduzca un nombre descriptivo para la nueva regla y haga clic en**Finalizar**(no mostrado).

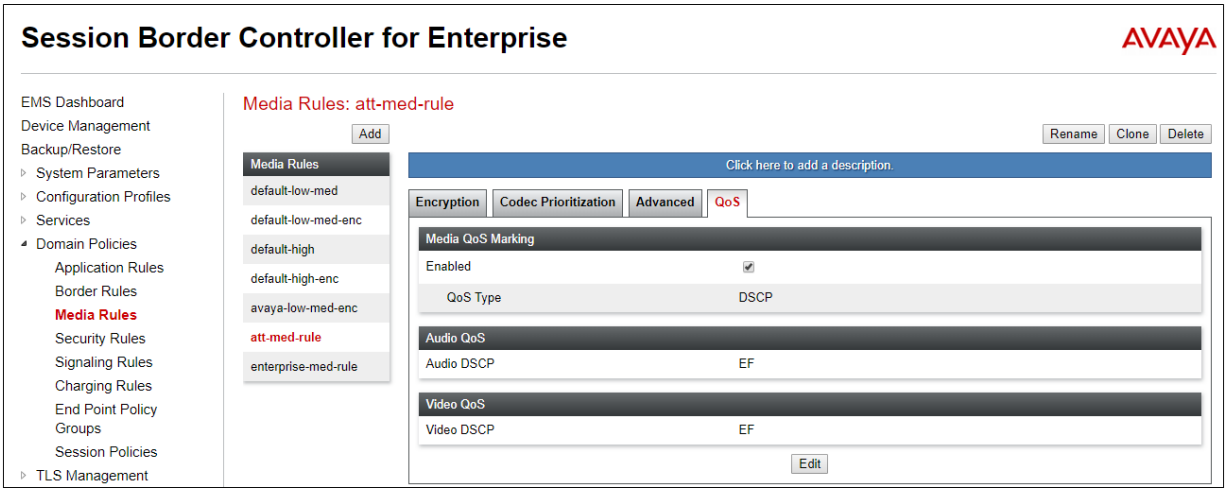
©2020 Avaya Inc. Todos los derechos reservados.

La regla de los medios**empresa-regla-médica**creado para IP Office se muestra a continuación.



Del mismo modo, el valor predeterminado**predeterminado-bajo-med**La regla se clonó para crear la regla de medios para AT&T.

La regla de medios denominada**att-med-regla**utilizado en la configuración de muestra para AT&T IPTF se muestra a continuación, con los valores DSCP**FE**para reenvío acelerado (valor predeterminado) para**QoS de medios**. Ver **Sección 2.2**, **artículo 4**por las limitaciones actuales.

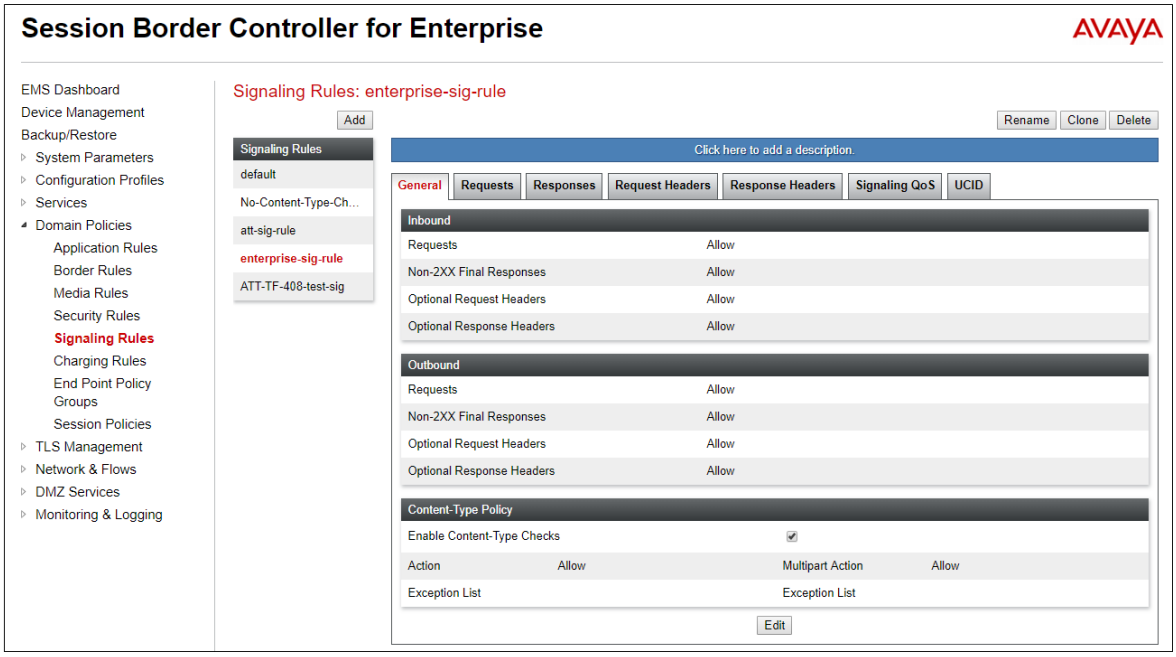


©2020 Avaya Inc. Todos los derechos reservados.

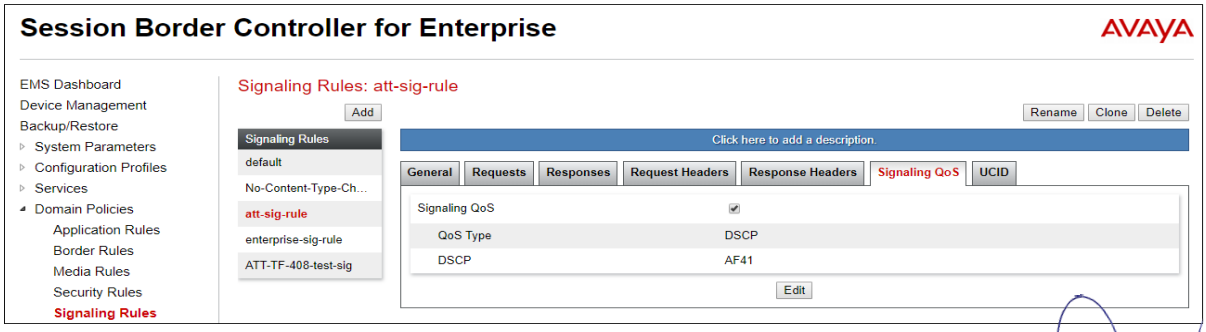
7.12. Reglas de señalización

Las reglas de señalización definen la acción que se debe realizar (permitir, bloquear, bloquear con respuesta, etc.) para cada tipo de mensaje de solicitud y respuesta de señalización específico de SIP. Cuando Avaya SBCE recibe los paquetes de señalización SIP, se analizan y se "coinciden con el patrón" según los criterios de señalización específicos definidos por estas reglas. Los paquetes que coinciden con los criterios definidos por las reglas de señalización se etiquetan para una mayor coincidencia de políticas.

Clonar y modificar el**defecto**regla de señalización para agregar la calidad de servicio adecuada a la señalización SIP. Para clonar una regla de señalización, vaya a**Políticas de dominio→Reglas de señalización**. Con el **defecto**regla elegida, haga clic en**Clon**. Introduzca un nombre descriptivo para la nueva regla y haga clic en**Finalizar**(no mostrado). En la configuración de muestra, la regla de señalización**regla de firma empresarial**no cambia con respecto a la regla predeterminada.



Regla de señalización**regla del sig del att**también se clonó de la regla predeterminada y se usó para AT&T. El valor DSCP **AF41**para el reenvío asegurado (valor predeterminado) se configuró para**QoS de señalización**. Ver**Sección 2.2**, **artículo 4** por las limitaciones actuales.

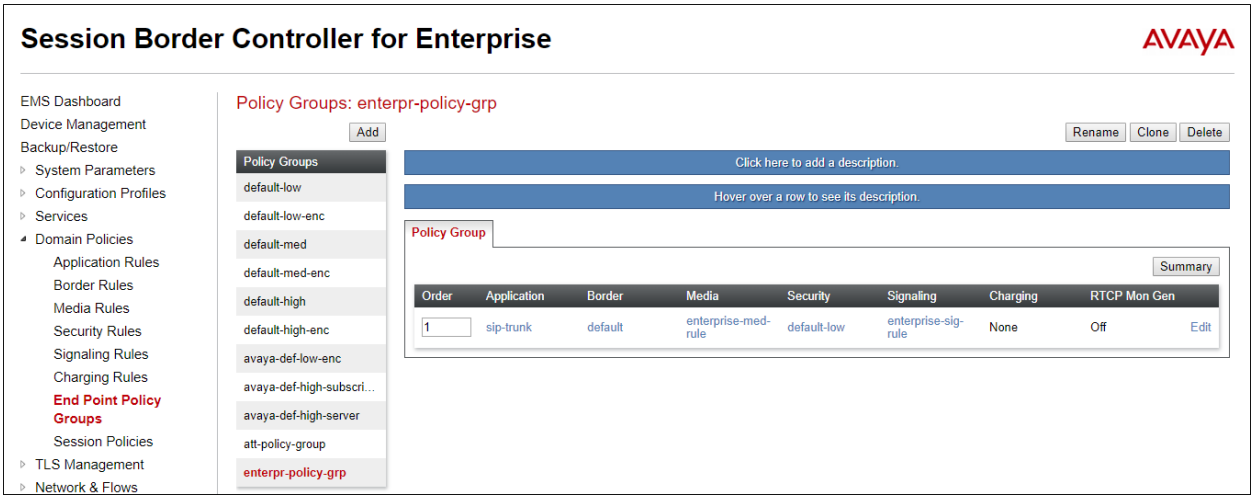


©2020 Avaya Inc. Todos los derechos reservados.

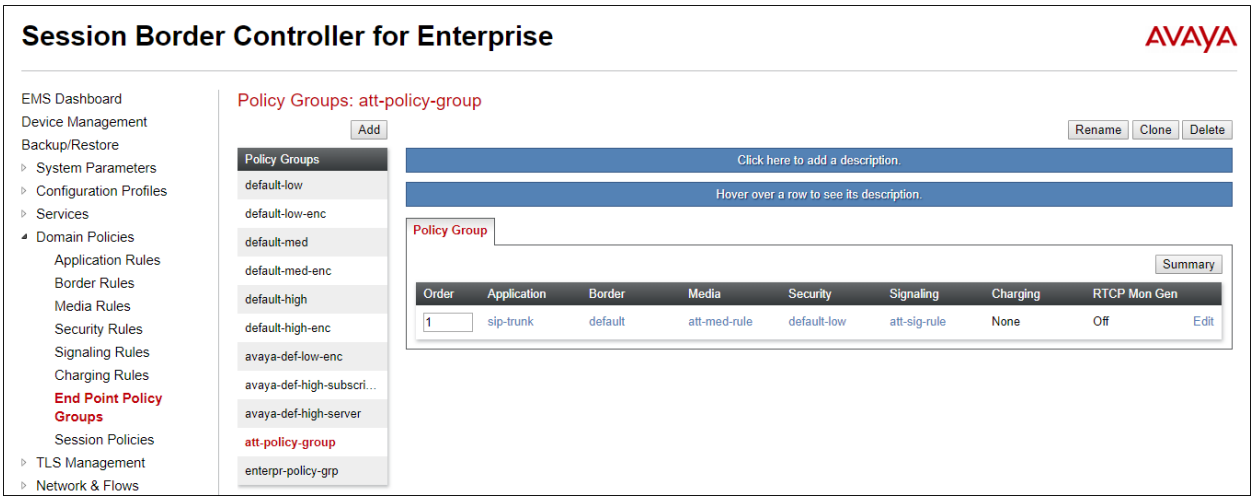
7.13. Grupos de políticas de punto final

Las reglas creadas dentro de la sección Política de dominio se asignan a un Grupo de políticas de punto final. Luego, el grupo de políticas de punto final se aplica a un flujo de servidor en**Sección 7.15**.

Para crear un nuevo grupo de políticas, vaya a**Políticas de dominio→Grupos de políticas de punto final**y haga clic en **Agregar**Como se muestra abajo. La siguiente pantalla muestra la**enterpr-policy-grp**creado para IP Office. Los detalles de las reglas no predeterminadas elegidas se muestran en las secciones anteriores.



La siguiente pantalla muestra la**grupo de directivas att**creado para AT&T. Los detalles de las reglas no predeterminadas elegidas se muestran en las secciones anteriores.



©2020 Avaya Inc. Todos los derechos reservados.

7.14. Opciones avanzadas

En**Sección 7.4**, los rangos de puertos UDP de medios requeridos por AT&T están configurados (**16384**–**32767**). Sin embargo, de manera predeterminada, Avaya SBCE ya asigna parte de este rango para uso interno (22000 - 31000). Los siguientes pasos reasignan los rangos de puertos utilizados por Avaya SBCE, por lo que el rango requerido por AT&T se puede definir como se muestra en**Sección 7.4**.

Paso 1-Seleccione**Configuración específica del dispositivo→Opciones avanzadas**del menú de la izquierda lado.

Paso 2-Selecciona el**Rangos de puertos**pestaña.

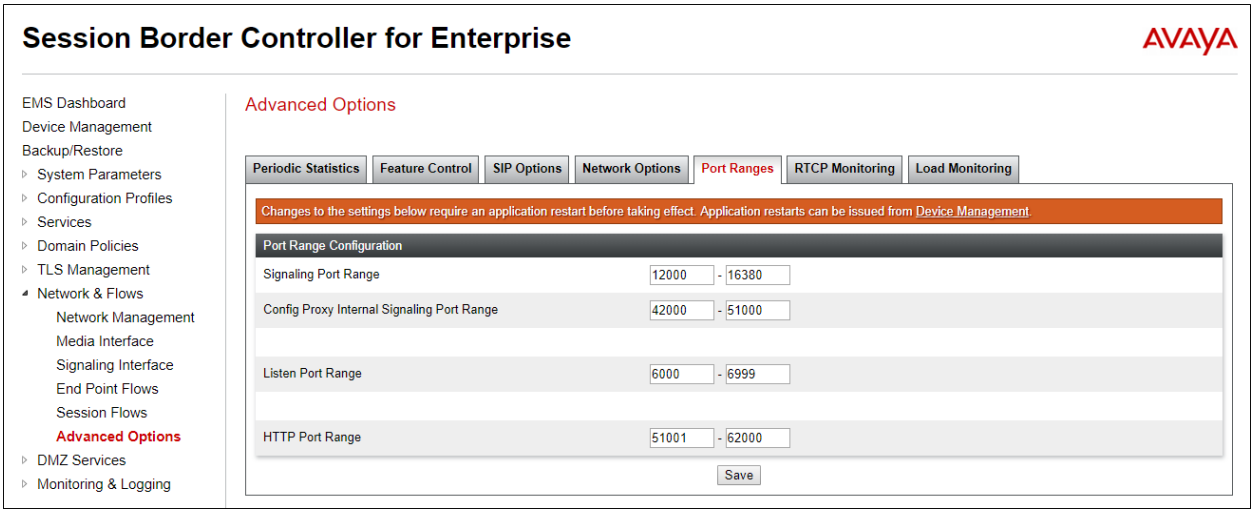
Paso 3-En el**Rango del puerto de señalización**fila, cambie el rango a**12000**–**16380**

Paso 4-En el**Intervalo de puertos de señalización interna del proxy de configuración**fila, cambie el rango a**42000**–**51000**.

Paso 5–En el**Intervalo de puertos de escucha**fila, cambie el rango a**6000**–**6999**.

Paso 6–En el**Intervalo de puertos HTTP**fila, cambie el rango a**51001**–**62000**.

Paso 7-Seleccione**Ahorrar**. Tenga en cuenta que los cambios en estos valores requieren un reinicio de la aplicación (ver**Sección 7.1**).



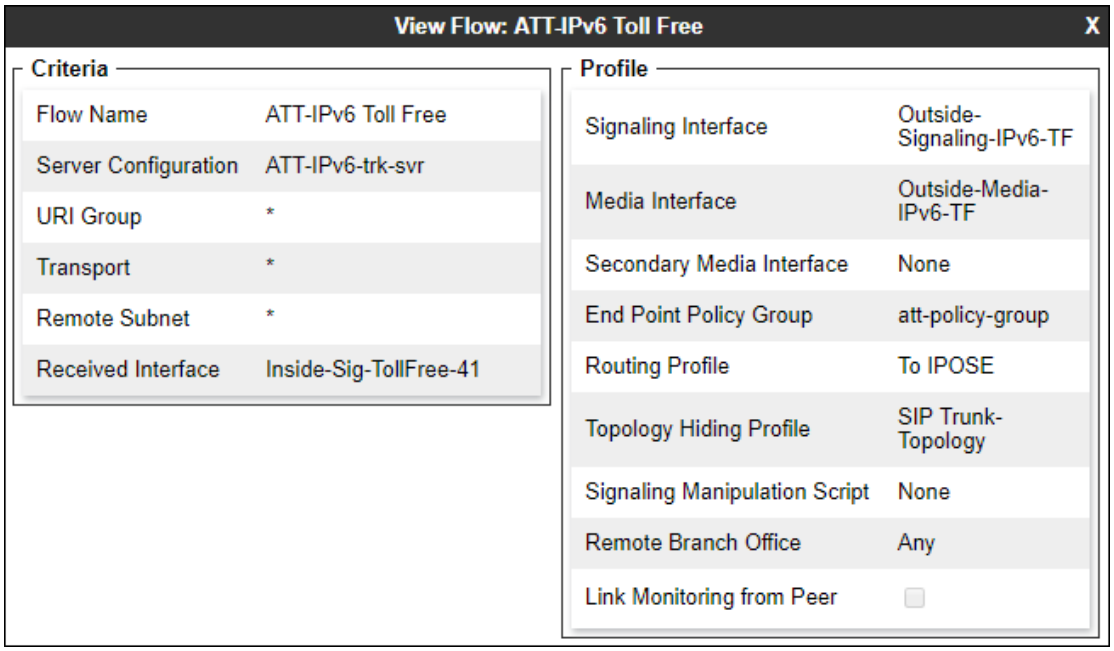
©2020 Avaya Inc. Todos los derechos reservados.

7.15. Flujos de punto final: flujo de servidor

Cuando Avaya SBCE recibe un paquete, el contenido del paquete (direcciones IP, URI, etc.) se usa para determinar qué flujo coincide. Una vez que se determina el flujo, el flujo apunta a una política que contiene varias reglas relacionadas con el procesamiento, los privilegios, la autenticación, el enrutamiento, etc. Una vez que se aplica el enrutamiento y se determina el punto final de destino, se aplican las políticas para este punto final de destino. El contexto se mantiene para ser aplicado a futuros paquetes en el mismo flujo.

Cree un flujo de servidor para el servicio IP Office y AT&T IPTF. Para crear un flujo de servidor, vaya a **Redes y flujos→Flujos de punto final**. Selecciona el**Flujos de servidor**pestaña y haga clic**Agregar**(no mostrado).

La siguiente pantalla muestra el flujo denominado**TCA IPTF**visto desde la configuración de ejemplo. Este flujo utiliza las interfaces, las políticas y los perfiles definidos en las secciones anteriores.



©2020 Avaya Inc. Todos los derechos reservados.

Una vez más, seleccione el**Flujos de servidor**pestaña y haga clic**Agregar**. La siguiente pantalla muestra el flujo denominado**IPO – Llamada gratuita**visto desde la configuración de ejemplo. Este flujo utiliza las interfaces, las políticas y los perfiles definidos en las secciones anteriores.

View Flow: IPO Flow IPTF IPv6 X

Criteria

Flow Name	IPO Flow IPTF IPv6
Server Configuration	IPOSE-Call-Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside-Signaling-IPv6-TF

Profile

Signaling Interface	Inside-Sig-TollFree-41
Media Interface	Inside-Media-TollFree
Secondary Media Interface	None
End Point Policy Group	enterpr-policy-grp
Routing Profile	To ATT IPv6
Topology Hiding Profile	IPOSE-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	

©2020 Avaya Inc. Todos los derechos reservados.

8. Configuración del servicio gratuito de IP de AT&T

AT&T proporciona la dirección IP del elemento fronterizo del servicio IPTF, los números DID de acceso y los dígitos DNIS asociados utilizados en la configuración de referencia. Además, las funciones de AT&T IPTF y sus números de acceso asociados también son asignados por AT&T. AT&T requiere que se proporcione la dirección IP pública (B1) de Avaya SBCE al servicio IPTF, como parte del proceso de aprovisionamiento. Para más información consultar referencia**[11]**.

9. Pasos de verificación

Los siguientes procedimientos se pueden usar para verificar la versión 11.0 de Avaya IP Office y la versión 8.0.1 de Avaya SBCE con la configuración del servicio AT&T IPTF.

9.1. Servicio gratuito de IP de AT&T

Se pueden ejecutar los siguientes escenarios para verificar la funcionalidad con el servicio AT&T IPTF:

- Realice llamadas entrantes, responda las llamadas y verifique que exista una ruta de conversación bidireccional. Verifica que las llamadas permanezcan estables por varios minutos y se desconecte correctamente.
- Llamadas entrantes usando los códecs G.729A y G.711 ULAW.
- Verifique las funciones básicas de las llamadas, como espera, transferencia y conferencia.
- Realice una llamada entrante a un teléfono, pero no conteste la llamada. Verifique que la llamada cubra el correo de voz (p. ej., Voicemail Pro). Recupere el mensaje localmente o desde PSTN.

- Utilizando los números y códigos de acceso de IPTF apropiados, verifique las funciones iniciadas por DTMF de "Legacy Transfer Connect".
- Fax entrante usando T.38 o G.711. Ver**Sección 2.2**por limitaciones.
- OPCIONES SIP monitoreo de la salud del troncal SIP.

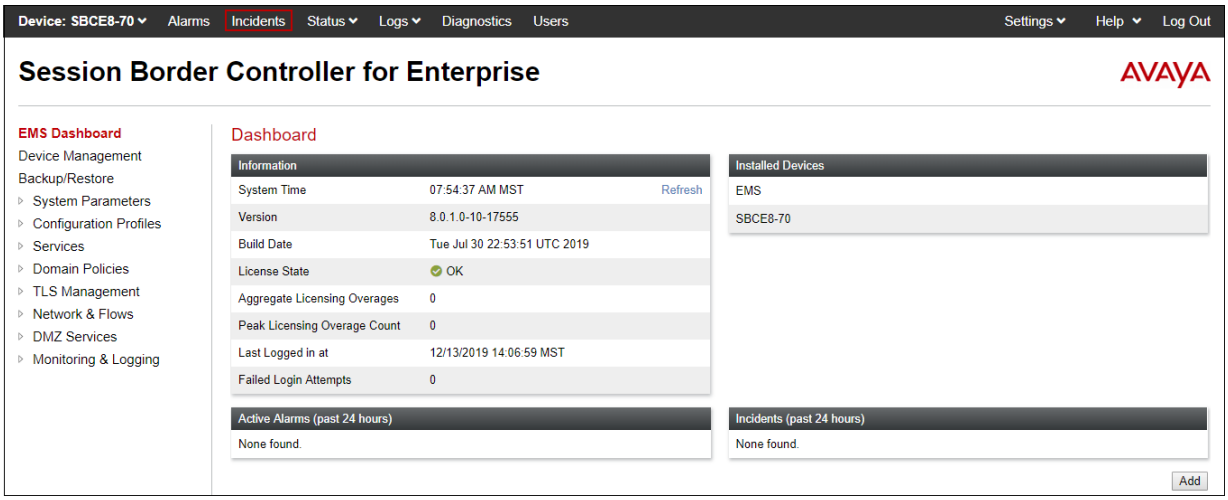
©2020 Avaya Inc. Todos los derechos reservados.

9.2. Avaya SBCE

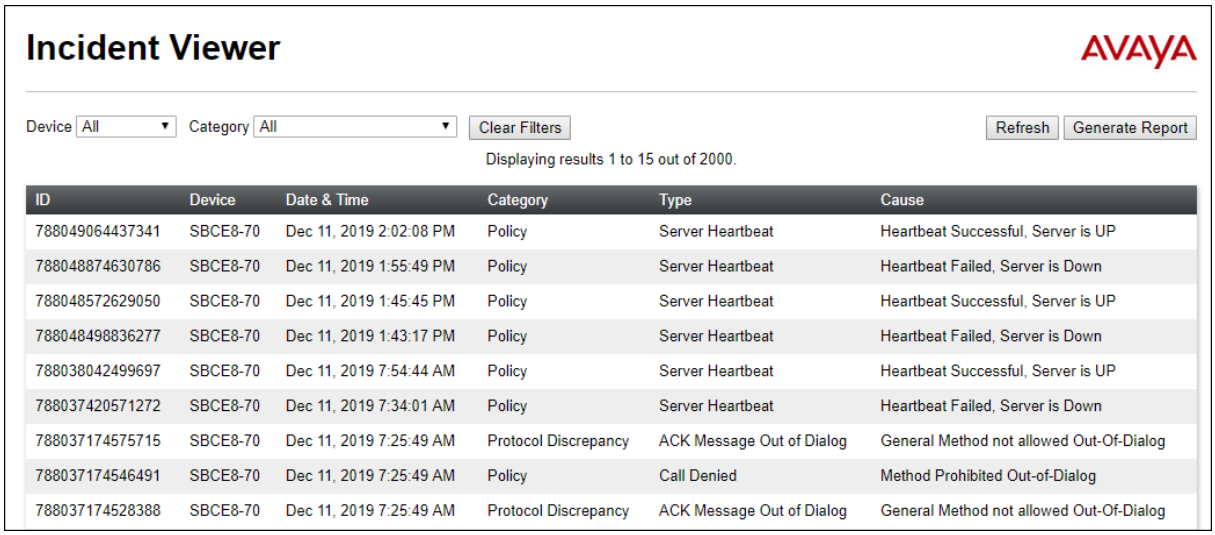
Esta sección proporciona pasos de verificación que se pueden realizar con Avaya SBCE.

9.2.1. incidentes

Se puede acceder al Visor de incidentes desde el menú de navegación superior de Avaya SBCE como se destaca en la siguiente captura de pantalla.



Use el Visor de incidentes para verificar Server Heartbeat y solucionar fallas de enrutamiento.

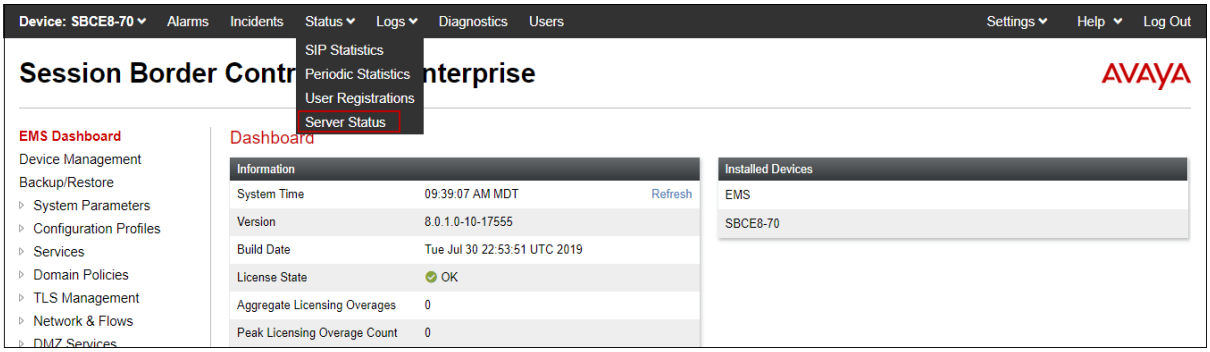


ID	Device	Date & Time	Category	Type	Cause
788049064437341	SBCE8-70	Dec 11, 2019 2:02:08 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
788048874630786	SBCE8-70	Dec 11, 2019 1:55:49 PM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
788048572629050	SBCE8-70	Dec 11, 2019 1:45:45 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
788048498836277	SBCE8-70	Dec 11, 2019 1:43:17 PM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
788038042499697	SBCE8-70	Dec 11, 2019 7:54:44 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
788037420571272	SBCE8-70	Dec 11, 2019 7:34:01 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
788037174575715	SBCE8-70	Dec 11, 2019 7:25:49 AM	Protocol Discrepancy	ACK Message Out of Dialog	General Method not allowed Out-Of-Dialog
788037174546491	SBCE8-70	Dec 11, 2019 7:25:49 AM	Policy	Call Denied	Method Prohibited Out-of-Dialog
788037174528388	SBCE8-70	Dec 11, 2019 7:25:49 AM	Protocol Discrepancy	ACK Message Out of Dialog	General Method not allowed Out-Of-Dialog

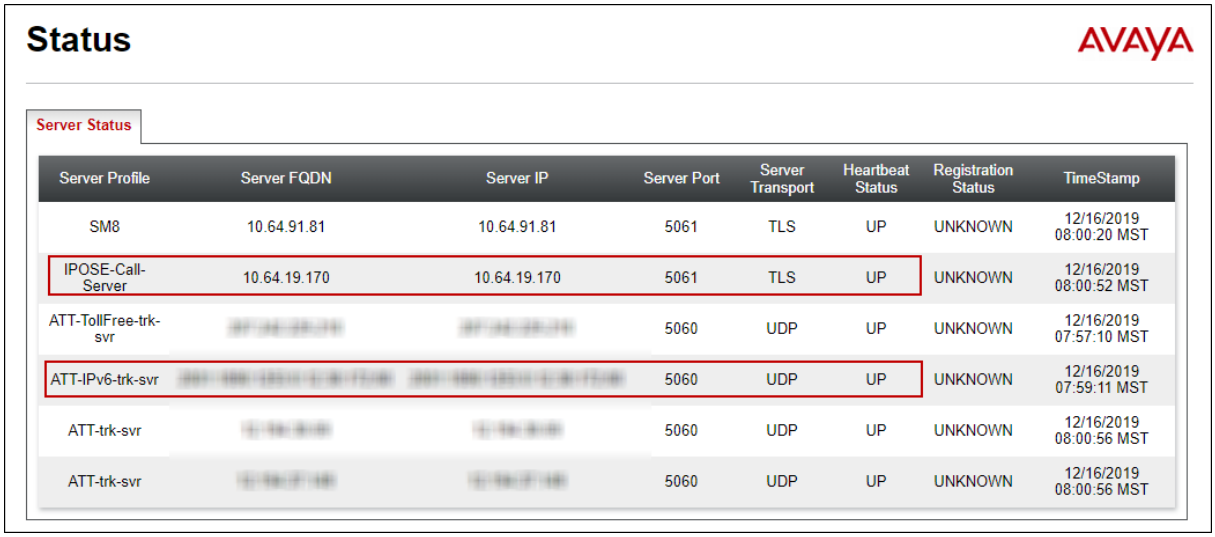
©2020 Avaya Inc. Todos los derechos reservados.

9.2.2. El estado del servidor

los**El estado del servidor**Se puede acceder desde el menú de navegación superior de Avaya SBCE seleccionando el **Estado**menú, y luego**El estado del servidor**.



los**El estado del servidor**La pantalla proporciona información sobre el estado de la conexión a los servidores SIP conectados. Esta funcionalidad requiere que Heartbeat esté habilitado en el perfil del servidor SIP, como se configuró en**Sección 7.7**.

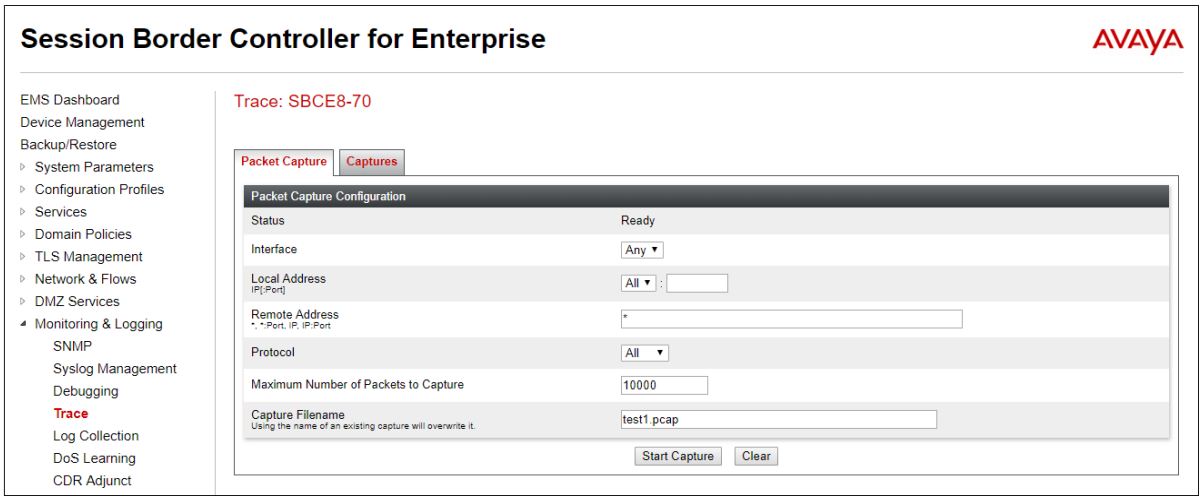


Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
SM8	10.64.91.81	10.64.91.81	5061	TLS	UP	UNKNOWN	12/16/2019 08:00:20 MST
IPOSE-Call-Server	10.64.19.170	10.64.19.170	5061	TLS	UP	UNKNOWN	12/16/2019 08:00:52 MST
ATT-TollFree-trk-svr	[redacted]	[redacted]	5060	UDP	UP	UNKNOWN	12/16/2019 07:57:10 MST
ATT-IPv6-trk-svr	[redacted]	[redacted]	5060	UDP	UP	UNKNOWN	12/16/2019 07:59:11 MST
ATT-trk-svr	[redacted]	[redacted]	5060	UDP	UP	UNKNOWN	12/16/2019 08:00:56 MST
ATT-trk-svr	[redacted]	[redacted]	5060	UDP	UP	UNKNOWN	12/16/2019 08:00:56 MST

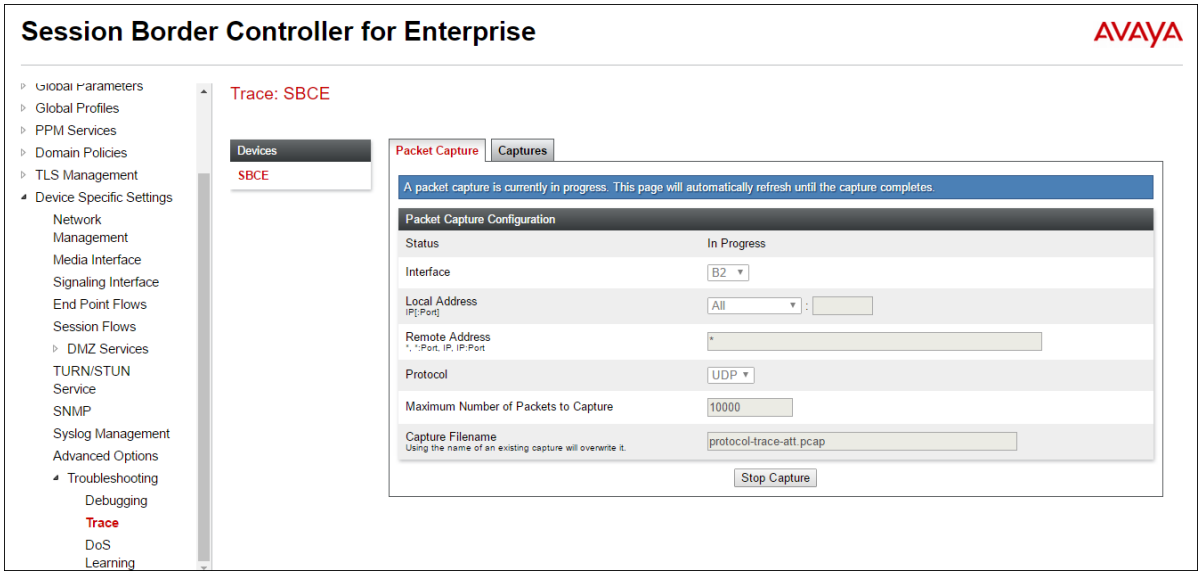
©2020 Avaya Inc. Todos los derechos reservados.

9.2.3. Trazas de protocolo

Para rastrear una llamada, navegue hasta**Monitoreo y registro→Rastro**y seleccione el**Captura de paquetes**pestaña. Complete los campos para los parámetros de captura y haga clic en**Iniciar captura**Como se muestra abajo.

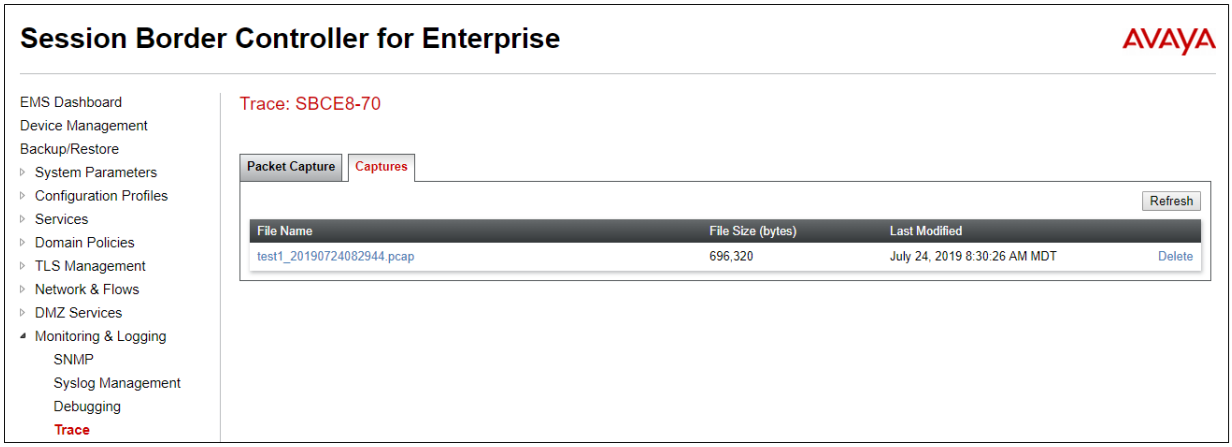


Cuando el rastreo haya alcanzado el número deseado de paquetes, el rastreo se detendrá automáticamente o, alternativamente, presionará el**Detener captura**botón en la parte inferior.



©2020 Avaya Inc. Todos los derechos reservados.

Selecciona el**capturas**pestaña para ver los archivos creados durante la captura de paquetes.



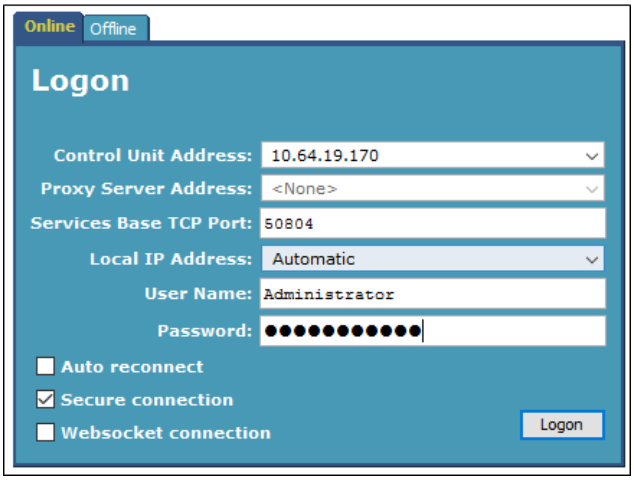
El archivo de captura de paquetes se puede descargar y luego ver usando un analizador de protocolo de red como Wireshark.

9.3. Oficina IP de Avaya

Los siguientes elementos se pueden usar para analizar o solucionar problemas de las operaciones de Avaya IP Office.

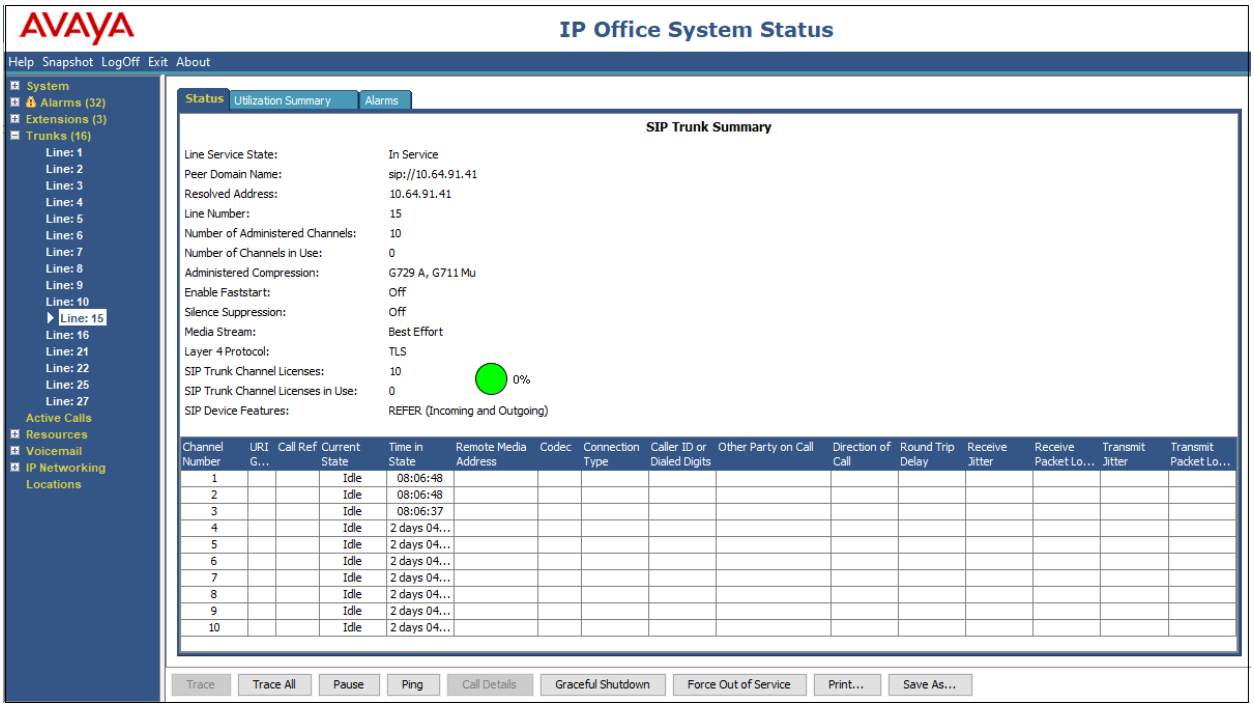
9.3.1. Aplicación de estado del sistema

La aplicación de estado del sistema IP Office de Avaya se puede utilizar para verificar el estado del servicio de la línea SIP. Desde la aplicación IP Office Manager, seleccione**Expediente→Avanzado→Estado del sistema**. Por debajo **Dirección IP de la unidad de control**seleccione la dirección IP del sistema IP Office bajo verificación. Inicie sesión con las credenciales adecuadas.

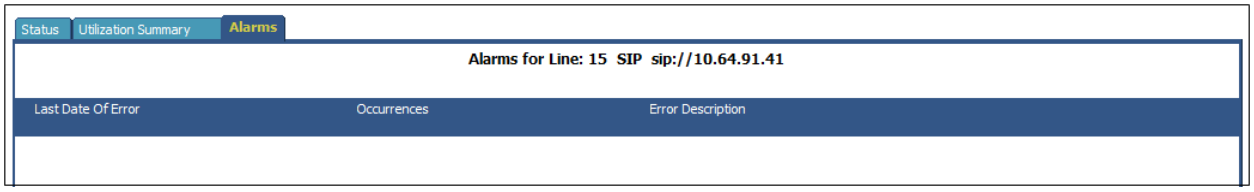


©2020 Avaya Inc. Todos los derechos reservados.

Después de iniciar sesión, seleccione**Bañador**→**Línea: 15**en el menú de navegación izquierdo. (La línea SIP 15 está configurada en **Sección 5.5**). Se muestra una pantalla como la que se muestra a continuación. En la parte inferior izquierda, el**Rastrear todo**Se puede presionar el botón para mostrar la información de seguimiento a medida que se realizan llamadas utilizando esta línea SIP. los**Silbido**El botón se puede utilizar para hacer ping al otro extremo de la troncal SIP (p. ej., Avaya SBCE).



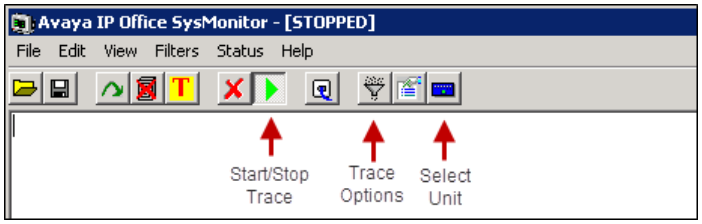
S**eléctrico**en el**alarmas**y verifique que no haya alarmas activas en la línea SIP.



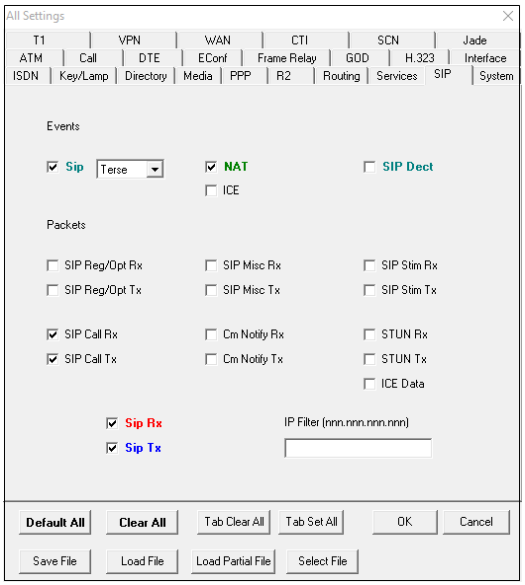
©2020 Avaya Inc. Todos los derechos reservados.

9.3.2. Aplicación de supervisión del sistema

La aplicación Avaya IP Office Monitor se puede usar para monitorear y solucionar problemas de mensajes de señalización en el troncal SIP. Inicie la aplicación desde**comienzo→Programas→Oficina de PI→ Monitor**en la PC donde se instaló IP Office Manager. Haga clic en el**Seleccionar Unidad**en la barra de tareas y seleccione la dirección IP del sistema IP Office bajo verificación.



Al hacer clic en el**Opciones de seguimiento**icono en la barra de tareas y seleccionando el**SORBO**La pestaña permite modificar el umbral utilizado para capturar eventos, tipos de paquetes a capturar, filtros, etc. Adicionalmente, el color utilizado para representar los paquetes en la traza se puede personalizar haciendo clic derecho sobre el tipo de paquete y seleccionando el color deseado. .



©2020 Avaya Inc. Todos los derechos reservados.

10. Conclusión

Como se ilustra en estas Notas de aplicación, Avaya IP Office versión 11.0 y Avaya Session Border Controller for Enterprise versión 8.0.1 se pueden configurar para interoperar correctamente con el servicio gratuito de IP de AT&T mediante IPv6 y**AVPN**o**MIS/PTN**conexiones de transporte, utilizando las características de servicio enumeradas en**Sección 2.1**, y dentro de las limitaciones descritas en**Sección 2.2**.

La configuración de referencia que se muestra en estas Notas de aplicación es representativa de la configuración básica de un cliente empresarial y tiene como objetivo proporcionar una guía de configuración para complementar la documentación de otros productos de Avaya. Se basa en pruebas formales de cumplimiento de interoperabilidad como parte del programa Avaya DevConnect Service Provider.

11. Referencias adicionales

Avaya:

La documentación del producto de Avaya está disponible enhttp://soporte.avaya.com . Puede encontrar información adicional de Avaya IP Office en:http://herramientas de marketing.avaya.com/knowledgebase/

[1]*Implementación de la solución IP Office Platform Server Edition*, versión 11.0, mayo de 2018

[2]*IP Office Platform 11.0, Implementación de servidores IP Office de Avaya como máquinas virtuales,*abril 2019

[3]*Plataforma IP Office 11.0, Implementación de Avaya IP Office Essential Edition (IP500 V2)*, enero de 2020.

[4]*Administración de Avaya IP Office Platform con Manager, versión 11.0,*febrero 2019.

[5]*Administración de la plataforma IP Office de Avaya con Web Manager, versión 11.0 FP4*, febrero de 2019.

[6]*IP Office Platform 11.0, administración de Avaya IP Office Platform Voicemail Pro*, diciembre de 2019.

[7]*IP Office Platform 11, teléfonos IP Office SIP con ASBCE, edición 03f*, abril de 2019

[8]*Implementación de Avaya Session Border Controller en un entorno virtualizado*. Versión 8.0.x, Problema 4 de agosto de 2019.

[9]*Administración de Avaya Session Border Controller para empresas*, versión 8.0.x, número 4, agosto de 2019.

[10]*RFC 3261 SIP: Protocolo de inicio de sesión*.https://www.ietf.org/rfc/rfc3261.txt

Servicio IPTF de AT&T:

[11] Descripción del servicio de llamada gratuita IP de AT&T - https:// www.business.att.com/products/ip-toll-free.html

©2020 Avaya Inc. Todos los derechos reservados.

©2020 Avaya Inc. Todos los derechos reservados.
Avaya y el logotipo de Avaya son marcas comerciales de Avaya Inc. Todas las marcas comerciales identificadas por ® y ™ son marcas comerciales registradas o marcas comerciales, respectivamente, de Avaya Inc. Todas las demás marcas comerciales son propiedad de sus respectivos dueños. La información proporcionada en estas Notas de aplicación está sujeta a cambios sin previo aviso. Se cree que las configuraciones, los datos técnicos y las recomendaciones proporcionadas en estas Notas de aplicación son precisas y confiables, pero se presentan sin garantía expresa o implícita. Los usuarios son responsables de la aplicación de cualquier producto especificado en estas Notas de aplicación.

Envíe por correo electrónico cualquier pregunta o comentario relacionado con estas Notas de aplicación junto con el nombre completo del título y el nombre del archivo, ubicado en la esquina inferior derecha, directamente al Programa Avaya DevConnect en devconnect@avaya.com .

Avaya Contact Center Select Solution Description

Release 7.0.3
Issue 02.05
July 2018

© 2016-2018, Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

Avaya, the Avaya logo, Avaya one-X® Portal, Avaya Aura® Communication Manager, Avaya Aura® Experience Portal, Avaya Aura® Orchestration Designer, Avaya Aura® Session Manager, Avaya Aura® System Manager, and Application Enablement Services are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 11
Purpose 11
Intended audience 11
Related resources 11
Avaya Contact Center Select Documentation 11
Viewing Avaya Mentor videos 14
Support 14
Chapter 2: Changes in this release 15
Feature changes in the Release 7.0 base build 15
Automatic insertion of a leading digit before dialing numbers using Agent Desktop Phonebook 15
Avaya Contact Center Select supports Microsoft Windows Server 2012 R2 15
Avaya Media Server changes 15
Contact Center Agent Browser application 16
Contact Center Manager Administration password expiry 17
Contact Center Manager Administration support for Caché database 17
Contact Center services secured by default 17
Emergency license expiry notification 18
Force password change when users log on to Contact Center Manager Administration for the first time 18
New Avaya Contact Center Select Hardware Appliance 18
New Avaya Contact Center Select minimum hardware specifications 19
New Avaya Contact Center Select minimum virtual machine specifications 19
Password aging in Contact Center Manager Administration 19
Report Creation Wizard 20
Serviceability enhancements in Contact Center 7.0 20
Support for adding company images and logos to signatures 20
Support for copying the CLID of a customer using Agent Desktop 20
Support for displaying login history in Contact Center Manager Administration, Agent Desktop, and Security Manager 21
Support for forced Not Ready reason codes 21
Support for scripting using CLID and Wild CLID in SIP environments 21
Temporary lock out of Contact Center Manager Administration users 21
Feature changes in Release 7.0 Feature Pack 1 22
Agent Desktop uses a user directory as the default file browsing directory 22
Automatic refreshing of non-staffed skillsets for Real-time Reporting 22
Avaya Contact Center Select supports IP Office Release 10 22
Contact Control Service SDK 23
Embedded web browsers in Agent Desktop use the latest version of Internet Explorer installed on the client system 23

Página1920 de 3226.

File extension restrictions for attachments 23
Improved operational performance for Business Continuity 23
Instant Messaging feature supports Microsoft Skype for Business 2015 24
New application for installing Feature Packs and Service Packs 24
Multimedia account passwords must meet minimum complexity criteria 24
Provision of adding a friendly name for a web chat agent 24
Removal of the default Agent Desktop Dashboard password 25
Skillset list sorted when creating a billboard display 25
Support for the Open Queue Open Interface 25
VMware 6.0 support 25
Whisper Coaching 25
Feature changes in Release 7.0 Feature Pack 2 26
Agent Desktop integrated login 26
Agent skillset assignment guardrails 26
Increased CCMM customer contact ratio 26
Offline Security Store 26
Remote Desktop Services support for Agent Desktop 26
Removal of default security configuration 27
REST API integration 27
Synchronization of accssync user changes to IP Office 27
VMware 6.5 support 27
Feature changes in Release 7.0 Feature Pack 3 27
Ability to store email attachments in the database 28
Contact Center database encryption 28
Data Management - customer privacy 28
REST API Enhancements 28
Security Manager support for chained certifcates 28
Support for applying a restriction flag to a customer 28
Other changes in Release 7.0 29
Agent Desktop no longer supports deployment as a thick client 29
Avaya Contact Center Select OVA file no longer available 29
IP Office supported versions 29
Microsoft Exchange Server supported versions 29
Microsoft Internet Explorer releases no longer supported 29
Secure Sockets Layer communications is no longer supported 30
Windows Server 2008 is no longer supported 30
Other changes in Release 7.0 Feature Pack 1 30
Contact Center security improvements 30
Server Message Block signing enabled on Windows Server 2012 30
Third-party components updated 31
Other changes in Release 7.0 Feature Pack 2 31
CCMA users must login before changing password 31
Installation account for Contact Center install 31

Página1921 de 3226.

Third-party components updated..... 31
Other changes in Release 7.0 Feature Pack 3..... 32
Avaya Aura® Media Server update..... 32
Contact Center backwards compatibility with previous version of Agent Desktop..... 32
IP Office supported versions..... 32
Third-party components updated..... 33
Chapter 3: Avaya Contact Center Select overview..... 34
Licensing..... 36
User Data Synchronization..... 39
Topology..... 40
IP Office supported versions..... 43
Overview of solution configuration..... 44
Simple voice call flow example..... 46
Sample Orchestration Designer voice flow applications..... 47
Multimedia contacts processing..... 50
Simple email message flow..... 51
Call Recording..... 52
Remote Agents..... 53
Avaya Contact Center Select domain and workgroup support..... 54
Avaya Security Advisories..... 56
Avaya Contact Center Select Business Continuity..... 56
Upgrades and migrations..... 56
Reporting Source of Call Disconnect..... 57
Automatically forward IP Office voicemail to multimedia agents..... 58
Limitations..... 59
Chapter 4: Avaya Contact Center Select DVD..... 63
Platform Vendor Independence server specification..... 65
Entry-level server specification..... 65
Mid-range server specification..... 66
High-end server specification..... 68
Contact Center hard disk partition sizes..... 69
Server performance and firmware settings..... 70
Server firmware..... 71
Unified Extensible Firmware Interface..... 71
Power and performance management..... 72
Disk caching and RAID..... 72
Non-Uniform Memory Architecture and memory..... 73
Hyper-Threading..... 73
Unused hardware devices..... 73
Summary..... 74
Avaya Contact Center Select DVD software specification..... 74
Server naming requirements..... 74
Microsoft security hotfixes..... 75

Página1922 de 3226.

Operating system updates 75
Third-party software requirements 77
Guidelines for the use of antivirus software 78
Avaya Contact Center Select DVD licensing 80
Chapter 5: Avaya Contact Center Select software appliance 81
Avaya Contact Center Select virtual machine 83
Contact Center virtual machine hard disks and partitions 84
Server naming requirements 85
Microsoft security hotfixes 85
Operating system updates 85
Third-party software requirements 87
Guidelines for the use of antivirus software 88
Avaya Aura® Media Server OVA 90
Avaya WebLM OVA 91
VMware host server specification and profiling 92
VMware profiling examples 95
Virtualization considerations 97
VMware features 98
VMware vSphere Host considerations 99
Server performance and firmware settings 100
VMware networking best practices 103
Avaya Contact Center Select VMware snapshot considerations 104
Avaya Aura® Media Server VMware snapshot considerations 105
Guidance for storage requirements 105
Performance monitoring and management 106
Troubleshooting VMware 107
Software Appliance Licensing 108
Chapter 6: Avaya Contact Center Select hardware appliance 109
Hardware Appliance server specification 110
Avaya Contact Center Select hardware appliance software specifications 112
Server naming requirements 113
Microsoft security hotfixes 113
Operating system updates 113
Third-party software requirements 115
Guidelines for the use of antivirus software 116
Hardware Appliance Licensing 118
Chapter 7: Solution capacity limits and supported features 120
Avaya Contact Center Select maximum capacity limits 120
Avaya Contact Center Select maximum configuration limits 123
Avaya Contact Center Select supported features 123
Supported Telephony Features 129
Supported Telephony Devices 138
Remote access support 140

Página1923 de 3226.

Communication Control Toolkit supported functionality 140
Chapter 8: Avaya Aura® Experience Portal Integration 145
Data transfer methods 146
Avaya Aura® Experience Portal Orchestration Designer 146
Voice XML 147
Call Control XML 147
SIP-enabled Avaya Contact Center Select 147
P-Intrinsic SIP Header 148
User-to-User Information 149
Universal Call Identifier 149
Front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center 149
Call flow example for front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center 151
Back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center 153
Call flow example using back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center 154
Back-end Avaya Aura® Experience Portal using Context Creation and SIP-enabled Contact Center 155
Call flow example using back-end Avaya Aura® Experience Portal with the Context Creation sample application 158
Avaya DevConnect 159
Chapter 9: Administration client computer requirements 160
Administrator computer hardware requirements 160
Client operating system requirements 161
Administration Client Citrix support 162
Third-party software requirements 163
Chapter 10: Agent Desktop computer requirements 164
Agent Desktop localized languages 164
Agent Desktop computer hardware requirements 165
Client operating system requirements 166
Third-party software requirements 167
Agent Desktop client network infrastructure requirements 167
Remote Desktop Services support 174
Client Citrix support 176
Agent Desktop network ports 176
Chapter 11: Contact Center Agent Browser application requirements 177
Web browser requirements 178
Chapter 12: Avaya Contact Center Select secure TLS communications 180
HTTPS security basics 180
Avaya Contact Center Select security store 181
Avaya Contact Center Select Security Manager 184
TLS Security in a Business Continuity environment 186
Migrating secured Contact Center systems 187

Página1924 de 3226.

Avaya Contact Center Select Security store notifications..... 187
Server Message Block signing..... 188
Chapter 13: Avaya Contact Center Select port matrix..... 189
Contact Center Manager Server port requirements..... 189
Contact Center Manager Administration port requirements..... 190
Communication Control Toolkit port requirements..... 191
Contact Center Multimedia port requirements..... 192
Avaya Aura® Media Server port requirements..... 193

Página1925 de 3226.

Chapter 1: Introduction

Purpose

This document describes an Avaya solution from a holistic perspective focusing on the strategic, enterprise, and functional views of the architecture. This document also includes a high-level description of each verified reference configuration for the solution.

Intended audience

This document is intended for personnel who want to understand how the solution and related verified reference configurations meet customer requirements.

Related resources

Avaya Contact Center Select Documentation

The following table lists the documents related to Avaya Contact Center Select. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Use this document to:	Audience
Overview		
Avaya Contact Center Select Solution Description	This document provides a technical description of Avaya Contact Center Select. It describes the product features, specifications, licensing, and interoperability with other supported products.	Customers and sales, services, and support personnel
Avaya Contact Center Select Documentation Catalog	This document describes available Avaya Contact Center Select documentation	Customers and sales, services, and support personnel

Table continues…

Página1926 de 3226.

Title	Use this document to:	Audience
	resources and indicates the type of information in each document.	
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe the statistics and data in the historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors
Implementing		
Deploying Avaya Contact Center Select DVD	This document contains information about Avaya Contact Center Select DVD installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the Avaya Contact Center Select server.	Implementation personnel
Deploying Avaya Contact Center Select Software Appliance	This document contains information about Avaya Contact Center Select Software Appliance (VMware) preparation, deployment, initial configuration, and verification. This document contains information about maintaining and troubleshooting the software appliance.	Implementation personnel
Deploying Avaya Contact Center Select Hardware Appliance	This document contains information about Avaya Contact Center Select Hardware Appliance (physical server) installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the hardware appliance.	Implementation personnel
Avaya Contact Center Select Business Continuity	This document contains information about deploying Avaya Contact Center Select Business Continuity.	Implementation personnel
Upgrading and patching Avaya Contact Center Select	This document contains information about upgrading and patching Avaya Contact Center Select.	Implementation personnel and system administrators
Administering		
Administering Avaya Contact Center Select	This document contains information and procedures to configure the users, skillsets, and contact center configuration data. This document contains information about creating Avaya Contact Center Select real-time and historical reports.	System administrators and contact center supervisors
Avaya Contact Center Select Advanced Administration	This document contains information about managing the Avaya Contact Center Select	System administrators

Table continues…

Página1927 de 3226.

Title	Use this document to:	Audience
	server, licensing, and multimedia configuration.	
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Contact Center Orchestration Designer.	System administrators
Maintaining		
Contact Center Event Codes	This document contains a list of errors in the Contact Center suite and recommendations to resolve them. This document is a Microsoft Excel spreadsheet.	System administrators and support personnel
Using		
Using Agent Desktop for Avaya Contact Center Select	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors
Using the Contact Center Agent Browser application	This document provides information and procedures for agents who use the Agent Browser application to log on to Contact Center and perform basic tasks.	Contact center agents

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Página1928 de 3226.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Página1929 de 3226.

Chapter 2: Changes in this release

This section describes the new features and changes in Avaya Contact Center Select Release 7.0.

Feature changes in the Release 7.0 base build

See the following sections for information about new features in the Release 7.0 base build.

Automatic insertion of a leading digit before dialing numbers using Agent Desktop Phonebook

In Contact Center Release 7.0, administrators can configure a setting that gives agents the ability to automatically add a leading digit before dialing of any number using Agent Desktop Phonebook. If administrators enable this feature, the plus sign (**+**) before the phone numbers in Phonebook is replaced with a trunk access code. The trunk access code is added before the phone number. Therefore, agents do not need to manually add a leading digit to call externally or forward a call using Phonebook.

Avaya Contact Center Select supports Microsoft Windows Server 2012 R2

Avaya Contact Center Select Release 7.0 is supported on the Microsoft Windows Server 2012 R2 operating system. Avaya Contact Center Select Release 7.0 is not supported on Microsoft Windows Server 2008 R2. Customers upgrading to Avaya Contact Center Select Release 7.0 must migrate to a new Microsoft Windows Server 2012 R2 server.

Avaya Media Server changes

Avaya Media Server is now called Avaya Aura® Media Server. Avaya Contact Center Select Release 7.0 supports only Avaya Aura® Media Server Release 7.7.

Página1930 de 3226.

Avaya Contact Center Select Release 7.0 no longer requires or uses the Contact Center Services For Avaya Media Server (CCSA) component. Avaya Contact Center Select Release 7.0 integrates directly with Avaya Aura® Media Server Release 7.7 using Media Server Markup Language (MSML) based communication.

Avaya Contact Center Select and Avaya Aura® Media Server use the MSML language to control how Route Point calls are anchored and treated. Avaya Contact Center Select also uses MSML to control Route Point call features such as Barge-in, Observe, Zip Tone, and Whisper Skillset announcements.

In Contact Center Manager Administration (CCMA) *Media Services and Routes* configuration, Avaya Aura® Media Server Release 7.7 instances now provide a new MSML-based service type named ACC_APP_ID. This new ACC_APP_ID service type replaces the CONF service type provided by Avaya Media Server Release 7.6.

The following features, previously configured in Avaya Media Server Element Manager, are now configured in Contact Center Manager Administration (CCMA).

- Barge-in tone
- Observation tone
- Call Force Answer Zip tone
- Custom Zip tones
- Whisper Skillset announcement

Enable or disable Barge-in and Observation tones in CCMA *Global Settings*.

Upload the tone and announcement .WAV files in CCMA *Prompt Management*.

Configure Call Force Answer Zip Tone and Whisper Skillset in CCMA *Call Presentation Classes*.

Avaya Aura® Media Server supports only the following deployment options:

- Co-resident with Avaya Contact Center Select on a Windows Server 2012 R2 server
- Standalone on a Red Hat Enterprise Linux 6.x 64–bit server

Avaya Aura® Media Server is also available as an Open Virtual Appliance (OVA) package. You can use this OVA file to create an Avaya Aura® Media Server virtual appliance on a VMware host.

Contact Center Agent Browser application

Contact Center Release 7.0 includes an Agent Browser application. Voice-only Contact Center agents can use the Agent Browser application to log on to Contact Center and perform basic tasks. The Agent Browser application is supported in SIP-enabled Contact Center solutions only.

Página1931 de 3226.

Contact Center Manager Administration password expiry

In Contact Center Release 7.0, administrators can configure that the password used for Contact Center Manager Administration (CCMA) expires after a specified duration. By default, the CCMA password expiry feature is disabled.

If administrators enable the password expiry feature, by default the CCMA password expires after 30 days and CCMA also displays a CCMA password expiry warning 14 days prior to password expiry. Administrators can configure both the expiry period and the password expiry warning duration using the CCMA Security Settings dialog.

Contact Center Manager Administration support for Caché database

In Contact Center Release 7.0, Contact Center Manager Administration (CCMA) stores information in a Caché database. Contact Center Release 7.0 stores agent, user, statistical, scheduling, and reporting information in Caché databases. This simplifies Contact Center data management, migration, and maintenance. This also simplifies the resiliency configuration processes.

In Contact Center Release 7.0, Contact Center Manager Administration (CCMA) does not store information using Active Directory Lightweight Directory Services (AD-LDS) or Microsoft Access databases.

Contact Center services secured by default

The Contact Center Release 7.0 base build includes a number of services and connections that you can secure using Transport Layer Security (TLS). By default, Contact Center installs commonly used Web services and CTI connections with security enabled. This feature includes enhancements to the Contact Center Certificate Management tool to make it easier to manage server and root certificates.

On a new Contact Center install, the following connections and services use TLS by default:

- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM) Administration
- Agent Desktop
- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Contact Center Web Services

Página1932 de 3226.

- Communication Control Toolkit (CCT) Web Administration

You can turn off Web services security after installation and initial configuration. If you choose to leave Web Services security enabled, replace the Contact Center default security store with a new security store containing a signed server certificate and root certificate from your Certificate Authority (CA).

Emergency license expiry notification

When an emergency license is provided to a customer, a daily Windows event is generated. The Windows event warns the customer of the number of days left for the emergency license to expire. Customers can then address the situation in which the Avaya customer service representative provided the emergency license, before the emergency license expires. For example, if your Avaya customer service representative activates the emergency license file on your system because the connection between Contact Center License Manager and Contact Center Manager Server cannot be fixed within the 30-day grace period, then you can use the emergency license to re-establish the connection between Contact Center License Manager and Contact Center Manager Server.

Force password change when users log on to Contact Center Manager Administration for the first time

In Contact Center Release 7.0, administrators can configure a setting, using the CCMA Security Settings dialog, that forces users to change their password when they log on to Contact Center Manager Administration (CCMA) for the first time. In Contact Center Release 7.0, the force password change feature is disabled by default.

For fresh installations of Contact Center Release 7.0 Feature Pack 1, CCMA security settings are enabled by default. If you are upgrading from Contact Center Release 7.0 version, your existing CCMA security settings do not change.

Passwords must not match the previous password and must contain the following:

- Only English and special characters
- 8 to 20 characters
- A number
- An uppercase letter
- A lowercase letter
- No spaces

New Avaya Contact Center Select Hardware Appliance

Avaya Contact Center Select Release 7.0 is offered as a Hardware Appliance.

Página1933 de 3226.

The Avaya Contact Center Select Release 7.0 Hardware Appliance specification has improved to meet the increased requirements of the included Microsoft Windows Server 2012 R2 operating system. The Release 7.0 Hardware Appliance new hard disks support increased multimedia offline data retention.

New Avaya Contact Center Select minimum hardware specifications

Avaya Contact Center Select Release 7.0 continues to support Platform Vendor Independence (PVI) for physical server hardware deployments. Avaya Contact Center Select Release 7.0 defines three new minimum levels of hardware specification; a new Entry-level, a new Mid-range, and a new High-end server hardware specification. For Avaya Contact Center Select Release 7.0 installations on physical servers, only the new PVI server hardware specifications are supported.

New Avaya Contact Center Select minimum virtual machine specifications

Avaya Contact Center Select Release 7.0 continues to support VMware and virtualization. Avaya Contact Center Select Release 7.0 defines three new minimum levels of virtual machine specification; a new Entry-level, a new Mid-range, and a new High-end virtual machine specification. For virtualized Avaya Contact Center Select Release 7.0 installations on virtual machines, only the new virtual machine specifications are supported.

Password aging in Contact Center Manager Administration

Password aging protects organizations from malicious users gaining unauthorized access to Contact Center, because a stolen password is useful to the intruder only for a limited time.

Contact Center Release 7.0 contains a setting that implements password aging for Contact Center Manager Administration (CCMA).

In Contact Center Release 7.0, the password aging feature is disabled by default. If administrators enable the password aging feature, by default the maximum password age is set to 30 days. Users must change the passwords for CCMA when the maximum password age is reached. Administrators can configure the maximum password age for CCMA using the CCMA Security Settings dialog.

For new installations of Contact Center Release 7.0 Feature Pack 1, Contact Center Manager Administration (CCMA) security settings are turned on by default. If you are upgrading from Contact Center Release 7.0, your existing CCMA security settings are not modified.

Página1934 de 3226.

Report Creation Wizard

Avaya Contact Center Select Release 7.0 now supports Report Creation Wizard (RCW). RCW is a Web-based interface in which you can create and edit reports. You can import and schedule the reports in Historical Reporting. You can access RCW from the Historical Reporting component of Contact Center Manager Administration.

Serviceability enhancements in Contact Center 7.0

The following are the serviceability enhancements in Contact Center 7.0:

- Upgraded third-party controls in Agent Desktop
- Enhanced security in Contact Center Manager Administration
- Prevention of Orchestration Designer flow application changes until all Contact Center services start

Support for adding company images and logos to signatures

Contact Center Release 7.0 supports adding company images and logos to email signatures and automatic email signatures. Automatic signatures are automatically added at the bottom of an outgoing email message.

Support for copying the CLID of a customer using Agent Desktop

In Contact Center Release 7.0, the agents can use the **Copy CLID** button on the Agent Desktop toolbar to copy the Calling Line Identification (CLID) number of a customer to the clipboard. Agents can copy the telephone number of the caller when administrators configure Agent Desktop to display the name of the caller using the contacts directory integration.

For incoming calls, Agent Desktop copies the value of the AD_CLID intrinsic when agents click the **Copy CLID** button. For outgoing calls, Agent Desktop copies the value of the CALLED_NUMBER intrinsic when agents click the **Copy CLID** button.

Note:

Agents can copy the CLID of a customer using Agent Desktop only for voice calls in a SIP-enabled Contact Center.

Página1935 de 3226.

Support for displaying login history in Contact Center Manager Administration, Agent Desktop, and Security Manager

In Contact Center Release 7.0, Contact Center Manager Administration, Agent Desktop, and Security Manager display the date and time of your last login. Contact Center Manager Administration and Security Manager also displays the number of failed login attempts before a successful login. With the number of failed attempts, users can identify whether a malicious user tried to log in with their credentials after the last successful login.

By default the login history out feature is disabled. Administrators can enable this feature using the CCMA Security Settings dialog.

Support for forced Not Ready reason codes

In Contact Center Release 7.0, administrators can configure a setting that forces agents and supervisor/agents to enter a Not Ready reason code when changing their status to Not Ready.

Note:

The default code or no code applies when Contact Center returns the contact to a queue because the contact has not been answered within the presentation class guidelines set for the agent.

When a logged in agent exits Agent Desktop by clicking X in the Top bar, the agent goes into the Default Not Ready state.

Support for scripting using CLID and Wild CLID in SIP environments

Contact Center Release 7.0 supports scripting using Calling Line ID (CLID) and Wild CLID intrinsics when creating workflows or scripts for a SIP deployment.

Temporary lock out of Contact Center Manager Administration users

In Contact Center Release 7.0, administrators can configure a setting which temporarily locks out Contact Center Manager Administration (CCMA) users, if users incorrectly enter the application password a specified number of times.

In Contact Center Release 7.0, the temporary lock out feature is disabled by default,. If administrators enable the temporary lock out feature, by default users can incorrectly enter the password three times before CCMA locks the user account for three minutes. Administrators can

Página1936 de 3226.

configure both the number of times that the users can enter an incorrect password and the lock out period using the CCMA Security Settings dialog.

For new installations of Contact Center Release 7.0 Feature Pack 1, Contact Center Manager Administration(CCMA) security settings are turned on by default. If you are upgrading from Contact Center Release 7.0 version, your existing CCMA security settings are not modified.

Feature changes in Release 7.0 Feature Pack 1

See the following sections for information about new features in Release 7.0 Feature Pack 1.

Agent Desktop uses a user directory as the default file browsing directory

From Release 7.0 Feature Pack 1, Contact Center changes the default directory that Agent Desktop uses for file browsing to a user directory instead of a system directory. Browsing files using a user directory ensures that agents cannot browse to a hidden drive such as `C:\` and improves security on a workstation. A user directory is the directory that Agent Desktop opens by default, if an agent has defined a default attachment folder. If an agent has not defined a default attachment folder or if the default attachment folder no longer exists then by default Agent Desktop opens the `Documents` folder on the client computer.

Automatic refreshing of non-staffed skillsets for Real-time Reporting

From Release 7.0 Feature Pack 1, Contact Center Manager Administration Real-Time Reporting automatically refreshes every 20 seconds the list of non-staffed skillsets with the most recent information.

Avaya Contact Center Select supports IP Office Release 10

Avaya Contact Center Select supports IP Office Release 10. Avaya Contact Center Select solutions that use IP Office Release 10 can benefit from an increase in agent counts by enabling Direct Media on the IP Office lines (IP Office Line or IP Office SIP Line) that target inbound calls at Avaya Contact Center Select.

Página1937 de 3226.

Contact Control Service SDK

From Release 7.0 Feature Pack 1, Contact Center includes the Contact Control Service SDK. This SDK builds on the capabilities of existing Contact Center APIs by adding support for outbound voice calls in solutions that integrate Proactive Outreach Manager (POM). The Contact Control Service SDK supports the Java programming language. You can develop custom clients for Contact Center using the Contact Control Service SDK.

Embedded web browsers in Agent Desktop use the latest version of Internet Explorer installed on the client system

From Release 7.0 Feature Pack 1, Contact Center checks and uses the latest version of Internet Explorer, up to Internet Explorer 11, installed on the client system for embedded web browser in Agent Desktop. Agent Desktop checks the version of Internet explorer installed on your system and forces all embedded browsers used in Agent Desktop to use the installed version up to Internet Explorer 11. Using the latest Internet Explorer version, enables screen pops to render better and you can also take advantage of HTML5.

File extension restrictions for attachments

From Release 7.0 Feature Pack 1, Contact Center administrators can use the Contact Center Multimedia (CCMM) Administration utility to configure the supported list of file extensions that agents can attach to emails. When agents add a file attachment to an email, Agent Desktop displays the configured list of file attachment extensions in the Open dialog box. If the attachment type is not in the configured list, Agent Desktop displays a warning message and does not attach the file to the email.

Improved operational performance for Business Continuity

From Release 7.0 Feature Pack 1, Contact Center improves the operational performance of Business Continuity. This results in moving the standby server shadow journal database files to the database journal partition.

This change does not impact the minimum partition size of the database journal drive.

Página1938 de 3226.

Instant Messaging feature supports Microsoft Skype for Business 2015

From Release 7.0 Feature Pack 1, the Contact Center Instant Messaging feature integrates with Microsoft Skype for Business 2015. Integration and operation is identical with releases of Microsoft Lync already supported in the Contact Center 7.0 base release.

New application for installing Feature Packs and Service Packs

From Release 7.0 Feature Pack 1, Contact Center includes a new application, Release Pack Installer (RPI), for installing Feature Packs and Service Packs.

Feature Pack and Service Pack ZIP files include the Release Pack Installer (RPI) executable. The RPI ensures that you do not need to manually un-install software patches before upgrading Contact Center. It also ensures that third party software updates remain consistent, and facilitates roll-back to a previous patch lineup.

Multimedia account passwords must meet minimum complexity criteria

From Release 7.0 Feature Pack 1, Contact Center requires multimedia accounts to meet the minimum password complexity criteria. If you are an agent or supervisor who handles multimedia contacts, Agent Desktop forces you to change your password if you log on using the default password or your password that does not meet the minimum password complexity criteria.

Passwords must fulfill the following complexity criteria:

- Must be between 8 to 20 characters
- Must contain a number
- Must contain at least one uppercase letter and at least one lowercase letter
- Must not contain spaces
- Must not contain any of these characters: \ & : < > |

Agents can change the multimedia account password using the **Preferences** tab in the User Preferences screen. Administrators also can change multimedia account passwords using the Multimedia Administration utility.

Provision of adding a friendly name for a web chat agent

From Release 7.0 Feature Pack 1, Contact Center administrators can add a friendly name or nickname for a web chat agent. If administrators configure the Friendly Name label, the nickname

Página1939 de 3226.

of the web chat agent is displayed in agents' responses to web chat messages. Administrators can also choose that the friendly name is displayed in welcome messages.

Removal of the default Agent Desktop Dashboard password

From Release 7.0 Feature Pack 1, Contact Center has removed the default password that was required to access Agent Desktop Dashboard. You can collect and upload log files or videos to the Contact Center server without entering a password.

Skillset list sorted when creating a billboard display

From Release 7.0 Feature Pack 1, Contact Center sorts the skillset list alphabetically when you create a billboard display. The skillset drop-down list is grouped by contact type and then sorted alphabetically within the contact type group.

Support for the Open Queue Open Interface

From Release 7.0 Feature Pack 1, Avaya Contact Center Select (ACCS) supports the Open Queue Open Interface.

The Open Queue Open Interface delivers existing Open Queue functions to third-party applications that use a Web service. Third-party applications can add and remove contacts of a specific type in Contact Center.

VMware 6.0 support

From Release 7.0 Feature Pack 1, Contact Center supports virtualized environments on VMware 6.0. There is no change to the virtual server specifications required to run Contact Center on VMware 6.0.

Whisper Coaching

From Release 7.0 Feature Pack 1, SIP-enabled Contact Centers extend the Supervisor Observe feature to include Whisper Coaching. Using Whisper Coaching, a supervisor can talk to an agent on a skillset call with a customer, without being heard by the customer. In the coaching mode, a supervisor can hear everything that is said on the call. However, the advice that the supervisor provides is audible only to the agent.

Whisper Coaching improves agent training and performance because supervisors can coach the agent by whispering advice to the agent.

Página1940 de 3226.

Feature changes in Release 7.0 Feature Pack 2

See the following sections for information about new features in Release 7.0 Feature Pack 2.

Agent Desktop integrated login

From Release 7.0 Feature Pack 2, agents no longer need to login separately to CCMM. Agent Desktop authenticates users based on their Windows session credentials only. If your Windows session credentials do not match your CCT user credentials, Agent Desktop prompts you to authenticate using your CCT user credentials.

Agent skillset assignment guardrails

From Release 7.0 Feature Pack 2, you cannot run the same agent skillset assignment concurrently. You must wait until the assignment completes before you run it again. This prevents a potential CCMA performance impact.

Increased CCMM customer contact ratio

From Release 7.0 Feature Pack 2, the customer to contact ratio in Contact Center Multimedia (CCMM) has been increased to 1:1000 (or 1 customer record per 1000 contacts).

Offline Security Store

From Release 7.0 Feature Pack 2, you can create an offline store using Security Manager. This allows you to minimize downtime if you want to replace your current security store. When your offline store is created, you can swap between the active store and the offline store. You can make the offline store the active store at any point using Security Manager. You must stop Contact Center services before making the offline store active.

Remote Desktop Services support for Agent Desktop

From Release 7.0 Feature Pack 2, Contact Center supports using Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop.

Removal of default security configuration

From Release 7.0 Feature Pack 2, for new installations Contact Center no longer provides a default security store and default security certificates. At the installation stage, you can now use the Ignition Wizard to create a security store, generate a Certificate Signing Request (CSR) and import a Certificate Authority root certificate. Alternatively, you can choose to skip security configuration at the installation stage and configure your security certificates later in the commissioning process using Security Manager.

REST API integration

From Release 7.0 Feature Pack 2, Contact Center allows you to invoke REST API in a Contact Center workflow. REST (Representational state transfer) provides efficient scalable services for web communications.

A Contact Center workflow can request data using scripting commands, and the workflow uses the TfeRestService to request and retrieve data from the REST API.

Synchronization of accssync user changes to IP Office

From Release 7.0 Feature Pack 2, Avaya Contact Center Select synchronizes accssync user password changes to IP Office. When you change the accssync user password, Contact Center Manager Administration automatically updates the password on IP Office.

VMware 6.5 support

From Release 7.0 Feature Pack 2, Contact Center supports virtualized environments on VMware 6.5. There is no change to the virtual server specifications required to run Contact Center on VMware 6.5.

Feature changes in Release 7.0 Feature Pack 3

See the following sections for information about new features in Release 7.0 Feature Pack 3.

Ability to store email attachments in the database

From Release 7.0 Feature Pack 3, there is an option to save new email attachments in the MULTIMEDIA database instead of on the file system. You can configure this option using the Multimedia Administration utility.

Contact Center database encryption

From Release 7.0 Feature Pack 3, you can encrypt and decrypt the Contact Center database using Security Manager. To encrypt the database, you must create and activate an encryption key and use it to encode the files in the Contact Center Caché database.

Data Management - customer privacy

From Release 7.0 Feature Pack 3, you can use the Multimedia Data Management utility to act on privacy requests from contact center customers. For example, if a customer exercises their right to access information or their right to be forgotten, you can use the Multimedia Data Management utility to satisfy these requests.

REST API Enhancements

From Release 7.0 Feature Pack 3, the Contact Center REST API supports GET, POST, PUT, or DELETE request methods. Using the TFE REST Configurator, you can now add environments which enable the use of environment variables in REST requests.

Contact Center workflows now support the CONVERT and JSON GET ELEMENT command.

Security Manager support for chained certifcates

From Release 7.0 Feature Pack 3, Security Manager supports importing chained certificates.

Support for applying a restriction flag to a customer

From Release 7.0 Feature Pack 3, you can apply a restriction flag to a customer using Agent Desktop. This can help your Contact Center to comply with General Data Protection Regulation (GDPR). For example, add a restricted flag to indicate to agents not to initiate unsolicited email messages to customers without consent.

Other changes in Release 7.0

See the following sections for information about other changes in the Release 7.0 base build.

Agent Desktop no longer supports deployment as a thick client

From Release 7.0, Contact Center does not support deployment of Agent Desktop as a thick client. You can deploy Agent Desktop using either the click-once deployment or an MSI file.

Avaya Contact Center Select OVA file no longer available

Avaya Contact Center Select Release 7.0 is not available as an Open Virtual Appliance (OVA) file. You can use the Avaya Contact Center Select Release 7.0 DVD or ISO image to build a range of VMware virtual machines. Avaya Contact Center Select continues to support VMware virtualization, productivity, efficiency, and flexibility. Avaya Contact Center Select Release 7.0 supports integration with the Avaya WebLM Release 7.0 and Avaya Aura® Media Server Release 7.7 OVAs.

IP Office supported versions

Avaya Contact Center Select Release 7.0 does not support integration with IP Office 9.0.3 or 9.0.4.

Avaya Contact Center Select Release 7.0 supports integration with IP Office 9.1.x, minimum 9.1.4 or later. For more information about the supported IP Office versions, refer to the Avaya Contact Center Select Release Notes.

Microsoft Exchange Server supported versions

Contact Center Release 7.0 does not support Microsoft Exchange Server 2003. Contact Center Release 7.0 supports only Microsoft Exchange Server 2007, Microsoft Exchange Server 2010, and Microsoft Exchange Server 2013.

Microsoft Internet Explorer releases no longer supported

Contact Center Release 7.0 does not support Microsoft Internet Explorer releases 8.0 or 9.0. Contact Center Release 7.0 supports only Microsoft Internet Explorer 10.0 (32-bit version only), and 11.0 (32-bit version only).

Página1944 de 3226.

Secure Sockets Layer communications is no longer supported

Contact Center Release 7.0 does not support Secure Sockets Layer (SSL) for secure connections. Contact Center supports only Transport Layer Security (TLS). This is to remove security vulnerabilities that exist in SSL.

Third-party or custom applications connecting to Contact Center must support TLS 1.0 or later. Removal of support of SSL can have implications for existing third party or custom applications. Before migrating from a previous Release, check third-party or custom applications that connected securely to Contact Center, to ensure that these applications support TLS.

Windows Server 2008 is no longer supported

Avaya Contact Center Select Release 7.0 is supported only on Microsoft Windows Server 2012 R2. Avaya Contact Center Select Release 7.0 is not supported on Microsoft Windows Server 2008 R2. Customers upgrading to Avaya Contact Center Select Release 7.0, must migrate to a new Microsoft Windows Server 2012 R2 server.

Other changes in Release 7.0 Feature Pack 1

See the following sections for information about other changes in Release 7.0 Feature Pack 1.

Contact Center security improvements

From Release 7.0 Feature Pack 1, Contact Center introduces additional security improvements to keep current with the latest standards in the industry. These improvements include restrictions to web services access, locking down of user accounts, and changes to the way Contact Center manages passwords and keys. Many of these improvements are internal to Contact Center operation and have no impact on end-user operations.

Any security improvement that is visible to end users, or changes the way in which users work with Contact Center, has a separate topic in this section.

Server Message Block signing enabled on Windows Server 2012

From Release 7.0 Feature Pack 1, both the Contact Center DVD and the Release Pack installer modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital tag into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

Página1945 de 3226.

If you do not want to use SMB signing, you can disable it by modifying the Windows Server 2012 local group policy.

Third-party components updated

Release 7.0 Feature Pack 1 upgrades the Contact Center Tomcat and Java third-party components to recent versions. This improves security and ensures that Contact Center remains current with recent updates.

The Release Pack Installer automatically updates these components.

Other changes in Release 7.0 Feature Pack 2

See the following sections for information about other changes in Release 7.0 Feature Pack 2.

CCMA users must login before changing password

From Release 7.0 Feature Pack 2, CCMA users must login before changing their password. When changing a password in CCMA, users can now change the password of the currently logged in user only.

Installation account for Contact Center install

From Release 7.0 Feature Pack 2, you can use any account with local administrative rights to install Contact Center, provided that you disable the Admin Approval Mode security feature on the Contact Center server. You can also use any account with local administrative rights to upgrade and patch Contact Center; you do not need to always use the same administrative account to perform these tasks.

Third-party components updated

Release 7.0 Feature Pack 2 upgrades a number of third-party components to recent versions, such as Caché, Contact Center Tomcat, and .NET Framework. This improves security and ensures that Contact Center remains current with recent updates.

The Release Pack Installer automatically updates these components.

Other changes in Release 7.0 Feature Pack 3

See the following sections for information about other changes in Release 7.0 Feature Pack 3.

Avaya Aura® Media Server update

Contact Center Release 7.0 Feature Pack 3 supports Avaya Aura® Media Server Release 7.8.

From Contact Center Release 7.0 Feature Pack 3, installing the Windows version of Avaya Aura® Media Server co-resident with a Voice and Multimedia Contact Server is no longer supported. When you deploy a Voice and Multimedia Contact Server with Avaya Aura® Media Server, Contact Center installs the Linux version of Avaya Aura® Media Server on a Hyper-V instance on your Voice and Multimedia Contact Server.

This process is fully automated by the Contact Center software installer for fresh installs, and by the Contact Center Release Pack Installer (RPI) for upgrades. In both cases, you can use the Update Configurator utility to update Avaya Aura® Media Server to the latest supported version and apply all necessary configuration. After a reboot following an install or upgrade, the Update Configurator utility launches.

Contact Center backwards compatibility with previous version of Agent Desktop

From Release 7.0 Feature Pack 3, Contact Center supports backwards compatibility with the previous Feature Pack or Service Pack version of Agent Desktop. This allows you to upgrade the Contact Center server without the requirement to upgrade Agent Desktop in a single maintenance window. For example, if you upgrade to Release 7.0 Feature Pack 3, you can use the Release 7.0 Feature Pack 2 version of Agent Desktop.

New Agent Desktop features added in the latest Contact Center release are not available until you upgrade Agent Desktop to that release.

Backwards compatibility is not supported for major or minor releases. For example, if you upgrade to Release 7.1, you cannot use the Release 7.0 version of Agent Desktop.

IP Office supported versions

Avaya Contact Center Select Release 7.0 Feature Pack 3 does not support integration with IP Office 9.1.

Avaya Contact Center Select Release 7.0 Feature Pack 3 supports integration with IP Office 10.1 and 11.0. For more information about the supported IP Office versions, refer to the Avaya Contact Center Select Release Notes.

Página1947 de 3226.

Third-party components updated

Release 7.0 Feature Pack 3 upgrades a number of third-party components to recent versions, such as Caché, Contact Center Tomcat, and .NET Framework. This improves security and ensures that Contact Center remains current with recent updates.

The Release Pack Installer automatically updates these components.

Página1948 de 3226.

Chapter 3: Avaya Contact Center Select overview

Avaya Contact Center Select is a context-sensitive, collaborative, voice and multimedia customer experience solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform. Avaya IP Office is a flexible and scalable phone system designed specifically for small and midsize enterprises. IP Office supports a wide range of phones and devices for use in contact centers.

Avaya Contact Center Select uses SIP and CTI interfaces to communicate with the IP Office platform. This integration gives Avaya Contact Center Select access to and control of a wide range of IP Office phones and features. Customers integrating Avaya Contact Center Select with the IP Office platform gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility. Agent Desktop supports specified IP Office phones and also supports multimedia contact types.

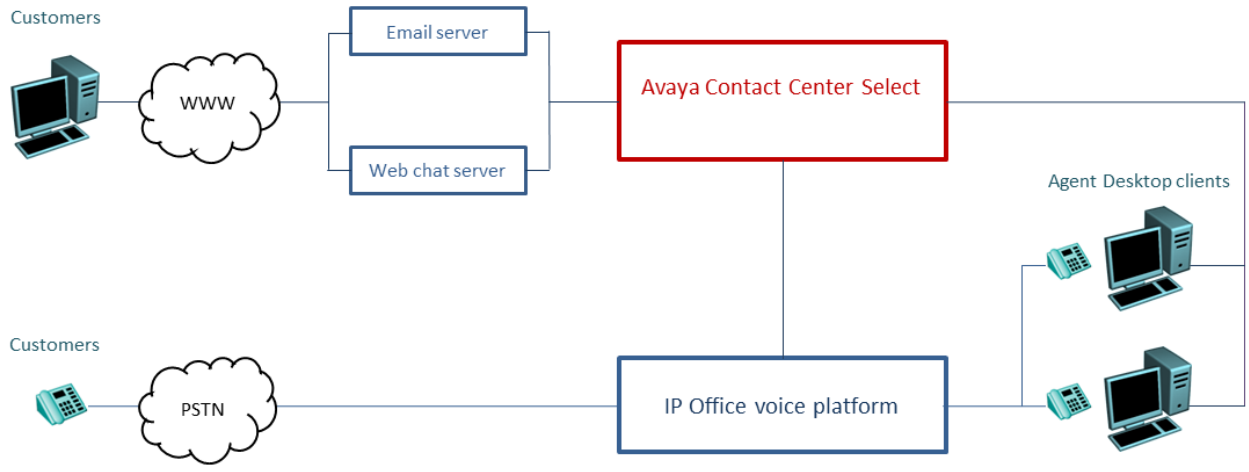


Figure 1: Typical contact center solution using voice and multimedia enabled Avaya Contact Center Select and the Avaya IP Office voice phone system

Avaya Contact Center Select provides a feature rich voice and multimedia solution with integrated routing and reporting for the small to midsize enterprises. Avaya Contact Center Select provides unified contact center and IP Office phone user account management for agents and supervisors.

Página1949 de 3226.

Voice-enabled agents and supervisors created in Avaya Contact Center Select are automatically added to the IP Office platform. Avaya Contact Center Select synchronizes user (agent and supervisor) information between Avaya Contact Center Select and the IP Office platform.

Avaya Contact Center Select is offered in the following deployment types:

- **Avaya Contact Center Select DVD**; The Avaya Contact Center Select DVD contains the application software. The Avaya Contact Center Select DVD deployment option supports Platform Vendor Independence (PVI). The customer supplies the Microsoft Windows 2012 R2 operating system license and server hardware that meets one of the Avaya Contact Center Select PVI server specifications.
- **Avaya Contact Center Select software appliance**; The Avaya Contact Center Select software appliance is a set of VMware virtualized servers; an Avaya Contact Center Select virtual machine, an Avaya Aura® Media Server OVA, and a WebLM OVA. The customer supplies the VMware resources and operating system license for the VMware virtual machine (guest).
- **Avaya Contact Center Select hardware appliance**; The Avaya Contact Center Select hardware appliance is a physical server with the application software already loaded and partially preconfigured. Avaya supplies the server hardware and a license for the Microsoft Windows 2012 R2 operating system.

Avaya Contact Center Select supports the following routed contact types:

- Voice
- Email
- Outbound
- Web communications (Web chat)
- SMS text messages
- Fax messages
- Scanned documents
- Voice mail messages

Avaya Contact Center Select also supports peer-to-peer Instant Messaging and Presence Notifications. To support the email-based contact types, you must add an email server to your solution. To support the Web communications contact type, you must add a Web communications server to your solution.

The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.

Avaya Contact Center Select is quick to deploy and offers a feature rich voice and multimedia solution. Avaya Contact Center Select provides sample configuration data to support rapid deployment and integration with IP Office. You can modify the sample data to meet your solution's requirements and add to the data as your solution expands. You can also use the sample data to learn more about Avaya Contact Center Select. The sample data includes the following data:

- Supervisors and agents

- Skillsets
- Orchestration Designer voice flow applications
- Activity codes
- CDN (Route Points)
- Multiplicity Presentation Classes
- Real-time reports
- Historical reports
- User data synchronization account for IP Office

Avaya Contact Center Select provides a simplified voice prompt management utility. The contact center supervisor can perform prompt management work without requiring administrator access to the Avaya Aura® Media Server server. Avaya Contact Center Select provides a number of status monitoring utilities to monitor the integration points with the IP Office platform. Avaya Contact Center Select also provides an always-on graphical troubleshooting dashboard running on the server.

Licensing

Avaya Contact Center Select supports the following licensed agent packages:

Name	Description	Notes
Agent licenses	Agent licenses determine the number of agents that can log on to Contact Center. Licensing is available for the following types of agents: • voice agent • outbound agent • email agent (covering FAX messages, SMS text messages, voice mail messages, and scanned document messages) • Web communications agent (or Web chat agent)	

Avaya Contact Center Select supports the following licensed features:

Name	Description	Notes
Multiplicity	Multiplicity is the ability of an agent to handle multiple concurrent multimedia contacts. At any one time an agent can be active on a voice and multimedia contact. However, when one contact is active; the others automatically are on hold. The maximum number of concurrent multimedia or non-voice contacts that an agent can be assigned is five.	

Table continues…

Página1951 de 3226.

Name	Description	Notes
Web Based Statistics	If Web Reporting server is enabled, agents and supervisors can use Agent Desktop to view real-time reports for call handling, skillset data, and state information on Agent Desktop.	
Remote Agent	Remote Agent is a solution that extends a Contact Center to an agent's preferred environment, allowing them to handle skillset calls regardless of location. Remote Agent solutions connect contact center calls to the agent's telephone (home telephone or mobile), without the agent needing special hardware.	
Outbound	Use the Multimedia server and the Outbound Campaign Management Tool in Contact Center Manager Administration to create progressive outbound campaigns on which calls are passed to agents and made from the Contact Center.	

For Avaya Contact Center Select (ACCS) integration with IP Office Server Edition, IP Office Server Edition requires the following licenses:

- One Avaya IP Endpoint license for Avaya Contact Center Select integration.
- One Power User license for every ACCS agent or supervisor agent that is configured for any of the following:
  - configured to use IP Office Avaya Communicator for Windows.
  - configured to operate as an ACCS Remote Agent.
  - configured to use an IP Office physical phone with IP Office remote worker functionality. Only IP Office physical phones using IP Office remote worker functionality require a Power User license; other physical phone users do not require a Power User license.
- One Server Edition license. One license for each node in the Small Community Network (SCN).
- IP Endpoint licenses – either Avaya or Third-Party depending on the IP phones used in your solution. Provision one IP Endpoint license for each configured endpoint.
  - IP Office Avaya Communicator for Windows users do not require an IP endpoint license, only an IP Office user license.
  - If your solution uses digital phones only from an IP Office 500V2 Expansion then you do not require endpoint licenses.
- One CTI Pro license or Third Party API license for IP Office.
- One ACCS license for IP Office.
- Voicemail Pro Additional Voicemail Channels, up to a maximum of 350.
- SIP Trunk licenses or channels to support the trunks used in your solution.
- Voicemail Pro Recording Administrators. One instance on each node of the SCN that calls are recorded from. If all recording is to be done on the Primary node then one instance is required. This license enables Contact Recorder.

Página1952 de 3226.

For Avaya Contact Center Select (ACCS) integration with IP Office 500V2 (non-Server Edition), IP Office 500V2 requires the following licenses:

- One Avaya IP Endpoint license for Avaya Contact Center Select integration.
- One Power User license for every ACCS agent or supervisor agent that is configured for any of the following:
  - configured to use IP Office Avaya Communicator for Windows.
  - configured to operate as an ACCS Remote Agent.
  - configured to use an IP Office physical phone with IP Office remote worker functionality. Only IP Office physical phones using IP Office remote worker functionality require a Power User license; other physical phone users do not require a Power User license.
- Preferred Edition License.
- Essential Edition License.
- IP Endpoint licenses – either Avaya or Third-Party depending on the IP phones used in your solution.
  - IP Office Avaya Communicator for Windows users do not require an IP endpoint license, only an IP Office user license.
  - If your solution uses only digital telephones then you do not require endpoint licenses.
- One CTI Pro license.
- Voicemail Pro Additional Voicemail Channels.
- SIP Trunk licenses or channels licenses to support the trunks used in your solution.
- Voicemail Pro Recording Administrators. One instance on each node of the Small Community Network (SCN) that the calls are recorded from. If all recording is to be done on the Primary node then one instance is required. This license enables Contact Recorder. Contact Recorder requires a separate Application Server.

When Avaya Contact Center Select is deployed with an IP Office Resilience pair, ensure the IP Office Secondary system contains the following licenses to enable Avaya Contact Center Select connectivity:

- One Avaya IP End point license
- One CTI Pro license

This applies to both Avaya Contact Center Select standalone and Avaya Contact Center Select Business Continuity configurations. The IP Office Secondary system does not require the inclusion of Voicemail Pro Recordings Administrators license system or Voicemail Pro licenses, because the Call Recording functionality is licensed from the IP Office Primary system.

The Avaya Contact Center Select base software bundle provisions one Contact Recorder system license plus 1 Voicemail Pro port for every voice agent for Call Recording.

An Avaya Contact Center Select voice agent license provisions one Voicemail Pro port for Call Recording.

Página1953 de 3226.

Avaya Contact Center Select uses Avaya WebLM as the license provider. Each Avaya WebLM instance supports a single Avaya Contact Center Select.

Hotdesking / Free-seating

Hot desking / Free-seating environments are supported with ACCS and IP Office physical phones and softphones.

Hotdesking with physical phones

Each physical IP phone requires an IP Endpoint license.

Power User licenses are not required to use IP Office physical phones unless using the IP Office remote worker functionality.

Example:

Requirement: 100 seat ACCS with 100 IP physical phones and 200 possible agents:

- Order 100 ACCS voice agents + 100 IP Endpoint licenses.
- If all agents require IP Office remote worker functionality also order 200 Power User licenses.

Hotdesking with softphones

Each ACCS agent requires a Power User license.

IP Endpoint licenses are not required for the softphones.

Example:

Requirement: 100 seat ACCS with 100 softphones and 200 possible agents:

- Order 100 ACCS voice agents + 200 Power User licenses.

Maximum number of supported nodes

Avaya Contact Center Select supports the following maximum number of IP Office nodes:

- For IP Office 10.x or 11.0 Select (Server Edition) Switch R630 or OVA, ACCS supports 150 nodes in total, consisting of a Primary, a Secondary, and 148 expansions.
- For IP Office 10.x and 11.0 Select (Server Edition) with any hardware other than R630/OVA, ACCS supports 32 nodes in total, consisting of a Primary, a Secondary, and 30 expansions.

User Data Synchronization

Avaya Contact Center Select provides unified administration for contact center agents and IP Office users. The users (agents and supervisors) that you configure in Avaya Contact Center Select are automatically mirrored to the connected IP Office.

When you create an agent in Contact Center Manager Administration, you can choose to create a local Windows user account on the Avaya Contact Center Select server or map to an existing Windows domain user account. Avaya Contact Center Select automatically creates a matching user account in IP Office.

Página1954 de 3226.

When you modify agent details in Avaya Contact Center Select, the corresponding IP Office user details are automatically updated. If you delete an agent in Avaya Contact Center Select, the corresponding IP Office user is not deleted.

The data synchronization mechanism works in one direction; from Avaya Contact Center Select to IP Office. The Avaya Contact Center Select administrator can manually force data synchronization from Avaya Contact Center Select.

Topology

In a contact center solution using Avaya Contact Center Select and an IP Office telephone system, the following network and connectivity topology considerations apply.

Avaya Contact Center Select (ACCS) supports the following deployment options:

- Avaya Contact Center Select DVD
- Avaya Contact Center Select Software Appliance
- Avaya Contact Center Select Hardware Appliance

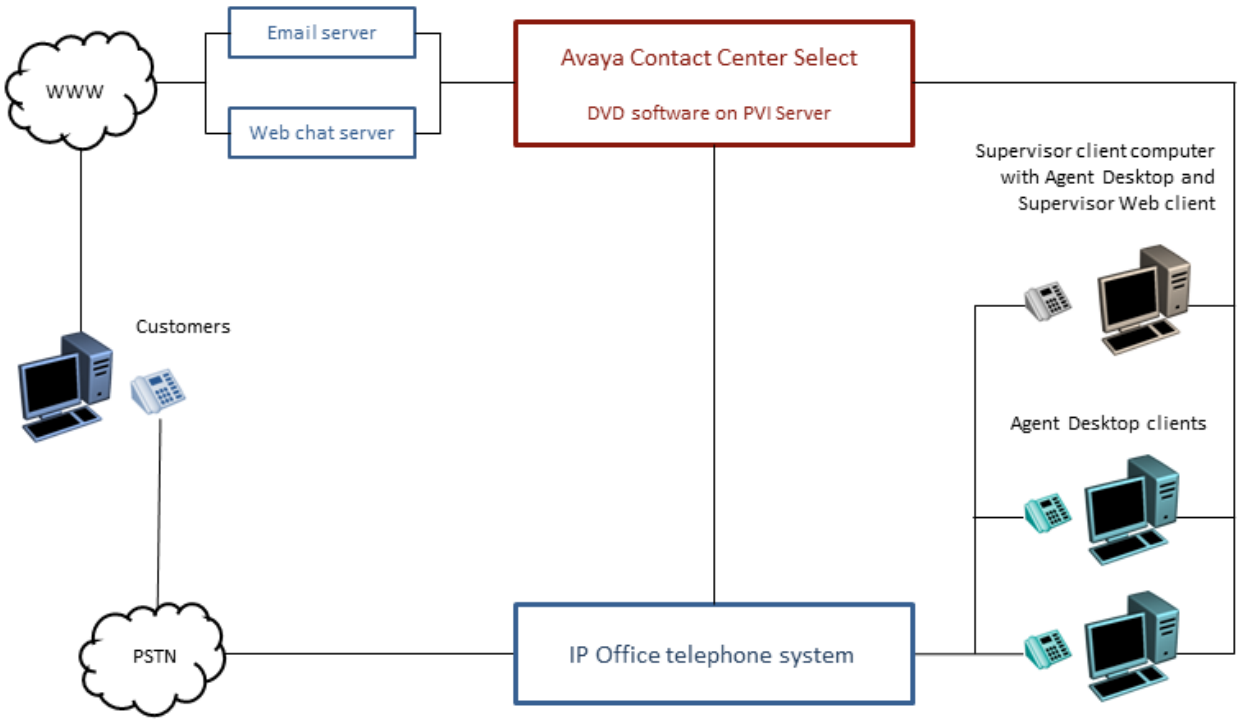


Figure 2: Typical Avaya Contact Center Select DVD deployment

Página1955 de 3226.

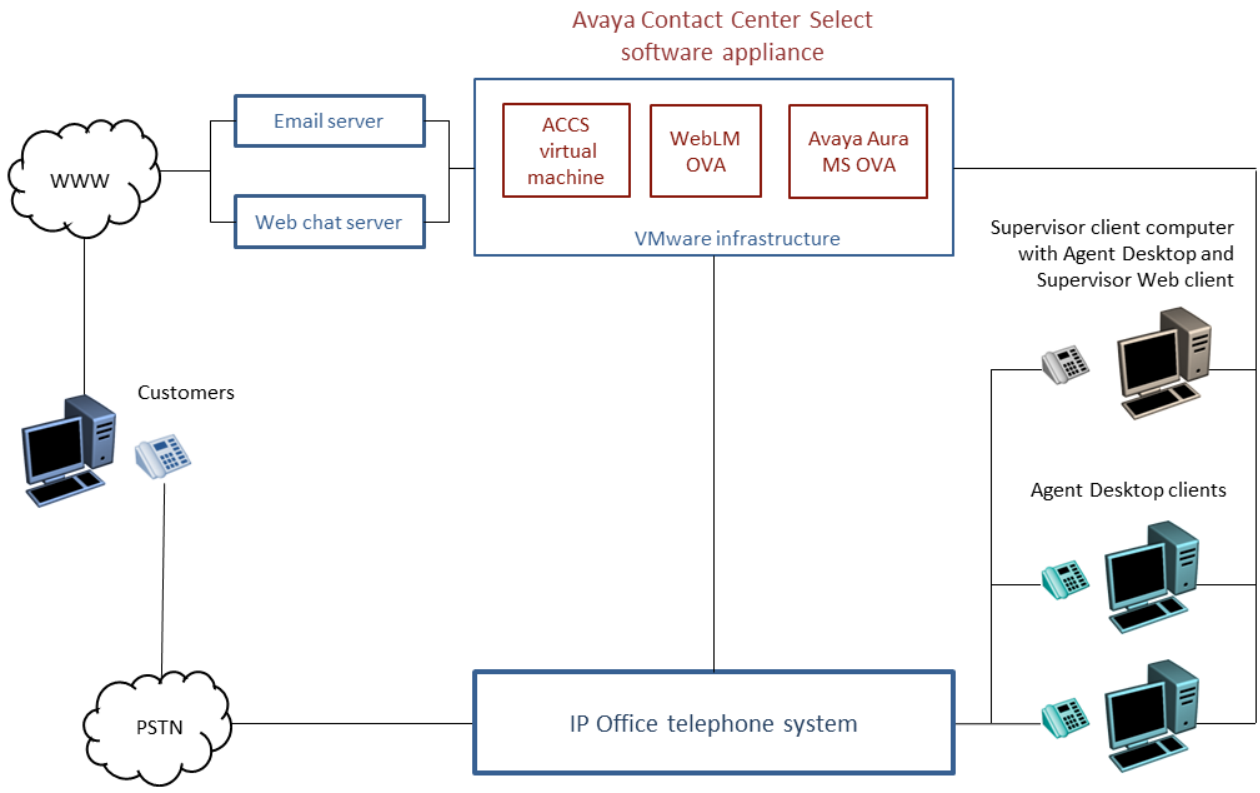


Figure 3: Typical Avaya Contact Center Select software appliance solution

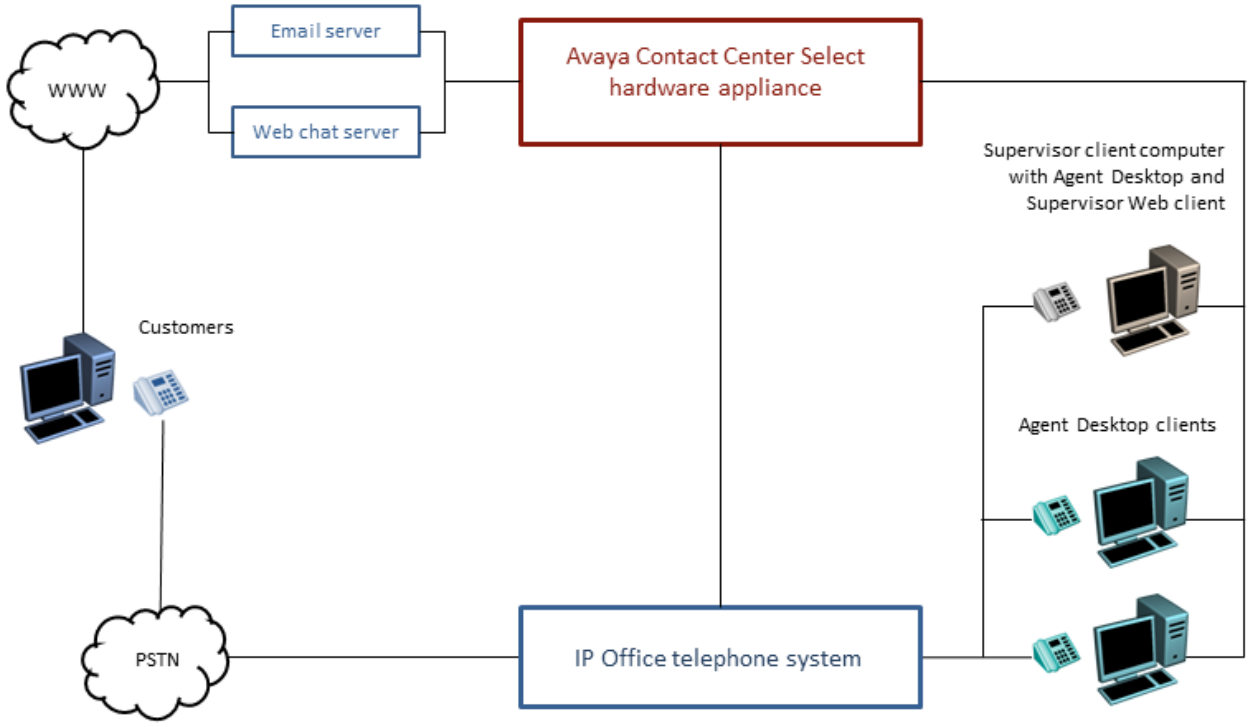


Figure 4: Typical Avaya Contact Center Select hardware appliance solution

The following connectivity and network layout conditions apply to all Avaya Contact Center Select solutions:

- The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.
- Each Avaya Contact Center Select connects to a single IP Office Server Edition Primary server. Avaya Contact Center Select does not support connecting to an IP Office Secondary server. Alternatively, each Avaya Contact Center Select can connect to a single IP Office 500V2 Standard Mode with an Advanced Edition license.
- A Small Community Network (SCN) is a system of networked IP Office telephone systems that can, among other features, share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select. Avaya Contact Center Select connects to the IP Office Server Edition Primary server of the SCN.
- To support an IP Office SCN, Avaya Contact Center Select must connect to an IP Office Server Edition Primary server in that SCN network.
- The Avaya Contact Center Select server and the connected IP Office telephone system must be located in the same campus location.
- To support the email-based multimedia contact types, you must install and commission an email server in your solution.
- To support the Web Communications (Web chat) contact type, you must install and commission a Web chat server in your solution.

Página1957 de 3226.

- Each Avaya WebLM instance supports a single Avaya Contact Center Select.
- Each Avaya Aura® Media Server instance supports a single Avaya Contact Center Select.
- A single instance of Contact Center Manager Administration (CCMA) can manage only a single Avaya Contact Center Select.
- If you are using the Avaya Contact Center Select Software Appliance, the Avaya Contact Center Select virtual machine, the WebLM virtual machine, and the Avaya Aura® Media Server virtual machine must all be hosted on VMware servers located at the same campus location. The Avaya Contact Center Select Software Appliance supports hosting the Avaya Contact Center Select virtual machine, the WebLM virtual machine, and the Avaya Aura® Media Server virtual machine on one VMware host server. The Avaya Contact Center Select virtual machine host server and the connected IP Office telephone system must be located at the same campus location.
- Each Supervisor client computer communicates with the Avaya Contact Center Select server. Each Agent Supervisor client computer has Agent Desktop software and Microsoft Internet Explorer installed on it. The Supervisor uses Internet Explorer to access the Contact Center Manager Administration Web client. The Supervisor uses Contact Center Manager Administration to perform basic agent configuration and to run reports. The Agent Supervisor uses Agent Desktop software to handle customer calls, to accept emergency or supervisor calls from agents and to observe calls or Web communication contacts. Each Supervisor computer with Agent Desktop requires an associated IP Office telephone.
- Each Agent client computer communicates with the Avaya Contact Center Select server. Each Agent computer has Agent Desktop software and Microsoft Internet Explorer installed on it. The Agent uses Internet Explorer to download the Agent Desktop client software. The Agent uses Agent Desktop software to handle customer calls. Each Agent computer requires an associated IP Office telephone.
- Multicast or Unicast must be enabled on the underlying data network between the clients and the Avaya Contact Center Select server for supervisor and agents.
- Avaya Contact Center Select Business Continuity adds additional network connectivity and layout considerations to the solution. For more information, see *Avaya Contact Center Select Business Continuity*.

IP Office supported versions

Each Avaya Contact Center Select connects to a single IP Office Server Edition Primary server. Avaya Contact Center Select Business Continuity-enabled solutions support connecting to an IP Office Secondary server. A Small Community Network (SCN) is a system of networked IP Office telephone systems that can share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select. The Avaya Contact Center Select server and the connected IP Office server must be located at the same campus location.

To support an IP Office SCN, Avaya Contact Center Select must connect to an IP Office Server Edition Primary server in that SCN network.

Página1958 de 3226.

Avaya Contact Center Select supports only the following versions of IP Office:

- IP Office Server Edition Release 10.1, or 11.0
- IP Office 500V2, Release 10.1, or 11.0 software, Standard Mode, Advanced Edition license

Avaya Contact Center Select does not support other versions of IP Office. For more information about the supported IP Office versions, refer to the Avaya Contact Center Select Release Notes.

Avaya Contact Center Select does not support IP Office 500V2 Basic mode.

Overview of solution configuration

This section provides an overview of how to install and commission an Avaya Contact Center Select and IP Office platform-based solution. By describing the commissioning steps, this section also describes how Avaya Contact Center Select integrates with IP Office.

Avaya Contact Center Select uses the IP Office TAPID interface and SIP open standards to integrate with the IP Office platform. Avaya Contact Center Select uses the IP Office TAPID interface to monitor and control the agent endpoints of the IP Office platform. The IP Office TAPID interface gives Avaya Contact Center Select CTI call control of the IP Office users and extensions representing Avaya Contact Center Select agents. Avaya Contact Center Select uses a *SIP User Extension Number* to register and integrate with IP Office. This gives Avaya Contact Center Select SIP session management of the IP Office voice calls.

IP Office configuration for Avaya Contact Center Select

Configure IP Office to support integration with Avaya Contact Center Select. This configuration overview does not include IP Office basic configuration for system settings, licensing, or networking.

Using the IP Office Manager:

1. Configure the Avaya Contact Center Select Service User account details. On the System > Contact Center tab, configure the *CCMA Address*, *CCMA Username*, and *CCMA Password*.
2. Configure the System Voice over IP (VoIP) Domain Name. The Avaya Contact Center Select server uses this domain name for treatments and contact routing.
3. Add a user with the following specifications. Avaya Contact Center Select uses this SIP User Extension Number to register with IP Office:
    a. Device type set to *All Other Phone Types*.
    b. Extension type set to *SIP Extension*. For example, 6000.
    c. A numerical *Base Extension* number.
    d. On the User, enable *Call Waiting On*.
    e. On the User > Telephony > Supervisor Settings tab, configure the *Login Code*.

Página1959 de 3226.

4. Configure an IP Office solution short code to map a telephone number to the Avaya Contact Center Select *SIP User Extension Number*. For example, create a short code 6000|>>3000. All customer calls to telephone number 3000 are forwarded to 6000 and routed to Avaya Contact Center Select. If 3000 is configured as a CDN (Route Point), Avaya Contact Center Select treats the customer call and routes it to a contact center agent.
5. Add a H.323 or SIP extension for each Avaya Contact Center Select agent. Avaya Contact Center Select agents use these IP Office extensions to handle voice contacts.

Avaya Contact Center Select installation

During deployment, configure Avaya Contact Center Select to connect to IP Office.

Using the Avaya Contact Center Select Ignition Wizard (configuration utility):

1. Configure the IP Office platform details.
2. Configure the Service User account details.
3. Configure the *Domain Name* to match the IP Office VoIP domain name.
4. Configure a CDN (Route Point) number to match the *Code* number used by the IP Office short code.
5. Configure the *SIP User Extension Number* to match the above IP Office user with a SIP extension.
6. Configure the Avaya Contact Center Select server details, licensing, and optional multimedia settings.
7. Start Avaya Contact Center Select.

At start up, Avaya Contact Center Select uses the SIP User Extension Number details to register itself as a SIP device with IP Office. This registration permits the following functionality:

- Incoming calls destined for an Avaya Contact Center Select Route Point are delivered to the Avaya Contact Center Select server.
- Authorizes the Avaya Contact Center Select server to send outgoing SIP calls to IP Office (for agent routing of Avaya Contact Center Select calls).
- Enables Avaya Contact Center Select specific functionality on the IP Office platform.

Continue to commission Avaya Contact Center Select by adding option features as appropriate. Install Agent Desktop software on all agent computers. Continue to maintain Avaya Contact Center Select by making frequent data backups.

For more information about deploying and configuring Avaya Contact Center Select, including IP Office short codes, refer to:

- *Deploying Avaya Contact Center Select DVD*
- *Deploying Avaya Contact Center Select Software Appliance*
- *Deploying Avaya Contact Center Select Hardware Appliance*

Página1960 de 3226.

Simple voice call flow example

The following example shows how a customer call to IP Office is treated by Avaya Contact Center Select and then routed to an agent. By describing a sample call flow, this section also describes how Avaya Contact Center Select integrates with IP Office.

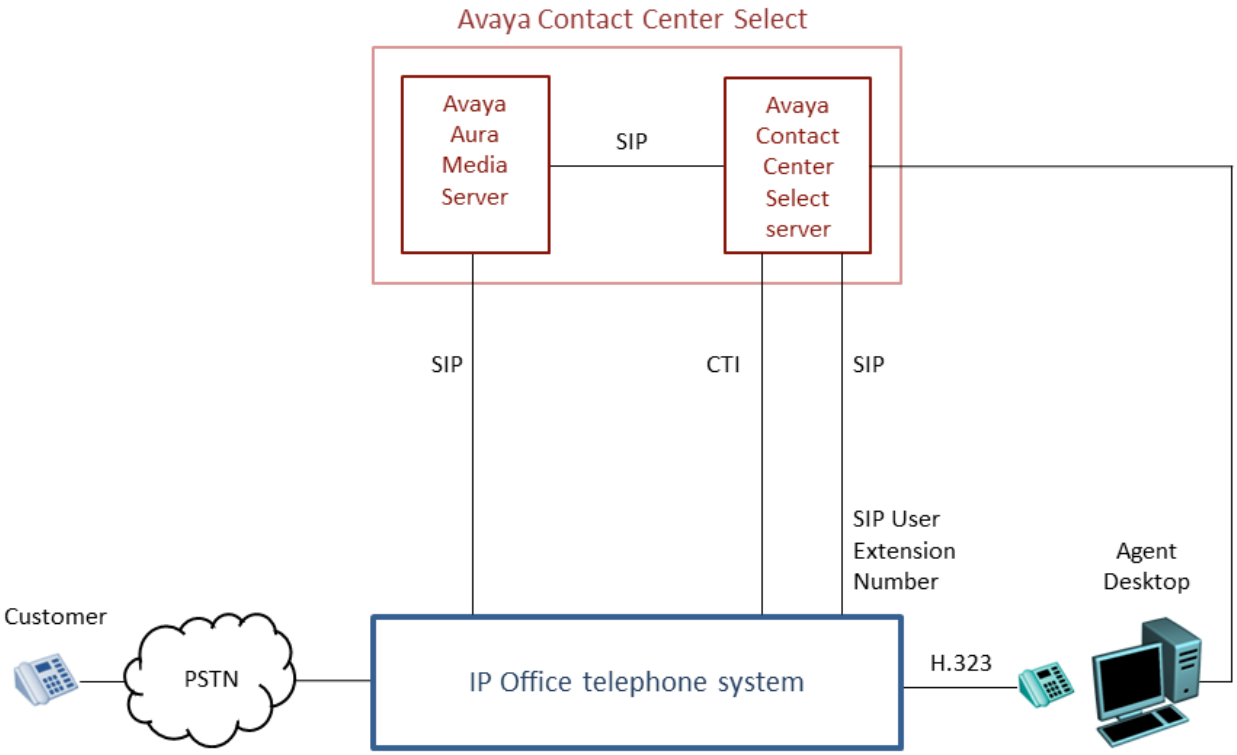


Figure 5: Communication links between Avaya Contact Center Select and IP Office

1. A Customer dials a number and the call arrives at an IP Office platform. For example, the customer dials 3000.
2. An IP Office short code (for example, 6000|>>3000) reroutes the customer call to Avaya Contact Center Select.
3. IP Office sends a SIP INVITE message to Avaya Contact Center Select.
4. When the SIP INVITE message arrives at Avaya Contact Center Select, it matches the call to one of its configured Route Point URIs and then anchors the customer call on an Avaya Aura® Media Server conference port.
5. The Avaya Aura® Media Server establishes a Real-Time Transport Protocol (RTP) media and voice path with the customer. Avaya Contact Center Select treats the customer's call using this conference port for the remainder of the call lifetime.
6. When Avaya Contact Center Select has identified a suitable available agent to handle this call, it sends a SIP INVITE message to IP Office. When the SIP INVITE message arrives at IP Office, it is sent to the destination agent H.323 desk phone.

Página1961 de 3226.

7. IP Office sends a H.323 request to the agent desk phone to indicate that a new customer call has arrived. The agent phone rings and IP Office sends a SIP 180 Ringing message (and a corresponding TAPID Offering CTI message) back to Avaya Contact Center Select. Avaya Contact Center Select uses this trigger to inform the Agent Desktop that a call is alerting on the desk phone. In this way, both the agent desk phone and the Agent Desktop software client show the customer call as ringing.
8. When the agent answers the customer call using Agent Desktop software, Avaya Contact Center Select sends a TAPID AnswerCall request to IP Office. This causes the agent desk phone to go off hook and answer the call. IP Office sends a SIP 200 OK message (and corresponding TAPID Connected CTI message) to Avaya Contact Center Select. Avaya Contact Center Select uses CTI to notify Agent Desktop that the customer call has been answered.
9. When the call is answered, Real-Time Transport Protocol (RTP) is sent from the agent desk phone to Avaya Aura® Media Server. Avaya Aura® Media Server conferences the agent and the customer, the customer and the agent can now communicate. The agent has answered the customer's phone call.
10. The call remains active until the customer or the agent releases the call.

Sample Orchestration Designer voice flow applications

Avaya Contact Center Select provides a number of sample Orchestration Designer flow applications that treat and route customer voice contacts. Orchestration Designer flow applications contain instructions that determine the sequence of steps that a contact follows after the contact arrives at Avaya Contact Center Select. These steps can include call treatments (such as music or ringback), call routing (such as skill-based routing), or interaction with the caller (entering account numbers).

Applications perform two major functions: they define the path a contact follows, and they provide treatments to a contact as the contact moves through Contact Center. You can also use the applications to track and record information about each step in the progress of a contact, and use this information to analyze how your contact center functions to improve service. Orchestration Designer flow applications are stored in an Avaya Contact Center Select database. Task Flow Executor, a component and service of Avaya Contact Center Select, runs the flow applications to treat customer contacts. A contact is not always answered immediately by an agent. You can provide treatments to the voice contacts while they wait in a queue. These treatments can tell callers the estimated amount of time before their call is answered, or play music to callers while they wait in queue. Additionally, you can use time of day, day of week, or contact center activity to determine how a contact is handled.

Avaya Contact Center Select provides a number of sample voice Orchestration Designer flow applications:

- Customer Service. This is the main application. It welcomes the customer to the contact center, performs some basic boundary checking, and plays a menu offering the customer a

Página1962 de 3226.

small selection of options (talk to the help desk, talk to support, enter your PIN, or leave a message).

- Voice_Skill1. This application forwards customer calls to voice skillset Skill1.
- Voice_Skill2. This application forwards customer calls to voice skillset Skill2.
- Collect_Digits. This application asks the customer to enter their PIN number using the digits on their phone. The application then plays the number back to the customer and asks them to confirm the PIN number.

Avaya Contact Center Select also provides a number of sample multimedia Orchestration Designer flow applications for the supported multimedia contact types.

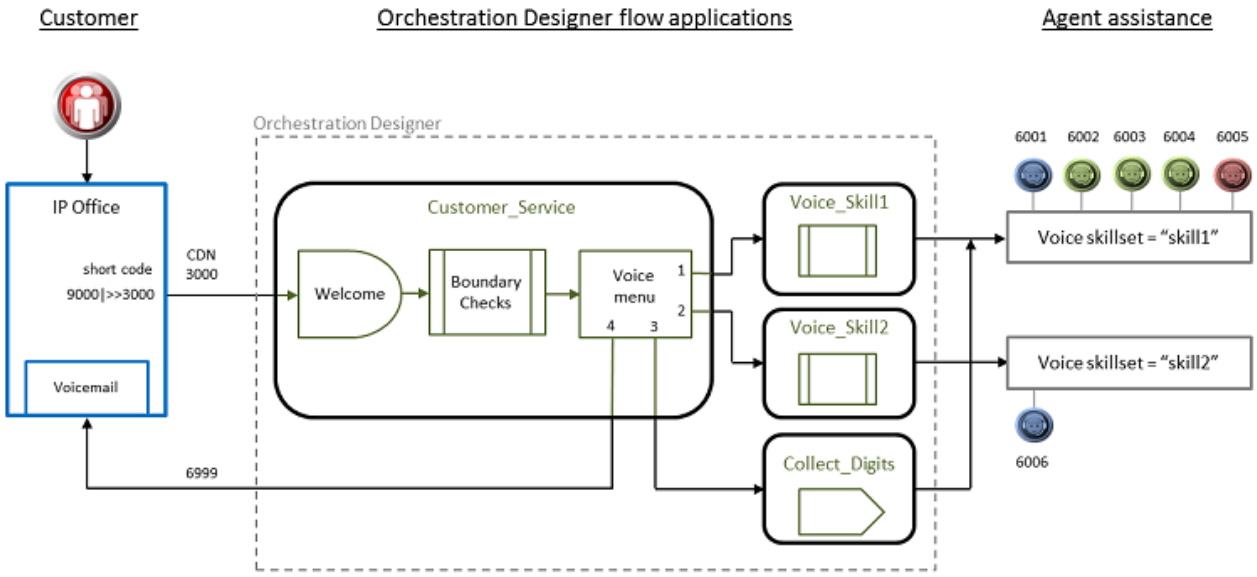


Figure 6: Treatment and routing of customer voice contacts to Avaya Contact Center Select by the sample Orchestration Designer flow applications

Sample Voice Prompt variables

The following table shows the audio media files used by the sample Orchestration Designer flow applications. Orchestration Designer uses these audio .WAV files to play messages (prompts) to the customer. The table shows which Orchestration Designer flow application uses each media file. The table also provides a transcript of the audio in each media file.

Prompt name	Prompt variable name in Orchestration Designer	Prompt transcript	Orchestration Designer flow using this prompt
Welcome_CS	Welcome_CS	"Welcome to the Contact Center."	Customer_Service

Table continues…

Página1963 de 3226.

Prompt name	Prompt variable name in Orchestration Designer	Prompt transcript	Orchestration Designer flow using this prompt
Menu_Selection_CS	Menu_Selection_CS	• “Press 1 to speak to an agent at the help desk. • Press 2 to speak to an agent in the support center. • Press 3 to Enter your Pin Number or any 8 Digits of your choosing. • Press 4 to leave a voice mail. • Press * to repeat this menu.”	Customer_Service
Voicemail_CS	Voicemail_CS	“Please wait while we direct you to our voice messaging system mailbox.”	Customer_Service
EnterDigits_CD	EnterDigits_CD	“Please enter your pin number or digits up to a maximum of 8 digits followed by the # key.”	Collect_Digits
ConfirmDigits_CD	ConfirmDigits_CD	“The digits you entered were ...”	Collect_Digits
ValidateDigits_CD	ValidateDigits_CD	“If that is correct press 1 followed by the # key or press 2 if you wish to retry followed by the # key.”	Collect_Digits
InvalidEntry_CS	InvalidEntry_CS	“That is an invalid entry please try again.”	Customer_Service
NoData_Entry_CS	NoData_Entry_CS	“You have not entered any data Please try again.”	Customer_Service
Emergency_CS	Emergency_CS	“The contact center is now in emergency mode and closed. We will reopen shortly.”	Customer_Service
OutOfHours_CS	OutOfHours_CS	“The contact center is now closed as it is out of hours.”	Customer_Service

Table continues…

Página1964 de 3226.

Prompt name	Prompt variable name in Orchestration Designer	Prompt transcript	Orchestration Designer flow using this prompt
Holidays_CS	Holidays_CS	“The contact center is now closed for holidays.”	Customer_Service
OutOfService_CS	OutOfService_CS	“All departments are out of service at this time. Please call back at a later time.”	Customer_Service
PromptSubmenu_CS	PromptSubmenu_CS	“Press 0 to speak to an agent, Press 1 to leave a voice mail, press, Press 9 to return to the main menu.”	Customer_Service – submenu 1 and 2
FirstRAN_CD	FirstRAN_CD	“This is the first announcement. Please wait while we try to connect you to our agents.”	Collect_Digits – Queuing Tab
SecondRAN_CD	SecondRAN_CD	“This is the second announcement. All our agents are still busy please wait.”	Collect_Digits – Iterate Queue Tab

You can use Contact Center Manager Administration (CCMA) *Prompt Management* to replace these media files with your own recordings. You can record your own voice prompts for the customer, or record voice prompts suitable for your locale (language and dialect). Avaya Contact Center Select provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a bit rate of 128kbits/sec.

Multimedia contacts processing

Contact Center receives multimedia contacts through two external interface points: the email server and the External Web server.

Email server contacts

Email server contacts are retrieved from a POP3 or IMAP capable email server using the Inbound Message Handler (IMH). The IMH runs at regular intervals. You can configure the settings for the IMH (such as the time between intervals and the number of email retrieved from each mailbox during each run) using Contact Center Manager Administration.

The IMH logs on to the mailboxes on the email server as listed in the Email Manager. It parses email in the mailboxes and stores them in the Contact Center Multimedia database. Any attachments associated with an email are stored in the Inbound attachment folder, as specified in Contact Center Manager Administration. After an email is successfully stored in the Contact Center Multimedia database, it is deleted from the email server.

Página1965 de 3226.

The IMH passes a received email to the Contact Center Multimedia rules engine, which applies rules relevant to the email based on the To address, and invokes the Outbound Message Handler (OMH) to send automatic responses, if any.

Contact Center Release 7.0 does not support Microsoft Exchange Server 2003.

Contact Center Release 7.0 supports only the following versions of Microsoft Exchange Server:

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013

External Web server transactions

Contact Center Multimedia receives contacts from the External Web server through the Contact Center Multimedia Web services. The Web services provide a Java API. This enables contacts to be written into the Contact Center Multimedia database, retrieved from the database, and have their status queried.

Contacts received through the Web services do not pass through the Rules Engine. The External Web server determines the skillset and priority assigned to the contact.

A set of sample pages is distributed through DevConnect to provide examples of how a Web server can access the Web services. You must create your own Web pages, with customized look, feel, and business logic.

Simple email message flow

Avaya Contact Center Select provides routed contact support for email messages. Customers send email messages requesting information or support to a published email address. Avaya Contact Center Select connects to the hosting email server and scans this mailbox (published email address) at regular intervals. Avaya Contact Center Select retrieves the customer's email messages from the email server, processes them (by keywords), and stores them in the database. Avaya Contact Center Select then generates a multimedia (email) contact for each email stored in the database, and routes it to an appropriate and available agent.

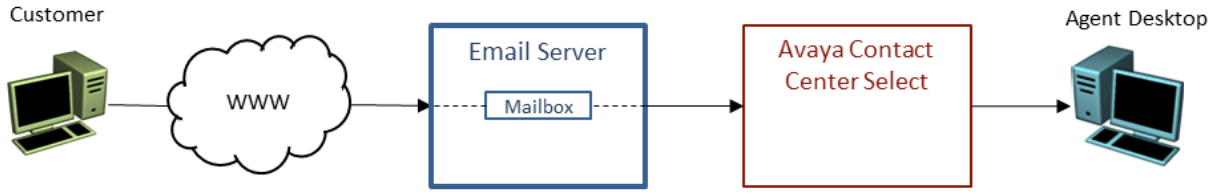


Figure 7: Avaya Contact Center Select process used to retrieve customer email messages and to route the messages as multimedia contacts to contact center agents

Página1966 de 3226.

When you install Avaya Contact Center Select, you configure the email server and a default recipient mailbox. The default settings ensure email messages go only to an agent with the ability to handle email messages. You can customize your contact center with additional skillsets, rule groups and email servers.

To further enhance your customer service, you can configure routing rules to use in rule groups. Use keyword groups and sender groups to decide how to route contacts. Configure which skillset and priority the email contact is assigned to, based on the input for routing contacts. Use automatic suggestions for the agent to reply quickly to an email or automatic responses to send a reply to the customer without agent interaction. You can close the contact immediately after the automatic response.

Avaya Contact Center Select supports Email Open Interfaces. You can develop a custom Web service that the Avaya Contact Center Select Email Manager can call when an email message is processed. The custom Web service can perform custom tasks such as manipulating the originating email and modifying the rule routing options.

For more information about configuring Avaya Contact Center Select email contacts and enhancing the customer experience, see *Avaya Contact Center Select Advanced Administration*.

Call Recording

Avaya Contact Center Select supports IP Office Call Recording. IP Office Call Recording provides regulatory type recording, including the option to pause automatic recording for Payment Card Industry (PCI) security compliance. Avaya Contact Center Select supports the Call Recording pause and resume feature when it is initiated from a physical phone set. By default, Avaya Contact Center Select agents have both inbound and outbound call recording enabled.

IP Office Call Recording has two main components:

- Voicemail Pro Voice Recording Library (VRL) records the inbound and outbound agent calls.
- IP Office Contact Recorder stores the recorded calls and associated metadata.

The recorded calls are stored in industry standard .WAV files. When each call is completed, Contact Recorder compresses the audio .wav file and updates the database with a record of the call. These files are stored in a hierarchy of folders on the IP Office server. Each recording results in a .wav file and the associated metadata stored in an XML file:

- Each .wav file contains the actual audio of the recording. Use the Contact Recorder Search and Replay application to locate and playback these recordings.
- Each .xml file contains metadata about the associated .wav recording file. The following are some examples of call recording metadata parameters:
  - Original CLI (P-Asserted-Identity)
  - Agent name
  - Skillset

Página1967 de 3226.

- Agent number
- conference parties
- start time of the recorded call
- end time of the recorded call

IP Office Call Recording is a licensed feature. Recordings consume Voicemail Pro channel licenses.

Pause Recording when on Hold: If an Avaya Contact Center Select call is being recorded and the agent puts the call on hold, IP Office Call Recording puts the recording in a suspended state (not terminated), adds a short beep to the recording, and when the call is retrieved from hold the recording is resumed. This entire call is stored in a single .wav file.

User Pause recording: If an Avaya Contact Center Select call is being recorded, and if the agent needs to collect payment card details from a customer, the agent can pause the recording to comply with Payment Card Industry (PCI) requirements. IP Office Call Recording puts the recording in a suspended state (not terminated) and adds a short beep to the recording. After collecting the payment card details, the agent resumes call recording. This entire call is recorded and stored in a single .wav file.

The Agent Desktop user interface does not have a pause button. Agents and agent supervisors must use their physical phone to pause and resume voice contact recording.

Remote Agents

Avaya Contact Center Select (ACCS) supports Remote Agents. This feature allows agents at remote locations to use a phone and Agent Desktop software to handle customer voice contacts routed from ACCS.

ACCS supports the following types of Remote Agent:

- Remote Agents using an IPsec compliant Avaya VPN Router and an Avaya IP desk phone. The Internet Protocol Security (IPsec) compliant Virtual Private Network (VPN) router extends the ACCS network across a public network such as the internet, giving the remote agents secure access to the contact center solution. In this solution type, the agent has a computer, an Avaya IP desk phone, and an Avaya VPN Router in their home or at their remote workplace location. The agent's Avaya IP desk phone and Agent Desktop computer connect to the Avaya VPN Router. The VPN Router connects to ACCS using the internet. The agent uses their Avaya IP desk phone and Agent Desktop software to handle customer voice and multimedia contacts.
- Remote Agents using an IPsec compliant Avaya VPN Router and an Avaya IP Office softphone. The Internet Protocol Security (IPsec) compliant Virtual Private Network (VPN) router extends the ACCS network across a public network such as the internet, giving the remote agents secure access to the contact center solution. In this solution type, the agent has a computer and an Avaya VPN Router in their home or at their remote workplace location. The agent's Agent Desktop computer and IP Office softphone connect to the Avaya

VPN Router. The VPN Router connects to ACCS using the internet. The agent uses Agent Desktop software and the IP Office softphone to handle customer voice and multimedia contacts. ACCS Remote Agent supports IP Office Avaya Communicator for Windows.

- Remote Agents using their existing third-party telephones. In this solution type, the agent has a standard residential analog phone and a computer in their home or at their remote workplace location. The agent's phone connects to ACCS using the Public Switched Telephone Network (PSTN) and the Agent Desktop software connects to ACCS using the internet. This type of Remote Agent uses the Telecommuter mode of operation. The agent uses a standard analog phone and Agent Desktop software to handle customer voice and multimedia contacts.

  To enable Remote Agent Telecommuter mode:

  1. Enable the *Offsite Agent* feature in *Server Configuration - Licensing*
  2. For each remote agent, enable *Offsite Agent Allowed* for each remote agent in CCMA.
  3. The agents can then use Agent Desktop to log on from home or another remote location. Agents log on using one of their configured remote phone numbers.

To use Remote Agent, ACCS agents must have a suitable laptop or desktop computer in their home or at their remote workplace location. The agents install Agent Desktop software on this computer. The agents must have a fast and reliable internet connection to the contact center solution. For more information, see *Avaya IP Office Manager*.

Remote Agents log on to Agent Desktop using the *Other Phone* mode. When they log on, the agent telephone rings. This is a nail-up call. Agents must answer this call on their telephone to complete logging on to Agent Desktop. After the logon completes, the agent phone is nailed-up and agents must use Agent Desktop for all subsequent telephony operations. When the agent logs out of ACCS by using the Log Out button on Agent Desktop, ACCS disconnects the nailed-up call. Multimedia contact types appear to a remote agent in exactly the same way as they do to an onsite agent.

Avaya Contact Center Select domain and workgroup support

The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.

After you deploy the Avaya Contact Center Select Hardware Appliance or Software Appliance, you can add the Avaya Contact Center Select server to a Windows domain.

You can add the Avaya Contact Center Select server to a Windows domain before or after you install the Avaya Contact Center Select software using the Avaya Contact Center Select DVD.

In an Avaya Contact Center Select Business Continuity enabled solution, the Avaya Contact Center Select servers must be in the same Windows domain. To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and standby servers. Avaya Contact Center Select agents are also supported in domains with a two-way trust relationship with

Página1969 de 3226.

the Avaya Contact Center Select server domain. Avaya Contact Center Select Business Continuity is not supported in a workgroup.

Avaya Contact Center Select domain considerations

Avaya Contact Center Select supports only a Windows Server Active Directory domain. Avaya Contact Center Select supports a single forest implementation. Avaya Contact Center Select supports agent integration within only those domains in the same forest as the Avaya Contact Center Select domain. Avaya Contact Center Select does not support agent integration across multiple forests, or in domains outside the Avaya Contact Center Select forest.

All Avaya Contact Center Select servers must be in the same Windows Active Directory domain. All Avaya Contact Center Select servers must be registered with the same Windows Active Directory Domain Controller. All Agent Desktop clients must be registered in this domain, or in domains with a two-way trust relationship with this Avaya Contact Center Select server domain.

The Avaya Contact Center Select firewall policy defines the services, network ports, and Windows accounts necessary for contact center voice and multimedia functionality. Avaya Contact Center Select does not provide or install a group policy. A group policy manages and configures software applications and user settings in a given environment. Avaya Contact Center Select cannot be customized to accommodate individual corporate domain structures or group policies, so corporate domains must meet Avaya Contact Center Select requirements.

If you plan to apply a corporate or custom group policy to the Avaya Contact Center Select (ACCS) servers and solution, you must first perform the following:

- Understand the ACCS services, ports, and user account requirements as specified by the ACCS firewall. For more information, see Microsoft Windows Firewall and Advanced Security on your ACCS server to view the inbound/outbound rules.
- Understand the ACCS network ports and transport types. For more information, see Avaya Contact Center Select port matrix on page 189.
- Design or modify your group policy to accommodate these existing ACCS services, ports, user accounts, and transport type requirements.
- Domain group policies and security policies can be configured to automate MS Windows updates, server backups, and password expiry rules for local users. These automated features are not supported by ACCS. If your group policies or security policies implement these automated features, place the ACCS servers in an Active Directory organizational unit (OU) container that protects the servers from these automated features.
- During Avaya Contact Center Select commissioning or during a maintenance window, apply and test your group policy. Ensure Avaya Contact Center Select call control, administration and maintenance capabilities are preserved. Do not apply an untested group policy to an Avaya Contact Center Select production environment. If necessary, modify your group policy to preserve Avaya Contact Center Select functionality.
- After successful testing, place ACCS back into production, and continue to monitor the contact center for adverse side effects of your group policy.

For more information about the Avaya Contact Center Select firewall policy and compatibility with corporate domain group policies, see *Avaya Aura Contact Center Security*.

Avaya Contact Center Select servers do not support Dynamic Host Configuration Protocol (DHCP). All Avaya Contact Center Select servers must have a static IP address. Agent Desktop client computers support both DHCP and static IP addresses.

Página1970 de 3226.

Avaya Security Advisories

Avaya Security Advisories are posted on the Avaya Security Support website at https://support.avaya.com/security. From the Avaya Support website, you can register to receive email notifications of Avaya Security Advisories.

The amount of time it takes to receive an Avaya Security Advisory varies depending on the vulnerability classification of the advisory. For more information about vulnerability classifications, responses, and maintenance policies, refer to the following documents:

- *Avaya's Product Security Vulnerability Response Policy*
- *Avaya's Security Vulnerability Classification*
- *Avaya's Maintenance Contract Requirements for Product Support*
- *Avaya Product Security Support Flow*

Avaya Contact Center Select Business Continuity

Business Continuity is an Avaya Contact Center Select (ACCS) licensed feature. ACCS solutions that support Business Continuity have two ACCS servers. One server, called the active server, processes customer contacts. The other ACCS server (standby or Remote Geographic Node) shadows the active server. If the active server fails, the other ACCS server can take over contact processing. This feature therefore provides ACCS redundancy, data resiliency, and disaster recovery.

For more information about Avaya Contact Center Select Business Continuity, see *Avaya Contact Center Select Business Continuity*.

Upgrades and migrations

Avaya Contact Center Select Release 7.0 is supported only on the Microsoft Windows Server 2012 Release 2 operating system. The Microsoft Windows Server 2012 R2 operating system and server must meet the requirements specified in *Avaya Contact Center Select Solution Description*. Avaya Contact Center Select supports only Microsoft Windows Server 2012 R2 Standard or Data Center editions.

Avaya Contact Center Select Release 6.4.2 is supported only on the Microsoft Windows Server 2008 R2 operating system. You cannot upgrade directly from Avaya Contact Center Select Release 6.4.2 on Windows Server 2008 R2 to Avaya Contact Center Select Release 7.0 on Windows Server 2012 R2. You can migrate agent and statistical information from your existing Avaya Contact Center Select Release 6.x solution to Avaya Contact Center Select Release 7.0 on a Windows Server 2012 R2 server.

Página1971 de 3226.

You can apply the most recent Avaya Contact Center Select patches to ensure that you have the most recent version of the application software, to resolve software issues.

You can apply patches to an Avaya Contact Center Select Business Continuity solution. Both Avaya Contact Center Select servers must be updated to the same patch level. Updating an Avaya Contact Center Select Business Continuity solution requires careful up-front planning.

To install an Avaya Contact Center Select Feature Pack or Service Pack, or to migrate an Avaya Contact Center Select server, you must schedule a maintenance cycle and restart the contact center. For more information, read the Feature Pack or Service Pack Readme file.

Migrating from Avaya Contact Center Select to Avaya Aura® Contact Center is not supported.

Migrating from Avaya NES Contact Center to Avaya Contact Center Select is supported.

Migrating from an Avaya Aura® Contact Center AML-based solution to Avaya Contact Center Select is supported.

The following table summarizes the supported migrations to Avaya Contact Center Select Release 7.0.

Existing	New
Avaya Contact Center Select Release 7.0 on Microsoft Windows Server 2012 Release 2	Avaya Contact Center Select Release 7.0 Feature Pack 3 on Microsoft Windows Server 2012 Release 2
Avaya Contact Center Select Release 6.4.2 on Microsoft Windows Server 2008 R2	
Avaya Aura® Contact Center AML-based solutions	

Reporting Source of Call Disconnect

Avaya Contact Center Select (ACCS) records which party on a contact center call is the first to disconnect from the call. In a typical contact center call, the person who disconnects or hangs up first is the source of call disconnect (SOCD). ACCS supports SOCD monitoring and reporting for inbound contact center contacts. In some countries the agent must not hang-up on a contact center caller. For example, the Brazilian Presidential Decree 6.523 requires that an agent must not disconnect the call while talking to a caller who rang the contact center. Therefore, ACCS records the source of call disconnect (SOCD).

The SOCD information appears in the *Associated Data* field in the Call by Call and Contact Summary reports. The SOCD feature provides the following information about routed contact center contacts:

- Called Party: identifies that the agent disconnected the call
- Calling Party: identifies that the caller disconnected the call
- Transfer: identifies that an agent transferred the call and completed the transfer
- Conference Party: identifies that the caller or an agent dropped from a call that the initial agent conferenced

Página1972 de 3226.

- Conference Tear Down: identifies that either the caller or the last agent dropped a call that an agent conferenced
- System: identifies that a system generated event released the call
- If a customer abandons the call, the ‘Disconnect Source’ is UNKNOWN but a ‘Final Disposition’ of abandoned is populated.

The following are some limitations of SOCD reporting:

- For direct (non contact center) calls to or from logged-in agents, SOCD is displayed as Unknown for all these call types.
- SOCD is recorded only for logged in ACCS agents. SOCD is not recorded if the ACCS agent is not logged in.
- If the agent that originally received the call starts a conference with another agent, and then drops from the conference, all subsequent SOCD information messages are Conference Tear Down. In this case, reports cannot show accurately which party dropped the call.

Automatically forward IP Office voicemail to multimedia agents

In an Avaya Contact Center Select (ACCS) solution licensed and configured to support multimedia agents, you can configure IP Office and Voicemail Pro to automatically forward voicemail messages to ACCS agents.

ACCS provides of sample *Customer Service* menu with a few basic options. This sample menu allows a caller to leave a voicemail message by selecting the voicemail option from the *Customer Service* menu. The caller is then routed to a pre-configured IP Office number from where they can leave a voicemail message. This pre-configured voicemail number is the *Callback Mailbox Number* option on the ACCS Ignition Wizard. Agents can use their phone and the IP Office voicemail system to listen to the caller’s voicemail message.

The IP Office administrator can configure the IP Office callback mailbox number and Voicemail Pro to automatically forward the voicemail message, as an email message with a .WAV file attachment, to an email address monitored by ACCS. ACCS can then treat the email contact and present it to an available multimedia agent. The agent can use their computer headphones to listen to the caller’s voicemail message in the .WAV file. ACCS agents cannot listen to .WAV file attachments using their IP Office phones.

For more information about forwarding voicemail messages to an email address, refer to your IP Office and Voicemail Pro documentation.

Página1973 de 3226.

Limitations

The following are some of the limitations of Avaya Contact Center Select (ACCS) solutions:

- ACCS registers with IP Office as a SIP User. ACCS must refresh this active registration repeatedly every 180 seconds to prevent the registration expiring. If ACCS fails to refresh the registration, IP Office begins to terminate all active ACCS calls.
  - In the event of an ACCS service or network outage of less than 180 seconds, SIP registration with IP Office might expire and active ACCS calls might begin to terminate.
  - In the event of an ACCS service or network outage of greater than 180 seconds, SIP registration with IP Office expires and IP Office begins to terminate all active ACCS calls.
- If an ACCS agent is directly part of an IP Office conference call and the agent invokes hold on this call, music-on-hold is not streamed by IP Office even if the number of parties on this conference drops to two. Agents can identify whether they are part of this scenario by checking their phone set display for the ‘Conference’ keyword.
- Agent Desktop always uses 3–line appearance with reserve last call appearance, regardless of the IP Office settings on the agent’s phone. When an agent logs on using Agent Desktop, the Agent Desktop phone configuration overrides the IP Office phone configuration.
- For CDN to CDN conference, join, barge-in, or emergency call scenarios, if an IP Office softphone agent is a party on this multi-party conference call and invokes hold, music-on-hold might be played into the active multi-party audio stream for a short period of approximately 500 milliseconds before being terminated.
- If a customer dials an agent and this first agent then initiates a consultation with a second agent, the second agent’s phone displays the customer’s phone number while the consultation call is ringing. After the second agent answers the consultation call, their phone then displays the phone number of the first agent. This is how IP Office processes consultations.
- Call Intrude: The IP Office Call Intrude feature permits an agent to join or barge-in on another agent’s call. ACCS implements Call Intrude as a Join conference. The intruded agent’s call is briefly placed on-hold to allow the conference to complete. The intruded party might notice the Held state change and consult call leg appear briefly as the operation completes. Hold music might be played briefly to the Intruded party call.
- Manual transfer from softphone: A transfer completed manually on the IP Office softphone appears to Agent Desktop as a Join transfer where a Join is carried out on the main and consult calls with the transferring party then dropped from the call.
- IP Office supports third-party integrations using the IP Office TAPI interface. These third-party integrations can potentially interfere with the operation of Avaya Contact Center Select. You must configure, implement, and monitor third-party integrations to avoid interfering with Avaya Contact Center Select. Third-party applications implementing the IP Office TAPID interface are not supported for controlling Agent devices.

Página1974 de 3226.

- Not all features invoked on the physical phoneset are reflected in Agent Desktop. The following scenarios are some examples of this:
  - Paging: Agents receiving an incoming Page call cannot answer this call using Agent Desktop. A Page call can be answered only on the user's phone. A Page call which is alerting on a user's phone is displayed in Agent Desktop as a connected call. Agent Desktop displays this call as connected if the user answers the Page. Agent Desktop drops this Page call if another user answers the Page.
  - Hold Reminder: If a call remains in the Held state longer than the IP Office system wide Hold Timeout configuration setting, then a Hold Reminder notification is displayed on the user's phone. A Hold Reminder notification can be an audio or visual notification. Agent Desktop does not support Hold Reminder notifications; in Agent Desktop the call remains in the Held state. Agents can use Agent Desktop to unhold the held call.
- When an ACCS agent logs on to an IP Office softphone, there is a short delay before the agent can use Agent Desktop software to control that softphone. This short delay can be up to 12 seconds long. Agents using an IP Office softphone are unable to answer incoming calls in Agent Desktop immediately after connecting the softphone to IP Office. However agents can answer these calls on their softphone. This limitation applies only to calls routed to the user in the immediate period after logging on to their softphone. If an agent attempts to answer a call in Agent Desktop during the short timeframe where answer is unavailable an error message is displayed in Agent Desktop. After the answer feature is available any subsequent attempts to answer a call in Agent Desktop are successful. But there is a limitation in that there is no notification in Agent Desktop that the Answer feature is now available.
- When an agent makes an outbound call using Agent Desktop, the Agent Desktop Hold button is immediately available. However, until the remote party answers the call and is connected, any attempt to Hold the call in Agent Desktop results in an error message being displayed.
- Avaya Contact Center Select does not support agent operation from the telephone only. This is commonly referred to as Telephone Mode only support. All Avaya Contact Center Select agents must use Agent Desktop for agent functionality.

The following are call flows that can experience limitations:

- Agent initiated calls (originate or transfer) to a Voicemail Pro call flow which invokes 'assisted transfer' telephony action to a Route Point CDN, are rejected by ACCS.
  - A workaround for this limitation is to use "Transfer" (blind transfer) on Voicemail Pro.
- Agent conferencing a call to a Voicemail Pro call flow which invokes any transfer telephony action ('assisted transfer' or 'transfer') to a Route Point CDN, can experience redirection limitations such as looping, redirected call being rejected by ACCS, incorrect CLID for the redirected call.
- Agent initiated calls to a remote expert where the remote expert forwards the call to a Route Point CDN, might be rejected by ACCS. The call might fail and can be retried.
- An agent conferencing a call (CC call or personal call) on ringing to a user which subsequently redirects the call to a Route Point CDN, causes ACCS to reject this redirected call. The agent remains on the call with the original caller and can reattempt the conference if desired.

Página1975 de 3226.

- An agent transferring a call (CC call or personal call) on ringing to a user which subsequently redirects the call to a Route Point CDN, can intermittently cause the CLID of the redirected call to be intermittently incorrect. The agent that routed this redirected call might notice an incorrect CLID.

ACCS does not support single-step transfer of Contact Center (CDN) calls to another ACCS agent. The agent receiving the transferred call can answer the call on their phone, but the call is not presented in Agent Desktop and the agent appears as idle in reporting.

- ACCS agents using Avaya Communicator.

  When working on a call in Avaya Communicator, selecting the ‘Transfer’ option from the drop-down menu associated with the call results in a single-step transfer. This is not supported by ACCS. The workaround is to use Agent Desktop to transfer CDN calls. Alternatively, instead of selecting the ‘Transfer’ option from the drop-down menu in Avaya Communicator, make an unrelated outbound call to the CDN. Then, in Avaya Communicator, drag the two calls together and select ‘Transfer’ from the resulting menu.

- ACCS agents using 1140E/1230 SIP desk phones.

  When transferring a call manually using 1140E/1230 SIP desk phones, the user is prompted Yes/No to consult with the destination party. Selecting ‘No’ results in a single-step transfer. This is not supported by ACCS. The workaround is to use Agent Desktop to transfer CDN calls. Alternatively, when using 1140E/1230 SIP desk phones to transfer calls, select ‘Yes’ to consult with the destination party.

ACCS agents must not configure Forward on No Answer (FONA) to the DN of another ACCS agent. A Contact Center (CDN) call transferred on ringing to an ACCS agent with FONA configured to another ACCS agent is not supported by ACCS. When FONA is applied and the call is forwarded, the ACCS agent receiving the forwarded call can answer the call on their endpoint but the call is not presented in Agent Desktop and the agent appears to be idle in reporting.

For ACCS agents using SIP endpoints (1140E/1230 desk phones, Avaya Communicator for Windows, or IP Office Softphone), a consult transfer/conference call initiated from the SIP endpoint cannot be completed using Agent Desktop. Avaya recommends that agents use Agent Desktop for both the initiation and completion of transfers and conferences.

ACCS agents using IP Office Softphones can experience some limitations when performing Hold/Unhold in Agent Desktop after being transferred to another party. The limitation occurs only when an ACCS agent using IP Office Softphone is transferred to an IP Office user who is also using an IP Office Softphone or Avaya 1140E/1230 desk phones. In Agent Desktop, the Hold/Unhold request does not work, the call state does not change on the IP Office Softphone, and Agent Desktop does not display an error message. In a limited number of cases, due to a limitation of the IP Office Softphone, the call can drop after a period of time. This limitation does not apply to customer calls or when either leg of the transfer operation is a Contact Center (CDN/Route Point) call. To avoid this limitation, Avaya recommends that ACCS agents using IP Office Softphone perform Hold/Unhold operations using the IP Office Softphone.

Página1976 de 3226.

Note:

Ensure the Avaya Contact Center Select *Redirection* feature is enabled. To enable redirection, log on to Contact Center Manager Administration and navigate to **Configuration** > **Global Settings** > **Redirection Settings** > **Media Shuffling on Transfer**.

Página1977 de 3226.

Chapter 4: Avaya Contact Center Select DVD

The Avaya Contact Center Select DVD software provides a context-sensitive, collaborative, voice and multimedia customer experience solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform. Avaya IP Office is a flexible and scalable phone system designed specifically for small and midsize enterprises. IP Office supports a wide range of phones and devices for use in contact centers.

The Avaya Contact Center Select DVD deployment option supports Platform Vendor Independence (PVI). PVI gives the customer the flexibility to purchase a server that meets the Avaya Contact Center Select server requirements and conforms to the customer's corporate standards. To use the Avaya Contact Center Select DVD deployment option, the customer must provide the following:

- Server hardware that meets the Avaya Contact Center Select Platform Vendor Independence (PVI) specification.
- Microsoft Windows 2012 Release 2 Standard or Datacenter Edition operating system and license.

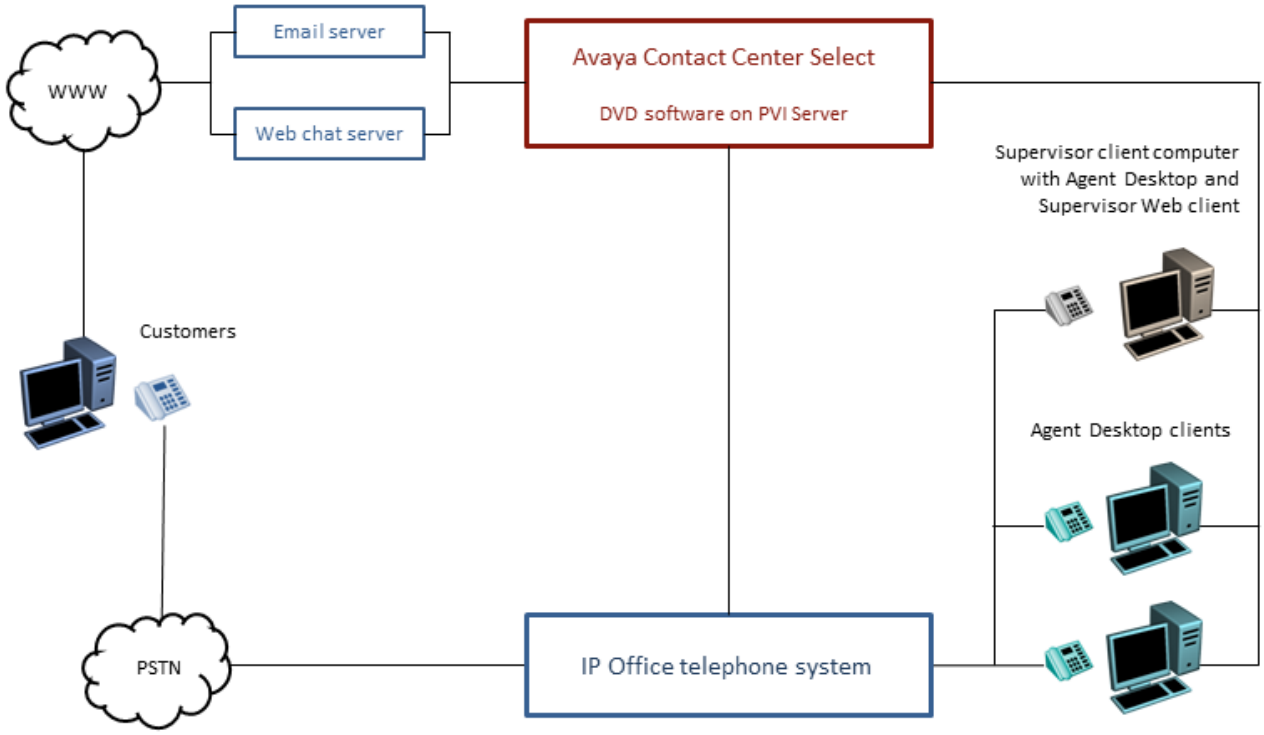


Figure 8: Topology of a typical Avaya Contact Center Select solution

Avaya Contact Center Select is preloaded with sample users, skillsets, and contact center parameters. You can use this sample data to rapidly commission the solution and make the first routed call and email contact. Avaya Contact Center Select delivers quick and simplified contact center deployment. After the basic telephony features are working, you can then configure multimedia contacts, multiplicity, custom prompts, other enhanced features and functions to improve your customer's experience.

To deploy Avaya Contact Center Select software using the DVD software, perform the following:

- Obtain a server that meets the Avaya Contact Center Select PVI requirements.
- Configure the server and format the hard disk partitions to the required specifications.
- Install the Microsoft Windows 2012 Release 2 Standard or Datacenter edition operating system.
- License and activate the Microsoft Windows 2012 R2 operating system.
- Obtain an Avaya Contact Center Select DVD and license.
- Use the Avaya Contact Center Select DVD to install the software components and applications.
- Use the Avaya Contact Center Select Configuration Ignition Wizard to rapidly deploy a functional contact center solution.

The Avaya Contact Center Select DVD is supported only on the Microsoft Windows 2012 Release 2 Standard or Datacenter edition operating system.

The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.

Página1979 de 3226.

Note:

The Avaya Contact Center Select with Avaya Aura® Media Server DVD deployment option does not support VMware.

Platform Vendor Independence server specification

The Avaya Contact Center Select DVD deployment option supports Platform Vendor Independence (PVI). PVI gives the customer the flexibility to purchase a server that meets the Avaya Contact Center Select server requirements and conforms to the customer's corporate standards. To use the Avaya Contact Center Select DVD deployment option, the customer must provide server hardware that meets the Avaya Contact Center Select PVI specification.

The Avaya Contact Center Select DVD deployment option supports the following PVI server specifications:

- Entry-level server specification on page 65
- Mid-range server specification on page 66
- High end server specification on page 68

The high-end server specifications support the same maximum agent capacity and call rate figures. The mid-range server specification supports a reduced agent capacity and call rate.

For information about achieving the maximum performance from your server hardware, see Server performance and BIOS settings on page 70.

Entry-level server specification

The following table lists the minimum specifications for an entry-level single 4-core server.

Specification	Configuration	Comment
CPU	Single 4-core Intel Xeon E3-1275L v3 2.70 GHz	Select a CPU that meets or exceeds the benchmark rating for the Intel Xeon E3-1275L v3 2.70 GHz CPU. Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked High End CPU passmark rankings here: http://www.cpubenchmark.net • AMD processors are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.

Table continues…

Página1980 de 3226.

Specification	Configuration	Comment
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	32 GB minimum	For maximum performance, Avaya recommends that all DIMM slots are populated.
Disk Type and Speed	SATA, SAS, minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • Solid State Drives (SSDs) are not supported.
Total Disk size	• 900 GB minimum • 1.2 TB recommended	• 900 GB disks required for 300 GB Multimedia partition. • 1.2 TB disks required for 600 GB Multimedia partition. Avaya recommends a 600 GB multimedia partition to support longer offline data retention. • For information about the hard disk partitions, see Contact Center hard disk partition sizes on page 69.
RAID	Hardware RAID 1, RAID 5, or RAID 10	• Battery backed hardware RAID controller with 512 MB cache minimum. • Requires duplicate drives with identical specifications.
DVD Drive	One dual-layer DVD drive	• 16X or faster recommended • DVD/Blu-Ray combo drives are supported.
Network Interface	Dual NIC 1 Gbit/s or faster	• NIC must support Receive Side Scaling (RSS) with a minimum of 4 queues and minimum Receive Buffer size of 500. • Only Ethernet is supported.

For information about achieving the maximum performance from your server hardware, see Server performance and BIOS settings on page 70.

Mid-range server specification

The following table lists the minimum specifications for a mid-range dual 6–core server.

Página1981 de 3226.

Specification	Configuration	Comment
CPU	Dual 6–core Intel Xeon X5660 2.80 GHz	Select a CPU that exceeds the benchmark rating for the Dual 6–core Xeon Intel Xeon X5660 2.80 GHz. Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked High End CPU passmark rankings here: http://www.cpubenchmark.net • AMD processors are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	32 GB minimum	For maximum performance, Avaya recommends that all DIMM slots are populated.
Disk Type and Speed	SAS, minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • Solid State Drives (SSDs) are not supported.
Total Disk size	• 900 GB minimum • 1.2 TB recommended	• 900 GB disks required for 300 GB Multimedia partition. • 1.2 TB disks required for 600 GB Multimedia partition. Avaya recommends a 600 GB multimedia partition to support longer offline data retention. • For information about the hard disk partitions, see Contact Center hard disk partition sizes on page 69.
RAID	Hardware RAID 1, RAID 5, or RAID 10	• Battery backed hardware RAID controller with 512 MB cache minimum. • Requires duplicate drives with identical specifications.
DVD Drive	One dual-layer DVD drive	• 16X or faster recommended • DVD and Blu-Ray combo drives are supported.

Table continues…

Página1982 de 3226.

Specification	Configuration	Comment
Network Interface	Dual NIC 1 Gbit/s or faster	• NIC must support Receive Side Scaling (RSS) with a minimum of 4 queues and minimum Receive Buffer size of 500. • Only Ethernet is supported.

For information about achieving the maximum performance from your server hardware, see Server performance and BIOS settings on page 70.

High-end server specification

The following table lists the minimum specifications for a high-end server with dual 8–core CPU.

Specification	Configuration	Comment
CPU	Dual 8–core Intel Xeon E5-2670 2.60GHz	Select a CPU that equals or exceeds the benchmark rating for the Dual 8–core Intel Xeon E5-2670 60GHz CPU. Relative benchmark comparisons only apply for CPUs with the same number of cores. You can make CPU comparisons by viewing the benchmarked High End CPU passmark rankings here: http://www.cpubenchmark.net **Note:** CPUs based on more than 12 cores are not supported • AMD processors are not supported.
CPU - Minimum Clock Speed	2400 MHz	CPU clock speed must meet or exceed the minimum clock speed of 2400 MHz.
CPU - Required Technologies	Hyper-Threading	• 1 x additional logical core for each physical core. • Hyper-Threading must be enabled.
RAM	32 GB minimum	For maximum performance, Avaya recommends that all DIMM slots are populated.
Disk Type and Speed	SAS, minimum 10000 RPM	• Avaya recommends using 15000 RPM disks. • Solid State Drives (SSDs) are not supported.

Table continues…

Página1983 de 3226.

Specification	Configuration	Comment
Total Disk size	• 900 GB minimum • 1.2 TB recommended	• 900 GB disks required for 300 GB Multimedia partition. • 1.2 TB disks required for 600 GB Multimedia partition. Avaya recommends a 600 GB multimedia partition to support longer offline data retention. • For information about the hard disk partitions, see Contact Center hard disk partition sizes on page 69.
RAID	Hardware RAID 1, RAID 5, or RAID 10	• Battery backed hardware RAID controller with 512 MB cache minimum. • Requires duplicate drives with identical specifications.
DVD Drive	One dual-layer DVD drive	• 16X or faster recommended. • DVD and Blu-ray combo drives are supported.
Network Interface	Dual NIC 1 Gbit/s or faster	• NIC must support Receive Side Scaling (RSS) with a minimum of 4 queues and minimum Receive Buffer size of 500. • Quad NICs are required for virtualized environments where this server is a VMware ESXi host. • Only Ethernet is supported.

For information about achieving the maximum performance from your server hardware, see Server performance and BIOS settings on page 70.

Contact Center hard disk partition sizes

Select your hard disk size and configure the required partitions. For each partition, specify a volume size in MBs that when formatted results in a disk partition that is equal to or greater than the required minimum partition size.

For improved multimedia offline data retention, Avaya recommends using 1.2 TB hard disks with a 600 GB partition for multimedia storage.

Página1984 de 3226.

Table 1: Contact Center hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	900 GB hard disk Minimum size partition	1.2 TB hard disk Minimum size partition
Operating System drive Excluding the 350 MB Windows boot loader *System Reserved* partition.	C:	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	120 GB NTFS partition	120 GB NTFS partition
DVD drive For continuity and consistency, Avaya recommends using Drive letter E: for the DVD drive. However, Contact Center supports any DVD Drive letter, other than the Drive letters listed here for the hard disk partitions.	E:	—	—
Voice Contact Server database drive	F:	200 GB NTFS partition	200 GB NTFS partition
Multimedia Contact Server database drive	G:	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	100 GB NTFS partition	100 GB NTFS partition
	Total	801 GB of NTFS partitions on a formatted 900 GB hard disk.	1101 GB of NTFS partitions on a formatted 1.2 TB hard disk.

Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore as a minimum, the Contact Center server must have two 900 GB hard disks or two 1.2 TB hard disks with identical specifications.

Server performance and firmware settings

The Basic Input Output System (BIOS) of a server configures the hardware components and boots the operating system from a storage device. The server operating system (OS) then uses the BIOS to control the server hardware. You must configure the server BIOS settings to ensure optimum performance from the underlying server hardware. For most BIOS settings, you must choose between optimizing a server for power savings or for server performance. For real-time applications such as Avaya Contact Center Select, you must always choose the server BIOS settings that ensure the optimum performance from the underlying server hardware.

Server manufacturers provide their own motherboards, BIOS, hardware, and firmware. Determining the BIOS configuration for your server's hardware can be challenging. There are several BIOS settings that can significantly impact the system performance. When optimizing for

Página1985 de 3226.

system performance, you must select the BIOS settings that enhance the system performance over those that contribute to power savings. Other BIOS settings and recommendations are not as straight forward. Start by consulting the manufacturer's technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions.

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Server firmware

Firmware is a computer program that is stored on the server motherboard or on an add-on hardware controller. The firmware stored on the server motherboard is called the Basic Input Output System (BIOS). The BIOS is responsible for the behavior of the system when it is first switched on and for passing control of the server to the operating system. Firmware is also stored in hardware components such as Redundant Array of Independent Disks (RAID) controllers.

Routinely consult the manufacturer's technical data for your servers and, where appropriate, apply the most recent BIOS and firmware updates. The steps required to update firmware or a system BIOS vary depending on the hardware vendor and the component to be updated. Typically, the manufacturer supplies a firmware updating utility. Keeping your server BIOS and firmware at a supported level can improve reliability, serviceability, and help ensure optimum performance.

Unified Extensible Firmware Interface

The Unified Extensible Firmware Interface (UEFI) specification defines the interface between the operating system and the server firmware. Similar to the BIOS, UEFI is installed by the server manufacturer and it is the first program to run when the server is turned on. UEFI firmware provides some technical advantages over the traditional BIOS system.

Contact Center software, when deployed on physical servers, supports UEFI.

Contact Center software, when deployed on VMware virtual machines, does not support UEFI.

Contact Center does not support the UEFI Secure Boot feature.

Select the firmware boot option, BIOS or UEFI, on the server before installing the Windows Server 2012 R2 Operating System and the Contact Center software. Refer to your hardware vendor's documentation on how to change and implement the required firmware boot option. Changing the firmware boot option after the Operating System has been installed renders the server unbootable and this is not supported.

Página1986 de 3226.

Power and performance management

For real-time applications such as Avaya Contact Center Select, you must always select the hardware, BIOS, firmware, and Operating System settings that enhance the system performance over those that contribute to power savings.

Intel Xeon CPUs offer two main power management options: C-states and Intel Turbo Boost.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to full power on.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power.

These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described below. Other server makes and models can have other terminology but equivalent BIOS settings.

The following are the recommended BIOS settings for the Dell PowerEdge servers:

- Set the Power Management Mode to Maximum Performance.
- Set the CPU Power and Performance Management Mode to Maximum Performance.
- Processor Settings: set Turbo Mode to enabled
- Processor Settings: set C States to disabled

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to Static High Mode.
- Disable Processor C-State Support
- Disable Processor C1E Support
- Disable QPI Power Management
- Enable Intel Turbo Boost

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Disk caching and RAID

Hard disk drives use cache memory to improve read and write access to the disk drives. In write-back mode caching, the disk or RAID controller writes data from the server to cache memory and acknowledges write completion to the server. The server is free to perform other tasks while the disk controller transfers the data from the write cache to the disk drives. This approach significantly increases write performance.

Avaya Contact Center Select supports hardware RAID-1, RAID-5, and RAID-10. RAID technology provides disk data redundancy as well as error detection and correction. For maximum security and mission-critical solutions, Avaya recommends that all Contact Center servers contain a RAID

Página1987 de 3226.

controller. Hardware RAID-1, RAID-5, and RAID-10 are the only levels and types of RAID supported.

Read the hardware documentation for your server to determine how to configure disk caching. Typically, disk caching can be configured as a BIOS setting, a RAID setting, a RAID controller setting, or as an Operating System setting. Some RAID controllers expose the ability to manipulate the Caching Policy through the OS and therefore the OS level setting can override the BIOS level setting. Refer to your hardware documentation for more information about configuring disk caching. Avaya Contact Center Select does not support Operating System level disk caching, software disk caching, or software RAID. Avaya Contact Center Select requires battery backed hardware RAID caching to avoid data loss and possible database corruption on power outage.

Non-Uniform Memory Architecture and memory

Non-uniform memory access (NUMA) is a computer memory design used in multiprocessing, where the memory access time depends on the memory location relative to the processor. Using NUMA, a processor can access its own local memory faster than non-local memory (memory local to another processor or memory shared between processors). For Avaya Contact Center Select, the server must support and implement NUMA.

In the server BIOS settings, configure the memory operating mode for performance optimization and disable Node Interleaving. For example, for a Dell server configure “Memory Operating Mode” as “Optimizer Mode”, and configure “Node Interleaving” as “Disabled”. Refer to your hardware documentation for more information about NUMA and memory performance.

Hyper-Threading

Hyper-Threading is Intel’s proprietary technology for increasing parallel computational power (processor multi-tasking) by allowing the operating system (OS) to see and address each physical processor core as if it were two virtual processors. It also enables the OS and applications to share work between those virtual processors whenever possible, thereby making full use of the available resources.

Enable Hyper-Threading on the Avaya Contact Center Select server.

Unused hardware devices

On the server, disconnect or disable unused and unnecessary physical hardware devices such as: COM ports, LPT ports, USB controllers, Network interfaces, and Storage controllers. You must retain some USB devices for the mouse and keyboard. Disabling unnecessary hardware devices improves server performance and security. Consult the manufacturer’s technical data for your servers for information about disabling unused hardware devices in the BIOS.

Summary

For real-time applications such as Avaya Contact Center Select, choose server BIOS settings that optimize for performance in preference to power savings. Start by consulting the manufacturer's technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions. Avaya recommends that you enable CPU Hyper-Threading. By enabling BIOS options such as CPU Prefetchers and CPU Hyper-Threading, the system performance can be improved effectively. When tuning system BIOS settings for performance, you must consider the various processor and memory options. Experiment with other options to find the optimum setting for your specific hardware and Contact Center solution.

Configure the server hardware, BIOS, firmware, and Operating System settings to select system performance over power savings.

Avaya Contact Center Select DVD software specification

The Avaya Contact Center Select DVD contains the following software components:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server Hyper-V instance on the Windows Server 2012 server
- Avaya Contact Center Select Firewall policy
- Default Avaya Contact Center Select configuration data
- Configuration Ignition Wizard

The Avaya Contact Center Select DVD is supported only on the Microsoft Windows 2012 Release 2 Standard or Datacenter edition operating system.

Server naming requirements

Server names must adhere to RFC1123 (Requirements for Internet Hosts), which specifies that a host name must adhere to the following:

- Use only characters a to z, A to Z, and 0 to 9 can be used in a host name.

Página1989 de 3226.

- You can use a hyphen (-), but not to start or end the host name.
- Host names must be 6 to 15 characters in length.
- Host names must not start with a number.
- Do not use the underscore character (_) and period character (.).
- Do not use spaces in the host name.

The Contact Center server must be able to resolve the host name or computer name of all other servers within the configuration. If you have a Domain Name Service (DNS) server, make sure an entry exists for each server. If you do not have a DNS server, manually update the HOSTS file on each server with the host name or computer name of all other servers to ensure that all clients can interpret the server names.

If network connectivity on your network requires the use of Fully Qualified Domain Names (FQDN), then the FQDN of each computer must be resolvable between all servers associated with Contact Center.

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from Technical Support website) for the list of applicable Microsoft security hotfixes to apply.
- Back up the entire server, and then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Operating system updates

Operating system updates includes service updates and service packs.

Service updates

Given the number of operating system security service updates and the complexity inherent in any network, create a systematic and accountable process for identifying and applying service updates. To help create such a process, you can follow a series of best practices guidelines, as documented in the National Institute of Standards and Technology (NIST) Special Bulletin 800-40, Procedures for Handling Security Patches.

This bulletin suggests that if an organization has no central group to coordinate the storage, evaluation, and chronicling of security service updates into a library, then system administrators or the contact center administrator must fulfill this role. In addition to these guidelines, whenever possible, follow Microsoft recommendations regarding newly discovered vulnerabilities and that you promptly install Microsoft security service updates.

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solutions testing strategy during each test

Página1990 de 3226.

cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes.

Finally, you must perform a full system backup before you update the system to ensure that a rollback is possible, if required. If a Contact Center application does not function properly after you apply a Microsoft security service update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update). For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Contact Center Manager.

For more information about updating, see the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List* on http://support.avaya.com.

Service packs

Avaya has a policy to implement co-residency testing of all new operating service packs for compatibility with the suite of Contact Center applications as soon as they are available. In practice, because a service pack can contain a significant amount of new content, Avaya requires that you wait until compatibility testing is complete before you apply the service pack. Note that operating system service packs are typically tested with the most recent Contact Center application SP and, therefore, an upgrade to a new service pack requires an upgrade to the most recent Avaya SP.

Before you upload a new service pack, you must perform a full system backup (for system rollback as in the updating scenario).

Important:

Service pack compatibility for all Contact Center applications is documented in the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* on the website at http://support.avaya.com.

Java Runtime Environment updates

Contact Center supports only specific versions of Java Runtime Environment (JRE). During installation, Contact Center disables JRE automatic updates on the contact center servers.

Important:

Updating to an unsupported version of JRE can cause the contact center to stop working and can require the reinstallation of the contact center server.

Dynamic Host Configuration Protocol support

Contact Center applications (CCMS, CCMA, CCT, CCMM, LM, and Avaya Aura® Media Server) do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Agent Desktop client computers support both DHCP and static IP addresses.

Página1991 de 3226.

Third-party software requirements

Due to the mission-critical, real-time processing that Contact Center applications perform, you must not install any other application class software on the server. You can install certain utility class software on the server, providing it conforms to the guidelines in this section.

Application class software generally requires a certain amount of system resources and must not be installed on a server running Contact Center applications. The installation of third-party applications can cause Contact Center applications to operate outside of the known engineering limits and can create potential unknown system problems (for example, CPU contentions, increased network traffic loading, and disk access degradations).

Certain third-party utility class software applications, such as hardware diagnostics or backup tools, generally require less system resources during the normal operation of Contact Center applications and are permitted. Exceptions are utilities such as screen savers, which can cause system problems and degrade performance.

Antivirus software is classified as a utility and is subject to the generic guidelines in the following section.

Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

- During run-time, the utility must not degrade the contact center application beyond an average percentage of CPU use (see each specific application section in this document for the recommended maximum CPU usage level). Furthermore, the utility must not lower the minimum amount of free hard disk space required by contact center application and the Windows Operating system.
- The utility must not cause improper software shutdowns or out-of-sequence shutdowns.
- The utility must not administer the contact center application.
- If the utility has a database, it must not affect the contact center application database.
- Disk compression utilities must not be used.
- Memory tweaking utilities used to reclaim memory that is unused by Microsoft must not be used.
- The installation or uninstallation of the third-party software must not impact or conflict with the contact center application (for example, it must not cause DLL conflicts). If such conflicts are discovered, a server rebuild might be necessary.
- The implementation personnel must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production. Support personnel can ask for the results of the testing during fault diagnosis. As part of fault diagnosis, the distributor or end user might be asked to remove third-party software.
- HyperTerminal must not be installed on the server as it interferes with the operation of Contact Center.

Página1992 de 3226.

Guidelines for the use of antivirus software

This section describes the Avaya Contact Center Select antivirus software requirements.

Avaya Contact Center Select supports the following antivirus products:

- Symantec Antivirus
- McAfee

For more information about Avaya Contact Center Select anti-virus considerations and supported versions, see *Avaya Contact Center Select Security Reference Guide* available from the Avaya Support website at http://support.avaya.com.

You can deploy antivirus products from other vendors subject to the following guidelines:

- Infected file quarantine policy on the server and client: antivirus software can be configured to clean up the detected virus automatically and files must be quarantined if infected files cannot be cleaned. Contact Avaya to verify whether the quarantine file is part of our product files or dependent system file. If a virus is detected, remove the server from the network immediately during virus eradication to prevent further virus propagation.
- Do not connect a contact center application platform directly to the Internet to download virus definitions or updated files. Furthermore, Avaya recommends that you do not use a contact center application client PC to connect to the Internet. Instead, download virus definitions and updated files to another location on the customer network and manually load them from this interim location onto the contact center application platform.
- Perform the previous steps to download Contact Center application service packs (SP). This method limits access to the Internet, and thus reduces the risk of downloading infected files.
- Scan all SP files, DVD-ROMs, and floppy disks before you upload or install to the server. This practice minimizes any exposure to infected files from outside sources.
- Capacity considerations: running virus scan software can place an additional load on a contact center application platform. The implementation personnel must run the performance monitor tool on the server to gauge CPU usage. If the antivirus software scan causes the platform average CPU usage to exceed the recommended percentage for longer than 20 minutes, the antivirus software must not be loaded onto the contact center application platform.
- Product Support does not provide support on the configuration of antivirus software, but offer guidance where possible. Direct questions or problems on antivirus software to the appropriate vendor.
- If performance or functionality issues are raised to Avaya support personnel as part of the fault diagnosis, you might be asked to remove third-party utility software or antivirus software.

Several maintenance tasks are automatically activated at 12:00 midnight. Therefore, you must schedule virus scans at a time other than midnight.

Página1993 de 3226.

Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- `F:\Avaya\Contact Center\Databases\`
- `<additional database drive>:\Avaya\Contact Center\Databases\`
- TSM_OAM files located in the following folders:
  - D:\Avaya\Contact Center\Manager Server\iccm\bin\data
  - D:\Avaya\Contact Center\Manager server\iccm\data
  - D:\Avaya\Contact Center\Manager Server\iccm\sdm\log
- `D:\Avaya\Contact Center\Manager Server\bin\tools2.exe` File access errors occur in the Scan Activity log if you do not exclude this file from scanning.
- `D:\Avaya\Contact Center\Manager Server\iccm\logs` (SIP logs)
- `D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\` (SIP log configuration files)
- `D:\Avaya\Contact Center\Common Components\CMF`
- `D:\Avaya\Contact Center\Manager Administration\Apps\` (including sub-directories)
- The folder where you store Service Packs and patches

Contact Center Multimedia interacts with an external email system and enables agents to send attachment files from their computers to the Avaya Contact Center Select server. Both methods of retrieving data are potential sources of software infection.

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Avaya Contact Center Select server do not have a virus. Contact Center Multimedia does not block specific attachment file types. Third-party antivirus software must be installed on the Portal Server according to guidelines in this document for such utilities.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.

  Exclude the Contact Center Multimedia database partition from being scanned.
- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.
- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

Página1994 de 3226.

Warning:

Running a Virus Scan on the Contact Center Multimedia attachment folder, which contains thousands of files, can use significant CPU time on a server and can cause drastic slowdown in agent's response times. Avaya recommends that you run scans, if necessary, during off-peak hours.

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in `<Install_drive>:\Avaya\Cache\CacheSys`. Databases and journal files are installed in `<Install_drive>:\Avaya\Contact Center\Databases`.

Exclude the Caché Journal file folder; `G:\Avaya\`

For Avaya Aura® Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

- `D:\Avaya\MAS\Multimedia_Applications\MAS\platdata`
- `D:\Avaya\MAS\Multimedia_Applications\MAS\common\log`

Avaya Contact Center Select DVD licensing

The Avaya Contact Center Select DVD deployment option requires a Nodal Enterprise license delivered as a WebLM XML file. This license file is used to control access to licensed features such as multimedia contacts and multiplicity.

Contact Center License Manager provides central control and administration of licensing for Avaya Contact Center Select. Each Contact Center License Manager includes a local instance of WebLM. When the Contact Center License Manager service starts, it extracts WebLM license keys from the local WebLM instance. Contact Center License Manager then converts the WebLM license keys into local PLIC license keys and distributes the keys the Avaya Contact Center Select applications as required.

- Obtain the WebLM Host ID for your Avaya Contact Center Select server.
- Use the WebLM Host ID to obtain a nodal WebLM license file from the Avaya Product Licensing and Delivery System (PLDS).
- You load the license file onto the Avaya Contact Center Select server as you run the configuration utility when you are deploying the Avaya Contact Center Select server. You can also load the license file after the configuration process. When Contact Center License Manager loads the license, if the unique number in the license does not match the WebLM Host ID, then License Manager shuts down and Avaya Contact Center Select cannot process contacts. If the unique number in the license matches the WebLM Host ID, then License Manager provides license keys, and Avaya Contact Center Select processes customer contacts.

Página1995 de 3226.

Chapter 5: Avaya Contact Center Select software appliance

For increased productivity, efficiency, and flexibility, Avaya Contact Center Select supports VMware virtualization.

You can use a single Open Virtual Appliance (OVA) package to distribute a virtual appliance. For example, an Avaya Aura® Media Server OVA package includes all of the Open Virtualization Format (OVF) information required to create an Avaya Aura® Media Server virtual appliance on a VMware host. A virtual appliance contains a preinstalled, preconfigured operating system and an application stack optimized to provide a specific set of services.

Avaya Contact Center Select offers a software appliance package that consists of the following components:

- Avaya Contact Center Select virtual machine
- Avaya Aura® Media Server OVA
- Avaya WebLM OVA

The Avaya Aura® Media Server and Avaya WebLM OVAs are prepackaged and ready for deployment. For the Avaya Contact Center Select virtual machine, you must build a suitably specified virtual machine and then install product software from the Avaya Contact Center Select DVD or ISO image.

Página1996 de 3226.

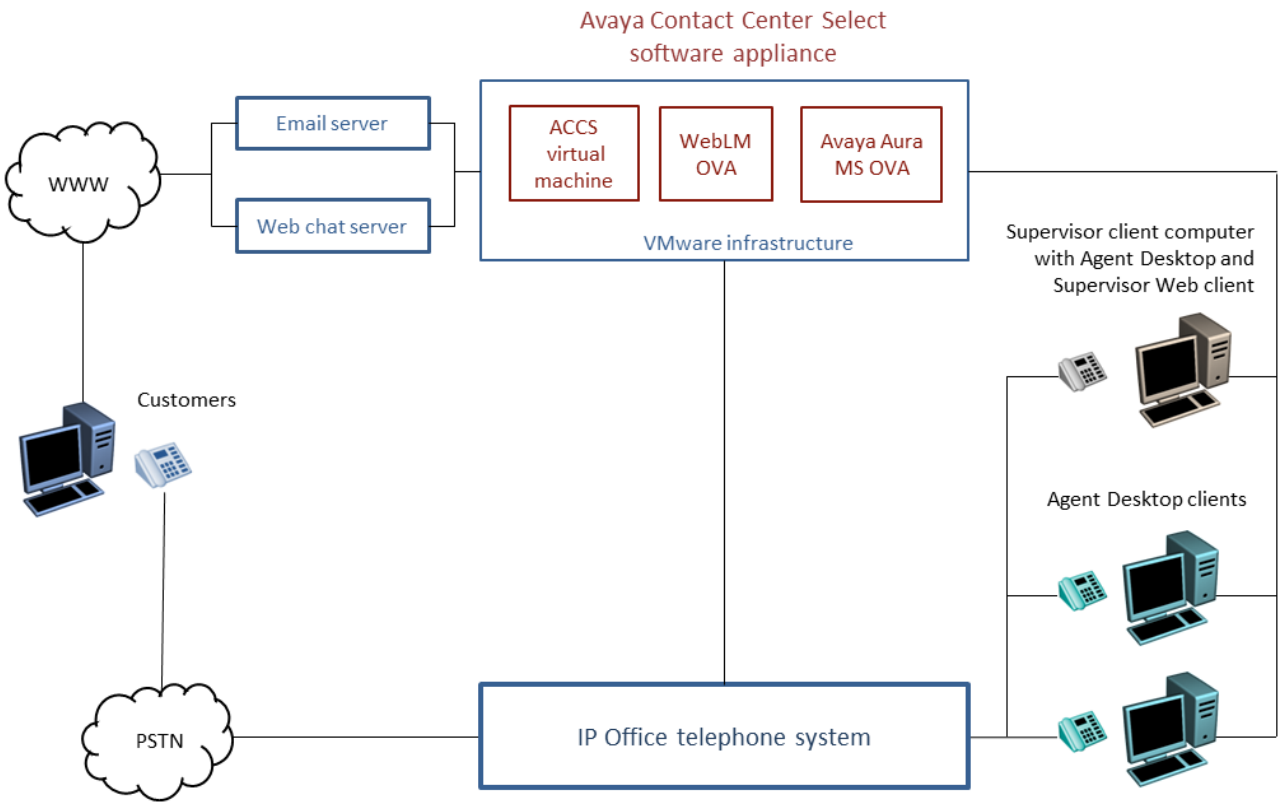


Figure 9: Typical virtualized contact center solution using Avaya Contact Center Select, Avaya Aura® Media Server, and Avaya WebLM deployed on a single VMware host server

You can use VMware vSphere or vCenter and these components to create virtual machines in your virtualized environment. The OVA packages are created as VMware hardware version 8 archives.

The Avaya Contact Center Select software appliance is supported only with the following virtualization environments:

- ESXi 5.5
- ESXi 6.0
- ESXi 6.5

Note:

VMFS 5.54 or later is required for all supported versions of ESXi.

Avaya Contact Center Select supports the Avaya WebLM virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

Avaya Contact Center Select supports the Avaya Aura® Media Server virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

Página1997 de 3226.

For more information about the Avaya Contact Center Select software appliance components, see the following:

- Avaya Contact Center Select virtual machine on page 83
- Avaya Aura Media Server OVA on page 90
- Avaya WebLM OVA on page 91

Avaya Contact Center Select virtual machine

Create the Avaya Contact Center Select virtual machine to provide context-sensitive and skill-based routing for customer voice and multimedia contacts.

The Avaya Contact Center Select virtual machine (guest) contains the following contact center application software.

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Default Avaya Contact Center Select configuration data
- Firewall policy

To create the Avaya Contact Center Select virtual machine, perform the following:

1. Create a VMware virtual machine with the hardware characteristics:
2. Install the Windows Server 2012 Release 2 Standard or Datacenter edition English operating system on the virtual machine.
3. License and activate the Microsoft Windows 2012 R2 operating system.
4. Configure the server and format the hard disk partitions to the required specifications.
5. Install VMware Tools on the server.
6. Obtain an Avaya Contact Center Select DVD or ISO image.
7. Obtain an Avaya Contact Center Select license file.
8. Use the Avaya Contact Center Select DVD or ISO image to install the software components and applications.
9. Use the Avaya Contact Center Select Configuration Ignition Wizard to rapidly deploy a functional contact center solution.

Página1998 de 3226.

10. Continue to monitor the VMware real-time resources.

Each Avaya Contact Center Select virtual machine requires a Linux-based Avaya Aura® Media Server. Each Avaya Contact Center Select virtual machine also requires an additional, separate, Avaya WebLM licensing manager server.

Contact Center virtual machine hard disks and partitions

Create individual virtual hard disks for each of the required partitions for your Contact Center virtual machine. When creating a virtual hard disk for the Operating System partition, create a hard disk size 1GB greater that the required partition size to accommodate the creation of any additional Windows partitions which might be created automatically as part of the Windows Server 2012 R2 install.

For example, for an Operating System partition size requirement of 80GB, create an 81GB virtual hard drive. For each additional Contact Center required partition, create a virtual hard drive greater than or equal to the partition size requirement. The virtual hard disk must be of sufficient size such that when the associated partition is created and formatted it has a size matching the required partition size for the install.

For improved multimedia offline data retention, Avaya recommends using a 600 GB partition for multimedia storage. The multimedia 600 GB partition requires SAN Storage.

Table 2: Contact Center Virtual Machine hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	Minimum partition sizes	Recommended partition sizes, 300 GB multimedia partition	Recommended partition sizes, 600 GB multimedia partition
Operating System drive	C:	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	100 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition
DVD drive	E:	—	—	—
Voice Contact Server database drive	F:	180 GB NTFS partition	200 GB NTFS partition	200 GB NTFS partition
Multimedia Contact Server database drive	G:	200 GB NTFS partition	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	80 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition
	Total	641 GB of Thick Provisioned disk space in a VMware datastore.	801 GB of Thick Provisioned disk space in a VMware datastore.	1101 GB of Thick Provisioned disk space in a SAN datastore.

Página1999 de 3226.

If using 900 GB Raid–1 disks, use the above Minimum Partition size option.

Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore, the VMware host server must implement Hardware RAID-1 or better.

Server naming requirements

Server names must adhere to RFC1123 (Requirements for Internet Hosts), which specifies that a host name must adhere to the following:

- Use only characters a to z, A to Z, and 0 to 9 can be used in a host name.
- You can use a hyphen (-), but not to start or end the host name.
- Host names must be 6 to 15 characters in length.
- Host names must not start with a number.
- Do not use the underscore character (_) and period character (.).
- Do not use spaces in the host name.

The Contact Center server must be able to resolve the host name or computer name of all other servers within the configuration. If you have a Domain Name Service (DNS) server, make sure an entry exists for each server. If you do not have a DNS server, manually update the HOSTS file on each server with the host name or computer name of all other servers to ensure that all clients can interpret the server names.

If network connectivity on your network requires the use of Fully Qualified Domain Names (FQDN), then the FQDN of each computer must be resolvable between all servers associated with Contact Center.

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from Technical Support website) for the list of applicable Microsoft security hotfixes to apply.
- Back up the entire server, and then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Operating system updates

Operating system updates includes service updates and service packs.

Service updates

Given the number of operating system security service updates and the complexity inherent in any network, create a systematic and accountable process for identifying and applying service

Página2000 de 3226.

updates. To help create such a process, you can follow a series of best practices guidelines, as documented in the National Institute of Standards and Technology (NIST) Special Bulletin 800-40, Procedures for Handling Security Patches.

This bulletin suggests that if an organization has no central group to coordinate the storage, evaluation, and chronicling of security service updates into a library, then system administrators or the contact center administrator must fulfill this role. In addition to these guidelines, whenever possible, follow Microsoft recommendations regarding newly discovered vulnerabilities and that you promptly install Microsoft security service updates.

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solutions testing strategy during each test cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes.

Finally, you must perform a full system backup before you update the system to ensure that a rollback is possible, if required. If a Contact Center application does not function properly after you apply a Microsoft security service update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update). For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Contact Center Manager.

For more information about updating, see the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List* on http://support.avaya.com.

Service packs

Avaya has a policy to implement co-residency testing of all new operating service packs for compatibility with the suite of Contact Center applications as soon as they are available. In practice, because a service pack can contain a significant amount of new content, Avaya requires that you wait until compatibility testing is complete before you apply the service pack. Note that operating system service packs are typically tested with the most recent Contact Center application SP and, therefore, an upgrade to a new service pack requires an upgrade to the most recent Avaya SP.

Before you upload a new service pack, you must perform a full system backup (for system rollback as in the updating scenario).

Important:

Service pack compatibility for all Contact Center applications is documented in the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* on the website at http://support.avaya.com.

Java Runtime Environment updates

Contact Center supports only specific versions of Java Runtime Environment (JRE). During installation, Contact Center disables JRE automatic updates on the contact center servers.

Página2001 de 3226.

Important:

Updating to an unsupported version of JRE can cause the contact center to stop working and can require the reinstallation of the contact center server.

Dynamic Host Configuration Protocol support

Contact Center applications (CCMS, CCMA, CCT, CCMM, LM, and Avaya Aura® Media Server) do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Agent Desktop client computers support both DHCP and static IP addresses.

Third-party software requirements

Due to the mission-critical, real-time processing that Contact Center applications perform, you must not install any other application class software on the server. You can install certain utility class software on the server, providing it conforms to the guidelines in this section.

Application class software generally requires a certain amount of system resources and must not be installed on a server running Contact Center applications. The installation of third-party applications can cause Contact Center applications to operate outside of the known engineering limits and can create potential unknown system problems (for example, CPU contentions, increased network traffic loading, and disk access degradations).

Certain third-party utility class software applications, such as hardware diagnostics or backup tools, generally require less system resources during the normal operation of Contact Center applications and are permitted. Exceptions are utilities such as screen savers, which can cause system problems and degrade performance.

Antivirus software is classified as a utility and is subject to the generic guidelines in the following section.

Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

- During run-time, the utility must not degrade the contact center application beyond an average percentage of CPU use (see each specific application section in this document for the recommended maximum CPU usage level). Furthermore, the utility must not lower the minimum amount of free hard disk space required by contact center application and the Windows Operating system.
- The utility must not cause improper software shutdowns or out-of-sequence shutdowns.
- The utility must not administer the contact center application.
- If the utility has a database, it must not affect the contact center application database.
- Disk compression utilities must not be used.
- Memory tweaking utilities used to reclaim memory that is unused by Microsoft must not be used.

Página2002 de 3226.

- The installation or uninstallation of the third-party software must not impact or conflict with the contact center application (for example, it must not cause DLL conflicts). If such conflicts are discovered, a server rebuild might be necessary.
- The implementation personnel must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production. Support personnel can ask for the results of the testing during fault diagnosis. As part of fault diagnosis, the distributor or end user might be asked to remove third-party software.
- HyperTerminal must not be installed on the server as it interferes with the operation of Contact Center.

Guidelines for the use of antivirus software

This section describes the Avaya Contact Center Select antivirus software requirements.

Avaya Contact Center Select supports the following antivirus products:

- Symantec Antivirus
- McAfee

For more information about Avaya Contact Center Select anti-virus considerations and supported versions, see *Avaya Contact Center Select Security Reference Guide* available from the Avaya Support website at http://support.avaya.com.

You can deploy antivirus products from other vendors subject to the following guidelines:

- Infected file quarantine policy on the server and client: antivirus software can be configured to clean up the detected virus automatically and files must be quarantined if infected files cannot be cleaned. Contact Avaya to verify whether the quarantine file is part of our product files or dependent system file. If a virus is detected, remove the server from the network immediately during virus eradication to prevent further virus propagation.
- Do not connect a contact center application platform directly to the Internet to download virus definitions or updated files. Furthermore, Avaya recommends that you do not use a contact center application client PC to connect to the Internet. Instead, download virus definitions and updated files to another location on the customer network and manually load them from this interim location onto the contact center application platform.
- Perform the previous steps to download Contact Center application service packs (SP). This method limits access to the Internet, and thus reduces the risk of downloading infected files.
- Scan all SP files, DVD-ROMs, and floppy disks before you upload or install to the server. This practice minimizes any exposure to infected files from outside sources.
- Capacity considerations: running virus scan software can place an additional load on a contact center application platform. The implementation personnel must run the performance monitor tool on the server to gauge CPU usage. If the antivirus software scan causes the platform average CPU usage to exceed the recommended percentage for longer than 20 minutes, the antivirus software must not be loaded onto the contact center application platform.

Página2003 de 3226.

- Product Support does not provide support on the configuration of antivirus software, but offer guidance where possible. Direct questions or problems on antivirus software to the appropriate vendor.
- If performance or functionality issues are raised to Avaya support personnel as part of the fault diagnosis, you might be asked to remove third-party utility software or antivirus software.

Several maintenance tasks are automatically activated at 12:00 midnight. Therefore, you must schedule virus scans at a time other than midnight.

Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- `F:\Avaya\Contact Center\Databases\`
- `<additional database drive>:\Avaya\Contact Center\Databases\`
- TSM_OAM files located in the following folders:
  - D:\Avaya\Contact Center\Manager Server\iccm\bin\data
  - D:\Avaya\Contact Center\Manager server\iccm\data
  - D:\Avaya\Contact Center\Manager Server\iccm\sdm\log
- `D:\Avaya\Contact Center\Manager Server\bin\tools2.exe` File access errors occur in the Scan Activity log if you do not exclude this file from scanning.
- `D:\Avaya\Contact Center\Manager Server\iccm\logs` (SIP logs)
- `D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\` (SIP log configuration files)
- `D:\Avaya\Contact Center\Common Components\CMF`
- `D:\Avaya\Contact Center\Manager Administration\Apps\` (including sub-directories)
- The folder where you store Service Packs and patches

Contact Center Multimedia interacts with an external email system and enables agents to send attachment files from their computers to the Avaya Contact Center Select server. Both methods of retrieving data are potential sources of software infection.

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Avaya Contact Center Select server do not have a virus. Contact Center Multimedia does not block specific attachment file types. Third-party antivirus software must be installed on the Portal Server according to guidelines in this document for such utilities.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.

Página2004 de 3226.

Exclude the Contact Center Multimedia database partition from being scanned.

- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.
- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

Warning:

Running a Virus Scan on the Contact Center Multimedia attachment folder, which contains thousands of files, can use significant CPU time on a server and can cause drastic slowdown in agent's response times. Avaya recommends that you run scans, if necessary, during off-peak hours.

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in `<Install_drive>:\Avaya\Cache\CacheSys`. Databases and journal files are installed in `<Install_drive>:\Avaya\Contact Center\Databases`.

Exclude the Caché Journal file folder; `G:\Avaya\`

For Avaya Aura® Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

- `D:\Avaya\MAS\Multimedia_Applications\MAS\platdata`
- `D:\Avaya\MAS\Multimedia_Applications\MAS\common\log`

Avaya Aura® Media Server OVA

Avaya Aura® Media Server is a software based media processing platform. Deploy the Avaya Aura® Media Server OVA to provide the conference services required by Avaya Contact Center Select.

The Avaya Aura® Media Server OVA creates and configures a virtual machine containing Avaya Aura® Media Server software. The resulting virtual machine contains a Linux operating system, hard disk drive, third-party components, system configuration, firewall settings, and Avaya Aura® Media Server application software.

You can deploy the Avaya Aura® Media Server OVA on the same VMware host server as the Avaya Contact Center Select virtual machine and the Avaya WebLM OVA. Alternatively, you can deploy the Avaya Aura® Media Server OVA standalone on a separate VMware host server.

The Avaya Aura® Media Server OVA contains information about the virtual machine specification, operating system, and application software. This OVA contains the following components:

- Red Hat Enterprise Linux 6.x - 64bit

Página2005 de 3226.

- Avaya Aura® Media Server Release 7.8 software
- IP tables firewall file application
- VMware Tools. Do not update the VMware Tools software on this virtual machine unless instructed to do so by Avaya.

The Avaya Aura® Media Server OVA package has the following default hardware configuration:

vCPU	Minimum CPU speed	Virtual memory required	Number of NICs	Virtual disk storage required	
4	2400 MHz	4.5 GB (4608 MB)	1 VMXNET3	Size	50 GB
				Deploy the Avaya Aura® Media Server OVA using Thick Provision Lazy Zeroed. Avaya Aura® Media Server does not support thin provisioning.	

Note:

Avaya Contact Center Select does not support Avaya Aura® Media Server using these default deployment settings. After you deploy the Avaya Aura® Media Server OVA, re-configure the virtual machine to have 4 or 8 CPUs and at least 8 GB RAM.

In a virtualized Avaya Contact Center Select environment, you can use VMware to load the Avaya Aura® Media Server OVA package into a virtual machine in your contact center solution. The virtualized Avaya Contact Center Select server can then use the virtualized Avaya Aura® Media Server as a voice media processor.

Deploy the Avaya Aura® Media Server OVA using Disk Format - Thick Provision Lazy Zeroed. Avaya Aura® Media Server does not support thin provisioning.

Avaya WebLM OVA

Deploy the Avaya WebLM Release 7.1 OVA to provide solution licensing. You can deploy the Avaya WebLM OVA on the same VMware host server as the Avaya Contact Center Select virtual machine and the Avaya Aura® Media Server OVA. Alternatively, you can also deploy the Avaya WebLM OVA standalone on a separate VMware host server.

Each Avaya Contact Center Select supports one WebLM license manager server. Each WebLM license manager server supports one Avaya Contact Center Select. For increased efficiency and flexibility, the WebLM licensing manager supports the VMware Virtual Appliance and Open Virtualization Archive (OVA) deployment mechanisms. In a virtualized Avaya Contact Center Select environment, you can use VMware to load the WebLM OVA package onto a separate virtual machine in your contact center solution. The virtualized Avaya Contact Center Select server can then use the virtualized WebLM server as the license manager.

The WebLM OVA contains a hardened Linux operating system.

The Avaya WebLM OVA requires the following:

Página2006 de 3226.

vCPU	Minimum CPU speed	Virtual memory reservation	Number of NICs	Virtual disk storage reservation
1	—	2 GB	1 shared	35 GB

Note:

Do not change any of these Avaya WebLM OVA VMware virtual machine settings.

The WebLM OVA uses the following network mapping:

WebLM Server VM Interface	Application
Eth0	License management

The WebLM server for VMware is packaged as a vAppliance ready for deployment using either VMware vSphere Client or VMware vCenter.

Deploy the WebLM OVA using Disk Format - Thick Provision Lazy Zeroed. WebLM does not support thin provisioning in production environments.

VMware host server specification and profiling

This section specifies the VMware resources required to support the Avaya Contact Center Select software appliance for a number of solution sizes. The Avaya Contact Center Select (ACCS) software appliance consists of the following components:

- Avaya Contact Center Select virtual machine
- Avaya Aura® Media Server OVA
- Avaya WebLM OVA

The Avaya Contact Center Select, Avaya Aura® Media Server, and Avaya WebLM virtual machines are supported on a single VMware host or on separate VMware hosts.

VMware host server minimum CPU specification

Configure each VMware virtual machine with the CPU resources to support an ACCS software appliance component. For each virtual machine and required agent count, configure a specified number of vCPU cores and CPU Reservations in MHz. Each vCPU core must have a corresponding underlying physical CPU core on the VMware host. The performance of each physical CPU core, and corresponding vCPU core, is determined by the VMware server processor and hardware.

ACCS VMware profiling uses a Dual 8-core Intel Xeon E5-2670 2.60GHz CPU as a reference CPU. This reference processor has 16 physical CPU cores. Each of these 16 cores has an individual benchmark value that is one sixteenth of the overall benchmark score of the reference processor. You use this individual core benchmark value to compare the cores from different processors and to select suitable VMware host hardware for ACCS virtualization.

Página2007 de 3226.

The individual core benchmark value for the processor in your VMware host server must be equal to or greater than 90% of the individual core benchmark value for the ACCS reference processor.

Follow these steps to ensure your proposed VMware host CPUs meet the ACCS minimum requirements.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the reference CPU: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference CPU benchmark from website / Number of cores in reference CPU)
- Using the https://cpubenchmark.net website, determine the individual core benchmark value for your VMware host server CPU.

  Individual core benchmark value = (Your host server CPU benchmark from website / Number of cores in host server CPU)
- To support ACCS virtualization, the individual core benchmark value of your VMware host must be equal to or greater than 90% of the reference individual core benchmark value.

To support an Avaya Contact Center Select software appliance component, your VMware host must have a sufficient number of CPU cores each with at least the minimum individual core benchmark value.

VMware host server minimum resources

Use the following tables to determine the minimum VMware resources required to support a range of agent counts and system contact rates.

Table 3: Avaya Contact Center Select virtual machine VMware resource requirements

Maximum number of supported Agents	**250**	**400**
Maximum System Contact Rate (system contacts per hour)	**5000**	**8000**
Email Contact Rate (Emails per hour)	750	750
WebChat Contact Rate (WebChats per hour)	375	375
Number of CPUs (Minimum CPU clock speed 2400 MHz)	4	6
CPU Reservation (MHz)	9560	14340
Minimum RAM (GB)	16	16
Minimum RAM Reservation (MB)	16384	16384
Minimum Disk Size (GB) - Thick Lazy Provisioning	641	641
Virtual Network Interface Cards (1 GB) VMXNET3	1	1

Note 1: The System Contact Rate is the total maximum combined contact rate across all supported contact types.

Note 2: Multimedia contact rates are applicable only if multimedia is part of the solution. Email contacts per hour (Eph). Standard Web chats per hour (WCph). Standard Web chat maximum capacity is based off an average chat duration of 5 minutes. The maximum number of simultaneous Web Chat sessions is 50.

Página2008 de 3226.

Table 4: Avaya Aura® Media Server virtual machine VMware resource requirements

Maximum number of supported agents	**200**	**400**
Maximum supported sessions	**500**	**1000**
Number of CPUs (Minimum CPU clock speed 2400 MHz)	4	8
CPU Reservation (MHz)	9560	19120
Minimum RAM (GB)	8	8
Minimum RAM Reservation (MB)	8192	8192
Minimum Disk Size (GB) - Thick Lazy Provisioning	50	50
Virtual Network Interface Cards (1 GB) VMXNET3	1	1

Avaya Aura® Media Server is supported only on virtual machines with 4 or 8 CPUs.

Table 5: Avaya WebLM virtual machine VMware resource requirements

Maximum supported license requests	**5000**
Number of CPUs (Minimum CPU clock speed 2300 MHz)	1
CPU Reservation (MHz)	2290
Minimum RAM (GB)	2
Minimum RAM Reservation (MB)	2048
Minimum Disk Size (GB)	35
Virtual Network Interface Cards (1 GB) VMXNET3	1

VMware host server resource monitoring and management

When the Avaya Contact Center Select software appliance is virtualized and commissioned, continue to monitor and manage its real-time VMware resources.

- The VMware host server must not be overcommitted. The total number of vCPUs assigned across all virtual machines must be less than the host's physical core count.
- Virtual CPU (vCPU) resource requirements refer to physical cores only and not logical cores associated with Hyper-Threading.
- Ensure VMware Tools is installed on all virtual machines. This is required for VMXNET3 support and VMware performance monitoring and management.
- 16 GB of RAM is the minimum RAM footprint for reduced agent count deployments. Depending on your solution requirements, your ACCS virtual machine might need 20 GB RAM.
- If the total average CPU usage spikes above 50% for sustained periods, add additional CPU resources to the Contact Center virtual machine.
- If ACCS software appliance virtual machine monitoring indicates resource starvation, add additional resources as necessary.
- Depending on your solution's call complexity, you might need to add additional VMware resources as necessary.

Página2009 de 3226.

- Depending on your solution's administration and reporting requirements, you might need to add additional VMware resources as necessary. Avaya recommends running large or complex reports during off-peak hours.
- The minimum CPU Reservation (MHz) figure is based on the minimum supported clock speed. To fully reserve each CPU, reserve the number of CPUs multiplied by the virtualization host's core clock speed.
- The supported agent counts and associated contact processing is modelled using simple contact processing with moderate reporting and administration.

Job Aid

The Avaya Contact Center Select High-end PVI server specification (see High-end server specification on page 68), configured as a VMware host, can support the Avaya Contact Center Select software appliance up to the maximum agent count and system contact rate.

VMware profiling examples

This section provides a few worked examples of profiling ACCS solutions for virtualization using VMware.

Example 1

An ACCS solution is to support 230 agents at a call rate of 4600 voice contacts per hour.

Using the tables in the **VMware host server minimum resources** section, calculate the minimum number of CPUs. The following table specifies the minimum number of VMware CPUs for this example solution.

Virtual Machine	CPUs
ACCS virtual machine	4
AAMS virtual machine	8
WebLM virtual machine	1
ACCS software appliance total:	**13**
ESXi Hypervisor	1
ESXi host minimum:	**14**

The minimum number of CPU cores needed is 14 in total. This means that the VMware host must have at least a Dual 8-core (16 physical cores) CPU. Each of these CPU cores must have an individual core benchmark value equal to or greater than 90% of the individual core benchmark value for the ACCS reference processor.

The next step is to determine if a proposed server CPU is suitable.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the ACCS reference processor: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference processor benchmark from website / Number of cores in reference CPU)

  For example:

Página2010 de 3226.

Using the reference Dual 8-core Intel Xeon E5-2670 2.60GHz CPU

The reference Dual 8-core CPU has a benchmark score of, for example, 18653.

Reference individual core benchmark value = (18653 / 16)

Reference individual core benchmark value = 1165

90% of Reference individual core benchmark value = 1050

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the proposed VMware host server processor.

  Individual core benchmark value = (The host server processor benchmark from website / Number of cores in host server processor)

  For example:

  Using a proposed Dual 8-core Intel Xeon E5-2640 v3 2.60GHz.

  The Dual 8-core CPU has a benchmark score of, for example, 20885.

  Individual core benchmark value = (20885 / 16)

  Individual core benchmark value = 1305

  1305 > 1050, so the proposed Dual 8-core Intel Xeon E5-2640 v3 2.60GHz is suitable.

The following table lists the total minimum resources required for this example solution.

Virtual Machine	CPUs	Minimum RAM	Minimum Disk Size
ACCS virtual machine	4	16 GB	641 GB
AAMS virtual machine	8	8 GB	50 GB
WebLM virtual machine	1	2 GB	35 GB
Minimum ACCS Software Appliance resources:	13	26 GB	726 GB

Example 2

An ACCS solution is to support 50 agents at a call rate of 1000 voice contacts per hour.

Using the tables in the **VMware host server minimum resources** section, calculate the minimum number of CPUs. The following table specifies the minimum number of VMware CPUs for this example solution.

Virtual Machine	CPUs
ACCS virtual machine	4
AAMS virtual machine	4
WebLM virtual machine	1
ACCS software appliance total:	**9**
ESXi Hypervisor	1
ESXi host minimum:	**10**

The minimum number of CPU cores needed is 10 in total. This means that the VMware host must have at least a Dual 6-core (12 physical cores) CPU.

Página2011 de 3226.

Each of these CPU cores must have an individual core benchmark value equal to or greater than 90% of the individual core benchmark value for the ACCS reference processor.

The next step is to determine if a proposed server CPU is suitable.

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the ACCS reference processor: Dual 8-core Intel Xeon E5-2670 2.60GHz.

  Reference individual core benchmark value = (Reference processor benchmark from website / Number of cores in reference CPU)

  For example:

  Using the reference Dual 8-core Intel Xeon E5-2670 2.60GHz CPU

  The reference Dual 8-core CPU has a benchmark score of, for example, 18653.

  Reference individual core benchmark value = (18653 / 16)

  Reference individual core benchmark value = 1165

  90% of Reference individual core benchmark value = 1050

- Using the https://cpubenchmark.net website, determine the individual core benchmark value for the proposed VMware host server processor.

  Individual core benchmark value = (The host server processor benchmark from website / Number of cores in host server processor)

  For example:

  Using a proposed Dual 6-core Intel Xeon X5690 3.47GHz

  The Dual 6-core CPU has a benchmark score of, for example, 9239.

  Individual core benchmark value = (14363 / 12)

  Individual core benchmark value = 1197

  1197> 1050, so the proposed Dual 6-core CPU is suitable.

The following table lists the total minimum resources required for this example solution.

Virtual Machine	CPUs	Minimum RAM	Minimum Disk Size
ACCS virtual machine	4	16 GB	641 GB
AAMS virtual machine	4	8 GB	50 GB
WebLM virtual machine	1	2 GB	35 GB
Minimum ACCS Software Appliance resources:	9	26 GB	726 GB

Virtualization considerations

Using virtualization in a contact center enterprise solution requires careful up-front planning, engineering, and implementation. While the technical and business advantages are clear, virtualization imposes extra considerations when designing the contact center solution

Página2012 de 3226.

architecture. Environmental isolation allows multiple operating systems to run on the same VMware host machine. While virtualization offers these forms of isolation, virtualization environments do not provide performance isolation. The behavior of one virtual machine can adversely affect the performance of another virtual machine on the same host. Most modern virtualization environments provide mechanisms that you can use to detect and reduce performance interference. You must carefully engineer your virtualized contact center solution to avoid performance interference.

If you plan to install non-Contact Center software applications on the other guests of a host server with Contact Center installed, you must carefully analyze the impact of these applications on the contact center solution and provide extra performance isolation to safeguard Contact Center functionality.

Important:

Deploy Contact Center on an enterprise-grade virtual environment with the most recent hardware that supports hardware-assisted virtualization. Avaya recommends that you apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a virtualization infrastructure.

VMware features

Avaya Contact Center Select is a collection of real-time applications running on the MS Windows Server 2012 R2 operating system. Avaya Contact Center Select provides real-time call control, multimedia handling, and statistical reporting.

Avaya Aura® Media Server is a real-time media processing application running on the Red Hat Enterprise Linux (RHEL) operating system. Avaya Aura® Media Server provides the real-time conferencing and media processing capabilities for Avaya Contact Center Select.

Some VMware features require CPU, Disk I/O, or networking resources to function. Running these VMware features can cause resource constraints and impact the real-time performance of the Avaya Contact Center Select and Avaya Aura® Media Server Virtual Machines (VMs). These features are therefore not supported while Avaya Contact Center Select or Avaya Aura® Media Server are active.

Some VMware features are not supported by Avaya Contact Center Select or Avaya Aura® Media Server. Some other VMware features are supported only while the Avaya Contact Center Select or Avaya Aura® Media Server Virtual Machines are stopped for maintenance.

The following table shows the Avaya Contact Center Select and Avaya Aura® Media Server level of support for VMware features.

Página2013 de 3226.

VMware Feature	Supported on active Avaya Contact Center Select VM	Supported during Avaya Contact Center Select VM maintenance window	Supported on active Avaya Aura® Media Server VM	Supported during Avaya Aura® Media Server VM maintenance window
Cloning	No	Yes	No	No
Distributed Power Management (DPM)	No	Yes	No	Yes
Distributed Resources Scheduler (DRS)	No	Yes	No	Yes
Distributed Switch	Yes	Yes	Yes	Yes
Fault Tolerance	No	No	No	No
High Availability (HA)	No	No	No	No
Snapshots	No	See Avaya Contact Center Select VMware snapshot considerations on page 104	No	See Avaya Aura Media Server VMware snapshot considerations on page 105
Storage DRS	No	Yes	No	Yes
Storage Thin Provisioning	No	N/A	No	N/A
Storage vMotion	No	Yes	No	Yes
Suspend & Resume	No	N/A	No	N/A
vMotion	No	Yes	No	No

VMware vSphere Host considerations

When planning virtual machines (guests) on your host system, the total resources needed by the virtual machines running on the host server must not exceed the total capacity of the host. It is good practice to under-commit CPU and memory resources on the host. If the host CPU capacity is overloaded, Contact Center does not function correctly.

Important:

Avaya Contact Center Select is not supported on an over-committed host where the total virtual resources from all virtual machines hosted exceeds the physical resources of the host.

Hardware-Assisted Virtualization

Most recent enterprise-level processors from Intel support virtualization. There are two generations of virtualization support: the first generation introduced CPU virtualization; the second generation included CPU virtualization and added memory management unit (MMU) virtualization. For the best performance, make sure your system uses processors with at least second-generation hardware-assist features.

Página2014 de 3226.

Virtual Machine File System (VMFS)

VMware virtual machines and snapshots are stored in a Virtual Machine File System (VMFS) datastore. To support Avaya Contact Center Select on a virtual machine, the VMware datastore containing Contact Center must be VMFS 5.54 or later. If you upgrade an existing VMware host server, ensure the associated datastore is upgraded to VMFS 5.54 or later.

Hardware-Assisted CPU Virtualization (Intel VT-x)

The first generation of hardware virtualization assistance includes VT-x from Intel. These technologies automatically trap sensitive interrupts, eliminating the overhead required to do so in software. This allows the use of a hardware virtualization (HV) virtual machine monitor (VMM).

Hardware-Assisted MMU Virtualization (Intel EPT)

More recent enterprise-level processors also include a feature that addresses the overheads due to memory management unit (MMU) virtualization by providing hardware support to virtualize the MMU. VMware vSphere supports this feature in Intel processors, where it is called Extended Page Tables (EPT).

Storage Area Network (SAN)

A Storage Area Network (SAN) is a dedicated storage network that provides access to consolidated block level storage. SANs are used to make storage devices such as disk arrays, accessible to servers so that the devices appear as locally attached to the operating system.

When Avaya Contact Center Select is installed on virtual machines it supports a SAN. You must monitor the Contact Center demand on the SAN storage device. Adhere to your vendor-specific SAN configuration recommendations to ensure the SAN storage device meets the demands of Contact Center.

Disk drive provisioning

Provision sufficient hard disk drive space on the host server to support all the guest virtual machines, an ISO library, and provision additional space for snapshot image storage.

Server performance and firmware settings

The Basic Input Output System (BIOS) of a server configures the hardware components and boots the operating system from a storage device. The server operating system (OS) then uses the BIOS to control the server hardware. You must configure the server BIOS settings to ensure optimum performance from the underlying server hardware. For most BIOS settings, you must choose between optimizing a server for power savings or for server performance. For real-time applications such as Avaya Contact Center Select, you must always choose the server BIOS settings that ensure the optimum performance from the underlying server hardware.

Server manufacturers provide their own motherboards, BIOS, hardware, and firmware. Determining the BIOS configuration for your server’s hardware can be challenging. There are several BIOS settings that can significantly impact the system performance. When optimizing for system performance, you must select the BIOS settings that enhance the system performance over those that contribute to power savings. Other BIOS settings and recommendations are not as

Página2015 de 3226.

straight forward. Start by consulting the manufacturer's technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions.

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Server firmware

Firmware is a computer program that is stored on the server motherboard or on an add-on hardware controller. The firmware stored on the server motherboard is called the Basic Input Output System (BIOS). The BIOS is responsible for the behavior of the system when it is first switched on and for passing control of the server to the operating system. Firmware is also stored in hardware components such as Redundant Array of Independent Disks (RAID) controllers.

Routinely consult the manufacturer's technical data for your servers and, where appropriate, apply the most recent BIOS and firmware updates. The steps required to update firmware or a system BIOS vary depending on the hardware vendor and the component to be updated. Typically, the manufacturer supplies a firmware updating utility. Keeping your server BIOS and firmware at a supported level can improve reliability, serviceability, and help ensure optimum performance.

Power and performance management

For real-time applications such as Avaya Contact Center Select, you must always select the hardware, BIOS, firmware, and Operating System settings that enhance the system performance over those that contribute to power savings.

Intel Xeon CPUs offer two main power management options: C-states and Intel Turbo Boost.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to full power on.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power.

These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described below. Other server makes and models can have other terminology but equivalent BIOS settings.

The following are the recommended BIOS settings for the Dell PowerEdge servers:

- Set the Power Management Mode to Maximum Performance.
- Set the CPU Power and Performance Management Mode to Maximum Performance.
- Processor Settings: set Turbo Mode to enabled
- Processor Settings: set C States to disabled

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to Static High Mode.
- Disable Processor C-State Support
- Disable Processor C1E Support

Página2016 de 3226.

- Disable QPI Power Management
- Enable Intel Turbo Boost

Configure the server hardware, firmware, and Operating System settings to select system performance over power savings.

Disk caching and RAID

Hard disk drives use cache memory to improve read and write access to the disk drives. In write-back mode caching, the disk or RAID controller writes data from the server to cache memory and acknowledges write completion to the server. The server is free to perform other tasks while the disk controller transfers the data from the write cache to the disk drives. This approach significantly increases write performance.

Avaya Contact Center Select supports hardware RAID-1, RAID-5, and RAID-10. RAID technology provides disk data redundancy as well as error detection and correction. For maximum security and mission-critical solutions, Avaya recommends that all Contact Center servers contain a RAID controller. Hardware RAID-1, RAID-5, and RAID-10 are the only levels and types of RAID supported.

Read the hardware documentation for your server to determine how to configure disk caching. Typically, disk caching can be configured as a BIOS setting, a RAID setting, a RAID controller setting, or as an Operating System setting. Some RAID controllers expose the ability to manipulate the Caching Policy through the OS and therefore the OS level setting can override the BIOS level setting. Refer to your hardware documentation for more information about configuring disk caching. Avaya Contact Center Select does not support Operating System level disk caching, software disk caching, or software RAID. Avaya Contact Center Select requires battery backed hardware RAID caching to avoid data loss and possible database corruption on power outage.

Non-Uniform Memory Architecture and memory

Non-uniform memory access (NUMA) is a computer memory design used in multiprocessing, where the memory access time depends on the memory location relative to the processor. Using NUMA, a processor can access its own local memory faster than non-local memory (memory local to another processor or memory shared between processors). For Avaya Contact Center Select, the server must support and implement NUMA.

In the server BIOS settings, configure the memory operating mode for performance optimization and disable Node Interleaving. For example, for a Dell server configure “Memory Operating Mode” as “Optimizer Mode”, and configure “Node Interleaving” as “Disabled”. Refer to your hardware documentation for more information about NUMA and memory performance.

Performance management and VMware

For VMware host servers, to allow the VMware kernel to control CPU power saving while maximizing server performance when required, it is possible to set power management in the BIOS to “OS Control Mode”. The VMware hypervisor can then provide balanced performance and power management. This BIOS setting and VMware feature combination does not meet the real-time performance requirements of Avaya Contact Center Select. Avaya Contact Center Select does not support the BIOS “OS Control Mode” settings or its equivalents.

Página2017 de 3226.

Virtualization technology

When virtualization technology is enabled, the BIOS enables processor virtualization features and provides virtualization support to the operating system through the DMAR table. In general, only virtualized environments such as VMware take advantage of these features.

For VMware host servers, enable all available Virtualization Technology options in the hardware BIOS. For Intel based hosts: Enable Intel virtualization (VT-x) and if available enable Extended Page Tables (EPT). The available virtualization settings vary by hardware provider and BIOS version. Read your hardware provider's documents covering virtualization support to determine which settings to configure.

Hyper-Threading

Hyper-Threading is Intel’s proprietary technology for increasing parallel computational power (processor multi-tasking) by allowing the operating system (OS) to see and address each physical processor core as if it were two virtual processors. It also enables the OS and applications to share work between those virtual processors whenever possible, thereby making full use of the available resources.

Enable Hyper-Threading on the Avaya Contact Center Select server.

Unused hardware devices

On the server, disconnect or disable unused and unnecessary physical hardware devices such as: COM ports, LPT ports, USB controllers, Network interfaces, and Storage controllers. You must retain some USB devices for the mouse and keyboard. Disabling unnecessary hardware devices improves server performance and security. Consult the manufacturer’s technical data for your servers for information about disabling unused hardware devices in the BIOS.

Summary

For real-time applications such as Avaya Contact Center Select, choose server BIOS settings that optimize for performance in preference to power savings. Start by consulting the manufacturer’s technical data for your server. Avaya recommends that you then test your solution in order to make the best BIOS configuration decisions. Avaya recommends that you enable CPU Hyper-Threading. By enabling BIOS options such as CPU Prefetchers and CPU Hyper-Threading, the system performance can be improved effectively. When tuning system BIOS settings for performance, you must consider the various processor and memory options. Experiment with other options to find the optimum setting for your specific hardware and Contact Center solution.

Configure the server hardware, BIOS, firmware, and Operating System settings to select system performance over power savings.

VMware networking best practices

There are many different ways of configuring networking in a VMware environment. Review the VMware networking best practices documentation before deploying Avaya applications on an

Página2018 de 3226.

ESXi host. This section is not a substitute for the VMware documentation. For improved performance and best practice, Contact Center uses Network Adapter type VMXNET 3.

The following are some suggested networking best practices:

- Separate network services to achieve greater security and performance. Create a vSphere *Standard Switch* with dedicated NICs for each service. Separate VMware Management, iSCSI (SAN traffic), and VM networks to separate physical NICs. If separate switches are not possible, consider port groups with different VLAN IDs.
- All physical NICs that are connected to the same vSphere *Standard Switch* must be connected to the same physical network.
- Configure all VMkernal vNICs to the same MTU (IP Maximum Transmission Unit).
- Configure Contact Center to use Network Adapter type VMXNET 3.

For more information about VMware networking best practices, refer to the VMware documentation.

Avaya Contact Center Select VMware snapshot considerations

VMware snapshots save the current state of the virtual machine, so you can return to it at any time. Snapshots are useful when you need to revert a virtual machine repeatedly to the same state, but you don't want to create multiple virtual machines.

The following considerations apply when using snapshots with Avaya Contact Center Select on VMware:

- Snapshots must be taken during an Avaya Contact Center Select maintenance window. Do not take a snapshot of a Contact Center virtual machine while Contact Center is running. Snapshots have a negative impact on the performance of a virtual machine over time. You must Delete All snapshots at the end of the maintenance window and *Consolidate* snapshots if required, before putting the Contact Center virtual machine back into production. For more information about consolidating snapshots, refer to VMware documentation. Before taking the snapshot, shutdown all Contact Center services and stop the Caché database instance using the Caché Cube.
- Create a snapshot for the Contact Center virtual machines all at the same time. Likewise, when you restore a snapshot, restore all snapshots to ensure the data is consistent across the Contact Center suite.
- When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed Microsoft Windows OS and security updates, and lapsed domain accounts on the contact center. Isolate the restored virtual machine until these issues are resolved.
- By default, a Windows Server 2012 R2 machine account password is changed every 30 days. This is an important consideration when reverting to a snapshot of a virtual machine that has been in use for more than 30 days, as it can cause the machine to lose its connection to the Windows domain. If this issue occurs, rejoin the Windows Server 2012 R2 virtual machine to the domain.

Página2019 de 3226.

VMware snapshots are not a replacement for Avaya Contact Center Select database backup (and restore) procedures and practices. You must continue to perform regular and frequent Contact Center backups. For more information about maintenance, see *Deploying Avaya Contact Center Select Software Appliance*.

Avaya Aura® Media Server VMware snapshot considerations

VMware snapshots save the current state of the virtual machine, so you can return to it at any time. Snapshots are useful when you need to revert a virtual machine repeatedly to the same state, but you don't want to create multiple virtual machines.

The following considerations apply when using snapshots with Avaya Aura® Media Server on VMware:

- Snapshots must be taken during an Avaya Aura® Media Server maintenance window. Do not take a snapshot of an Avaya Aura® Media Server virtual machine while the contact center is running. Snapshots have a negative impact on the performance of a virtual machine over time. You must Delete All snapshots at the end of the maintenance window and *Consolidate* snapshots if required, before putting the Avaya Aura® Media Server virtual machine back into production. For more information about consolidating snapshots, refer to VMware documentation.
- When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed Linux operating system updates and security updates. Isolate the restored virtual machine until these issues are resolved.

VMware snapshots are not a replacement for Avaya Aura® Media Server database backup (and restore) procedures and practices. For more information about maintenance, see *Deploying Avaya Contact Center Select Software Appliance*.

Guidance for storage requirements

Input/Outputs per Second (IOPS) is a measure of the maximum number of reads and writes to *non-contiguous* storage locations performed per second. IOPS measurements are associated with smaller files and more continuous changes, and comprise the workloads most typical in real-time enterprise applications such as Avaya Contact Center Select.

In a virtualized environment, any given storage array must be designed to have an IOPS capacity exceeding the sum of the IOPS required for all resident applications.

For a fully loaded Avaya Contact Center Select instance, the IOPS is:

- Average: 105
- Maximum: 1488

These IOPS figures include Avaya Contact Center Select and the underlying operating system loads.

Página2020 de 3226.

Performance monitoring and management

You must continuously monitor and measure the performance of the Contact Center host server. You can use VMware vSphere vCenter to measure the critical host performance metrics in real-time. VMware vCenter aggregates and archives performance data so that data can be visualized and reported on.

Configure VMware vCenter statistics collection to collect 5 minute and 30 minute Interval Duration data for the host at Statistics Level 3. Retain the 5 minute Interval Duration data for 3 days and retain the 30 minute Interval Duration for 1 week.

Generate performance reports using vCenter Report Performance and archive these reports to provide a baseline performance reference. Generate and store 1-day and 1-week reports. Store the associated vCenter Report Summary with the performance reports. You must analyze performance reports after changes to the host to assess the impact of the change on the host.

Monitor, acknowledge, and resolve VMware vCenter alarms. In particular, you must immediately investigate and resolve host CPU usage and host memory usage alarms.

In addition, the command-line tools “esxtop” and “resxtop” are available to provide a fine-grained look at real-time metrics. There are a number of critical CPU-related counters to watch out for:

- If the load average listed on the first line of the CPU Panel is equal to or greater than the number of physical processors in the system, this indicates that the system is overloaded.
- The usage percentage of physical CPUs on the PCPU line can indicate an overloaded condition. In general, 80 percent usage is a reasonable ceiling in production environments. Use 90 percent as an alert to the VMware administrator that the CPUs are approaching an overloaded condition, which must be addressed.
- %RDY - The percentage of time a schedulable entity was ready to run but is not scheduled to a core. If %RDY is greater than 10 percent, then this can indicate resource contention.
- %CSTP - The percentage of time a schedulable entity is stopped from running to allow other vCPUs in the virtual machine to catch up. If %CSTP is greater than 5 percent, this usually means the virtual machine workload is not using VCPUs in a balanced fashion. High %CSTP can be an indicator of a system running on an unconsolidated snapshot.

For more information about using esxtop or resextop, see the *VMware Resource Management Guide*.

Memory Reservations

Use VMware Reservations to specify the minimum amount of memory for a Contact Center virtual machine. VMware Reservations maintain sufficient host memory to fulfill all reservation guarantees. ESX does not power-on a virtual machine if doing so reduces the amount of available memory to less than the amount reserved. Using reservations can reduce the total number of virtual machines that can be hosted on a VMware host server. After all resource reservations have been met, ESX allocates the remaining resources based on the number of shares and the resource limits configured for your virtual machine.

Página2021 de 3226.

Troubleshooting VMware

Virtualization platform performance issues can result with Contact Center performance problems. The virtualization platform includes the host and the running virtual machines on the host. The Contact Center performance problems can include (but are not limited to) high CPU usage, link instability, defaulted or abandoned calls.

You must logically and systematically investigate any Contact Center performance issues to rule out virtualization performance problems. All deviations from the published specifications must be investigated and resolved before the Contact Center software investigation is initiated. For more information, refer to the VMware vSphere documentation.

To support troubleshooting VMware resourcing issues, collect information about the following VMware Key Performance Indicators (KPIs).

VMware vSphere Host KPIs:

- Physical CPU
  - PCPU - Physical CPU usage.
  - CPU load average - Average CPU load average of host.
- Physical Memory
  - SWAP/MB - Memory swap usage statistics.

VMware vSphere Virtual Machine (VM) KPIs:

- vCPU
  - CPU RDY - Time VM was ready to run, but was not provided CPU resource.
  - CPU WAIT - Percentage of time spent in the blocked or busy wait state.
  - AMIN - Reservation allocated.
  - ASHRS - CPU shares allocated.
  - CPU CSTP - Amount of time a Symmetric Multi-Processing (SMP) VM was ready to run, but was delayed due to co-vCPU scheduling contention.
- Disk I/O
  - GAVG - Average guest operating system read latency per read operation.
  - DAVG/rd - Average device read latency per read operation.
  - DAVG/wr - Average device write latency per write operation.
  - RESETS/s - Number of commands reset per second.
  - ABRTS/s - Number of disk commands abandoned per second.
- Network
  - %DRPTX - Percentage of packets dropped when transmitting.

Página2022 de 3226.

- %DRPRX - Percentage of packets dropped when receiving.

- Memory
  - MCTLSZ - Amount of physical memory reclaimed memory balloon statistics.

Software Appliance Licensing

Contact Center License Manager supports only the Virtualized Environment deployment of Avaya WebLM server.

When Contact Center License Manager starts, it extracts WebLM license keys from the remote WebLM server. Contact Center License Manager then converts the WebLM license keys into local PLIC license keys and distributes the keys to the Avaya Contact Center Select applications as required. Contact Center License Manager distributes PLIC license keys to Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia, and Avaya Aura® Media Server as required.

When Contact Center License Manager requests licenses from a remote Avaya WebLM server, it reserves all the Contact Center licenses available on that server. Contact Center therefore supports only the PLDS standard license file (SLF) type. Avaya Contact Center Select does not support the WebLM Enterprise model. Contact Center supports WebLM in nodal contact centers. WebLM does not support Contact Center corporate licensing.

Contact Center License Manager distributes nodal license keys to all configured Avaya Aura® Media Servers in the solution. Configure Avaya Aura® Media Server as a Media Server in Contact Center Manager Administration. Contact Center License Manager, when restarted, pushes license keys to that Avaya Aura® Media Server. Do not configure WebLM licensing on Avaya Aura® Media Server servers.

How to obtain a license

Avaya Contact Center Select uses a remote WebLM server to provide nodal licensing control.

1. Obtain the Avaya WebLM host ID from the WebLM user interface.
2. Use the WebLM host ID to obtain WebLM license keys from the Avaya Product Licensing and Delivery System (PLDS).
3. Enter these license keys on the remote Avaya WebLM server. Contact Center License Manager connects to the remote WebLM server and uses the Contact Center-specific license keys from it to control Contact Center licensed features. Contact Center does not import the license file to a Contact Center server; WebLM stores the license file on the WebLM server.

You can use the License Manager Configuration Utility to check which Contact Center features are licensed and how many agent licenses are available.

Página2023 de 3226.

Chapter 6: Avaya Contact Center Select hardware appliance

This section describes the Avaya Contact Center Select hardware appliance. The Avaya Contact Center Select hardware appliance is a physical rack mount server with the application software already loaded and partially preconfigured.

To deploy the Avaya Contact Center Select hardware appliance, you must activate the Windows operating system using the provided MS Windows product key, configure the server network setting, and then use a simple configuration wizard to rapidly commission the solution. At install time, the Avaya Contact Center Select hardware appliance server automatically launches a simple configuration wizard that you use to rapidly deploy a functional contact center solution. The Avaya Contact Center Select hardware appliance server is preloaded with sample users, skillsets, and contact center parameters. You can use this sample data to rapidly commission the solution and make the first routed call and email contact. The Avaya Contact Center Select hardware appliance server delivers quick and simplified contact center deployment. After the basic telephony and email features are working, you can then configure multimedia contacts, multiplicity, custom prompts, and other enhanced features and functions to improve your customer's experience.

You must activate the Microsoft Windows operating system on the Avaya Contact Center Select hardware appliance using the provided Microsoft Windows product key. The provided Microsoft Windows product key is displayed on a sticker attached to the top of the Avaya Contact Center Select hardware appliance server.

Página2024 de 3226.

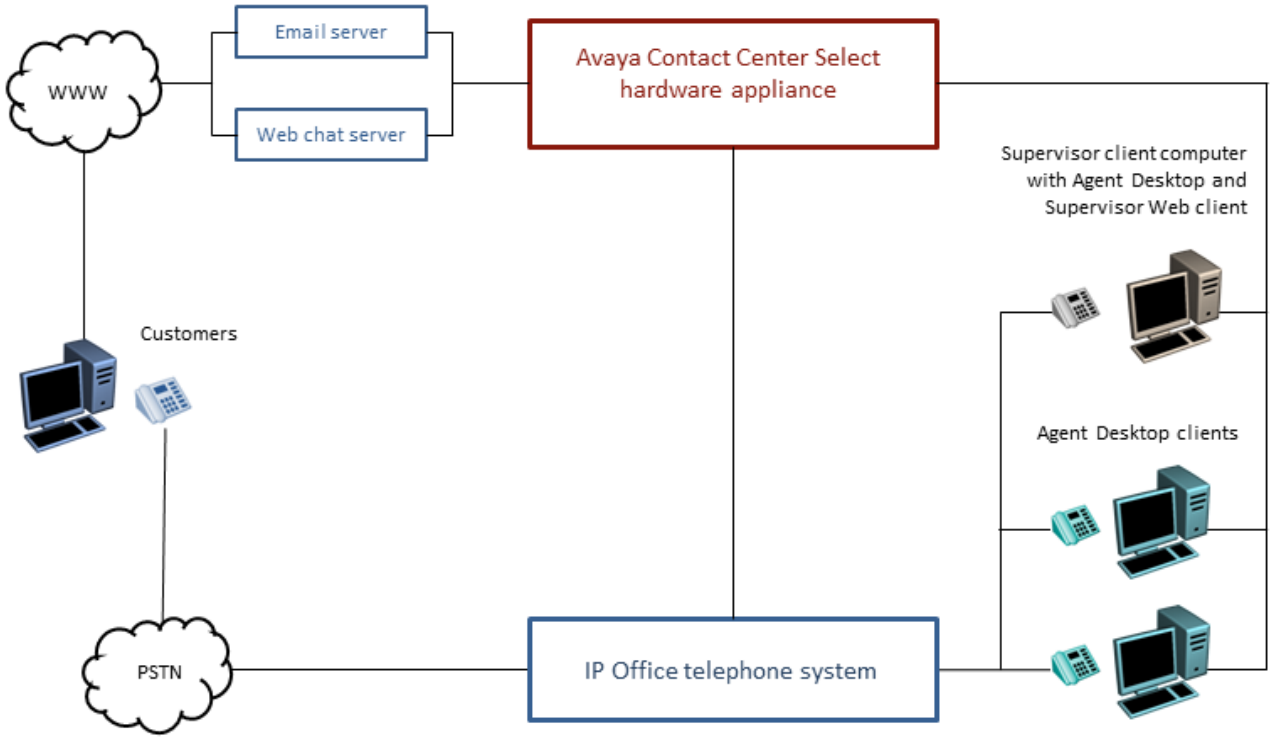


Figure 10: Topology of a typical Avaya Contact Center Select hardware appliance solution

- Hardware Appliance server specifications on page 110
- Avaya Contact Center Select hardware appliance software specifications on page 112
- Hardware Appliance Licensing on page 118

Hardware Appliance server specification

The Contact Center Hardware Appliance is a rack mount server preconfigured to support Contact Center.

Contact Center is a collection of real-time applications running on the Microsoft Windows Server 2012 R2 operating system. Contact Center provides real-time call control, multimedia handling, and real-time statistical reporting.

Important:

The Contact Center Hardware Appliance server supplied by Avaya is optimized to provide the real-time computational, networking, and logging resources required by Contact Center. You must not modify the Hardware Appliance server, unless instructed to do so by Avaya:

- Do not add additional internal hardware devices to this server.

Página2025 de 3226.

- Do not change or upgrade the server BIOS version or settings.
- Do not change the server hardware settings.
- Do not update the server firmware.
- Do not change or upgrade the device drivers.
- Do not modify the hard disk partitions.
- Do not change the *Windows Update* application settings on the server.
- Do not upgrade the Java Runtime Environment (JRE) supplied on the Hardware Appliance.

Due to the real-time processing that Contact Center applications perform, you must not install any other application class software on the server. You can install only the supported antivirus and remote support utility class software on this server.

Install only the Microsoft Windows Server 2012 R2 Operating System patches and hotfixes supported by Contact Center. For more information about the supported Operating System patches, see the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List* on http://support.avaya.com.

The following table lists the server specifications for the Contact Center Hardware Appliance server.

Specification	Quantity	Configuration	Comment
Form factor	1	Rack mount, 1U chassis	PowerEdge R630 rack mount server.
CPU	2	2.6 GHz E5-2640v3	—
RAM	12	4GB DDR4 RDIMM	—
Hard Disk	2	1.2 TB 10K Drives 2.5" SAS	—
RAID Controller	1	RAID1 PERC 730 1GB	—
Optical Drive	1	16X DVD +/-RW Drive SATA	—
Network Interface	2	Dual Port PCIe NIC 1GbE	Only Ethernet supported.
Power supply	2	750 Watt AC	—
Power cables	2	Power cables	Localized to region.
Additional interfaces		• 2 front USB ports • 2 back USB ports • Front video connector	—
Additional hardware	1	Rack mount kit	—
Weight	—	47.5 lbs approximately 21.5 kilograms approximately	—

Página2026 de 3226.

Avaya Contact Center Select hardware appliance software specifications

Avaya Contact Center Select is offered as a hardware appliance server. The Avaya Contact Center Select hardware appliance server contains the following software:

- Microsoft Windows 2012 R2 Standard Edition operating system. The operating system is not activated until the end customer applies the Microsoft Windows license attached to the server.
- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server with Quick Fix Engineering (QFE) patches
- Default Avaya Contact Center Select configuration data
- Service Packs
- Firewall policy
- Configuration wizard

The Windows 2012 R2 operating system on the shipped hardware appliance server is not activated. The Contact Center hardware appliance provides a Microsoft Windows Server 2012 R2 product license key. The Microsoft Windows Server 2012 R2 product license key is printed on a label attached to the top of the Contact Center Hardware Appliance server. You must activate the Microsoft Windows operating system within 30 days of the initial power-up. Otherwise the Avaya Contact Center Select hardware appliance server stops working.

The following table shows the operating system on the Avaya Contact Center Select hardware appliance server.

Operating System	International Versions Supported	Minimum Service Pack Supported
Windows Server 2012 Release 2 Standard Edition	English	

Página2027 de 3226.

Server naming requirements

Server names must adhere to RFC1123 (Requirements for Internet Hosts), which specifies that a host name must adhere to the following:

- Use only characters a to z, A to Z, and 0 to 9 can be used in a host name.
- You can use a hyphen (-), but not to start or end the host name.
- Host names must be 6 to 15 characters in length.
- Host names must not start with a number.
- Do not use the underscore character (_) and period character (.).
- Do not use spaces in the host name.

The Contact Center server must be able to resolve the host name or computer name of all other servers within the configuration. If you have a Domain Name Service (DNS) server, make sure an entry exists for each server. If you do not have a DNS server, manually update the HOSTS file on each server with the host name or computer name of all other servers to ensure that all clients can interpret the server names.

If network connectivity on your network requires the use of Fully Qualified Domain Names (FQDN), then the FQDN of each computer must be resolvable between all servers associated with Contact Center.

Microsoft security hotfixes

You must operate your server with the most current Microsoft patches.

- Review the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* (available from Technical Support website) for the list of applicable Microsoft security hotfixes to apply.
- Back up the entire server, and then shut down all Contact Center services before you apply any Microsoft security hotfixes using the Microsoft instructions.
- Apply Microsoft security updates on a timely basis.

Operating system updates

Operating system updates includes service updates and service packs.

Service updates

Given the number of operating system security service updates and the complexity inherent in any network, create a systematic and accountable process for identifying and applying service updates. To help create such a process, you can follow a series of best practices guidelines, as documented in the National Institute of Standards and Technology (NIST) Special Bulletin 800-40, Procedures for Handling Security Patches.

Página2028 de 3226.

This bulletin suggests that if an organization has no central group to coordinate the storage, evaluation, and chronicling of security service updates into a library, then system administrators or the contact center administrator must fulfill this role. In addition to these guidelines, whenever possible, follow Microsoft recommendations regarding newly discovered vulnerabilities and that you promptly install Microsoft security service updates.

Whenever possible, Avaya incorporates the most recent operating system security recommendations and service updates in an integrated solutions testing strategy during each test cycle. However, due to the urgent nature of security service updates when vulnerabilities are discovered follow Microsoft guidelines as they are issued, including any Microsoft installation procedures and security service update rollback processes.

Finally, you must perform a full system backup before you update the system to ensure that a rollback is possible, if required. If a Contact Center application does not function properly after you apply a Microsoft security service update, you must remove the service update and revert to the previous version of the application (from the backup you made before applying the service update). For added security, always determine whether Avaya verified the Microsoft service update for compatibility with Contact Center Manager.

For more information about updating, see the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Compatibility List* on http://support.avaya.com.

Service packs

Avaya has a policy to implement co-residency testing of all new operating service packs for compatibility with the suite of Contact Center applications as soon as they are available. In practice, because a service pack can contain a significant amount of new content, Avaya requires that you wait until compatibility testing is complete before you apply the service pack. Note that operating system service packs are typically tested with the most recent Contact Center application SP and, therefore, an upgrade to a new service pack requires an upgrade to the most recent Avaya SP.

Before you upload a new service pack, you must perform a full system backup (for system rollback as in the updating scenario).

Important:

Service pack compatibility for all Contact Center applications is documented in the *Contact Center Portfolio Service Packs Compatibility and Security Hotfixes Applicability List* on the website at http://support.avaya.com.

Java Runtime Environment updates

Contact Center supports only specific versions of Java Runtime Environment (JRE). During installation, Contact Center disables JRE automatic updates on the contact center servers.

Important:

Updating to an unsupported version of JRE can cause the contact center to stop working and can require the reinstallation of the contact center server.

Página2029 de 3226.

Dynamic Host Configuration Protocol support

Contact Center applications (CCMS, CCMA, CCT, CCMM, LM, and Avaya Aura® Media Server) do not support Dynamic Host Configuration Protocol (DHCP). All Contact Center servers must have a static IP address.

Agent Desktop client computers support both DHCP and static IP addresses.

Third-party software requirements

Due to the mission-critical, real-time processing that Contact Center applications perform, you must not install any other application class software on the server. You can install certain utility class software on the server, providing it conforms to the guidelines in this section.

Application class software generally requires a certain amount of system resources and must not be installed on a server running Contact Center applications. The installation of third-party applications can cause Contact Center applications to operate outside of the known engineering limits and can create potential unknown system problems (for example, CPU contentions, increased network traffic loading, and disk access degradations).

Certain third-party utility class software applications, such as hardware diagnostics or backup tools, generally require less system resources during the normal operation of Contact Center applications and are permitted. Exceptions are utilities such as screen savers, which can cause system problems and degrade performance.

Antivirus software is classified as a utility and is subject to the generic guidelines in the following section.

Generic guidelines for utility-class software applications

The following are generic guidelines for utility-class software:

- During run-time, the utility must not degrade the contact center application beyond an average percentage of CPU use (see each specific application section in this document for the recommended maximum CPU usage level). Furthermore, the utility must not lower the minimum amount of free hard disk space required by contact center application and the Windows Operating system.
- The utility must not cause improper software shutdowns or out-of-sequence shutdowns.
- The utility must not administer the contact center application.
- If the utility has a database, it must not affect the contact center application database.
- Disk compression utilities must not be used.
- Memory tweaking utilities used to reclaim memory that is unused by Microsoft must not be used.
- The installation or uninstallation of the third-party software must not impact or conflict with the contact center application (for example, it must not cause DLL conflicts). If such conflicts are discovered, a server rebuild might be necessary.
- The implementation personnel must perform tests to ensure these conditions and recommendations are met before you place the Contact Center application into production.

Página2030 de 3226.

Support personnel can ask for the results of the testing during fault diagnosis. As part of fault diagnosis, the distributor or end user might be asked to remove third-party software.

- HyperTerminal must not be installed on the server as it interferes with the operation of Contact Center.

Guidelines for the use of antivirus software

This section describes the Avaya Contact Center Select antivirus software requirements.

Avaya Contact Center Select supports the following antivirus products:

- Symantec Antivirus
- McAfee

For more information about Avaya Contact Center Select anti-virus considerations and supported versions, see *Avaya Contact Center Select Security Reference Guide* available from the Avaya Support website at http://support.avaya.com.

You can deploy antivirus products from other vendors subject to the following guidelines:

- Infected file quarantine policy on the server and client: antivirus software can be configured to clean up the detected virus automatically and files must be quarantined if infected files cannot be cleaned. Contact Avaya to verify whether the quarantine file is part of our product files or dependent system file. If a virus is detected, remove the server from the network immediately during virus eradication to prevent further virus propagation.
- Do not connect a contact center application platform directly to the Internet to download virus definitions or updated files. Furthermore, Avaya recommends that you do not use a contact center application client PC to connect to the Internet. Instead, download virus definitions and updated files to another location on the customer network and manually load them from this interim location onto the contact center application platform.
- Perform the previous steps to download Contact Center application service packs (SP). This method limits access to the Internet, and thus reduces the risk of downloading infected files.
- Scan all SP files, DVD-ROMs, and floppy disks before you upload or install to the server. This practice minimizes any exposure to infected files from outside sources.
- Capacity considerations: running virus scan software can place an additional load on a contact center application platform. The implementation personnel must run the performance monitor tool on the server to gauge CPU usage. If the antivirus software scan causes the platform average CPU usage to exceed the recommended percentage for longer than 20 minutes, the antivirus software must not be loaded onto the contact center application platform.
- Product Support does not provide support on the configuration of antivirus software, but offer guidance where possible. Direct questions or problems on antivirus software to the appropriate vendor.
- If performance or functionality issues are raised to Avaya support personnel as part of the fault diagnosis, you might be asked to remove third-party utility software or antivirus software.

Página2031 de 3226.

Several maintenance tasks are automatically activated at 12:00 midnight. Therefore, you must schedule virus scans at a time other than midnight.

Avaya recommends that you exclude the following files and folders from scans (both real-time and scheduled):

- `F:\Avaya\Contact Center\Databases\`
- `<additional database drive>:\Avaya\Contact Center\Databases\`
- TSM_OAM files located in the following folders:
  - D:\Avaya\Contact Center\Manager Server\iccm\bin\data
  - D:\Avaya\Contact Center\Manager server\iccm\data
  - D:\Avaya\Contact Center\Manager Server\iccm\sdm\log
- `D:\Avaya\Contact Center\Manager Server\bin\tools2.exe` File access errors occur in the Scan Activity log if you do not exclude this file from scanning.
- `D:\Avaya\Contact Center\Manager Server\iccm\logs` (SIP logs)
- `D:\Avaya\Contact Center\Manager Server\iccm\sgm\config\` (SIP log configuration files)
- `D:\Avaya\Contact Center\Common Components\CMF`
- `D:\Avaya\Contact Center\Manager Administration\Apps\` (including sub-directories)
- The folder where you store Service Packs and patches

Contact Center Multimedia interacts with an external email system and enables agents to send attachment files from their computers to the Avaya Contact Center Select server. Both methods of retrieving data are potential sources of software infection.

Avaya recommends the following guidelines for antivirus software:

- Antivirus software must be installed on the email server to ensure that problems are caught at source.
- Agent computers require antivirus software to ensure that attachments sent to the Avaya Contact Center Select server do not have a virus. Contact Center Multimedia does not block specific attachment file types. Third-party antivirus software must be installed on the Portal Server according to guidelines in this document for such utilities.
- Ensure the antivirus software is configured to permit outbound email messages. For example, configure the McAfee antivirus software *Access Protection* option not to block *Prevent mass mailing worms from sending mail*. Alternatively, add the Contact Center Multimedia “EmailManager.exe” process to the McAfee *Processes to exclude* list.

  Exclude the Contact Center Multimedia database partition from being scanned.
- If firewalls on individual computers are enabled on the Agent Desktop computer, the Report Listener might be flagged as trying to access the Internet. The properties must be configured to allow access for the Report Listener to Contact Center Multimedia through the firewall.

Página2032 de 3226.

- You must not enable the Microsoft Updater to Auto-Run. Microsoft Updater is configured to alert level so you can schedule updates for off- peak hours.

Warning:

Running a Virus Scan on the Contact Center Multimedia attachment folder, which contains thousands of files, can use significant CPU time on a server and can cause drastic slowdown in agent's response times. Avaya recommends that you run scans, if necessary, during off-peak hours.

To avoid database integrity problems, Avaya recommends that you exclude all CACHE.DAT files, journal files, the cache.cpf file, and any Caché-related files from antivirus scans.

Caché software is installed in `<Install_drive>:\Avaya\Cache\CacheSys`. Databases and journal files are installed in `<Install_drive>:\Avaya\Contact Center\Databases`.

Exclude the Caché Journal file folder; `G:\Avaya\`

For Avaya Aura® Media Server, you must exclude the following files and folders from scans (both real-time and scheduled):

- `D:\Avaya\MAS\Multimedia_Applications\MAS\platdata`
- `D:\Avaya\MAS\Multimedia_Applications\MAS\common\log`

Hardware Appliance Licensing

The Avaya Contact Center Select Hardware Appliance deployment option uses a Nodal Enterprise license delivered as a WebLM XML file. This license file is used to control access to licensed features such as multimedia contacts and multiplicity.

Contact Center License Manager provides central control and administration of licensing for Avaya Contact Center Select. Each Contact Center License Manager includes a local instance of WebLM. When the Contact Center License Manager service starts, it extracts WebLM license keys from the local WebLM instance. Contact Center License Manager then converts the WebLM license keys into local PLIC license keys and distributes the keys the Avaya Contact Center Select applications as required.

- Obtain the WebLM Host ID for your Avaya Contact Center Select server.
- Use the WebLM Host ID to obtain a nodal WebLM license file from the Avaya Product Licensing and Delivery System (PLDS).
- You load the license file onto the Avaya Contact Center Select server as you run the configuration utility when you are deploying the Avaya Contact Center Select server. You can also load the license file after the configuration process. When Contact Center License Manager loads the license, if the unique number in the license does not match theWebLM Host ID, then License Manager shuts down and Avaya Contact Center Select cannot process contacts. If the unique number in the license matches the WebLM Host ID, then License

Manager provides license keys, and Avaya Contact Center Select processes customer contacts.

Página2034 de 3226.

Chapter 7: Solution capacity limits and supported features

This section specifies the maximum capacity limits of Avaya Contact Center Select. This section also specifies the telephony features and devices supported by Avaya Contact Center Select.

- Avaya Contact Center Select maximum capacity limits on page 120
- Avaya Contact Center Select maximum configuration limits on page 123
- Avaya Contact Center Select supported features on page 123
- Supported Telephony Features on page 129
- Supported Telephony Devices on page 138
- Remote access support on page 140
- Communication Control Toolkit supported functionality on page 140

Avaya Contact Center Select maximum capacity limits

The maximum capacity for your solution is determined by your Avaya Contact Center Select deployment and the IP Office voice and call recording platform and Release.

You can install the Avaya Contact Center Select DVD on any server that meets the Platform Vendor Independence (PVI) server specifications. The Avaya Contact Center Select DVD supports three levels of PVI server specification; Entry-level, Mid-range, and a High-end PVI server specification. The maximum capacity figures for the Avaya Contact Center Select DVD depend on which PVI server specification is used. The High-end specification supports Avaya Contact Center Select to its maximum rated capacity.

The Avaya Contact Center Select software appliance is a set of virtualized servers; an Avaya Contact Center Select virtual machine, an Avaya Aura® Media Server OVA, and a WebLM OVA. You can deploy the Avaya Contact Center Select software appliance on a VMware ESXi host server that provides the required resources.

The Avaya Contact Center Select hardware appliance is a physical rack mount server with the application software already loaded and partially preconfigured. The supplied rack mount server supports Avaya Contact Center Select to its maximum rated capacity.

Página2035 de 3226.

The following table specifies the maximum capacity values supported by the Avaya Contact Center Select deployment types for each supported IP Office configuration.

Server type	Maximum Capacity	IP Office (IPO) configuration					
		IPO SE 10.1 or 11.0 R630, R620, DL360	**IPO SE - DL120**	**IPO 500V2 SIP trunks no CR**	**IPO 500V2 SIP trunks with CR**	**IPO 500V2 TDM trunks no CR**	**IPO 500V2 TDM trunks with CR**
Entry-Level Server	Maximum logged-in agents See Note 3	60	60	60	30	40	30
	Maximum CCMA supervisors	10	10	10	10	10	10
	Maximum System Contact Rate See Note 1	1200	1200	1200	600	800	600
	Maximum multimedia rate (WCph / Eph) See Note 2	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300
Mid-Range Server	Maximum logged-in agents See Note 3	150	125	60	30	40	30
	Maximum CCMA supervisors	30	30	30	30	30	30
	Maximum System Contact Rate See Note 1	3000	2500	1200	600	800	600
	Maximum multimedia rate (WCph / Eph) See Note 2	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600
High-End Server and Software Appliance	Maximum logged-in agents See Note 3	400 See Note 4	125	60	30	40	30
	Maximum CCMA supervisors	80	50	50	30	40	30
	Maximum System Contact Rate See Note 1	8000	2500	1200	600	800	600
	Maximum multimedia rate (WCph / Eph) See Note 2	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200
Hardware Appliance	Maximum logged-in agents See Note 3	400	125	60	30	40	30

Table continues…

Página2036 de 3226.

Server type	Maximum Capacity	IP Office (IPO) configuration					
		IPO SE 10.1 or 11.0 **R630, R620, DL360**	**IPO SE - DL120**	**IPO 500V2 SIP trunks no CR**	**IPO 500V2 SIP trunks with CR**	**IPO 500V2 TDM trunks no CR**	**IPO 500V2 TDM trunks with CR**
	Maximum CCMA supervisors	80	50	50	30	40	30
	Maximum System Contact Rate See Note 1	8000	2500	1200	600	800	600
	Maximum multimedia rate (WCph / Eph) See Note 2	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200

- **Note 1:** The System Contact Rate is the total maximum combined contact rate across all supported contact types.
  - For System Contact Rate calculations, Web chat contacts have a weighting equivalent to 2 email messages. One Web chat is equivalent to two email messages.
  - For System Contact Rate calculations, the total maximum number of supported contacts per hour = (Voice + Email + (Web chat * 2))
  - *Route to CDN* and *Transfer/Conference to CDN* each count as two calls.
  - Complex call flows with transfer and conference scenarios de-rate the supported number of concurrent contacts.
- **Note 2:** Multimedia contact rates are applicable only if Contact Center Multimedia (CCMM) is part of the solution. Email contacts per hour (Eph). Web chats per hour (WCph). Web chat capacity is based on a maximum of 500 simultaneous chat sessions with an average chat duration of 5 minutes.
- **Note 3**: This figure is also the combined maximum number for simultaneous use of Agent Desktop and the Agent Browser application. For example, on a high-end server Avaya Contact Center Select supports 350 Agent Desktops and 50 Agent Browser applications.
- **Note 4**: The incoming lines on IP Office (IP Office Line or IP Office SIP Line) that target inbound calls at Avaya Contact Center Select must have Direct Media enabled to support more than 250 simultaneously logged-in agents.

  With 400 Agents concurrently active on simple calls (no conference or transfer calls), the maximum number of calls in queue is 200. This figure is based on the maximum number of available sessions on Avaya Aura® Media Server.
- IP Office Call Recording (CR) is supported with IP Office 500V2. Avaya Contact Center Select supports Call Recording up to the maximum number of supported logged-in agents. Above this maximum limit, no one can leave a voicemail or record any other calls.

Página2037 de 3226.

Server type	ACCS specification	IP Office platform						
		IPO SE R620/R630	IPO SE DL360	IPO SE DL120	IPO 500V2 SIP Trunks No CR	IPO 500V2 SIP Trunks With CR	IPO 500V2 TDM Trunks No CR	IPO 500V2 TDM Trunks With CR
Entry-level Server	Logged-in agents	60	60	60	60	30	40	30
	CCMA Supervisors	10	10	10	10	10	10	10
	System Contact Rate	1200	1200	1200	1200	600	800	600
	MM Rate (WCph/Eph)	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300	150 / 300
Mid-range Server	Logged-in agents	150	150	125	60	30	40	30
	CCMA Supervisors	30	30	30	30	30	30	30
	System Contact Rate	3000	3000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600	300 / 600
High-end Server	Logged-in agents	400	400	125	60	30	40	30
	CCMA Supervisors	80	80	50	50	30	40	30
	System Contact Rate	8000	8000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200
Hardware Appliance	Logged-in agents	400	400	125	60	30	40	30
	CCMA Supervisors	80	80	50	50	30	40	30
	System Contact Rate	8000	8000	2500	1200	600	800	600
	MM Rate (WCph/Eph)	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200	600 / 1200

Figure 11: The maximum capacity values supported by the ACCS deployment types for each supported IP Office (IPO) configuration

Avaya Contact Center Select maximum configuration limits

The following table specifies the maximum overall configuration values supported by Avaya Contact Center Select.

Parameter	Maximum value
Maximum configured agents	1500
Maximum agents skillsets	3000
Maximum skillsets per agent	20
Maximum agents per skillset	400
Maximum supervisors per skillset	80
Maximum supervisors per system	600

Avaya Contact Center Select supported features

The following table specifies the main features supported by Avaya Contact Center Select:

Página2038 de 3226.

Feature	Supported	Provider
Voice Skills Based Routing	Yes	Avaya Contact Center Select
FIFO Queuing	Yes	Avaya Contact Center Select
Longest Idle Agent queuing	Yes	Avaya Contact Center Select
ANI Number Available	Yes	Avaya Contact Center Select
ANI Number Routing	Yes	Avaya Contact Center Select
DNIS Number Available	Yes	
DDI Number Routing	Yes	Avaya Contact Center Select
Night Service	Yes	Avaya Contact Center Select
Threshold overflow for skills	Yes	Avaya Contact Center Select
Visual External Alarm for exceeded threshold	Yes	Avaya Contact Center Select
Voice Contact Classification	Yes	Avaya Contact Center Select and Agent Desktop
Multi-parameter Screen Pop per contact type per skillset	Yes	Avaya Contact Center Select
Music On Hold	Yes	IP Office
Multi Source Music on Hold	No	
On–Hold Announcements	No	
Skill Announcements	Yes	Avaya Contact Center Select
Agent Ext In/DN Key	Yes	Avaya Contact Center Select and IP Office with three line appearance
Coverage to Voicemail Pro	Yes	Direct calls to an agent station receive the configured coverage treatment. Calls routed from Avaya Contact Center Select to Agents do not receive coverage treatment.
Play Prompt and Collect Digits	Yes	Avaya Contact Center Select
Wallboards with API	Yes	Dev Connect and Avaya Contact Center Select
Activity /Work Codes	Yes	Avaya Contact Center Select
Aux/Not Ready Reason Codes	Yes	Avaya Contact Center Select
After Call Work Codes	Yes	Avaya Contact Center Select
Real Time Display Indication ACW/Act/AUX/NotRdy Codes	Yes	Avaya Contact Center Select
Three Line Operation (3 call appearance lines)	Yes	Avaya Contact Center Select and IP Office

Table continues…

Página2039 de 3226.

Feature	Supported	Provider
Browser Based Agent Desktop	Yes	Avaya Contact Center Select and Agent Desktop Agent Desktop client is deployed using either the click-once deployment or an MSI file.
Browser Based Supervisor Desktop	Yes	Avaya Contact Center Select and Agent Desktop Supervisor Administration client use Internet Explorer based CCMA. Supervisor Agent client is deployed using either the click-once deployment or an MSI file.
Toll Free Queuing	Yes	Avaya Contact Center Select
Telephone Only Mode operation	No	
TLS transport type	Yes	Between IP Office and Avaya Contact Center Select
Report Creation Wizard	Yes	Avaya Contact Center Select
Media Server Zoning	No	
Contact Center Network Based Routing	No	
Mission Critical High Availability	No	Avaya Contact Center Select Business Continuity is supported.
Remote/Off-Site agent support	Yes	IP Office
IPv6 networking	No	
Database customization – import new Customer defined fields	No	

The following table specifies the multimedia features supported by Avaya Contact Center Select:

Feature	Sub feature	Supported	Provider
Multimedia Skills Based Routing		Yes	
Multimedia Management & Reporting		Yes	Avaya Contact Center Select
Multiplicity		Yes	Avaya Contact Center Select
Email Contact Handling		Yes	Avaya Contact Center Select

Table continues…

Página2040 de 3226.

Feature	Sub feature	Supported	Provider
	Email Auto Response	Yes	Avaya Contact Center Select
	Email Auto Acknowledge	Yes	Avaya Contact Center Select
	Customer Contact History	Yes	Avaya Contact Center Select
	Email Real Time Reporting	Yes	Avaya Contact Center Select
	Screen Pop based on Email	Yes	Avaya Contact Center Select
	Fax Contact Types	Yes	Avaya Contact Center Select
	Scanned Documents	Yes	Avaya Contact Center Select
	SMS Contact Inbound	Yes	Avaya Contact Center Select
Web Communications		Yes	Avaya Contact Center Select
	Web Chat	Yes	Avaya Contact Center Select
	Web Call-back	Yes	Avaya Contact Center Select
	Co-browsing	No	
Outbound	Preview/Progressive	Yes	Avaya Contact Center Select
Self Service Integration			
	Self Service Data and CTI to external IVR	No	
	On board Avaya Aura® Media Server IVR - play prompt and collect digits	Yes	
Workforce Optimization			
	Bulk Voice Recording	No	Avaya Contact Center Select
	Selective Recording	No	Using IP Office button
	Agent Initiated	No	Using IP Office button
	Quality Monitoring	No	
Workforce Management/ Forecasting		No	

Table continues…

Feature	Sub feature	Supported	Provider
External Threshold Alerter/Alarms		No	
Multi-Site Reporting		Yes	For distributed agents in an SCN network.
Supervisor /Agent Instant Messaging		No	
OPEN QUEUE Contact Types		Yes	
SOA Enabled		No	
IM (Routed) Contact Types		No	
Predictive Outbound		No	
Agent Desktop Softphone – H.323 or SIP		No	
Agent Greeting		No	

The following table specifies the reporting features supported by Avaya Contact Center Select:

Feature	Sub feature	Supported	Provider
Unified Multi Channel Real-time and Historical Reporting		Yes	Avaya Contact Center Select
Predefined Real-time and Historical Reports		Yes	Avaya Contact Center Select
Customer Customizable Reports		Yes	Avaya Contact Center Select
Customer Definable Reports		Yes	Using third-party tools interfacing using Avaya Contact Center Select ODBC
Report Creation Wizard (RCW)		Yes	Avaya Contact Center Select
Historical Reports			
	Scheduled	Yes	Avaya Contact Center Select
	Interval	Yes	Avaya Contact Center Select
	Daily	Yes	Avaya Contact Center Select

Table continues…

Feature	Sub feature	Supported	Provider
	Weekly	Yes	Avaya Contact Center Select
	Monthly	Yes	Avaya Contact Center Select
	Quarterly	No	
	Skillset	Yes	Avaya Contact Center Select
	Trunk	No	
	Agents	Yes	Avaya Contact Center Select
	Abandoned Contacts	Yes	Avaya Contact Center Select
	Overflow Contacts	Yes	Avaya Contact Center Select
	Threshold Exceeded	Yes	Avaya Contact Center Select
	Contact Classification	Yes	Avaya Contact Center Select
	Source Of Disconnect	Yes	Avaya Contact Center Select
	Agent Station Key	No	
	Email Report Notifications	Yes	Avaya Contact Center Select
	System Status Reports	Yes	Avaya Contact Center Select

The following table specifies Avaya Contact Center Select product interoperability:

Product name	Supported
Avaya Aura® Workforce Optimization (WFO)	No. Use IP Office call recording.
Avaya Workforce Optimization Select (AWFOS)	Yes, Release 5.2, 5.2.1, and 5.3.
Proactive Outreach Manager (POM)	No
Avaya Aura® Experience Portal	Yes, Release 7.1, 7.2, and 7.2.1.
Avaya IQ Reporting	No
Avaya Control Manager Agent and Supervisor Administration	No
Avaya Proactive Contact	No
Avaya one-X® Agent	No

Table continues…

Página2043 de 3226.

Product name	Supported
Social Media Manager	Yes (using the email contact type). Release 6.2.13 or later.
Avaya Aura® Presence Services	No
Avaya Communicator for Windows	Yes, softphone support.
Microsoft Lync (Release 2010 and 2013) and Microsoft Skype for Business 2015	Peer-to-peer IMs are supported. Routed IMs are not supported.

The following table specifies the Open Interfaces supported by Avaya Contact Center Select:

Open Interface name	Supported
Real-time Statistics Multicast (RSM)	Yes
Real-Time Display (RTD)	Yes
Database Integration Wizard (DIW) and Host Data Exchange (HDX)	Yes
Contact Center Multimedia (CCMM) Advanced Email Services	Yes
Contact Center Manager Administration (CCMA) Open Interfaces	Only for IP Office user data synchronization with Avaya Contact Center Select
Contact Center Multimedia Open Interfaces	Only for standard Web Chat communications (not supported for Agent Desktop).
Contact Center Multimedia Outbound Open Interfaces	Yes
Communication Control Toolkit (CCT) Open Interfaces	No
Open Queue	Yes
Open Networking	No
Meridian Link Services (MLS)	No
Communication Control Toolkit .NET SDK	Yes
Contact Control Service SDK	Yes
Contact Center Manager Server (CCMS) Open Interfaces	No
Avaya Contact Recording APIs	No
Salesforce Server Side support	Yes

Supported Telephony Features

The following tables list the IP Office telephony features available to a non-agent IP Office user and specify which features are supported on an Avaya Contact Center Select agent station.

Página2044 de 3226.

Basic Call Handling:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Tones	Yes	Yes	No	No	Agent Desktop does not play specific tones dependent on geography.
Caller ID	Yes	Yes	Yes	Yes	
Call Screening	Yes	No	No	No	
Hold	Yes	Yes	Yes	Yes	
Toggle Calls	Yes	Yes	No	No	Toggle calls is not applicable to Avaya Contact Center Select agents with 3-line appearance.
Hold Call Waiting	Yes	Yes	No	No	Same as Auto-hold-allowed.
Hold Music (Music on Hold)	Yes	Yes	Yes	Yes	Provided by IP Office.
Park	Yes	No	No	No	
Automatic Callback	Yes	No	No	No	
Direct Inward Dialing (DID/ DDI)	Yes	Yes	Yes	Yes	
Transfer	Yes	Yes	Yes	Yes	
Distinctive and Personalized Ringing	Yes	No	No	No	
Personalized Ringing	Yes	Yes	No	No	
Message Waiting Indication (MWI)	Yes	No	No	No	Supported on some physical stations. Not supported by Agent Desktop. Contact Center (CC) calls are prevented from going to voicemail so cannot result in MWI light on telephone. However, an agent handling a CC call sees the MWI light on their telephone if a personal

Table continues…

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
					call results in a new voicemail message while handling the CC call.
Visual Voice	Yes	No	No	No	Supported on some IP Office stations only and not by Agent Desktop. Contact Center (CC) calls are prevented from going to voicemail so cannot result in messages that can be processed using Visual Voice on telephone. However, an agent servicing a CC call can use Visual Voice on their telephone while servicing the CC call.

Advanced Call Handling:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Absence Text	Yes	Yes	No	No	
Call Tagging	Yes	Yes	No	No	The Call Tagging feature is equivalent to the Avaya Contact Center Select Call Attached Data feature.
Reclaim Call	Yes	No	No	No	
Hunt Group Enable/Disable	Yes	Yes	No	No	Ability of a user to enable and disable their membership of hunt groups.
Call Waiting	Yes	N/A	Yes	N/A	If an Avaya Contact Center Select agent is active on a call, then another CC call is not routed to that agent. If an Avaya Contact Center Select agent is active on

Table continues…

Página2046 de 3226.

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
					personal call, a CC call is not routed to the agent.
Do Not Disturb (DND)	No	No	No	No	Avaya Contact Center Select agents use NotReady (with reason code).
Dial Plan	N/A	N/A	N/A	N/A	Refers to the dial plan configuration on the IP Office. Configure a dial plan to route calls to extensions and agents.
Paging	Yes	Yes	No	No	Telephone must have a loudspeaker.
Intrude	Yes	Yes	No	No	Avaya Contact Center Select Supervisors can use Observe or Barge-in features.
Inclusion	Yes	Yes	No	No	
Private Call	Yes	Yes	No	No	
Hot Desking	Yes	Yes	N/A	N/A	This feature allows a number of users' non-exclusive use of the same extension. Once logged in, any calls to that user are routed to the physical extension they are logged in at.
Remote Hot Desking	Yes	Yes	N/A	N/A	This feature is the same as 'Hot Desking' but refers specifically to a user configured on a particular node logging in to an extension configured on another node in the Small Community Network (SCN).
Relay On/Off/ Pulse	N/A	N/A	N/A	N/A	
Pickup	Yes	No	No	No	
Call Recording	Yes	Yes	No	No	
Telecommuter Mode	No	No	No	No	
Twinning and Mobility	No	No	No	No	

Página2047 de 3226.

Key and Lamp Operation:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Appearance Buttons	N/A	N/A	N/A	N/A	
Line Appearance	N/A	N/A	N/A	N/A	Three lines maximum. A Line Appearance is a representation of a trunk line on the IP Office system where the indicator tracks the activity on the Line. Only external calls can be answered or made on Line Appearances.
Call Appearance Buttons	Yes	Yes	No*	No*	Individual calls are represented individually on Agent Desktop, but there is no concept of selecting a particular call appearance button which corresponds to the telephone.
Alerting/Ring Tone for Covered Calls	Yes	No	No	No	IP Office blocks Avaya Contact Center Select calls from covering.
Bridged Appearance Buttons	No	No	No	No	
External Call Lamp Indication	Yes	No	No	No	
Call Coverage	Yes	No	Yes	No	IP Office blocks Avaya Contact Center Select calls from covering.
Call Coverage Buttons	Yes	N/A	No	N/A	

Outbound Call Handling:

Página2048 de 3226.

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Account Codes	Yes	Yes	No	No	
Authorization Codes	Yes	Yes	No	No	
Dial Emergency	Yes	N/A	No	No	The Dial Emergency feature is equivalent to the ACCS Emergency Call feature.
Call Barring	N/A	N/A	N/A	N/A	Avaya Contact Center Select independent

Alternate Route Selection (ARS):

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Maximum Call Length	Yes	Yes	Yes	Yes	Avaya Contact Center Select independent
Transferable Dial Out Privilege	Yes	N/A	No	N/A	Avaya Contact Center Select independent
Idle Line Preference	Yes	N/A	No	N/A	Avaya Contact Center Select independent
Alternate Route Selection	N/A	N/A	N/A	N/A	Configure IP Office to select appropriate trunk to route calls on.

Forwarding:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Coverage to Operator	Yes	No	No	No	
Forward on Busy	Yes	No	No	No	

Table continues…

Página2049 de 3226.

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Forward on No Answer	Yes	No	No	No	
Forward Unconditional	Yes	No	No	No	
Unconditional Forward to Voicemail	Yes	No	No	No	
Forward Hunt Group	Yes	No	No	No	
Follow Me	Yes	No	No	No	

Avaya telephone features:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Programmable Buttons	Yes	Yes	No	No	
Busy Lamp Field (BLF) Indicators	Yes	Yes	No	No	Avaya Contact Center Select independent
Call History	Yes	Yes	No	No	
Language	Yes	Yes	No	No	Agent Desktop language is determined by the OS settings on the Agent Desktop client computer, not from the language configured for the IP Office extension.
Centralized Personal Directory	Yes	Yes	No	No	
Centralized System Directory	Yes	Yes	No	No	
Self-Administration	No	No	No	No	Avaya Contact Center Select agents are not allowed to modify telephone properties.

Table continues…

Página2050 de 3226.

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
On Hook Dialing	Yes	Yes	Yes	Yes	

Inbound Call Handling. Applies only in Failover Mode to IP Office Hunt Groups:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Incoming Call Routing	Yes	Yes	Yes	Yes	IP Office system configuration decides where incoming calls are routed. Once call routing is configured, calls to agents are displayed on the telephone and in Agent Desktop.
Hunt Groups	Yes	N/A	Yes	N/A	
Multi-site Networking/ Small Community Networking (SCN) Distributed Hunt	Yes	N/A	Yes	N/A	
Night Service	Yes	N/A	Yes	N/A	
Time Profiles	Yes	No	Yes	No	
Queuing	Yes	N/A	Yes	N/A	Configure system to limit the number of calls that can be waiting to be serviced in a hunt group. For example, when all parties in the group are busy.
Announcements	Yes	N/A	Yes	N/A	Configure system to play announcements to calls waiting to be services in a hunt group.

Contact Center features:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Acquire Call (Call Steal)	Yes	No	No	No	Acquire Call can behave like 'Reclaim Call' or 'Call Pickup' depending on how it is invoked and the state of the two users involved.
Monitor Calls	Yes	No	No	No	A user can monitor other party's calls by listening in.
Queue Threshold Alert	N/A	N/A	N/A	N/A	Queue Threshold Alert applies only in Failover Mode to IP Office Hunt Groups.
Login	N/A	N/A	N/A	N/A	Login applies only in Failover Mode to IP Office Hunt Groups.

System Short Codes:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
User Short Codes	Yes	Yes	No	No	
System Short Codes	Yes	Yes	No	No	
Post-Dialing Short Codes	Yes	Yes	No	No	
Incoming Number Short Codes	Yes	Yes	No	No	

Miscellaneous Features:

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Conference Calls	Yes	Yes	Yes	Yes	

Table continues…

IP Office telephony feature name	IP Office user station support		Avaya Contact Center Select agent station support		Notes
	Personal calls	CC calls	Personal calls	CC calls	
Coaching/Silent Intrusion/ Whisper Page	Yes	Yes	No	No	
Dial On Pickup	No	No	No	No	This IP Office feature is also known as Hotline. The feature automatically dials a specified extension when the telephone is taken off hook. Do not configure this feature for Avaya Contact Center Select agents.
Off Hook Operation	N/A	N/A	N/A	N/A	Analog station feature not supported by Avaya Contact Center Select.
E911 Emergency Call	Yes	N/A	Yes	N/A	

Supported Telephony Devices

This section specifies the telephony connection types and devices supported in an Avaya Contact Center Select solution. The Avaya Contact Center Select solution supports all of the IP Office platform trunks types. There is no direct integration between the Avaya Contact Center Select and IP Office trunking interfaces. The Avaya Contact Center Select contact center functionality is independent of these IP Office trunks.

The following table lists the stations and telephone types supported by Avaya Contact Center Select.

Agent Phone	Phone Model	Avaya Contact Center Select Supported	Notes
Analogue – All Models		No	
Digital	9500 Series	Yes	
	1400 Series	Yes	
	5400 Series 2400 Series	Yes	The 5400 series is not supported with IP Office 10.x or later.

Table continues…

Agent Phone	Phone Model	Avaya Contact Center Select Supported	Notes
IP: H.323	96x1	Yes	
	96x0	Yes	
	J129 IP deskphone J139 IP deskphone J169 IP deskphone J179 IP deskphone	Yes	Supported only with IP Office 11.0 or later.
	1600 Series	Yes	
	5600 Series 4610/4620x	Yes	Not supported with IP Office 10.x or later.
IP: SIP	IP Phone 1140E Model NTYS05 IP Phone 1230 Model NTYS20 IP Phone 1120e IP Phone 1220 J129 IP deskphone J139 IP deskphone J169 IP deskphone J179 IP deskphone	Yes	Supported when running IP Office SIP firmware. The 1120e and 1220 IP phones are supported only with IP Office 10.x or later. The J-series IP deskphones are supported only with IP Office 11.0 or later.
DECT – All Models		No	
Wi-Fi Wireless – All Models		No	
Avaya Communicator for Windows		Yes	Softphone support with IP Office.
IP Office Softphone		Yes	Supported as co-resident softphone on agent workstation with Agent Desktop. Not supported as integrated softphone.

The following table shows the Avaya Contact Center Select agent experience for various phone types.

Phone Type	Skillset on Agent Desktop		Skillset on the phone		PSTN Number	Recording Indication
	Ringing	Connected	Ringing	Connected		
96x0 (9640)	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

Phone Type	Skillset on Agent Desktop		Skillset on the phone		PSTN Number	Recording Indication
	Ringing	Connected	Ringing	Connected		
96x1 (9641)	Yes	Yes	Yes	Yes	Yes	Yes
J129	Yes	Yes	Yes	Yes	Yes	Yes
J139	Yes	Yes	Yes	Yes	Yes	Yes
J169	Yes	Yes	Yes	Yes	Yes	Yes
J179	Yes	Yes	Yes	Yes	Yes	Yes
56xx (5610)	Yes	Yes	Yes	No	Yes	Yes
46xx (4610)	Yes	Yes	Yes	No	Yes	Yes
16xx (1616)	Yes	Yes	Yes	Yes	Yes	Yes
Softphone	Yes	Yes	Yes	Yes	Yes	No
95xx (9504)	Yes	Yes	Yes	Yes	Yes	No
54xx (5410)	Yes	Yes	Yes	No	Yes	Yes
24xx (2420)	Yes	Yes	Yes	No	Yes	Yes
14xx (1408)	Yes	Yes	Yes	Yes	Yes	Yes

Remote access support

Avaya Contact Center Select supports remote access using the following:

- Microsoft Windows Remote Desktop
- IP Office Support Services (IPOSS)

Both of these support remote troubleshooting and technical support.

Communication Control Toolkit supported functionality

This section compares the features supported by Avaya Contact Center Select using Avaya IP Office with the features supported by Avaya Aura® Contact Center using Avaya Aura® Communication Manager or Avaya Communication Server 1000 (CS 1000).

Communication Control Toolkit and Agent Desktop implement and use these features. Agent Desktop is a client of Communication Control Toolkit so they support the same features.

The following tables list the basic Communication Control Toolkit call control functions.

Página2055 de 3226.

Table 6: Basic Communication Control Toolkit and Avaya Agent Desktop functions

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
Make Call	Yes	Yes	Yes
Hold Current Call	Yes	Yes The CS 1000 Swap Hold switch feature is not supported.	Yes
Unhold Call	Yes (Retrieve Call)	Yes (Retrieve Call)	Yes
Drop Current Call (Release)	Yes	Yes	Yes
Blind Transfer Call	No	Yes	No
Initiate Supervised Transfer	Yes	Yes	Yes
Complete Transfer	Yes	Yes	Yes
Initiate Conference Call	Yes	Yes (up to six parties)	Yes
Complete Conference Call	Yes	Yes	Yes
Call Forward	No	Yes	No
Cancel Call Forward	No	Yes	No
Join Conference	Yes, Avaya Aura® only	No	Yes
Deflect Calls	No	No	No
Get Status	Yes	Yes	Yes
Get Call Capabilities	Yes	Yes	Yes
Get Data	Yes	Yes	Yes
Delete Data	Yes	Yes	Yes
Append Data	Yes	Yes	Yes
Make Set Busy (Do Not Disturb)	No	Yes (on Agent Terminals only)	No
Get/Set UUI	Yes	No (UUI attached as call data)	Yes
Send DTMF (for example, credit card number to IVR)	Yes	Yes	Yes
Mute/Unmute	No	No	No
Consult	Yes	Yes (but must designate as transfer or conference)	Yes
Park/Unpark	No	No	No
Message Waiting Indicator	No	No	No

Table continues…

Página2056 de 3226.

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
HER (Host Enhanced Routing)	No	Yes	No
Answer	Yes	Yes	Yes

The fast transfer functionality does not support completing a fast transfer call to an external trunk number. This functionality is for predictive dialing environments in which the application sends a MakeCall request to an external customer number and, when the customer answers, the application sends the FastTransfer request to blind transfer the customer to a live agent.

The following table lists the Contact Center specific functions supported by Agent Desktop and Communication Control Toolkit.

Table 7: Contact Center-specific functions

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
Agent Login	Yes	Yes	Yes
Agent Logout	Yes	Yes	Yes
Set Ready	Yes	Yes	Yes
Set Not Ready	Yes	Yes	Yes
ACD Set Activity Code	Yes	Yes	Yes
ACD Set Not Ready/Reason Code	Yes	Yes	Yes
ACD Set After Call Work Item Code	Yes	Yes	Yes
Work Ready Key support	No	No	No
Agent Whisper	No	No	No
Observe call	Yes	No	Yes
Set Call treatment	No	Yes	No
Barge In	Yes	No	Yes
Call Supervisor	Yes	Yes	Yes
Emergency Key	Yes	Yes	Yes
Redirect to another skillset	No, must transfer to a CDN (Route Point)	No	No, must transfer to a CDN (Route Point)
Return a call to the queue skillset that it came from	No	No	No
Redirect to another skillset	No	No	No
Return a call to the queue skillset that it came from	No	No	No

Página2057 de 3226.

The following table lists the events delivered by Communication Control Toolkit.

Table 8: Communication Control Toolkit events

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
Ringing Event	Yes	Yes	Yes
Dialtone Event	No	No	No
Busy Event	No	No	No
Offering Event	Yes	Yes	Yes
Ringback Event	Yes	Yes	Yes
Inbound Connected Event	Yes	Yes	Yes
Outbound Connected Event	Yes	Partial	Yes
Connected Event	Yes	Yes	Yes
Disconnected Event	Yes	Yes	Yes
Held Event	Yes	Yes	Yes
Unheld Event	Yes	Yes	Yes
OnHold Pending Conference Event	Yes	Yes	Yes
Onhold Pending Transfer Event	Yes	Yes	Yes
Transferred Event	Yes	Yes	Yes
Conference Event	Yes	Yes	Yes
Initiated Transfer Event	Yes	Yes	Yes
Initiated Conference Event	Yes	Yes	Yes
Session Disconnect Event (includes shutdown)	Yes	Yes	Yes
Device Forward Event	No	No	No
Status Change Event	Yes	Yes	Yes
Notice Message Waiting Event	No	No	No
Notice No Message Waiting Event	No	No	No
Agent Logged out Event	Yes	Yes	Yes
Agent Logged in Event	Yes	Yes	Yes
Agent Ready Event	Yes	Yes	Yes
Agent Not Ready Event	Yes	Yes	Yes
Agent Busy Event	No	No	No

Table continues…

Página2058 de 3226.

Event	SIP-enabled Avaya Aura® Contact Center with Avaya Aura®	AML-based Avaya Aura® Contact Center using CS 1000	Avaya Contact Center Select using IP Office
Agent Work Ready Event	No	No	No
Activity Code Entered	Yes	Yes	Yes
WalkAway Activated	No	No	No
WalkAway Return	No	No	No
Emergency Invoked	No	No	No
Call Supervisor Invoked	No	No	No

Página2059 de 3226.

Chapter 8: Avaya Aura® Experience Portal Integration

Avaya Aura® Experience Portal is an open standards-based self-service software platform which offers industry leading reliability and scalability to help reduce costs and simplify operations.

Avaya Aura® Experience Portal is deployed on standard Linux servers and it supports integration with SIP-enabled systems, including Avaya Contact Center Select and IP Office.

The Avaya Aura® Experience Portal system consists of an Experience Portal Manager (EPM), which controls the Experience Portal system and Media Processing Platform (MPP) servers, which process all calls. The Experience Portal system typically includes an Automatic Speech Recognition (ASR) server, Text-to-Speech (TTS) speech servers, and application servers.

Avaya Contact Center Select supports the following types of integration with Avaya Aura® Experience Portal:

- Front-end Avaya Aura® Experience Portal
- Back-end Avaya Aura® Experience Portal using SIP header information
- Back-end Avaya Aura® Experience Portal using Context Creation

In a front-end Avaya Aura® Experience Portal integration, the customer call is processed first by Avaya Aura® Experience Portal and then by Avaya Contact Center Select. In a back-end Avaya Aura® Experience Portal integration, the customer call is processed first by Avaya Contact Center Select and then by Avaya Aura® Experience Portal. Avaya Contact Center Select supports front-end and back-end Avaya Aura® Experience Portal integration in a single solution.

The following mechanisms support transferring calls and call data between Avaya Aura® Experience Portal and Contact Center:

- SIP header information. SIP includes a number of message headers in each SIP message. These headers contain information that enables the receiver to understand and use the message properly. In a contact center solution, SIP headers can be used to transfer small amounts of call-related information between SIP-enabled applications. Avaya Contact Center Select supports the User-to-User Information (UUI) SIP header and the Avaya custom P-Intrinsics SIP private header.
- SIP INFO message body using Context Creation: If your call-related context information does not fit in a SIP User-to-User Information (UUI) header or in the larger P-Intrinsics header, you can use the sample Context Creation application to pass more context information from Avaya Aura® Experience Portal to Avaya Contact Center Select. This sample Context Creation application can return multiple values from Avaya Aura® Experience Portal, rather than the single value returned by the sample Play and Collect application. The Context Creation sample

Página2060 de 3226.

application can return call-related context information in a SIP INFO message body. A SIP INFO message body holds and transfers much more information than a SIP header.

In an IP Office platform based solution, Avaya Contact Center Select supports the following methods of integration with Avaya Aura® Experience Portal:

- SIP header information
- SIP INFO message using Context Creation

There are no additional licensing requirements for Avaya Contact Center Select and Avaya Aura® Experience Portal integration.

Data transfer methods

The following table shows the maximum amount of data supported by each transfer type:

Transfer method	Maximum data supported by Contact Center
UUI SIP header using ASAI	96 bytes maximum.
P-Intrinsics SIP header	Depends on your solution. Note 1
SIP INFO message body using Context Creation	8K bytes total maximum: • Maximum of 10 ASCII key-value pairs. • And 1K characters of Call Attached Data (CAD) within the CC application.
Note 1 The following limitations apply to P-Intrinsics SIP header information: • The amount of P-Intrinsics information associated with a call depends on the other SIP headers in the call and on the call flow path. Typically, Contact Center supports up to 10 ASCII key-value pairs of P-Intrinsics.	

Contact Center supports ASCII key-value pairs with a key name of up to 25 characters and a value size of up to 80 characters.

Avaya Aura® Experience Portal Orchestration Designer

Avaya Aura® Experience Portal Orchestration Designer is an Eclipse-based application development environment which supports the development of Voice XML and CCXML speech applications. Orchestration Designer generates Avaya Aura® Experience Portal compliant XML-based applications which are deployed on software application servers such as Apache Tomcat Server in a self-service solution.

Página2061 de 3226.

Voice XML

Voice XML (VXML) is a standard XML format for specifying interactive voice dialogs between a human and a computer. Voice XML is designed for creating audio dialogs that feature synthesized speech, digitized audio, recognition of spoken and DTMF key input, recording of spoken input, telephony, and mixed initiative conversations. A typical Voice XML play and collect application plays voice prompts to customers asking them to enter digits using their phone. The application then collects the customer digits and returns them for processing to the contact center.

Call Control XML

Call Control XML (CCXML) is a standard markup language for controlling how phone calls are placed, answered, transferred, conferenced, and more. CCXML works with Voice XML to provide an XML-based solution for any telephony application. Voice XML and CCXML are two separate languages and are not required in an implementation of either language. For example, CCXML can be integrated with a more traditional Interactive Voice Response (IVR) system and Voice XML dialog systems can be integrated with other call control systems.

SIP-enabled Avaya Contact Center Select

Avaya Contact Center Select uses Session Initiation Protocol (SIP) architecture to provide maximum interoperability and flexibility. SIP-enabled Avaya Contact Center Select simplifies solution architecture and CTI deployments. Avaya Contact Center Select SIP-enabled architecture and Contact Intrinsic data make it easy to develop screen pop applications, reducing the time, effort, and cost required to launch new capabilities.

Contact Center Manager Server (CCMS) contains a SIP Gateway Manager (SGM) component which is the call processor in a SIP-enabled Contact Center. The SIP Gateway Manager is a standalone SIP element that can receive and process calls from SIP-enabled communication systems such as IP Office.

Avaya Contact Center Select supports User-to-User Information (UUI) SIP header information and P-Intrinsic SIP header information. Contact Center uses the header information in each SIP call to generate call-related Contact Intrinsic information and Call Attached Data (CAD). This Contact Intrinsic data can contain information relevant to that call, the calling customer, and other information retrieved by self-service or third party applications. Contact Intrinsics are key-value pairs of relatively small amounts of data. Call Attached Data is a longer unstructured amount of data.

In a SIP-enabled contact center solution, the information stored in some SIP INFO messages can be used to transfer call-related information between SIP-enabled components. This call-related information enables the receiver to better understand and handle the call. If your call-related context information does not fit in a SIP User-to-User Information (UUI) header or in the larger P-

Página2062 de 3226.

Intrinsics header, you can use the sample Context Creation application to pass more context information from Avaya Aura® Experience Portal to Avaya Contact Center Select. The Context Creation sample application can inject multiple pieces of context information (Intrinsics and Call Attached Data) into Avaya Contact Center Select, whereas the Play and Collect sample application can retrieve only a single piece of data, for example collected digits. The call-related context information is returned in a SIP INFO message body. A SIP INFO message body holds and transfers much more information than a SIP header.

Contact Intrinsic data enriches the context and information presented to agents with each customer contact. Contact Intrinsic data makes it easy to develop screen pops, reducing the time, effort and cost required to launch new capabilities. Avaya recommends that you use Contact Intrinsic data.

P-Intrinsic SIP Header

Avaya Contact Center Select supports the custom P-Intrinsics private header. The Session Initiation Protocol (SIP) includes a number of message headers in each SIP message. These headers contain information that enables the receiver to understand and use the message properly. In a contact center solution, you can use SIP headers to transfer small amounts of call-related information between SIP-enabled applications. The application receiving this SIP message reads these headers and performs some action based on the contents of the headers. SIP header information can provide additional data about a call that applications can use to process that call.

You can use P-Intrinsics header information to pass context information between SIP-enabled applications. Avaya Contact Center Select parses the P-Intrinsics SIP header information and uses it to create Contact Intrinsics or Call Attached Data. You can use P-Intrinsics in conjunction with User-to-User (UUI) information if backwards compatibility with existing applications is required.

SIP private headers (P-Headers) are purely informational. They do not create new commands and they do not interfere with the regular transmission of SIP messages. SIP private headers are used only to pass extra information that the receiving application can use. Avaya Contact Center Select supports the P-Intrinsics SIP header in incoming SIP INVITE messages.

Components that support this private header include front-end IVRs systems such as Avaya Aura® Experience Portal and other SIP-enabled entities in the call flow.

P-Intrinsics information is not restricted by legacy limitations like UUI. P-Intrinsics information can grow in size, depending on other headers in the call, and on the call flow path. It can also be used to inject call attached data. It is therefore more flexible than UUI data. You can use both headers together, and customers can retain backwards compatibility with applications that already use UUI data.

Typical solution using P-Intrinsics

A front-end Avaya Aura® Experience Portal system uses XML speech applications and SIP header information to integrate with Avaya Contact Center Select. A self-service Voice XML speech application running on the Avaya Aura® Experience Portal – Application Server answers customer calls and gathers call-associated information based on customer’s answers and inputs.

Página2063 de 3226.

Experience Portal then transfers the customer call, complete with this call-associated information stored in the P-Intrinsics SIP header, to Avaya Contact Center Select.

Contact Center uses the P-Intrinsics header to generate Contact Intrinsic and/or Call Attached Data specific to that call. If this call is ultimately answered by an agent, the agent can use the call-related Contact Intrinsic data to access customer details. The agents might receive the Contact Intrinsic data in a screen pop, or they might need to access these details manually using Agent Desktop.

P-Intrinsics reduce the amount of time the agents spend on each call, improve the customer experience, and make Contact Center more efficient.

User-to-User Information

SIP-enabled systems can use User-to-User Information (UUI) to transmit small amounts of data between systems within SIP header messages.

Voice XML applications can use SIP header information to collect, store, and transport customer call-related information. Voice XML application can use customer interview data to modify the SIP header, and then pass the customer call along with updated header data to the next application in the solution. Voice XML applications can also use SIP header information to make processing decisions about a customer call. Examples of SIP header UUI data include a customer account number obtained during a self-service customer interview.

Agent Desktop and Contact Center Orchestration Designer can also modify User-to-User Information.

This SIP header UUI data can be used to support Avaya Aura® Application Sequencing.

Universal Call Identifier

Universal Call Identifier (UCID) is an Avaya proprietary call identifier used to help correlate call records between different systems. Universal Call Identifier information, where enabled, is added to the User-to-User Information (UUI) data in SIP calls.

This identifier can be generated by Avaya Aura® Experience Portal MPP server. Universal Call Identifier can be passed to Avaya Aura® Experience Portal through an application's SIP headers.

Front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

A combined Avaya Aura® Experience Portal self-service system and Avaya Contact Center Select solution gives your customers exceptional service and improved efficiency. Front-end self-service automation reduces contact center operating costs and improves Customer Satisfaction (CSAT).

Avaya Aura® Experience Portal uses XML speech applications and SIP messaging-based information to integrate with Avaya Contact Center Select. A self-service Voice XML speech application running on the Avaya Aura® Experience Portal Tomcat application server answers customer calls and modifies the call-associated User-to-User Information (UUI) based on customer answers and inputs. When customer calls are transferred to Contact Center agents, the agents use the call-related Contact Intrinsic data to access customer details. This reduces the amount of time the agents spend on each call, improves customer experience, making Contact Center more efficient.

Avaya recommends that you create your XML speech applications with Avaya Aura® Orchestration Designer. Avaya Aura® Experience Portal automatically includes all Orchestration Designer applications in the Application Summary report and Application Detail report. If you want these reports to display messages and status information from an application developed in a third-party tool, you must manually log the messages and status information from that application using the Application Logging Web service.

The following diagram shows a typical solution layout of a front-end Avaya Aura® Experience Portal self-service integration with Avaya Contact Center Select and IP Office.

Página2065 de 3226.

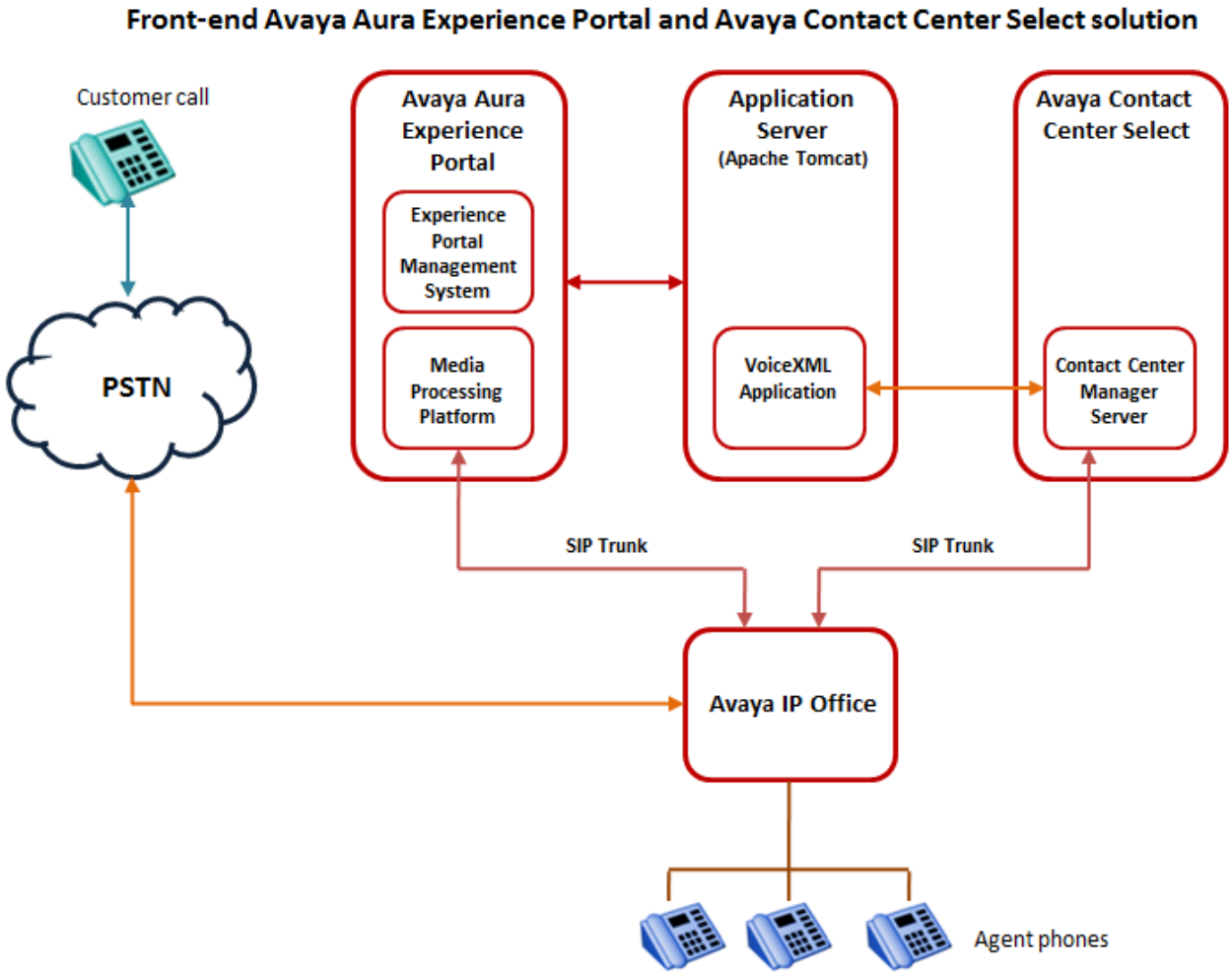


Figure 12: Example of front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

Call flow example for front-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

This call flow example shows how the Avaya Aura® Experience Portal system interacts with Avaya Contact Center Select to handle a typical automated front-end self-service customer transaction.

1. Incoming customer calls are routed to a Media Processing Platform (MPP) server in the Avaya Aura® Experience Portal system.
2. The MPP server checks the Dialed Number Identification Service (DNIS) for the incoming call and uses the configuration information downloaded from the Experience Portal Manager (EPM), server to match the number to a speech application on Avaya Aura® Experience Portal.

Página2066 de 3226.

3. The Experience Portal Management System starts an Avaya Voice Browser session and passes it the Universal Resource Indicator (URI) specified for the selected speech application.
4. The Avaya Voice Browser contacts the application server and passes it the URI.
5. The application server returns a Voice XML page to the Avaya Voice Browser.
6. Based on instructions on the Voice XML application, the MPP uses prerecorded audio files, Text-to-Speech (TTS), or both to play a prompt to start interaction with the caller.
7. If the customer responds by entering Dual-Tone Multi-Frequency (DTMF) digits, the MPP establishes a connection to a TTS server and the ASCII text in the speech application is forwarded for processing. The TTS server renders the text as audio output in the form of synthesized speech which the MPP then plays for the caller.
8. The customer chooses to speak to an agent.
9. The Voice XML application connects to the Contact Center Manager Server. The Voice XML application specifies a destination Controlled Directory Number (CDN) or Agent, transfer type (blind, bridged, or consult transfer), contact ID number, and UUI data generated Contact Intrinsics.
10. The Experience Portal Media Processing Platform (MPP) server completes the blind transfer of the customer call to the destination CDN.
11. The Contact Center Manager Server SIP Gateway Manager (SGM) is now controlling the customer call. The SGM routes the call to an appropriate agent skillset.
12. A Contact Center agent is offered the call. The agent can access customer details and Contact Intrinsics before answering the call.
13. The Contact Center agent receives the (customer and call) context information in a screen pop and answers the customer call.
14. The XML application terminates the call when it finishes execution or when the caller hangs up.

A combined Avaya Aura® Experience Portal self-service system and Avaya Contact Center Select solution gives customers exceptional service and improved efficiency. Front-end self-service automation reduces contact center operating costs and improves Customer Satisfaction (CSAT).

Avaya Aura® Experience Portal uses Voice XML applications and SIP header (UUI and P-Intrinsics) information to integrate with Avaya Contact Center Select. This gives enterprises complete flexibility and control of the integrated solution. The front-end Avaya Aura® Experience Portal self-service system and Avaya Contact Center Select solution is highly flexible and efficient. Avaya supplies sample Voice XML applications for the rapid integration of a front-end Avaya Aura® Experience Portal system with Avaya Contact Center Select.

Página2067 de 3226.

Back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

Avaya Aura® Experience Portal provides back-end Interactive Voice Response (IVR) services like text-to-speech, digit collection, music, and speech recognition. A combined Avaya Aura® Experience Portal system and Avaya Contact Center Select solution gives your customers exceptional service and improved efficiency. Back-end Interactive Voice Response (IVR) reduces contact center operating costs and improves Customer Satisfaction (CSAT).

In a typical back-end Avaya Aura® Experience Portal solution, customer calls to Avaya Contact Center Select are routed to Experience Portal applications for automated processing. Avaya Aura® Experience Portal applications play voice prompts asking the customer to select items from a menu, or to input account numbers. The customer responds by entering digits on their phone, or by speaking (Experience Portal supports optional Automatic Speech Recognition servers). The Experience Portal applications then collect the customer's response and return it to Avaya Contact Center Select for further treatments, or routing to the next available and appropriate Agent.

The following diagram shows a typical solution layout of Avaya Contact Center Select with a back-end Avaya Aura® Experience Portal integration.

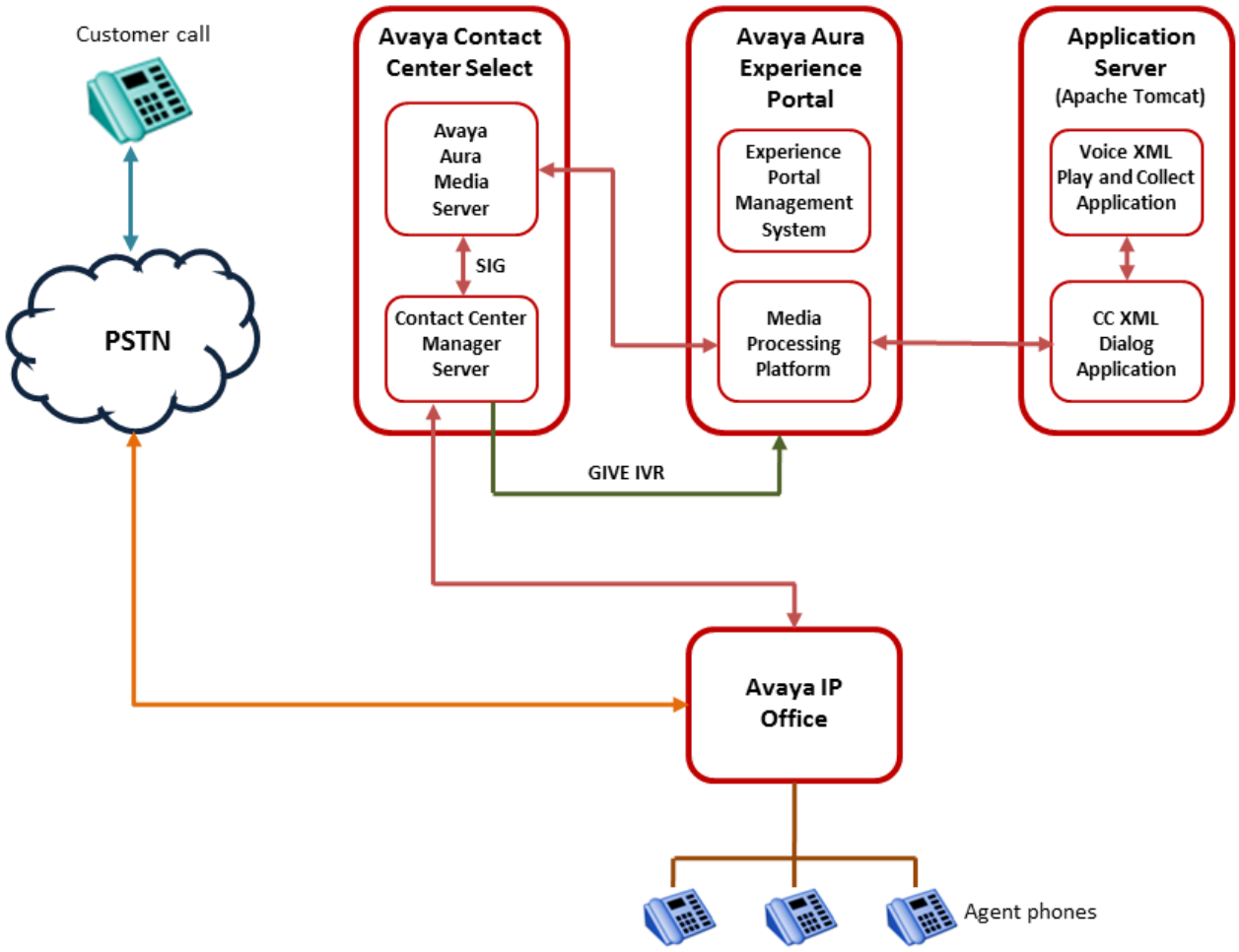


Figure 13: Example of back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

Call flow example using back-end Avaya Aura® Experience Portal and SIP-enabled Contact Center

This call flow example shows how the Avaya Aura® Experience Portal system interacts with Avaya Contact Center Select to handle a typical automated back-end Interactive Voice Response (IVR) customer transaction.

1. Incoming customer calls to the IP Office are routed to Avaya Contact Center Select.
2. Avaya Contact Center Select answers the call and runs a flow application, script, and/or optional primary scripts. A primary script is an application ran or referenced by the Master Script. Contact Center Manager Server records Master script and Primary script actions in statistical records.

Página2069 de 3226.

3. The Avaya Contact Center Select script issues a `GIVE IVR` for an external media server (XDIALOG), supplying the URI identifier of the Avaya Aura® Experience Portal.
4. Avaya Contact Center Select retains control of the call and sends a `SIP INVITE` message to Avaya Aura® Experience Portal. Avaya Contact Center Select specifies treatment parameters in the `SIP INVITE` message.
5. Avaya Aura® Experience Portal passes the call to a CCXML dialog application on the Apache Tomcat application server.
6. The CCXML dialog application accepts and retrieves IVR parameters from the `SIP INVITE` message.
7. The CCXML dialog application invokes the Play and Collect Voice XML application (PlayAndCollect) with the parameters retrieved from Avaya Contact Center Select. If available, SIP header UUI data is also extracted and passed to the Voice XML application.
8. The Play and Collect Voice XML application streams Real-time Transport Protocol (RTP) streams into the associated Avaya Aura® Media Server conference, and prompts the customer to enter digits on their phone.
9. The Play and Collect Voice XML application collects the digits entered by the customer.
10. The Play and Collect Voice XML application then passes the customer's digits back to the CCXML dialog application.
11. The CCXML dialog application returns the collected digits to Avaya Contact Center Select in a `SIP INFO` message.
12. The CCXML dialog application then drops out (`BYE`).
13. The Avaya Contact Center Select script retrieves the IVR collected digits.

A combined Avaya Contact Center Select and Avaya Aura® Experience Portal solution gives customers exceptional service and improved efficiency. Back-end Avaya Aura® Experience Portal automation reduces contact center operating costs and improves Customer Satisfaction (CSAT).

Avaya Contact Center Select uses Call Control XML and Voice XML applications to integrate with Avaya Aura® Experience Portal. This gives enterprises complete flexibility and control of the solution integration. The Avaya Aura® Experience Portal system and Avaya Contact Center Select solution is highly flexible and efficient. Avaya supplies sample Voice XML applications for the rapid integration of a back-end Avaya Aura® Experience Portal system with Avaya Contact Center Select.

Back-end Avaya Aura® Experience Portal using Context Creation and SIP-enabled Contact Center

Avaya Aura® Experience Portal provides back-end Interactive Voice Response (IVR) services like text-to-speech, digit collection, music, and speech recognition. A combined Avaya Aura®

Página2070 de 3226.

Experience Portal system and Avaya Contact Center Select solution gives your customers exceptional service and improved efficiency.

Avaya Contact Center Select provides generic sample applications to demonstrate how it integrates with Avaya Aura® Experience Portal. You can select a sample application that suits your integration, review the sample code, and customize it to your solution before deploying it in production.

In a SIP-enabled contact center solution, the information stored in some SIP INFO messages can be used to transfer call-related information between SIP-enabled components. This call-related information enables the receiver to better understand and handle the call. If your call-related context information does not fit in a SIP User-to-User Information (UUI) header or in the larger P-Intrinsics header, you can use the sample Context Creation application to pass more context information from Avaya Aura® Experience Portal to Avaya Contact Center Select.

The Context Creation sample application can inject multiple pieces of context information (Intrinsics and Call Attached Data) into Avaya Contact Center Select, whereas the Play and Collect sample application can retrieve only a single piece of data, for example collected digits.

In a typical back-end Avaya Aura® Experience Portal solution, customer calls to Avaya Contact Center Select are routed to Avaya Aura® Experience Portal applications for automated processing. Avaya Aura® Experience Portal applications play voice prompts asking the customer to select items from a menu, or to input account numbers. The customer responds by entering digits on their phone, or by speaking (Avaya Aura® Experience Portal supports optional Automatic Speech Recognition servers). The Avaya Aura® Experience Portal applications then collect the customer's response and return it to Avaya Contact Center Select for further treatments, or routing to the next available and appropriate Agent.

In a back-end integration where Avaya Aura® Experience Portal is using the Context Creation sample application, the Avaya Contact Center Select Orchestration Designer script sends a GIVR IVR (SIP INVITE) message into the Avaya Aura® Experience Portal system. The SIP INVITE message has “treatmenttype” set to “contextcreation”. Avaya Aura® Experience Portal passes the SIP call to a sample Dialog CC XML application. The Dialog CC XML and Context Creation VoiceXML applications process the call, and return hex-encoded call-related information. Because the “treatmenttype” was set to “contextcreation”, the Dialog application returns a SIP INFO message of type “application/x-aacc-info” to the Contact Center. The Contact Center SIP Gateway Manager (SGM) recognizes this SIP message type and converts the context information in the call into Contact Intrinsics. The Orchestration Designer script can then access and use the Contact Intrinsics for the call, and Contact Center can pass them on to Agent Desktop.

This sample Dialog and Context Creation applications can return multiple values from Avaya Aura® Experience Portal, rather than the single value returned by the Avaya Contact Center Select sample Play and Collect VoiceXML application. The Context Creation sample application supports more complex data. The call-related context information is returned in a SIP INFO message body. A SIP INFO message body holds and transfers much more information than a SIP header.

When using the Context Creation sample application, the SIP message body data is hex-encoded and XML-formatted (using the same encoding as P-Intrinsics).

Example of a single intrinsic in VoiceXML code (Note: spaces are not supported):

Página2071 de 3226.

```
<cc><i>CUSTOMER_SESSION_ID=12345</i></cc>
```

Example of the single intrinsic when Hex-encoded:

```
3c63633e3c693e435553544f4d45525f53455353494f4e5f49443d31323334353c2f693e3c2f63633e
```

The following diagram shows a typical solution layout of an Avaya Contact Center Select with a back-end Avaya Aura® Experience Portal integration.

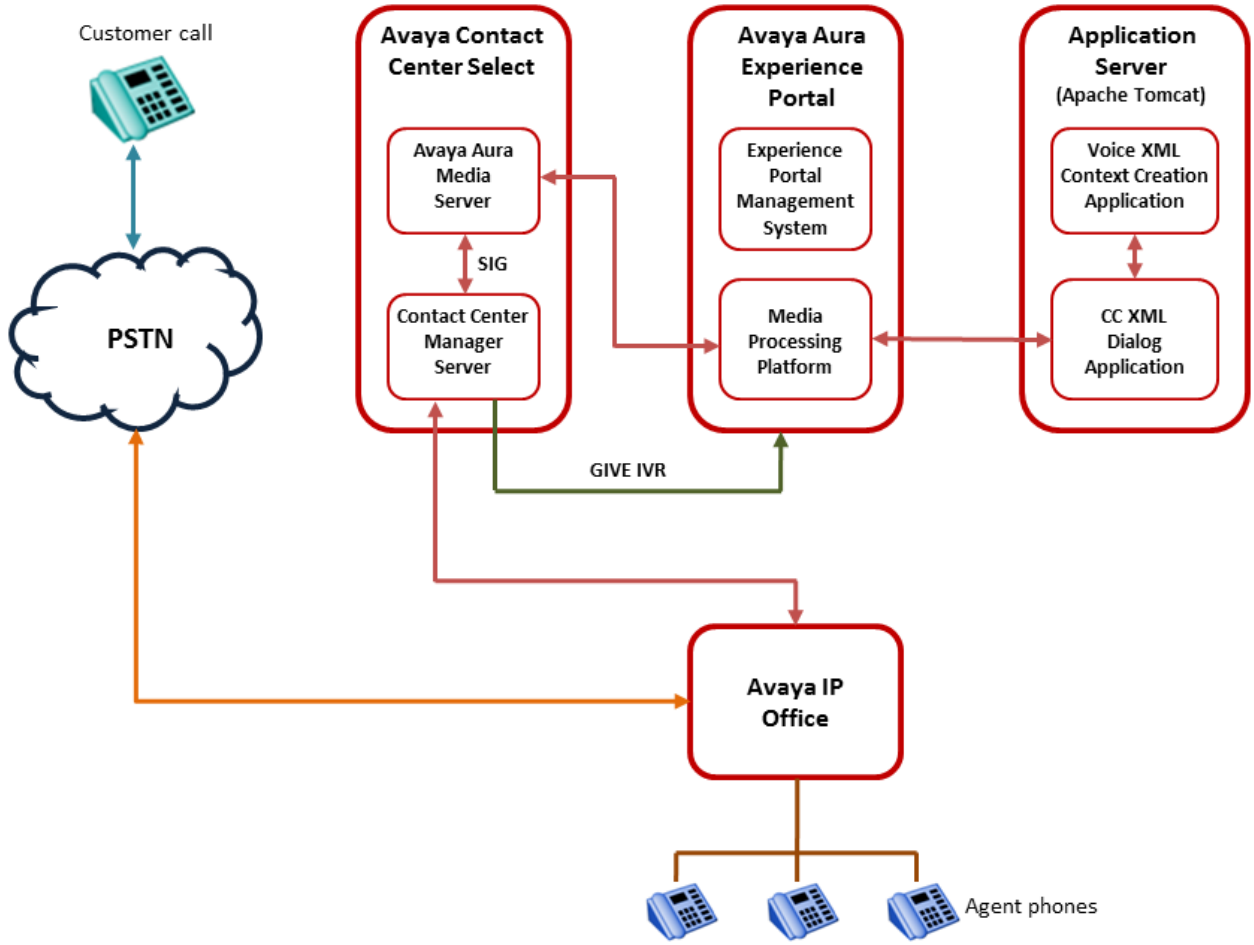


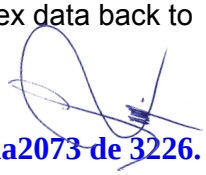
Figure 14: Example of back-end Avaya Aura® Experience Portal using the Context Creation sample application

Call flow example using back-end Avaya Aura® Experience Portal with the Context Creation sample application

This call flow example shows how the Avaya Aura® Experience Portal system interacts with Avaya Contact Center Select to handle a typical automated back-end Interactive Voice Response (IVR) customer transaction.

1. Incoming customer calls to IP Office are routed to Avaya Contact Center Select.
2. Avaya Contact Center Select answers the call and runs a script, and/or optional primary scripts. A primary script is an application ran or referenced by the Master Script. Contact Center Manager Server records Master script and Primary script actions in statistical records.
3. The Avaya Contact Center Select script issues a `GIVE IVR` for an external media server (XDIALOG), supplying the URI identifier of the Avaya Aura® Experience Portal.
4. Avaya Contact Center Select retains control of the call and sends a `SIP INVITE` message to Avaya Aura® Experience Portal. Avaya Contact Center Select specifies treatment parameters in the `SIP INVITE` message. The SIP INVITE message has “treatmenttype” set to “contextcreation”.
5. Avaya Aura® Experience Portal passes the call to the sample CCXML dialog application on the Apache Tomcat application server.
6. The CCXML dialog application accepts and retrieves IVR parameters from the `SIP INVITE` message.
7. The CCXML dialog application invokes the Context Creation Voice XML application with the parameters retrieved from Avaya Contact Center Select.
8. The Context Creation Voice XML application streams Real-time Transport Protocol (RTP) streams into the associated Avaya Aura® Media Server conference, and prompts the customer to enter digits on their phone.
9. The Context Creation Voice XML application collects the digits entered by the customer.
   - If the digits match the first account number (AccountA=123123) in the application’s config.properties file, the Context Creation application uses the “Context Data for account A” data from the configuration file and hex encodes it.
   - If the entered digits match the second account (AccountB=456456) in the application’s config.properties file, the Context Creation application uses the “Context Data for account B” data from the configuration file and hex encodes it.

   The sample Context Creation application uses the account number details from the configuration files for illustration purposes. In a real solution, you can extract the context data from anywhere; be it an external database, a Customer Relationship Management (CRM) system, or from context gathered within the Orchestration Designer application.
10. The Context Creation Voice XML application then passes the encoded hex data back to the CCXML dialog application.



Página2073 de 3226.

11. The CCXML dialog application returns the encoded hex data to Avaya Contact Center Select in a SIP INFO message. Because “treatmenttype” was set to “contextcreation”, the dialog application sets the type of the SIP message body to ‘application/x-aacc-info’.
12. The CCXML dialog application then drops out (`BYE`).
13. The Avaya Contact Center Select SIP Gateway Manager (SGM) recognizes this SIP message type and creates context information for the call by converting the hex encoded data in the SIP INFO message body into Contact Intrinsics.
14. The Avaya Contact Center Select script logs the returned value.

Avaya Contact Center Select uses Call Control XML and Voice XML applications to integrate with Avaya Aura® Experience Portal. This gives enterprises complete flexibility and control of the solution integration. The Avaya Aura® Experience Portal system and Avaya Contact Center Select solution is highly flexible and efficient. Avaya supplies sample Voice XML applications for the rapid integration of a back-end Avaya Aura® Experience Portal system with Avaya Contact Center Select.

Avaya DevConnect

The Avaya DevConnect Program provides a wide range of developer resources, including access to APIs and SDKs for Avaya products, developer tools, technical support options, and training materials. Registered membership is free to anyone interested in designing Avaya-compatible solutions. Enhanced Membership options offer increased levels of technical support, compliance testing, and co-marketing of innovative solutions compatible with standards-based Avaya solutions.

Avaya Contact Center Select supplies generic sample Avaya Aura® Experience Portal applications for demonstration purposes. If you plan to use these sample applications, you must review the sample code and customize it to your solution prior to deploying in production.

For more information, and to download the complete Avaya Aura® Experience Portal front-end self-service and Avaya Contact Center Select using SIP header sample files, see Orchestration Designer Sample Applications on www.avaya.com/devconnect.

Página2074 de 3226.

Chapter 9: Administration client computer requirements

This section provides the configuration requirements for the browser-based Avaya Contact Center Select administration client computers. Install this client computer to configure and administer Avaya Contact Center Select resources, to monitor performance, and to generate (real-time and historical) reports. You can also use this client computer to upload and download data using the Configuration Tool spreadsheets.

Administrator computer hardware requirements

The following table lists the minimum hardware requirements for the Administrator client computer.

Table 9: Client computer minimum hardware requirements

Hardware item	Minimum requirements	Additional information
CPU	1 Gigahertz (GHz) or faster CPU with support for PAE, NX, and SSE2	Physical Address Extension (PAE), NX processor bit (NX), and Streaming SIMD Extensions 2 (SSE2) are features of the processor. These CPU features are required to run Microsoft Windows 7.0 and Microsoft Windows 8.1. Dual- and quad-CPU systems are supported with or without Hyper-Threading enabled. AMD processors of the same or higher specification are also supported.
RAM	1 Gigabyte (GB) (32-bit) or 2 GB (64-bit)	Additional memory is required, if you run other memory intensive applications.
Hard disk space	16 GB (32-bit) or 20 GB (64-bit)	
Hard disk partitioning	No specific partitioning requirements	—
Hard disk speed	2.5 inch disk minimum speed: 10000 RPM	—

Table continues…

Hardware item	Minimum requirements	Additional information
	3.5 inch disk minimum speed: 7200 RPM	
Floppy drive	Not required	If a floppy drive is installed, it must be A.
DVD ROM	Not required	
Network interface	One network interface card	100 Mb/s Ethernet or higher is recommended.
Video card	Microsoft DirectX 9 graphics device with WDDM driver	1024 x 768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—

Client operating system requirements

The following table lists the operating system requirements for client computers.

Table 10: Client operating system requirements

Operating system	International versions supported	Minimum service pack
Windows 7 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	
Windows 8.1 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL)	

Table continues…

Página2076 de 3226.

Operating system	International versions supported	Minimum service pack
	Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	
Windows 10 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	

Administration Client Citrix support

Contact Center Manager Administration (CCMA) is supported in Citrix deployments. A Citrix server solution uses software to deliver on-demand Windows applications to physical desktops. This allows client users to access and use programs which are available on the Windows Server 2012 R2 operating system of the Citrix server. Contact Center Manager Administration supports the following versions of Citrix server:

- Citrix XenApp 6.5
- Citrix XenApp 7.x

Users access Contact Center Manager Administration through a Citrix client on their client computer, connecting through an Internet Explorer browser that runs on the Citrix server. The browser is available to users through a Citrix client on their client computer. In a client Citrix deployment of CCMA, you must install ActiveX controls on the Citrix server. For more information about installing ActiveX controls on the Citrix server, see *Avaya Contact Center Select Advanced Administration*.

Página2077 de 3226.

For more information about Citrix application publishing, see your Citrix documentation. For more information on how to configure your Citrix server to allow users to access CCMA, see *Avaya Contact Center Select Advanced Administration*.

Avaya Contact Center Select supports only the Multicast option for Real-Time Displays (RTDs) in a Citrix environment. Avaya Contact Center Select does not support the Unicast option for Real-Time Displays (RTDs) in a Citrix environment.

Important:

No Avaya Contact Center Select client components, other than Agent Desktop and Contact Center Manager Administration, are supported in a Citrix deployment. The Orchestration Designer (OD), Outbound Campaign Management Tool (OCMT), and CCMM Administration utility client components are supported in a Citrix deployment.

Third-party software requirements

This section describes the third-party software requirements for the administration client computer.

The following components are required on the administration client PC:

- Microsoft Internet Explorer 10.0 (32-bit version only), and 11.0 (32-bit version only).

  Note:

  You must run Internet Explorer in compatibility mode for Contact Center Manager Administration and Communication Control Toolkit.

- Microsoft Excel 2007 or later (for Configuration Tool only)

Contact Center Manager Administration supports only the 32-bit version of Microsoft Internet Explorer.

Contact Center Manager Administration does not support Microsoft Edge.

Página2078 de 3226.

Chapter 10: Agent Desktop computer requirements

This section provides the configuration requirements for the Agent Desktop client computers. Agent Desktop is a single-interface client application used by contact center agents to interact with customers. Agents download and install Agent Desktop client software from the Avaya Contact Center Select server. Avaya Contact Center Select agents use the Agent Desktop software in conjunction with an IP Office provisioned telephone.

Avaya Contact Center Select supports backwards compatibility with the previous Feature Pack or Service Pack version of Agent Desktop. This allows you to upgrade the Avaya Contact Center Select server without the requirement to upgrade Agent Desktop in a single maintenance window. For example, if you upgrade to Release 7.0 Feature Pack 3, you can use the Release 7.0 Feature Pack 2 version of Agent Desktop. New Agent Desktop features added in the latest Avaya Contact Center Select release are not available until you upgrade Agent Desktop to that release. Backwards compatibility is not supported for major or minor releases. For example, if you upgrade to Release 7.1, you cannot use the Release 7.0 version of Agent Desktop.

Note:

Agent Desktop does not support touch screen devices or tablets.

Note:

Agent Desktop does not support Network Address Translation (NAT).

Agent Desktop localized languages

Agent Desktop is supported in the following localized languages:

- English
- French
- German
- Italian
- Japanese
- Korean

Página2079 de 3226.

- Latin Spanish
- Brazilian Portuguese
- Russian
- Simplified Chinese

A single Avaya Contact Center Select solution, with the localization language patches installed, supports all of the Agent Desktop localized languages. For example, a single English language Voice and Multimedia Contact Server supports the English, Chinese, French, and Russian language versions of Agent Desktop client software.

Avaya Contact Center Select supports Agent Desktop client operating systems that use a different language family to the Contact Center server.

Agent Desktop computer hardware requirements

The following table lists the minimum hardware requirements for a computer running Agent Desktop software.

Table 11: Agent Desktop computer minimum hardware requirements

Hardware item	Minimum requirements	Additional information
CPU	1 Gigahertz (GHz) or faster CPU with support for PAE, NX, and SSE2	Physical Address Extension (PAE), NX processor bit (NX), and Streaming SIMD Extensions 2 (SSE2) are features of the processor. These CPU features are required to run Microsoft Windows 7.0 and Microsoft Windows 8.1. Dual- and quad-CPU systems are supported with or without Hyper-Threading enabled.
RAM	1 Gigabyte (GB) (32-bit) or 2 GB (64-bit)	Additional memory is required, if you run other memory intensive applications at the same time as Agent Desktop.
Hard disk space	16 GB (32-bit) or 20 GB (64-bit)	
Hard disk partitioning	No specific partitioning requirements	—
Hard disk speed	2.5 inch disk minimum speed: 10000 RPM 3.5 inch disk minimum speed: 7200 RPM	—
Floppy drive	Not required	If a floppy drive is installed, it must be A.

Table continues…

Página2080 de 3226.

Hardware item	Minimum requirements	Additional information
DVD ROM	Not required	
Network interface	One network interface card	100 Mb/s Ethernet or higher is recommended.
Video card	Microsoft DirectX 9 graphics device with WDDM driver	1024 x 768 pixels minimum resolution
Keyboard	One keyboard	—
Mouse	One mouse	—

Agent Desktop does not support touch screen devices or tablets.

Client operating system requirements

The following table lists the operating system requirements for client computers.

Table 12: Client operating system requirements

Operating system	International versions supported	Minimum service pack
Windows 7 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	
Windows 8.1 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA)	

Table continues…

Página2081 de 3226.

Operating system	International versions supported	Minimum service pack
	Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	
Windows 10 (32-bit and 64-bit)	English French (FR) German (DE) Italian (IT) Dutch (NL) Japanese (JA) Korean (KO) Latin Spanish (ES) Brazilian Portuguese (PT-BR) Russian (RU) Simplified Chinese (Zh-CN)	

Third-party software requirements

This section describes the third-party software requirements for Agent Desktop client computers.

Agent Desktop supports only Microsoft Internet Explorer 10.0 (32-bit version only) and 11.0 (32-bit version only).

Agent Desktop supports only the 32-bit version of Microsoft Internet Explorer.

Agent Desktop does not support Microsoft Edge.

Agent Desktop client network infrastructure requirements

Agent Desktop is a client application which communicates with the Avaya Contact Center Select server. For optimal Agent Desktop operation, the underlying contact center network infrastructure must provide adequate latency and bandwidth between the agent computer and the Avaya Contact Center Select server.

Página2082 de 3226.

This section provides a high-level overview of the data that is passed between Agent Desktop and the Avaya Contact Center Select server. It also sets out the recommended network values and likely impacts on agents if these values are not met. This section also describes the performance of Agent Desktop in varying Round Trip Time (RTT) and bandwidth environments.

Important:

Agent Desktop performance degrades as network Round Trip Time increases and network bandwidth decreases.

Network Latency

Network latency is a measure of the time delay experienced in a system, measured in Round Trip Time (RTT). RTT is the average Round Trip (packet) Time as measured using the ping command for a 1024-byte (1KB) data size.

For optimal performance, Avaya recommends a RTT of less than 80ms from the Agent Desktop client computer to the following Avaya Contact Center Select components:

- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Contact Center Manager Server (CCMS)

The RTT from the Agent Desktop client PC to the Avaya Contact Center Select server must be less than 120ms. For network environments with an RTT greater than 120ms, refer to the Citrix deployments of Agent Desktop in the next section.

RTT impacts on Voice traffic

This section describes how the underlying RTT and latency of the network affects the experience of handling voice traffic in Agent Desktop.

Agent Desktop used with a physical desk phone

The CCT component sends Computer Telephony Integration (CTI) signals to Agent Desktop, for example to prompt Agent Desktop to alert an incoming contact. These CTI signals are passed across the network as data. However, if the agent is using a physical desk phone, voice packets are transported across a network.

The following table details the time taken for the contact to alert on the Agent Desktop, compared to the time taken for the same contact to ring on the agent's phone, where the phone is subject to a constant RTT of 1ms.

RTT (ms)	Delay between desk phone ring and call alert on Agent Desktop	Delay between clicking Accept button on Agent Desktop and active voice path
1ms LAN	<0.5 Seconds	<0.5 Seconds
50ms	0.5 Seconds	1.0 Seconds
120ms	1.0 Seconds	2.5 Seconds

RTT impact on Multimedia Contacts

Página2083 de 3226.

Contact Center Multimedia contacts are also affected by network latency. Agent Desktop downloads Customer contacts from the Avaya Contact Center Select server and displays their contents as soon as they are fully retrieved.

The table below shows how varying RTTs affect multimedia contact display times – in this case, email contacts – on Agent Desktop. The “Customer Details/Customer History Display” column indicates how much time passes between the email being opened on the Agent Desktop and the additional context information being loaded and displayed. These sample times are for ideal laboratory conditions.

RTT (ms)	Email Display	Customer Details/Customer History Display
1ms LAN	2 Seconds	0 Seconds
50ms	3 Seconds	Additional 3 Seconds
100ms	4 Seconds	Additional 4 Seconds
120ms	4 Seconds	Additional 5 Seconds

This data was generated using a 20KB email message, a customer history containing 30 contacts of 20KB each, in a network where bandwidth is not limiting the data transfer. Email messages of different sizes generate different results.

Bandwidth

The network bandwidth available to Agent Desktop client computers for communication with Avaya Contact Center Select servers is critical to Agent Desktop performance. If voice traffic is carried on the same network, this traffic is often prioritized above other network traffic – this bandwidth is therefore not available to Agent Desktop. In many cases agents use other third party applications over the same network. The bandwidth requirements of these third party applications must be considered as part of the overall bandwidth calculations (in addition to bandwidth allocated for voice soft phones and for Agent Desktop).

Several factors affect the recommended bandwidth for Agent Desktop. Depending on which Contact Center Multimedia (CCMM) features are in use on a given Customer deployment, not all factors apply. Indicative calculations to estimate the actual bandwidth usage are presented below for the various contact types and features. To calculate the required bandwidth, the relevant figures for the deployed features and supported contact types can be combined to derive an overall figure.

The network usage can be one of two types:

Constant traffic	These require dedicated, permanently available network use for the lifetime of the consumption. Examples of this type of traffic include; statistics display in Agent Desktop, update of live Web chat contacts. Many factors influence constant traffic levels, for example the number of agents with a large number of assigned skillsets, the number of active supervisors running RTDs in unicast mode, and large numbers of skillsets in use (large data packet) even for multicast.
Bursty traffic	The display of multimedia contacts and multimedia contact history is bursty traffic. A significant amount of data is downloaded to the Agent Desktop over a number of seconds. The frequency of these download is driven by agent activity.

Table continues…

Página2084 de 3226.

	These require high usage of the available network for short times to download bursts of data. The time window that this data takes to download depends on the available network bandwidth at that time. Since this is not constant network consumption, a Kilo bits per second value is not reflective of the bandwidth required and a Kilo bit value has been provided instead.

Bandwidth impacts on Voice

If the agents are using a physical desk phone for voice or any other application which utilizes network bandwidth, this needs to be factored into the engineering of the network to meet the expected performance levels on Agent Desktop.

Retrieve Customer History on voice contacts

The Agent Desktop Customer History feature enables agents to retrieve voice callers' multimedia Customer history, from the Avaya Contact Center Select server, when a voice contact is accepted. Agent Desktop Customer History is an optional feature which is enabled in the CCMM Administration tool. These historical contacts can be of any multimedia contact type. Agent Desktop Customer History requires adequate bandwidth to function and it must be included in your network bandwidth planning calculations.

To calculate the impact of a voice callers' multimedia Customer history on bandwidth, consider voice contacts as an additional Multimedia contact type and add the number of voice contacts to your multimedia calculation for bandwidth calculations.

Multimedia Contact bandwidth requirements

This section details the bandwidth requirement of Agent Desktop Customer History for the following multimedia contact types:

- Email messages
- Fax messages
- Scanned Documents (SD)
- SMS text messages
- Outbound contacts
- Web Communications (WCs)

This section also details the bandwidth requirement for voice contact types if multimedia history display is enabled.

Some multimedia contact supports attachments and these attachments must also be included in network calculations:

- Email contacts are of variable size. The average email size is a reasonable estimate, and is used for Agent Desktop calculations.
- Fax messages are delivered as email attachments. Fax messages must be included in the attachment size and rate estimates.
- Outbound contacts from Avaya Contact Center Select solution do not have attachments.
- SMS test messages from customers. SMS test messages do not have attachments.

- Web chat messages do not have attachments.

The Agent Desktop Customer History feature enables agents to retrieve multimedia Customer history (containing up to 30 previous contacts), from the Avaya Contact Center Select server, when a multimedia contact is accepted. Agent Desktop Customer History requires adequate bandwidth to function and it must be included in your network bandwidth planning calculations. Retrieving Agent Desktop Customer history from the Avaya Contact Center Select server uses the bursty type of network data, and where the Customer history feature is enabled, it must be included in all network bandwidth calculations.

Example of calculating the bandwidth requirements of Agent Desktop Customer history downloads (based on ideal laboratory conditions):

N = Number of agents working on multimedia (MM) contacts. If the feature to display multimedia history with voice calls is activated, then N must include voice agents.

C = Maximum number of multimedia contacts per hour for the entire contact center solution. If the feature to display multimedia history with voice calls is activated, then C must include voice traffic per hour to all those agents.

avg_contact_size = average size of a contact in Kbits (not Kbytes). (Kbits = KBytes * 8). In many cases this is the average size of the incoming or outgoing email.

att_rate_in = percentage of incoming contact attachments. Contact attachments apply to email messages and fax messages.

att_rate_out = percentage of incoming email messages that are responded to with agent attached attachments in the reply.

avg_att_size = average size of an attachment in Kbits. Contact attachments apply to email messages and fax messages.

Note:

In-line attachments must also be included in the bandwidth calculations as regular attachments.

A key factor in calculating the minimum bandwidth for processing multimedia contacts is an assessment of the number of active agents that accept contacts in any one second period. The available bandwidth is shared across all of these agents in this time period.

The long term average number of agents active in any one second is calculated as follows:

$n_{average}$ = Roundup(C / 3600)

This equates to the average number of agents clicking the Accept button on the Agent Desktop at any one time. However, since the length of time it takes an agent to handle a contact is random, the number of agents clicking the Accept button is random. It is incorrect to engineer a bandwidth solution based solely on this average, as nearly 50% of the time more than $n_{average}$ agents are clicking the Accept button.

Therefore the number of active agent per second is calculated with a factor F as follows:

n_{active} = Roundup(F* C / 3600)

where F is an engineering factor between 3 and 10. A higher value for F must be used when N, the total number of agents processing multimedia contacts and multimedia history with voice

Página2086 de 3226.

contact, is lower than 50. The choice of value F is your decision. F reflects the amount of extra bandwidth to build into your network to handle both the inherently random distribution of agent activity which results in natural peaks of use and any data spike events attributable to your particular Contact Center business models, such as initial shift start times, promotions and emergencies. A higher value reduces the level of bandwidth limitation caused by the overlapping of multiple agent download of multimedia contacts.

Once F is defined, the minimum bandwidth (in Kbits per second) can be estimated as follows:

$BWMM_{min}$ =

n_{active} * ((avg_contact_size * 64) + 2000) + avg_att_size * (att_rate_in% + att_rate_out%) / 100) Kbps

Important:

The minimum recommended bandwidth available for processing multimedia contacts $BWMM_{min}$ must be greater than 10 Mbits per second.

The time to download and display contacts on Agent Desktop is directly impacted by the bandwidth available between the Avaya Contact Center Select server and Agent Desktop at the time when the contact is accepted in Agent Desktop. The impact of bandwidth limitation is observed as a delayed display of contact and contact history in the Agent Desktop.

The following table demonstrates the impact of limiting bandwidth on multimedia contact display times on Agent Desktop. The data was generated using a 20KB email message, a Customer history of 30 contacts of 20KB size each, with a fixed RTT of 80ms.

Available bandwidth	Email display	Customer Details/Customer History Display
1Mbps	3 Seconds	Additional 6 Seconds
3Mbp	3 Seconds	Additional 3 Seconds
5Mbps	3 Seconds	Additional 2 Seconds

Retrieve Customer History on Voice contacts

This optional feature enables Agent Desktop to retrieve voice callers' multimedia Customer history (containing up to 30 previous contacts), from the Avaya Contact Center Select server, at the time a voice contact is accepted. These historical contacts can be of any multimedia contact type. If this feature is activated, the size of this history can be added to your network planning by considering voice as an additional multimedia contact type and adding the number of voice contacts to your multimedia calculation.

Web Communication (WC) network bandwidth calculation

Processing web communications, after they have been received by the agent requires a constant level of bandwidth.

Network usage type: Constant

c = Number of WC contacts per hour

avg_session_length = Average length in seconds of WC session

Página2087 de 3226.

Data size: 50 Kbps per active WC contact

WC network bandwidth requirement (Kbps):

WC_{BW} = (c * 50Kbps * avg_session_length)/ 3600

Presence network bandwidth calculation

Presence updates require a constant level of bandwidth.

Network usage Type: Constant

N = Number of agents working on MM contacts

avg_pres = Average number of presence updates per user per hour

Data size: 7 Kb per Presence update

Presence network bandwidth requirement (in Kbps) = (N* 7Kb * avg_pres)/ 3600

CCMM Search network bandwidth calculation

Bandwidth must be provided for an agent carrying out multimedia searches.

Network usage Type: Bursty

N = Number of agents running searches

average_search = Average number of searches per hour

Data transmitted: 1280Kb per search

CCMM Search bandwidth requirement (in Kbps) = (1280Kb * average_search * N)/3600

CCMM Pull Mode network bandwidth calculation

Pull Mode allows agents to work outside the normal Avaya Contact Center Select routing mode. They personally select individual contacts from the Avaya Contact Center Select queues. Their view of the Avaya Contact Center Select queue is automatically updated using the same web services as the Avaya Contact Center Select CCMM search feature, and so uses the same bandwidth.

N = Number of agents working in Pull Mode

c = Number of contacts per hour per agent

Data transmitted: 1280Kb per search

CCMM Pull Mode search bandwidth requirement (in Kbps) = (1280Kb * c * N)/3600

Web Statistics network bandwidth calculation

Network usage Type: Bursty

N = Number of agents

avg_skills = Average number of skillsets per agent

Data transmitted: 3.2 Kb per skillset once a minute

Web Statistics bandwidth requirement: (3.2 Kb * avg_skills * N)/60

Agent Desktop downloads by agent

Agent Desktop is a smart client which is downloaded from the Avaya Contact Center Select server over the network onto each agent computer on initial install. On each software update (service pack or patch) the updated Agent Desktop is re-downloaded onto each agent computer. The download requirements of Agent Desktop must be considered when planning the bandwidth requirements to remote agents.

Summary of total bandwidth requirements

You must sum up all the applicable bandwidth demands listed above to arrive at a minimum bandwidth for the site. Calculate the cumulative bandwidth for all multimedia features.

Remote Desktop Services support

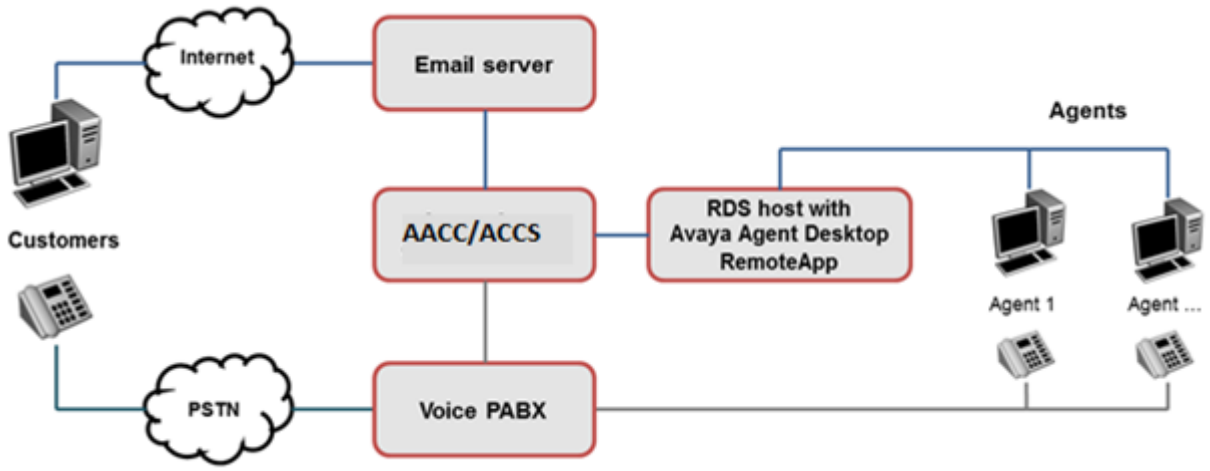
Avaya Contact Center Select (ACCS) supports using Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop.

Remote Desktop Services, formerly known as Terminal Services, allows a server to host multiple simultaneous client sessions. In the Remote Desktop Services (RDS) environment, an application runs entirely on the Remote Desktop Session Host (RD Session Host) server. The RDC client performs no local processing of application software. The server transmits the graphical user interface to the client. The client transmits the user's input back to the server. With RDS, only software user interfaces are transferred to the client system. All input from the client system is transmitted to the server, where software execution takes place.

You must use the Agent Desktop MSI package for Remote Desktop Services deployments. How you deploy and use Agent Desktop RDS clients depends on your solution requirements and virtualization infrastructure. For more information about building a client infrastructure using RDS, refer to the Microsoft Remote Desktop Services product documentation.

The following diagram shows a typical Remote Desktop Services solution with Agent Desktop hosted on the RDS Session Host server.

Página2089 de 3226.



Remote Desktop Services requires careful up-front planning and engineering. It requires some additional maintenance and full organizational support to deliver an enterprise grade contact center agent and customer experience.

RemoteApp:

RemoteApp allows you to make programs that are accessed remotely through Remote Desktop Services appear as if they are running on the end user's local computer. These programs are referred to as RemoteApp programs. Instead of being presented to the user in the desktop of the Remote Desktop Session Host (RD Session Host) server, the RemoteApp program is integrated with the client's desktop. The RemoteApp program runs in its own resizable window, can be dragged between multiple monitors, and has its own entry in the taskbar. If a user is running more than one RemoteApp program on the same RD Session Host server, the RemoteApp program shares the same Remote Desktop Services session.

Limitations:

The following limitations apply when you use Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop:

- Agent Desktop My Computer embedded softphone mode is not supported. Agents must use a desk phone, or use a supported softphone concurrently with Agent Desktop.
- Avaya recommends that the RDS server hosting Agent Desktop is located in the same Local Area Network (LAN) as the ACCS server. If the RDS server hosting Agent Desktop is not in the same LAN as the ACCS server, then the ACCS bandwidth, Round Trip Time, and networking requirements apply.
- ACCS supports the Multicast option only for Real-Time Displays (RTDs) in a RDS environment. Unicast is not supported in a RDS environment.
- You cannot use the ACCS server as the RDS host.
- Agents must define default template or attachment folders in Agent Desktop preferences to an AppData folder on the RDS host. Agents do not have access to shared or mapped drives. For more information on configuration settings for temporary folders on the RDS Host Server, refer to the Microsoft Remote Desktop Services product documentation.

For information about how to use Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop, see *Avaya Contact Center Select Advanced Administration*.

Client Citrix support

Agent Desktop is supported as a Citrix-published application. A Citrix server solution uses software to deliver on-demand Windows applications to physical desktops. This allows client users (agents in this case) to access and use programs which are available on the Windows Server 2012 R2 operating system of the Citrix server.

Agent Desktop supports the following versions of Citrix server:

- Citrix XenApp 6.5
- Citrix XenApp 7.x

On the Avaya Contact Center Select server the Agent Desktop folder is typically located in:

```
D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\client
```

This folder contains the entire Agent Desktop application. Copy this folder on the Agent Desktop server to the Citrix server. Then configure your Citrix server to publish Agent Desktop as a published application, accessed from this Agent Desktop folder on the Citrix server. On the Citrix server select the users (agents) allowed to run the Agent Desktop published application. For more information about Citrix application publishing, see your Citrix documentation. For more information on how to configure your Citrix server to publish Agent Desktop as a published application, see *Avaya Contact Center Select Advanced Administration*.

The Citrix server publishing Agent Desktop must be located in the same Local Area Network (LAN) as the Avaya Contact Center Select server.

Avaya Contact Center Select supports only the Multicast option for Real-Time Displays (RTDs) in a Citrix environment. Avaya Contact Center Select does not support the Unicast option for Real-Time Displays (RTDs) in a Citrix environment.

Agent Desktop network ports

Agent Desktop uses the following network ports to communicate with Contact Center components.

Feature	Component	Port number
HTTP (Web services)	CCMM	80
HTTP (Web services)	CCMM	443 (if TLS is enabled for CCMM)
CCT	CCT	29373
Voice History	CCMS	57772
Web Statistics	CCMS	9086

Página2091 de 3226.

Chapter 11: Contact Center Agent Browser application requirements

This section provides information on the configuration requirements for the Contact Center Agent Browser application.

Voice-only Contact Center agents can use the Agent Browser application to log on to Contact Center and perform basic tasks. The Agent Browser application does not provide call control, multimedia features, or supervisor functions. Agents must use a supported desktop phone for call control. The Agent Browser application supports the following tasks:

- logging on and off
- changing the agent status
- setting not ready reason codes
- setting activity codes
- setting after call work item codes
- calling your supervisor
- handling an emergency

The Contact Center Agent Browser application is supported only in SIP-enabled Contact Center solutions. All agents using Agent Browser require an associated Windows domain account, or a local Widows account, configured in CCMA, to log on to Agent Browser. If using a domain, the agent domain accounts must be in the same domain as the Contact Center server.

Agents access the Agent Browser application through a web browser, using the Contact Center server Fully Qualified Domain Name (FQDN). In Business Continuity solutions, agents must log on to the Agent Browser application using the FQDN of the Business Continuity pair.

In the event of a switchover to a Remote Geographic Node (RGN) server, agents must log on to the Agent Browser application using the FQDN of the RGN server.

The Agent Browser application does not support the Remote Agent feature.

You must access the Agent Browser application using HTTPS only. You must also install a valid TLS certificate, issued by a trusted Certificate Authority (CA), in Security Manager. To avoid certificate security warnings, install the root certificate of the CA on all client devices used to access the Agent Browser application. For more information, see Avaya Contact Center Select secure TLS communications on page 180.

If you use a mobile device to access the Agent Browser application, Avaya recommends using a medium size screen of 992 pixels or higher. Some mobile devices automatically lock after a defined

Página2092 de 3226.

timeout period — the Agent Browser application has no control over the automatic locking of mobile devices.

Language support

The Contact Center Agent Browser application supports the following languages:

- English
- French (FR)
- German (DE)
- Italian (IT)
- LA Spanish (ES)
- Brazilian Portuguese (PT-BR)
- Russian (RU)
- Simplified Chinese (Zh-CN)
- Traditional Chinese (Zh-TW)
- Japanese (JA)
- Korean (KO)

You can set the application language on the Settings menu of the Agent Browser application.

Web browser requirements

The Agent Browser application is hosted on the Internet Information Services (IIS) that is running on the Contact Center server. Agents access the application through a web browser. The following table lists the supported browsers.

Browser	Versions supported	Operation system
Microsoft Internet Explorer	11.0	• Windows 7 • Windows 8.1 • Windows 10
Microsoft Edge	20.10240	• Windows 10
Google Chrome	43.0.23	• Windows 7 • Windows 8.1 • Windows 10 • Android 4.4.2 • Android 5.0.1 • iOS 8.3

Table continues…

Página2093 de 3226.

Browser	Versions supported	Operation system
		• OS X Yosemite 10.10.3
Mozilla Firefox **Important:** The Agent Browser application does not support using the “Search for text when I start typing” feature in Firefox.	38.0.5	• Windows 7 • Windows 8.1 • Windows 10
Safari	8.0.5	• iOS 8.3 • OS X Yosemite 10.10.3

Página2094 de 3226.

Chapter 12: Avaya Contact Center Select secure TLS communications

Avaya Contact Center Select (ACCS) includes a number of services that you can secure by using the HTTPS protocol. At the installation stage, you can use the Ignition Wizard to create a security store, generate a Certificate Signing Request (CSR) and import a Certificate Authority root certificate. Alternatively, you can skip security configuration at the installation stage and configure your security certificates later using Security Manager.

HTTPS security basics

HTTPS is a secure protocol for Web communications. HTTPS provides both authentication of the Web server, and encryption of communications between the server and the client in both directions. HTTPS uses connections encrypted by the Transport Layer Security (TLS) protocol.

When a client initiates a secure connection with a server, the server returns its public cryptographic key in a server certificate. To ensure the integrity of the server certificate, it must be signed by a third party, called a Certificate Authority (CA). The client must have a root certificate from the CA that provided the signed server certificate. If the client has a matching root certificate, it completes the connection and secure communication is established.

Encryption levels, TLS versions, and SSL

Avaya Contact Center Select (ACCS) supports both the SHA1 and SHA2 cryptographic hash functions, with key sizes of 1024, 2048, or 4096. However, the SHA1 hash function and the 1024 key size do not provide the current industry-recommended level of encryption. ACCS supports SHA1 and a 1024 key size only to provide backward compatibility.

Avaya recommends that you use only SHA2 either a 2048 or 4096 key size. The default values for new security stores are SHA2 with a 2048 key size.

Secure Sockets Layer (SSL) also is obsolete, having a number of known weaknesses. Contact Center now uses only Transport Layer Security (TLS) for secure communications. Note that TLS is an extension of the older SSL protocol, and the industry frequently accepts and uses the term ‘SSL’ to refer to TLS.

Contact Center implements Transport Layer Security (TLS) version 1.2 as the default minimum version negotiated for secure communications. This is to avoid security vulnerabilities that exist in TLS 1.0. For backward compatibility and inter-operation with third-party or custom applications connecting to Contact Center, Administrators can set lower versions of TLS on certain

Página2095 de 3226.

communication channels. When a lower version of TLS is available, Contact Center still negotiates the highest level of TLS that the other application can support.

Server certificate

The server certificate, sometimes called a signed certificate, is the certificate that the server sends to a client that requests a secure service (HTTPS). The server certificate combines a public key used for encryption with an organization's details, and is signed by a certificate authority to allow clients to verify that it is valid. The client can use the server certificate to encrypt the data it sends to the server.

Certificate Authority

A Certificate Authority (CA) is a third-party organization that provides digital certificates that certify the owner of a public key for cryptography used in secure communications. If you use a single CA for all your security setup, it reduces you workload for security configuration, because you need to copy just a single root certificate to all clients. The root certificates for many well know CAs are frequently already embedded in common operating systems for clients and servers.

Root certificate

The root certificate proves the authenticity of the signed certificate. It contains a digital signature from a Certificate Authority (CA). To trust the server certificate sent to them by the server, clients must have a copy of the root certificate with the digital signature of the CA that signed the server certificate. Root certificates exported from different security stores work in the same way if they contain a digital signature from the same CA.

Server Certificate name

Each server certificate has a name, which normally derives from the server Fully Qualified Domain Name. If a server certificate name does not match the name of the website or web service to which the client connected, the client generates a warning. This impacts ACCS as follows:

- In Business Continuity (BC) systems, you need to commission your own certificates with Subject Alternative Names (SANs) to use the managed name of the campus HA pair. Therefore you must decide on the managed name before you set up your own certificates.

Subject Alternative Name

A Subject Alternative Name (SAN) is an extension to HTTPS that allows various values to be associated with a security certificate. These values are called "Subject Alternative Names", or SANs. There are several types of SAN values, but for ACCS only the DNS name type is relevant.

In ACCS you use SANs on security certificates to include the BC active, standby, and managed names in the server certificate, so that secure connections continue during a BC switchover and clients do not see warning messages.

When you create the ACCS security store in Security Manager, you can add SANs to the server certificate.

Avaya Contact Center Select security store

Avaya Contact Center Select (ACCS) includes a security store to enable secure communications over Transport Layer Security (TLS), both between ACCS applications and with external clients or

Página2096 de 3226.

third party applications. Customers must create a security store using either the Ignition Wizard or Security Manager, with a server certificate and root certificate from a Certificate Authority (CA).

ACCS also uses the Internet Information Services (IIS) security store for some services. On an ACCS server, Security Manager controls both the IIS security store and the ACCS security store. These two stores always use the same server certificate, which you configure in Security Manager.

Avaya Aura® Media Server also has a security store. You configure this store through Avaya Aura® Media Server Element Manager.

Figure 15: Example of security stores on a single ACCS server with co-resident Avaya Aura® Media Server

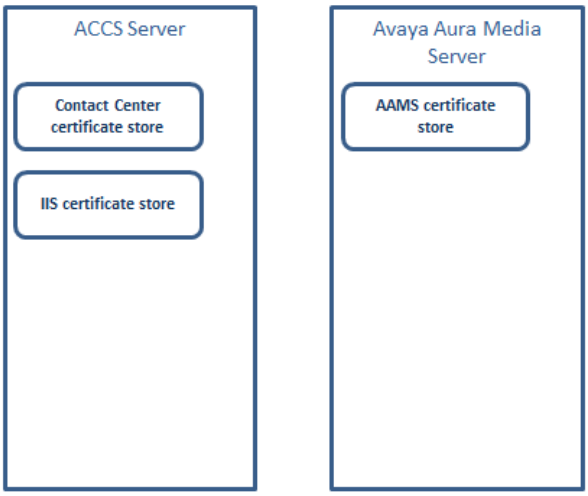


Figure 16: Example of security stores on an ACCS server with standalone Avaya Aura® Media Server

The following table lists the security stores on the ACCS servers:

Página2097 de 3226.

Security store	Applications	Services that use this store	Managed by
ACCS security store	CCMS, CCT	TAPI-D CTI link	ACCS Security Manager
Windows 2012 IIS security store	CCMA, CCMM	CCMA CCMM Administration Agent Desktop Multimedia Services Orchestration Designer Outbound Campaign Management Tool CCT Web Administration	ACCS Security Manager

ACCS services that can use TLS security

The following table lists all the ACCS services that must be secure, or can be configured to be not secure.

ACCS Service	Always secure	Security optional
TAPI-D CTI connection	Y	
Agent Browser application	Y	
CCMA Administration		Y
CCMM Administration		Y
Agent Desktop		Y
Orchestration Designer		Y
Outbound Campaign Management Tool		Y
ACCS Web Services		Y
CCT Web Administration		Y

- These services all use the server certificate that you configure in Security Manager. If you change this certificate, the change impacts all the services.
- You must use a certificate for TAPI-D CTI services and Agent Browser application. You generate this certificate in ACCS Security Manager. The CTI connection between ACCS and IPO requires Mutual Transport Layer Security (MTLS).

  The IPO server has a server certificate and must have the ACCS root certificate. The ACCS server has a server certificate and must have the IPO root certificate.
- You must use a certificate for Web Services, unless you turn off Web Services security. You use the certificate in Security Manager.
- You must use a certificate for Avaya Aura® Media Server. On an ACCS with Avaya Aura Media Server, you can use the server certificate you created in Security Manager.

Contact Center automatically backs up a new security store when you create it. This allows you to recover from situations where the store is damaged or deleted between sending the Certificate Signing Request (CSR) to a Certificate Authority (CA), and receiving a signed certificate back from

Página2098 de 3226.

the CA. The location for this automatic security store backup is `D:\Contact Center \autoBackUpCertStore`. Do not overwrite or delete this backup location.

Avaya Contact Center Select Security Manager

Avaya Contact Center Select (ACCS) includes a number of services that you can secure by using the HTTPS protocol.

ACCS Security Manager provides an interface for managing the security certificates in the ACCS security store and the IIS security store. ACCS supports the management of the IIS security store only through Security Manager: do not use IIS functions to manage the IIS security store on an ACCS server. Security Manager supports importing chained certificates, and places these certificates in the security store for distribution across the solution.

Server certificates

Each security store must have a server certificate signed by a CA, and a root certificate from the same CA. In ACCS, you can use the same server certificate in all the security stores on a single server. You can also generate different server certificates for each security store on a single server. You cannot use the same server certificate on two different servers.

Certificate Authority root certificates

When a client initiates a secure connection with a server, it must have a root certificate from the CA that provided the signed server certificate. If the client does not have a matching root certificate, it does not complete the connection. If the client has a root certificate from a given CA, it can trust any server certificate signed by that CA.

Avaya recommends that you use a single CA to sign all the certificates in your contact center. This simplifies the deployment process, because you need to distribute only a single root certificate to all the clients.

Página2099 de 3226.

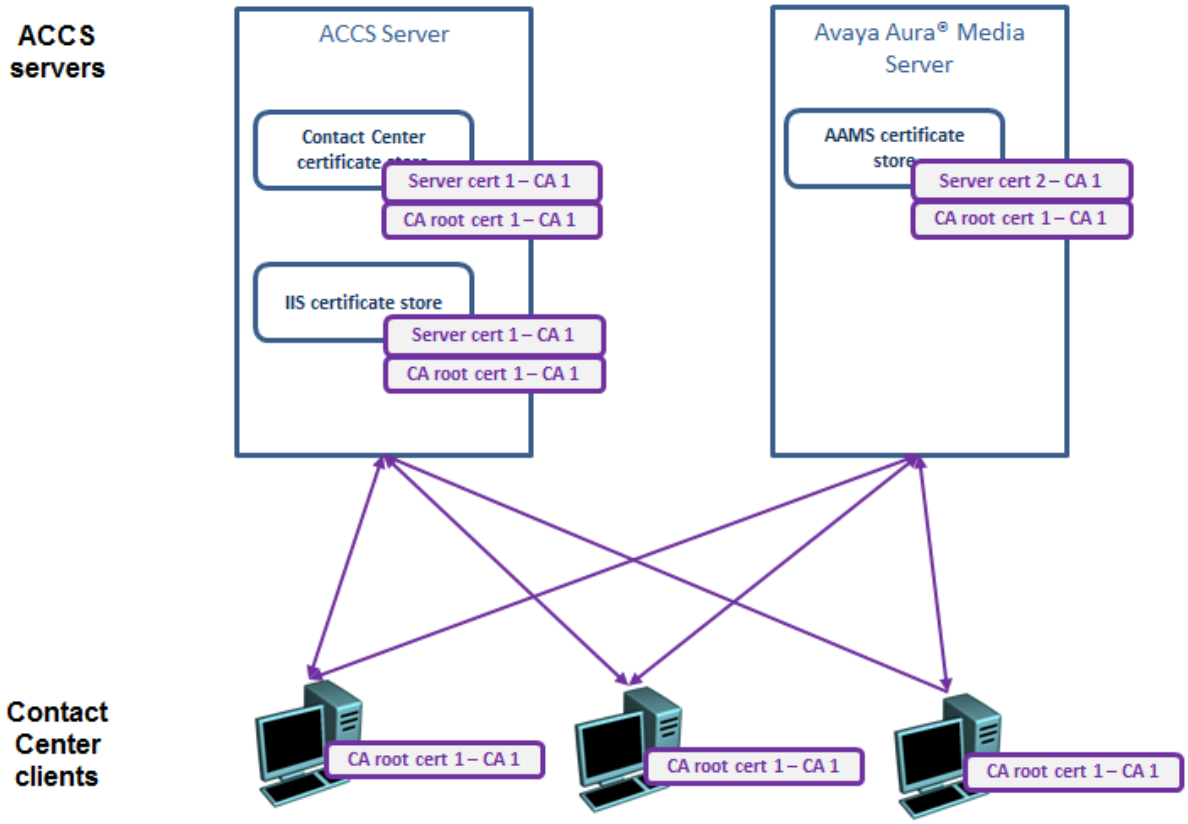


Figure 17: Example of how a single CA root certificate can work with different server certificates signed by the same CA

If you want to use different CAs to sign certificates for your different servers, you must copy the root certificate from each CA to all the clients in your contact center. For some ACCS Web services, ACCS servers can act as clients of other servers. Therefore you must ensure that the ACCS servers also have the required CA root certificates.

Página2100 de 3226.

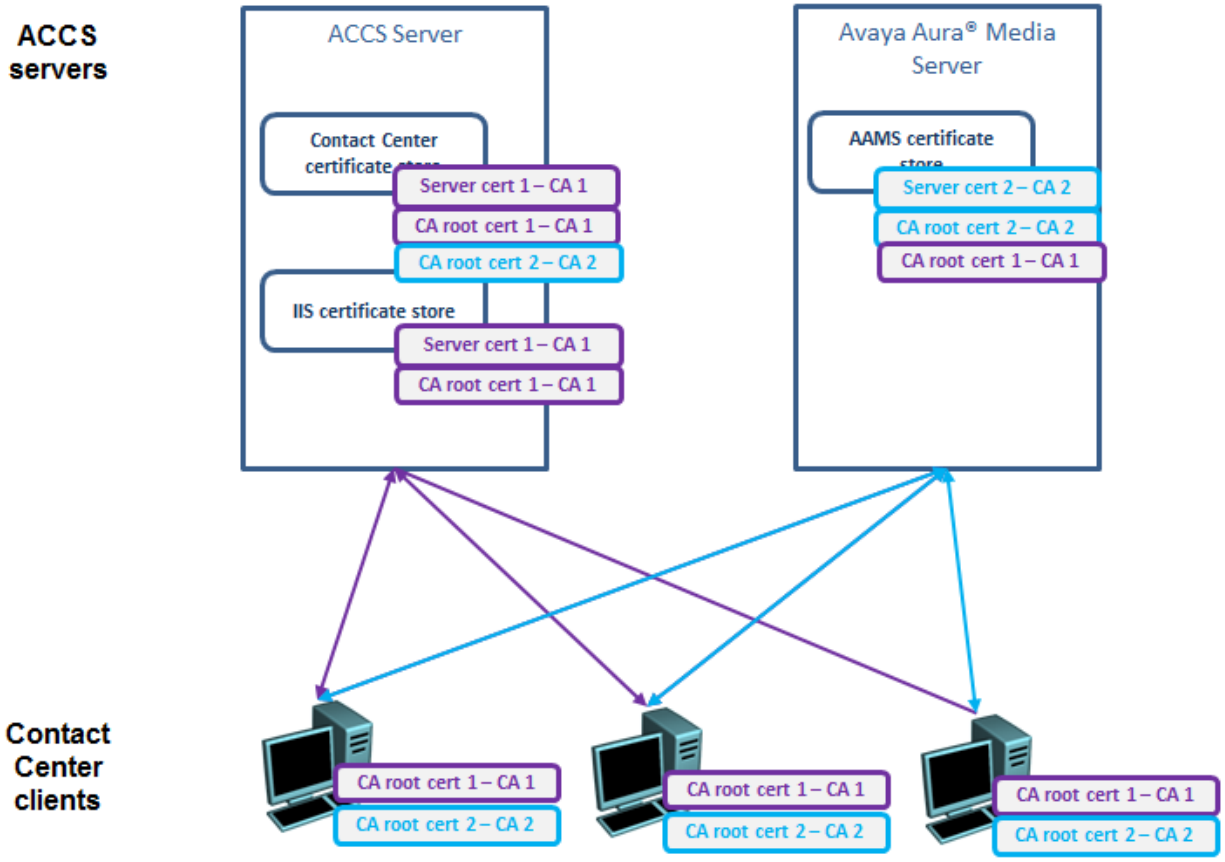


Figure 18: Example of how clients must have the CA root certificates from each CA that signed a server certificate, if the contact center uses server certificates signed by different CAs

You can distribute root certificates to client computers using a Group Policy on Microsoft Windows Server 2012.

TLS Security in a Business Continuity environment

If you implement Business Continuity (BC), Avaya Contact Center Select (ACCS) clients and servers must be able to communicate with the active contact center server, the standby contact center server, and the managed name of the BC server pair.

In a BC system, create a security store with Subject Alternative Names (SANs). The security store for a BC pair must have the common name of the ACCS server, and a SAN for:

- the ACCS server name
- the managed name of the BC pair

Página2101 de 3226.

This ensures clients connecting to ACCS using the managed name do not get warnings that the server certificate name does not match the server name.

ACCS supports using the same certificate on both the active server and the standby server in the BC pair.

Avaya recommends that you plan your BC active, managed, and standby names in advance of creating a new security store. In this way you can create your certificates once using SANs during the initial commissioning, instead of re-creating certificates when you commission BC.

Migrating secured Contact Center systems

You cannot migrate a Contact Center security store from Release 6.x to Release 7.0. If you are migrating a secure Contact Center system from Release 6.x, you must create a new security store on the Release 7.0 Contact Center server.

Avaya Contact Center Select Security store notifications

Security certificates contain an expiration date and they are not valid after this date. If the security certificates used by Avaya Contact Center Select (ACCS) expire, the contact center loses call control and stops functioning.

Security Manager provides a security store inspection utility to help you monitor and maintain valid security certificates. You can use Security Manager to schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. The inspection utility checks the status of the security certificates in the ACCS security store. If any of the security certificates are due to expire within a month, the inspection utility sends a notification email to the contact center administrator. The contact center administrator must then refresh the security certificates.

Security Manager provides the notification email; it cannot renew expired security certificates. For uninterrupted ACCS functionality, if you receive an email about upcoming certificate expiration dates, you must renew the security certificates before they expire. Security Manager uses the Microsoft Windows Task Scheduler to schedule the weekly security store inspection. You must ensure that there is a Microsoft Windows user account that has the necessary privileges from which Security Manager can schedule a task on Windows Task Scheduler. You can use the Windows administrator account that you used to install ACCS to add a task to Windows Task Scheduler.

Security Manager uses a specified Simple Mail Transport Protocol (SMTP) server to send the notification emails to the administrator’s email address. ACCS does not provide this SMTP server. You must provision this SMTP server and ensure that the ACCS server can communicate with it at all times. ACCS does not support Transport Layer Security (TLS) connectivity to this SMTP server.

Página2102 de 3226.

Server Message Block signing

Contact Center installs and updates modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital tag into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

If you do not want to use SMB signing, you can disable it by modifying the Windows Server 2012 local group policy.

Página2103 de 3226.

Chapter 13: Avaya Contact Center Select port matrix

This section lists the ports used by Avaya Contact Center Select. The Avaya Contact Center Select server contains the following components:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server

These components use the following ports.

Contact Center Manager Server port requirements

Contact Center Manager Server uses ports for communication between its own components. Most ports do not have implications for external network components like firewalls; however some ports might be used externally and therefore can affect an external firewall. In particular, port 10000 is a hard-coded port used to enable interoperability between Contact Center applications and external third-party applications (applications developed using the Real-Time Data (RTD) API).

No third-party application installed on Contact Center Manager Server can use the ports listed in the following table as it can cause the Contact Center Manager Server application to malfunction.

The following table shows the ports that Contact Center Manager Server uses.

Página2104 de 3226.

Table 13: Contact Center Manager Server port usage

CCMS port number	Functionality
445	TCP port used Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
1550	HDX CAPI
1972	Caché database, and Caché shadowing
4422	HDX NameService
12668–12670	TraceControl
10000	Hardcoded Toolkit Name Service
10001–10082	Networking
10038	NCP_CHANNEL—This channel is used to communicate between the NCP of one node to the NCP of another node. The NCP on one node sends sanity messages to the other node through this port.
10039	ASM_CHANNEL—Different modules like NCP and TFE send messages to ASM through this channel.
10040	NCP_ASM_CHANNEL—ASM uses this channel to send messages to NCP.
10060	ASM_Service—The ASM service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to the ASM service through this port.
10062	NCP_Service—The NCP service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to NCP on this port.
3998	License Manager destination port—This is the first of 10 consecutive ports required for license management.
3999–4007	License Manager client source port
3389	Remote Desktop Connection for support
9080–9083	Web Services Open Interfaces
9086	CC Web Statistics
9100	XMPP Web Service Server Port
9120	XMPP Web Service Client Port
57012	System Management and Monitoring Component (SMMC) system tray.

Contact Center Manager Administration port requirements

The following table shows the ports that Contact Center Manager Administration uses.

Página2105 de 3226.

Table 14: Contact Center Manager Administration port usage

CCMA port number	Functionality
TCP 80	For Internet Explorer communication.
TCP 443	For secure HTTP communication (only applicable if SSL is enabled for secure Internet Information Services (IIS) communication).
TCP Port 445	Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
TCP Port 3389	For remote desktop connection.
TCP Port 25 (SMTP)	For the Historical Reporting component to send email notifications when reports are printed and saved.
TCP Port 8200	For the Emergency Help component on the client PC.
UDP ports 6020, 6030, 6040, 6050, 6060, 6070, 6080, 6090, 6100, 6110, 6120, 6130	For the CCMA server to receive IP multicasting data from CCMA Server (needed for Real-Time Reporting and Agent Desktop Displays).
UDP ports 7020, 7030, 7040, 7050, 7060, 7070, 7080, 7090, 7100, 7110, 7120, 7130, 7140, 7150	For the CCMA server to send IP multicasting data to client PCs (needed for Real-Time Reporting and Agent Desktop Displays).
UDP ports 7025, 7035, 7045, 7055, 7065, 7075, 7085, 7095, 7105, 7115, 7125, 7135, 7145 and 7155	For the CCMA server to send IP unicast data to client PCs. This is an optional method of sending the data required for Real-Time Reporting. If you do not use the multicast method, then you must configure the unicast option. You can also use a combination of the two methods.
TCP Port 10000	Used by the Nameservice process on the CCMA server (nbnmsrvc.exe). It permits communication between the CCMA server and the server in Contact Center Manager Server. **Important:** The default port for the third-party software. This conflicts with the default port used by the CCMA Toolkit NameService. To avoid issues with CCMA functionality when using Veritas Backup Exec, you must change the default port of Veritas Backup Exec to another port number that is not being used by the network.
Default UDP port 3998	License Manager destination port.
Default UDP ports 3999 - 4007	License Manager destination source port.

Communication Control Toolkit port requirements

The following table shows the port numbers required for Communication Control Toolkit (CCT).

Página2106 de 3226.

Table 15: Communication Control Toolkit port usage

CCT port number	Functionality
1972	Caché database, and Caché shadowing solutions.
3998	License Manager (LM) destination port, which is the first of 10 consecutive ports required for license management.
3999 - 4007	LM client source ports.
5000	To connect to the server in CCMS.
8081	Default port of the Apache Tomcat Server which hosts the CCT Web Administration.
8085	For CCT services to access the CCT database.
8098	For the Contact Management Framework on the CCT server.
8099	For the Contact Management Framework on the CCT server.
8087	For CCT CMF component.
9000	For CCT WebAdmin component.
9010	For CCT CMF component.
11110	Used by the CCT Server service for the CMF Web Service - Callback port.
11111	Used by the CCT Server service for the CMF Web Service - Web server port.
29373	Listens for requests from CCT client applications.
29374	Data Access Layer Service listens for requests from CCT Remote Administration Console.

Contact Center Multimedia port requirements

The following table lists the configurable Multimedia ports.

Table 16: Contact Center Multimedia ports

Port	Host	Client	Network interface	Functionality
1972	Contact Center Multimedia	Contact Center Manager Administration Server	Contact Center Multimedia Caché database	Port opened on database for reporting. Caché database, and Caché shadowing.
445	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks.	Windows File and Printer Sharing for Microsoft Networks. Required when

Table continues…

Página2107 de 3226.

Port	Host	Client	Network interface	Functionality
				copying data between active and standby servers using Windows File Sharing.
110	Email server	Email Manager	Email server POP3	Receiving email
143	Email server	Email Manager	Email server IMAP	Receiving email
995	Email server	Email Manager	POP3 over SSL (optional)	Receiving secure email (optional)
993	Email server	Email Manager	IMAP over SSL (optional)	Receiving secure email (optional)
110	Email server	Email Manager	POP3 over TLS (optional)	Receiving secure email (optional)
143	Email server	Email Manager	IMAP over TLS (optional)	Receiving secure email (optional)
25	Email server	Email Manager	SMTP	Sending email
25	Email server	Email Manager	SMTP over TLS (optional)	Sending secure email (optional)
80	Contact Center Multimedia Server	Any Web services client (Agent Desktop, OCMT, and third-party Web services)	SOAP protocol	Accessing http Web services
29373	Communication Control Toolkit Server	Agent Desktop	Communication Control Toolkit	Remote access from clients to Communication Control Toolkit server (for Agent Desktop application)
57012	System Management and Monitoring Component (SMMC) system tray	System Management and Monitoring Component (SMMC) system tray	System Management and Monitoring Component (SMMC) system tray	Database shadowing

Avaya Aura® Media Server port requirements

The following table shows the port numbers required for Avaya Aura® Media Server on Windows Server 2012 R2.

Página2108 de 3226.

Table 17: Avaya Aura® Media Server port usage–Windows Server 2012 R2

Port	Type	Permit in TCP Filter	Description
1027	TCP	Yes	License Server
1028	TCP	No	System Monitor mchb
3306	TCP	Yes	MySQL
3389	TCP	Yes	Remote Desktop
3867	SCTP	No	Diameter over SCTP
3868	TCP	No	Diameter over TCP
3869	TCP	No	Diameter over TLS
4001	TCP	No	IvrMP MSLink
4004	TCP	No	Sip UA MSLink
4005	TCP	No	Resource Manager ExtSess
4014	TCP	No	SIP UA cmd i/f
4015	TCP	No	Resource Manager and i/f
6080	TCP	No	Agent Greeting
7080	TCP	No	ConfMP MSLink
7410	TCP	Yes	SoapServer
7411	TCP	Yes	SoapServer TLS
8080	TCP	Yes	EM HTTP
8443	TCP	Yes	EM HTTP(s)
11004	TCP	No	DiamC MSLink
11014	TCP	No	DiamC and i/f
19899	TCP	Yes	Resource Manager CPLink
19999	TCP	Yes	IvrMP ssdata
20005	TCP	Yes	CStore MSLink
20007	TCP	Yes	CStore RTFT
20009	TCP	Yes	IvrMP RTFT
21000	TCP	No	Voice XML Interpreter IPC
51000	TCP	No	Resource Manager IPC
51001	TCP	No	Legacy MPS Alarm deamon
51003	TCP	No	CCXML Interpreter IPC

The following table shows the port numbers required for Avaya Aura® Media Server on Linux.

Página2109 de 3226.

Table 18: Avaya Aura® Media Server port usage–Linux

Port	Type	Permit in TCP Filter	Description
1027	TCP	Yes	License Server
1028	TCP	No	System Monitor mchb
3306	TCP	Yes	MySQL
3867	SCTP	No	Diameter over SCTP
3868	TCP	No	Diameter over TCP
3869	TCP	No	Diameter over TLS
4001	TCP	No	IvrMP MSLink
4004	TCP	No	Sip UA MSLink
4005	TCP	No	Resource Manager ExtSess
4014	TCP	No	SIP UA cmd i/f
4015	TCP	No	Resource Manager cmd i/f
5060	TCP	Yes	SIP over TCP
5060	UDP	No	SIP over UDP
5061	TCP	Yes	SIP over TLS
6080	TCP	No	Agent Greeting
7080	TCP	No	ConfMP MSLink
7410	TCP	Yes	SoapServer
7411	TCP	Yes	SoapServer TLS
8080	TCP	Yes	EM HTTP
8443	TCP	Yes	EM HTTP(s)
11004	TCP	No	DiamC MSLink
11014	TCP	No	DiamC and i/f
19899	TCP	Yes	Resource Manager CPLink
19999	TCP	Yes	IvrMP ssdata
20005	TCP	Yes	CStore MSLink
20007	TCP	Yes	CStore RTFT
20009	TCP	Yes	IvrMP RTFT
20011	TCP	No	Resource Manager IPC
21000	TCP	No	Voice XML Interpreter IPC

UDP Port Range is required for media processing. All starting UDP ports are configurable.

Página2110 de 3226.

Table 19: Required UDP Port Range

Operating System	UDP Port Range
Windows Server 2012 R2	20000 to 45499
Linux	6000 to 32599

Página2111 de 3226.

Index

Numerics

1.2 TB ... 69
1200 GB ... 69
8–core CPU ... 68
900 GB ... 69

A

adding company images
  signatures ... 20
adding company logos
  signatures ... 20
AD-LDS ... 17
agent
  Whisper Coaching ... 25
agent browser application
  browser compatibility ... 178
  requirements ... 177
Agent Desktop
  automatic insertion of a leading digit ... 15
  Citrix support ... 176
  display login history ... 21
  file browsing directory changed to user directory ... 22
  force password complexity for Multimedia accounts ... 24
  support for copying CLID ... 20
  support for forced Not Ready reason codes ... 21
Agent Desktop embedded web browser
  uses the latest version of the Internet Explorer installed on the client system ... 23
Agent Desktop requirements ... 164
antivirus software ... 78, 88, 116
application sequencing ... 149
Avaya Aura Experience Portal ... 145
Avaya Aura Media Server ... 90
Avaya Aura Media Server port requirements ... 193
Avaya Media Server ... 15
Avaya Security Advisory ... 56

B

Barge-in and Observation tone ... 15
billboard display
  skillset list sorted ... 25
BIOS ... 70, 100
browser compatibility
  agent browser application ... 178
Business Continuity ... 56

C

Caché database ... 17
Call Control XML ... 147
call disconnect ... 57
Call Force Answer Zip Tone ... 15
call recording ... 52
capacity limits ... 120
CCMA
  Citrix ... 162
  incorrectly entering a password ... 21
  password aging ... 19
  password expiry ... 17
  temporary lock out ... 21
CCMA port requirements ... 190
CCMM port requirements ... 192
CCMS port requirements ... 189
CCSA ... 15
CCT port requirements ... 191
CCT supported functionality ... 140
CCXML ... 147
changes in this release ... 15
Citrix support
  Agent Desktop ... 176
CLID ... 21
client requirements ... 160
configuration ... 44
Contact Center install account ... 31
Contact Center Manager Administration
  display failed login attempts ... 21
  display login history ... 21
Contact Center Services ... 15
copying CLID ... 20

D

data synchronization ... 39
Data transfer ... 146
DHCP ... 76, 87, 115
disk caching ... 72, 102
disk partitions ... 84
displaying
  failed login attempts ... 21
  login history ... 21
domain ... 54
DVD ... 63, 65, 74, 80

E

email message flow example ... 51
emergency license ... 18
Entry-level server ... 65
Exchange Server ... 29
Experience Portal ... 153, 155
external server interactions ... 50

Página2112 de 3226.

F

features 7.0 Feature Pack 1
add friendly name for web chat agent ... 24
Agent Desktop browsing directory ... 22
attachment filetype restriction ... 23
automatic refresh of non-staffed skillsets for real-time reporting ... 22
force password complexity ... 24
latest version of the Internet Explorer installed on the client system for embedded web browser in Agent Desktop ... 23
removal of the default Agent Desktop Dashboard password ... 25
skillset list sorted for billboard display ... 25
Whisper Coaching ... 25
features 7.0 Feature Pack 2
Agent Desktop integrated login ... 26
agent skillset assignment guardrails ... 26
changing CCMA password ... 31
increased CCMM customer contact ratio ... 26
synchronization of accssync user changes ... 27
firmware ... 71, 101
forced Not Ready reason codes ... 21
force password change
user logs on to CCMA for the first time ... 18
functions of telephony server ... 140

G

global requirements server name ... 74, 85, 113
guidelines for Java Runtime Environment ... 76, 86, 114
guidelines for service packs ... 76, 86, 114
guidelines for service updates ... 75, 85, 113
guidelines for utility software ... 77, 87, 115

H

H.323 ... 149
hard disk partitions ... 69, 84
hardware ... 109
hardware appliance ... 18, 109, 110
Hardware Appliance ... 118
hardware-assisted virtualization ... 99
hardware requirements ... 65, 66, 68
hardware requirements, Administrator ... 160
hardware requirements, Agent Desktop ... 165
High-end solution ... 68
host considerations vmware ... 99
Hyper-Threading ... 73, 103

I

interactions with external multimedia servers ... 50
IOPS ... 105
IP Office support ... 43
IP Office versions ... 29, 32

J

Java Runtime Environment guidelines ... 76, 86, 114

L

licensing ... 80, 108, 118
Licensing ... 36
limitations ... 59
localized languages ... 164

M

maximum capacity ... 120
Microsoft Exchange Server ... 29
Mid-range server ... 66
minimum hardware specification ... 19
minimum virtual machine specification ... 19
multimedia accounts
force password complexity ... 24
match the minimum password complexity criteria ... 24
multimedia external server interactions ... 50

N

naming server requirements ... 74, 85, 113
network requirements ... 167
notification
emergency license expiry ... 18
not supported
Agent desktop thick client deployment ... 29
NUMA ... 73, 102

O

Observation tone ... 15
offline security store ... 26
operating system Java Runtime Environment guidelines ... 76, 86, 114
operating system packs guidelines ... 76, 86, 114
operating system requirements ... 161, 166
operating system service update guidelines ... 75, 85, 113

P

password aging
CCMA ... 19
password expiry
CCMA ... 17
performance ... 70, 100
performance management ... 72, 101
P-header ... 148
Phonebook
automatic insertion of a leading digit ... 15

Página2113 de 3226.

P-Intrinsics 148
port matrix 189
port requirements Avaya Aura Media Server 193
port requirements CCMA 190
port requirements CCMM 192
port requirements CCMS 189
port requirements CCT 191
ports 176
Private Header 148
PVI 65

R

RAID 72, 102
related documentation 11
remote access support 140
Remote Agents 53
Remote Desktop Servicesgent Desktop
    A 26, 174
Removal of default security configuration 27
requirements
    agent browser application 177
requirements Java Runtime Environments 76, 86, 114
requirements port Avaya Aura Media Server 193
requirements port CCMA 190
requirements port CCMM 192
requirements port CCMS 189
requirements port CCT 191
requirements server name 74, 85, 113
requirements service packs 76, 86, 114
requirements service updates 75, 85, 113
requirements utility software 77, 87, 115
REST API integration 27
restriction
    attachment filetypes 23

S

sample flows 47
Screen Pop 148
scripting
    CLID and Wild CLID 21
security 56
Security Manager
    display failed login attempts 21
    display login history 21
Server Message Block signing 188
server name requirements 74, 85, 113
serviceability enhancements
    Agent Desktop third-party controls upgrade 20
    security enhancements 20
service packs guidelines 76, 86, 114
service updates guidelines 75, 85, 113
Session Initiation Protocol 147
SGM 147
signatures
    add company images 20
signatures *(continued)*
    add company logos 20
SIP 147
SIP environment
    CLID and Wild CLID 21
SIP Gateway Manager 147
SIP signaling 149
skillset list sorted 25
snapshot considerations 104, 105
SOCD 57
software 109
software appliance 81
software specifications 112
software utility guidelines 77, 87, 115
support 14
supported main features 123
supported multimedia features 123
supported reporting features 123

T

Telephony Devices 138
telephony features 129
telephony server functions 140
temporary lock out
    CCMA 21
third-party software 163, 167
touchscreen 165
touch screen 165

U

UEFI 71
Universal Call Identifier 149
unused hardware 73, 103
user logs on to CCMA for the first time
    force password change 18
utility software guidelines 77, 87, 115
UUI 149

V

videos 14
virtualization 103
Virtualization 107
virtualization considerations 97
virtual machine 83, 84
VMware 102
vmware host 99
VMXNET 103
Voice XML 147
VXML 147

W

WebLM 91

Página2114 de 3226.

Whisper Skillset 15
Wild CLID 21
workgroup 54

Página2115 de 3226.

Administering Avaya IP Office™ Platform with Manager

March 11, 2021

Notices

© 2021 copy rights

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Server Edition Resiliency

Resilience

A single Server Edition Primary server supports redundant hard disk drives and power supply units. You can also configure Alternate Route Selection.

Add a Server Edition Secondary to provide resilience at any level. The Server Edition Secondary Server provides resilience for the Server Edition Primary Server users, H.323 and SIP extensions, hunt groups, and voicemail without any administration. The Server Edition Secondary server can provide resilience for Avaya one-X® Portal for IP Office.

A Server Edition Expansion System can be backed up to either the Server Edition Primary, Server Edition Secondary, or another Server Edition Expansion System. The dual star Multi-Site Network topology when a Server Edition Secondary Server is present supports diverse routing between all nodes.

For Server Edition Select deployments, IP Office Lines (SCN trunks) can be configured between Server Edition Expansion Systems. Hunt groups can be configured local to the Expansion system and resiliency for hunt groups and phones can be configured, with failover to the Server Edition Primary, Server Edition Secondary, or another Server Edition Expansion System.

At all times, no server hardware is forced to be idle, enabling you decide whether to provide true redundancy, or shared resource resilience.

The IP Office Server Edition Solution provides resilience for supported H.323 phones, SIP endpoints, and DECT R4 deployments. IP Office Lines between systems can be configured to allow control to be automatically passed to a backup IP Office when the home system is not available.

Resilient components

The following components of IP Office Server Edition Solution are resilient:

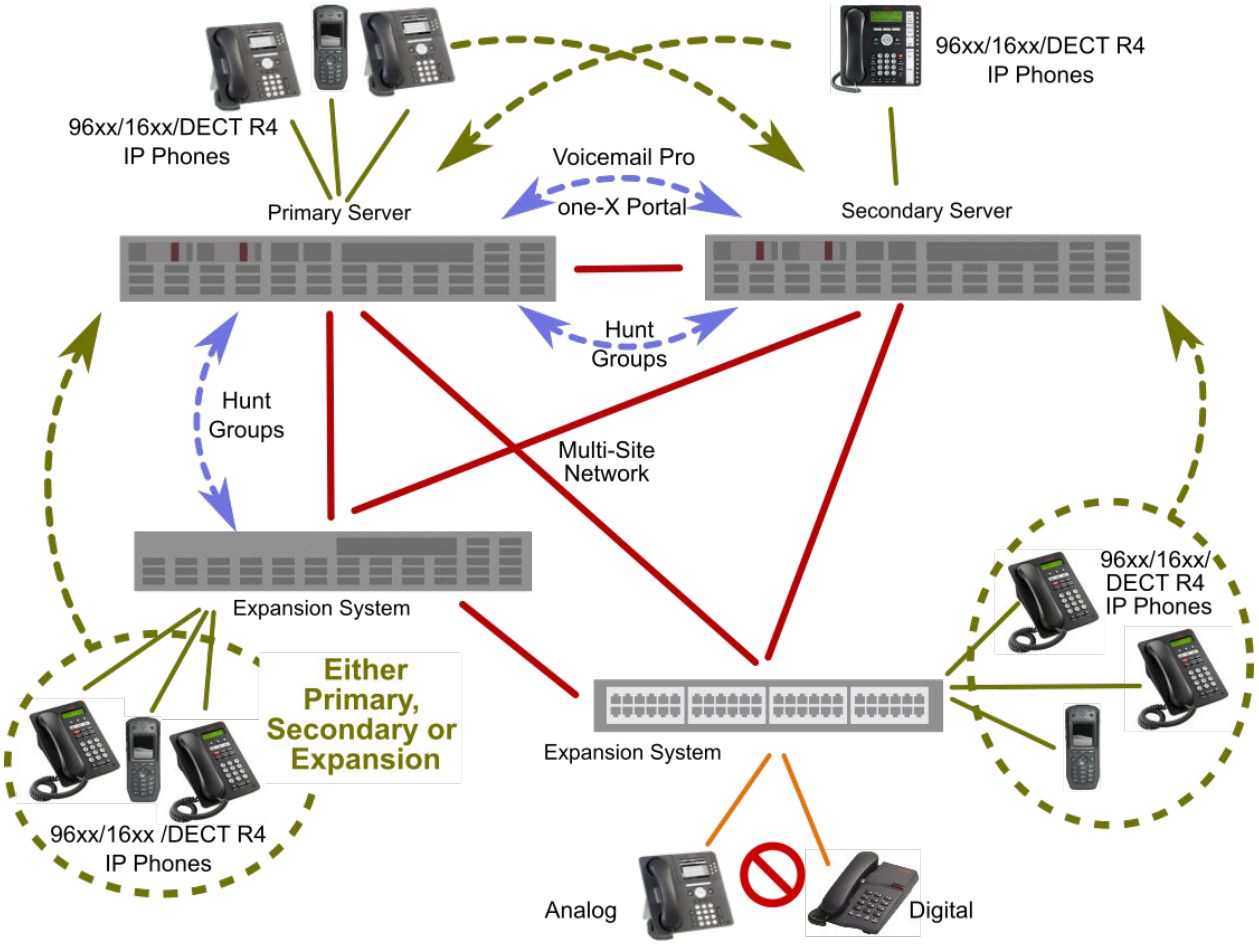
- IP Office Server Edition
- Voicemail Pro server
- Avaya one-X® Portal server
- H.323 telephones
- SIP endpoints
- DECT R4
- Hunt groups
- Interdevice links
- Trunks
- Incoming Call Routes
- Management

Multisite network

A multisite network enhances resilience by providing the following capabilities:

- Transparency for most of the features
- Resilience of users and hunt groups
- Back up system for Voicemail Pro
- Network topology provides resilience
- None of the hardware is idle
- Simple to activate resilience

Figure 1. Resiliency Architecture



Resilient management

You can continue to administer and manage the failure of IP Office Server Edition server and devices in an IP Office Server Edition Solution network through the Server Edition Secondary Server. This provides management without the offline capability, and a facility to realign the configuration after the outages have been resolved. The resynchronization feature highlights the time and source of configuration change and enables the administrator to decide which change set to retain. In addition, you can directly manage each device and application to allow configuration whilst isolated. You can use the resynchronization capability to realign the configurations after the devices are reconnected.

Avaya IP Office™ Platform Solution Description

Release 11.0.4
May 2019

© 2018-2019, Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order with a default of one (1) Cluster if not stated. “Cluster” means a group of Servers and other resources that act as a single system.

Enterprise License (EN). End User may install and use each copy or an Instance of the Software only for enterprise-wide use of an unlimited number of Instances of the Software as indicated on the order or as authorized by Avaya in writing.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

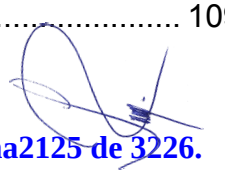
The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 7
Purpose 7
Change history 7
Chapter 2: Avaya IP Office™ Platform overview 10
IP Office editions 10
New in this release 11
Features 13
Topology 14
Networking 14
Private circuit switched voice networking 14
Public voice networking 15
Packet-based voice and data networking 18
Internet protocol telephony 19
Computer Telephony Integration 27
Components 29
Hardware components 29
Phones 38
IP Office applications 40
Chapter 3: Solution specifications 67
Reference configurations 67
IP Office editions 67
Other deployment options 73
Hardware and software options 84
Server specifications 85
Operating system and browser support 87
Customer-provided PC requirements 91
Virtual environment requirements 93
Interoperability 93
Phone interoperability 95
IP Office and Avaya Aura® Communication Manager interoperability 99
BCM and IP Office interoperability 100
Security specification 101
Platform and application security details 102
Port assignments 105
Typical upgrade paths 106
BCM with CS1000 to IP Office migration 107
IP Office Branch migration 108
Licenses 109
PLDS licensing 109



Página2125 de 3226.

Migration of ADI licenses 110
Server Edition Centralized and Nodal licensing 111
Basic Edition license for new systems 118
Essential Edition and Preferred Edition licenses 118
Server Edition licenses 119
Branch licenses 120
Small Community Network licenses 120
Trunk licenses 121
User licenses 122
IP endpoint licenses 126
Trial licenses 126
Upgrade licenses 127
Chapter 4: Resources 130
Documentation 130
Finding documents on the Avaya Support website 131
Training 131
Viewing Avaya Mentor videos 132
Additional IP Office resources 133
Product compatibility 133
Support 133
Using the Avaya InSite Knowledge Base 134
Accessing Avaya DevConnect Application Notes 134
Glossary list 136

Página2126 de 3226.

Chapter 1: Introduction

Purpose

This document describes IP Office from a holistic perspective focusing on the strategic, enterprise, and functional views of the architecture. This document also includes a high-level description of solution specifications and available reference configurations.

Change history

The following table describes major changes made in this document for each release.

Issue	Release date	Summary of changes
Release 11.0 FP4	February 2019	• Updated the What's new topic with the Release 11.0 FP4 features. • Updated Avaya Equinox™ topic to add content on Shared Control and Avaya Vantage™ support. • Updated Avaya one-X® Portal topic to add serviceability enhancements. • Updated the licensing information. • Updated the supported browsers section. • Updated Media Manager section to add new features supported in IP Office Release 11.0 FP4. • Listed VMWare ESXi 6.7 as a supported Hypervisor.

Table continues…

Página2127 de 3226.

Issue	Release date	Summary of changes
Release 11.0	May 2018	• Updated the What's new topic with the Release 11.0 features. • Removed references to IP Office Integrated Contact Reporter. • Removed references to IP Office Video SoftPhone as it is not supported in Release 11.0 • Added content about the following applications: - Cloud Operations Manager - Avaya Equinox™ client for IP Office - Avaya IP Office Web Client • Updated the Web Manager section to add content about Configuration Dashboard. • Updated Media Manager section to add new features supported in IP Office Release 11.0. • Added J169 and J179 phones to the phone interoperability and availability sections.
Release 10.1, Issue 1	June 2017	• Updated the "New in this release" section. • Added information about two new applications: IP Office Integrated Contact Reporter and IP Office Media Manager • Added information about additional hypervisor support in the "Virtual environment requirements" section • Added information about two new DECT phones: 3730 and 3735 • Added information about a new Management API/SDK, and two new CTI interfaces: Centralized CTI WebService API and SSI over Web Services • Added information about two new expansion modules: DS16B2 and DS30B2 • Added granular access information in the "Web Manager" section • Added extension information in the "System Status Application (SSA)" section • Updated the "Operating system and browser support" section

Table continues…

Página2128 de 3226.

Issue	Release date	Summary of changes
Release 10.0, Issue 1	July 2016	• Updated the “New in this release” section. • Replaced 3740 DECT handset references with 3745 DECT. • Updated Avaya Contact Center Select content. • Made the following major licensing updates: - Added more contextual information. - Updated license names and their associated codes. - Reorganized Server Edition licensing content. - Added Basic Edition licenses. - Clarified basic user license support.
Release 9.1, Issue 01.18	February 2016	This document was created to replace the *Avaya IP Office Product Description*.

Página2129 de 3226.

Chapter 2: Avaya IP Office™ Platform overview

The Avaya IP Office™ Platform is a cost-effective telephony system that supports a mobile, distributed workforce with voice and video on virtually any device. IP Office is an integrated, modular communications solution that scales up to 3000 extensions and 150 sites in a multisite network with resiliency. Match a deployment model to infrastructure needs from simple appliances to virtualized software in a data center with options in between. Improve customer experience and contact center agent efficiency with powerful, affordable multichannel functionality for voice, email and web chat. The solution combines collaboration software plus multichannel contact centers, networking, security and video.

IP Office provides a hybrid PBX with both Time Division Multiplexing (TDM) and IP telephony with trunk support, used in either mode or both concurrently. IP Office has data capabilities built-in, providing IP routing, switching and firewall protection, between LAN and WAN (LAN2).

In addition to basic telephony services and voicemail, IP Office offers both hard phone and soft phone options. Soft phone applications are designed to provide flexibility for remote workers and to allow workers to access telephony services, such as making and receiving calls, voicemail, and call forwarding from their computer or mobile device.

IP Office editions

IP Office also offers advanced features such as audio and video conferencing and voice over IP to meet the evolving needs of small, medium, and large enterprises.

IP Office is available in many deployment models based on the size of the enterprise and the features required using one or all the following elements:

- Virtualized IP Office software running in a virtual machine
- Dedicated server
- IP Office 500 V2 (IP500 V2) control unit

Página2130 de 3226.

Edition	Platform	Business size (users)	Addresses business needs
Basic Edition	IP500 V2	Less than 25	Simple telephony and messaging capabilities only
Essential Edition	IP500 V2	20–99	Simple telephony and messaging capabilities plus IP telephony with essential mobility
Preferred Edition	IP500 V2	21–250	Essential Edition capabilities plus unified communications with preferred mobility
Server Edition	Linux Server, IP500 V2 and Linux Expansion	100 — 2000	Preferred Edition on a software-based solution.
IP Office Select	Linux Server, IP500 V2 and Linux Expansion	100 — 3000	Preferred Edition on a software-based solution with increased scale and resiliency.
Server Edition or IP Office Select with Virtualized Software	Virtualized	100 — 2000 (or) 100 — 3000	Preferred Edition on a software-based solution with increased scale and resiliency.
Server Edition or IP Office Select hosted in Cloud	Cloud (Powered by Avaya)	100–2000 (or) 25–3000	Preferred Edition on a software-based solution with increased scale and resiliency.

IP Office Essential Edition and Preferred Edition are also referred to as IP Office Standard Mode. Each edition builds upon the next to offer additional functionality.

New in this release

IP Office™ Platform Release 11.0 Feature Pack 4 offers the following new features and capabilities:

Note:

Features are available worldwide unless otherwise specified. Not all features are supported on all platforms and phones. See the descriptions for details.

Fallback twinning

With this feature, IP Office redirects calls to the users twinned mobile number when the primary extensions are unreachable even if mobile twinning is disabled. This feature provides a mechanism for failing over to an external device such as mobile and PSTN if a customer site supporting IP Office phones, loses connectivity with the Cloud data center. The following two short codes are available for disabling and enabling mobile Fallback twinning:

- **Set Fallback Twinning Off**: To disable Fallback twinning

Página2131 de 3226.

- **Set Fallback Twinning On**: To enable Fallback twinning

IP Office Media Manager enhancements

The following features have been added to IP Office Media Manager:

- Delete recordings
- Audit trail: Administrators can keep track of the usage of recording files in IP Office Media Manager. The following type of usage of a recording can be tracked using this feature:
  - Delete
  - Download
  - Replay
  - Search

Security enhancements for registration of SIP devices

The new security enhancements enable administrators to allow or disallow registration of SIP devices in IP Office based on their User Agent strings. Administrators can use the configuration settings to add, modify, or remove SIP User Agent strings to SIP UA Blacklist, SIP UA Whitelist, and IP Whitelist. Subsequently, the **Allowed SIP User Agents** setting can be used to select which SIP User Agents are allowed for registering with IP Office.

Automatic user synchronization with Avaya Spaces

IP Office R 11.0 FP4 system users and user details created for Avaya Equinox™ can be automatically synchronized with Avaya Spaces server. To use and receive additional Avaya Spaces features, the details of users configured for Avaya Equinox™ need matching users configured on the Avaya Spaces server. The synchronization can be done manually or automatically.

Default extension password

The default extension password or PIN is different than the user password and is much stronger with a minimum of nine digits. IP Office R11.0 FP4 deployments provide for an auto-generated default extension PIN of 10 digits, which can be viewed and modified later. An eye icon next to the **Default Extension Password** field in the user interface can be used to view the existing default extension password.

Avaya Equinox™ support on Avaya Vantage™

Avaya Equinox™ is supported on Avaya Vantage™ phones K165 and K175 in IP Office R 11.0 FP4 deployments.

Route incoming SIP trunk calls based on an optional SIP header

IP Office can be configured to use the optional **P-Called-Party** header in incoming SIP message for call routing. IP Office reads the `P-Called-Party ID` header in the SIP message and routes the incoming SIP calls based on it.

SIP and H.323 Registrars disabled by default

To secure IP Office R 11.0 FP4 from vulnerabilities, the **H.323 Gatekeeper Enable** and **SIP Registrar Enable** fields are disabled by default. Whenever a new H.323 or SIP extension is added and the corresponding registrar is not enabled, IP Office system displays an error message and prompts to enable the fields. When resiliency support is enabled on an IP Office Line in systems having IP extensions and the systems do not have the corresponding registrars enabled,

Página2132 de 3226.

IP Office system displays an error message and prompts administrators to enable the corresponding registrars.

Avaya Equinox™ shared control

Avaya Equinox™ can now be used in shared control mode with desk phones. The shared control feature is available even when the Avaya Equinox™ client and desk phones are registered on different systems within the same network.

Conference Join

Conference Join feature allows two separate conferences to be joined into one single conference that contains all the previous participants of both the earlier conferences. Once the conferences have been joined it is not possible to revert to the two separate conferences again.

JEM 24 button module support on Avaya J169/J179 IP Phone

Avaya J169/J179 IP Phone can support up to three JEM24 button modules. Each JEM24 has 24 dual-LED buttons with adjacent button label display. The button LEDs are used to indicate the status of the button feature whilst pressing the button is used to access the feature. A single JEM24 supports 72 programmable button slots. These are arranged in 3-pages, with pages accessed using the module's page scroll button. When multiple modules are connected to a phone, each module only supports a single page of 24 programmable button slots.

The modules automatically match the display settings of the phone to which they are connected - color with Avaya J179 IP Phone or greyscale with Avaya J169 IP Phone, font size, background image, screen saver. The button modules are powered though the phone. For more information, see the *IP Office Platform R11.0 J100 Series Telephone User Guide*.

Avaya J139 IP Phone

IP Office support for Avaya J139 IP Phone. Avaya J139 IP Phone is an advanced SIP desk phone that supports IP Office interactive menus and button programming. Avaya J139 IP Phone does not support all the advanced knowledge worker and contact center features that are available in Avaya J169 IP Phone and Avaya J179 IP Phone phones. For more information, see the *IP Office Platform R11.0 J100 Series Telephone User Guide*.

Serviceability enhancements in Avaya one-X® Portal

Avaya one-X® Portal supports a number of serviceability features such as displaying count of logged-in sessions, user avatar, option to block client versions, option to track repeated failed login attempts, and option to clear all sessions of a user.

Simplified Web Self-Administration

The enhanced interface is focused on simplifying the configuration and make it easier for non-technical users and provides a three step self-guided wizard for setting up the basic account. By default the new capability, that is running the wizard, is enabled for all users but the administrator can disable the capability or modify as required.

Features

See *Avaya IP Office™ Platform Feature Description* for detailed feature descriptions.

Página2133 de 3226.

Topology

There are many options for IP Office topology. For detailed information about all the deployment scenarios, see the related *Reference Configuration* documents for each deployment scenario.

Figure 1: IP Office systems connected to a single IP Office Manager endpoint

Networking

Private circuit switched voice networking

Where leased line circuits are used within a private networking scenario, these E1 or T1 interfaces are typically configured to use Q.SIG signaling between sites.

Q.SIG provides a level of voice feature transparency between PBXs and is the favored signaling standard within multiple vendor and international voice networks. The IP Office E1 or T1 module terminates a QSIG connection with a 120 ohm RJ45 interface.

Página2134 de 3226.

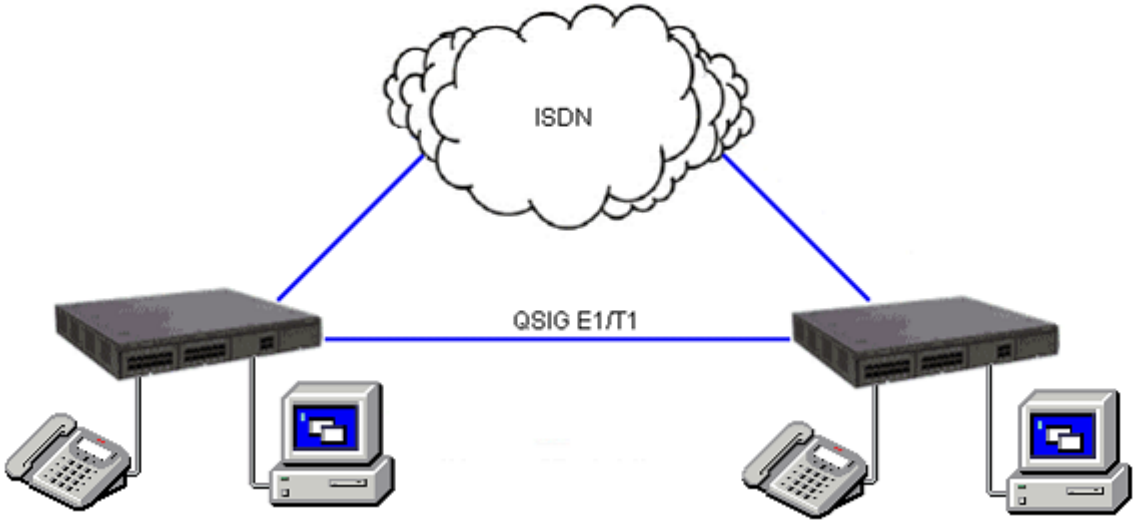


Figure 2: Circuit switched voice networking

IP Office supports the following Q.SIG services across this network:

Simple Telephony Call/Basic Call	ETS300 171/172
Circuit Switched Data Call/Basic Call	ETS300 171/172
Called/Calling Line ID Presentation	ETS300 173
Called/Calling Name Presentation	(SS-CNIP, SS-CONP, SS-CNIR) ETS300 237/238
Message Waiting	(SS-MWI) EN301 260/255
Transfer	(SS-CT) ETS 300 260/261

Public voice networking

IP Office supports a range of trunks and signaling modes for connection to the public switched telephone network (Central Office). Some of these lines are only available in certain territories; please check with your distributor for local availability. Primary rate trunks are available with either a single (24/30 channels) or dual trunk (48/60 channels).

ISDN Primary Rate (ETSI CTR4)

Service is provided by IP500V2 Universal PRI cards. ISDN Primary Rate provides 30 x 64K PCM speech channels over an E1 circuit and one signaling channel. Signaling Conforms to the ETSI Q. 931 standard with Cyclic Redundancy error Checking (CRC).

The following supplementary services are supported:

Página2135 de 3226.

Calling Line Identification Presentation (CLIP)	Provides the telephone number of the incoming call.
Calling Line Identification Restriction (CLIR)	Prevents the telephone number of the IP Office being presented on an outbound call.
Direct Dialing In (DDI)	Where the exchange provides the last x digits of the dialed number on an incoming call. This allows IP Office to route the call to different users or services.
Sub-addressing	Allows the transmission/reception of up to 20 digits, additional to any DDI/DID or CLIP information, for call routing and identification purposes.

IP Office supports the following features on both PRI and BRI trunks.

Note:

Feature availability depends on the ISDN service provider for which there may be charges.

Malicious Call Identification (MCID)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600) Short codes and button programming features are available so that users can trigger this activity at the ISDN exchange when required. This feature is NOT available on standard ISDN DSS1 telephones.
Advice of Charge (AOC)	(T3 digital and IP telephones only; Phone Manager) Advice of charge during a call (AOC-D) and at the end of a call (AOC-E) is supported for outgoing ISDN calls other than Q.SIG. The call cost is displayable on T3 telephones for call accounting purposes. IP Office allows configuration of call cost currency and a call cost mark-up for each user.
Call Completion to Busy Subscriber (CCBS)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, DECT telephones; Phone Manager) CCBS can be used where provided by the ISDN service provider. It allows a callback to be set on external ISDN calls that return busy. It can also be used by incoming ISDN calls to a busy user. This feature is not available on standard ISDN DSS1 telephones.
Partial Rerouting (PR)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, DECT telephones; Phone Manager) When forwarding a call on an ISDN channel to an external number using another ISDN channel, partial rerouting informs the ISDN exchange to perform the forward, thus freeing the channels to IP Office. This feature is not available on standard ISDN DSS1 telephones and it is not supported on Q.SIG.

Página2136 de 3226.

Explicit Call Transfer (ECT)	(Typically used by a third-party application) ECT is supported on the S0 interface. A Call to an S0 Endpoint can be transferred to any other device such as an analog, digital or IP endpoint or to any trunk. The normal usage of this feature is by a third party application connected through one or more S0 interfaces to IP Office. One example is the VoiceDirector, an automatic call assistant.

ISDN Basic Rate (ETSI CTR3)

Service is provided by IP500 V2 BRI cards. ISDN Basic Rate provides 2 x 64K PCM speech channels and one signaling channel using Q.931 signaling and CRC error checking. Both point to point and point to multipoint operation is supported. Multipoint lines allow multiple devices to share the same line; however point-to-point is the preferred mode.

Basic Rate supports all the services that are supported on the primary rate version with the addition of Multiple Subscriber Number. This service is usually mutually exclusive with the DDI/DID service and provides up to 10 numbers for routing purposes, very similar to DDI/DID.

E1R2 channel associated signaling

Service is provided by IP500 V2 Universal PRI cards.

The IP500 Universal PRI card configured as PRI E1R2 supports a single or dual RJ45 network connection. Each card provides channels that can be configured for MFC, Pulse or DTMF dialing dependent on the requirements of the network.

North American T1 Primary Rate

Service is provided by IP500 V2 Universal PRI cards. T1 Primary Rate provides up to 24 64K channels over a 1.54M circuit. Each channel of the T1 trunk can be independently configured (channelized) to support the following signaling emulations with handshake types of immediate, delay or wink.

- Loop-Start
- Ground-Start
- E&M Tie Line
- E&M DID
- E&M Switched 56K
- DID - Channels configured for DID/DDI support incoming calls only. The carrier or Central Office will provide the last x digits that were dialed to be used for call routing.
- Wink-Start

IP Office T1 trunks support both DNIS and ANI services, where available from the central office.

Dialed Number Identification String (DNIS)	Provides a string of digits to IP Office depending on the number dialed by the incoming caller. This string can then be used to route callers to individual extensions, groups or services.
Automatic Number Identification (ANI)	Provides IP Office with a number identifying who the caller is. This may then be used for routing or computer telephony applications.

T1 trunk cards incorporate an integral CSU/DSU, eliminating the need for an external unit. The CSU function allows the trunk to be put in loop-back mode for testing purposes. This can be set

Página2137 de 3226.

manually, using the monitor application, or automatically from a Central Office sending a Line Loop Back (LLB) pattern. The DSU function allows the T1 trunk to be shared between data and voice services.

North American Primary Rate Interface (PRI)

Service is provided by the IP500V2 Universal PRI cards. IP Office supports Primary Rate ISDN trunks on 5ESS or DMS100 central office switches provided by AT&T, Sprint, WorldCom and other Local Telcos. Channels can be pre-configured for the supported services or negotiated on a call-by-call basis.

Special services can be configured to route calls to local operators or pre-subscribed carriers for both national and international calls (SSS). Alternate carriers can also be selected through the configuration of IP Office Transit Network Selection (TNS) tables.

IP Office also supports the Calling Name and Number service over Primary Rate Trunks (NI2).

Analog trunks

Loop start	Loop start trunks are available on the IP Office Analog Trunk cards installed within the IP Office control unit, or on the Analog Trunk 16-port expansion modules (ATM16). The first two trunks on the ATM16 are automatically switched to power fail sockets in the event of power being interrupted. Powerfail is also available on the trunk card when fitted to a combination or phone card. They conform to the TIA/EIA-646-B standard. The loop start trunks also support incoming caller line identification (ICLID) conforming to GR-188-CORE and GR-31-CORE standards. IP Office can use this information to route calls or provide it to computer applications to display additional information about the caller.
Ground start	Ground Start trunks are only available on the ATM16, configured through IP Office Manager. The first two trunks on the module are automatically switched to power fail socket in the event of power being interrupted. They conform to ANSI T1.401 and TIA/EIA-646-B standards. Not available in all territories.

Packet-based voice and data networking

IP Office supports data network use for voice communication, called voice over IP (VoIP).

IP Office supports networked voice and data communications with the following services:

- Built-in IP router
- One link for voice and data networking
- Common access to the Internet; share files and send e-mails to other sites
- Support for RIP-2 protocol for dynamic data routing; IPSec VPN, firewall and NAT (Network Address Translation) and for security; Centralized management and proactive fault management via SNMP.

IP Office supports IP packet-based voice networking between sites through VoIP across the campus LAN or VoIP across the public network.

Página2138 de 3226.

In a factory or campus environment, voice calls can sent over 10/100 Mbps LAN connections on systems equipped with optional Voice Compression Modules (VCM). IP Office supports Diffserve by appropriately marking both RTP packets and signalling packets to facilitate network bandwidth management.

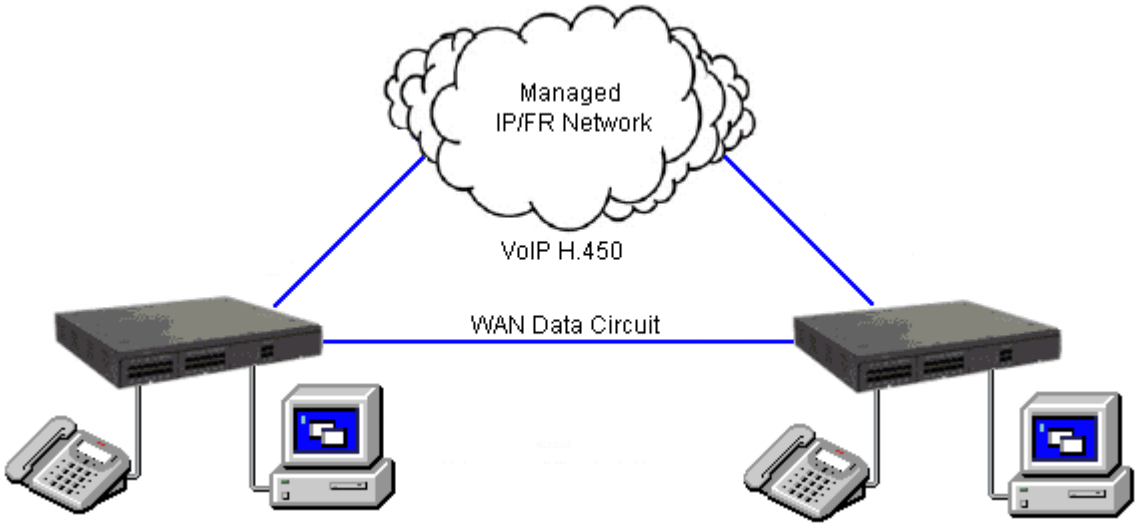


Figure 3: VoIP networking across IP network or WAN

IP Office can realize the benefits of Q.931 and H.450 supplementary service support across a public connection where an appropriate QoS connection can be established.

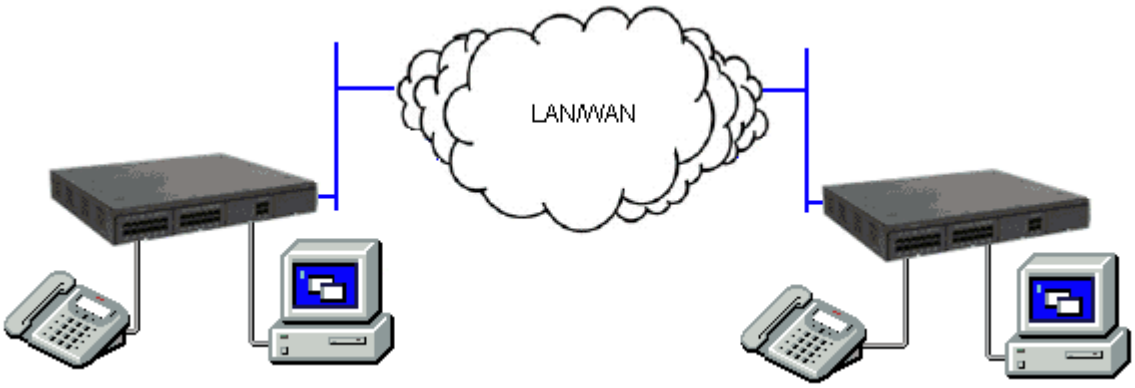


Figure 4: VoIP networking across the LAN

Internet protocol telephony

Internet Protocol (IP) refers to the type of rules that the network uses to send and receive signals. IP telephony converts voice communications into data packets. Conveniently, it runs on Ethernet LAN (local area network) technology. IP telephony unites a company's many locations, including mobile workers, into a single converged communications network.

IP Office is a converged telephony system; it combines aspects of traditional PABX telephony systems and IP data and telephony systems. IP Office supports PSTN, SIP, POTs, digital time

Página2139 de 3226.

division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist.

IP Office connects to the PSTN and to IP trunks providing a “hybrid” PABX function - where both legacy and future technologies can be used together to minimize operating costs and optimize business communications through both voice and data. The converged functionality works on multiple levels:

- Individual phone users can control the operation of their phone through applications running on their PC.
- Data traffic can be routed from the LAN interface to a telephony trunk interface.
- Voice traffic can be routed across internal and external data links. This option is referred to as voice over IP (VoIP).

Voice over IP (VoIP) and network assessments

Voice over IP (VoIP) means voice transmitted over a packet data network. VoIP is often referred to as IP telephony because it uses the internet protocols to make possible enhanced voice communications wherever IP connections exist.

The VoIP mode of operation can include external SIP trunks, IP trunks between customer systems and/or H.323 or SIP IP telephones for users. In either case the following factors must be considered:

- The IP Office control unit must be fitted with voice compression channels. These are used whenever an IP device (trunk or extension) needs to communicate with a non-IP device (trunk or extension) or to a device that uses a different codec.
- A network assessment is a mandatory requirement for all systems using VoIP. For support issues with VoIP, Avaya may request access to the network assessment results and may refuse support if those are not available or satisfactory.

A network assessment would include a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies, and setting voice quality objectives.
- The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support H.323, DHCP, TFTP and jitter buffers in H.323 applications.

An outline of the expected network assessment targets is:

Test	Minimum assessment target
Latency	Less than 150 ms
Packet loss	Less than 3%
Duration	Monitor statistics once every minute for a full week

Signaling protocols

In order to make use of VoIP, IP Office uses signaling protocols called H.323 and Session Initiation Protocol (SIP), to establish end-to-end connections for the voice path through an IP network. This

Página2140 de 3226.

connection ensures that each end is able to transmit and receive voice and provides the network addressing for end-to-end packet transmission. IP Office also connects the different technologies by translating the signals they use. For example an analog telephone can connect to a VoIP destination. This connection requires both the signaling and voice transmission to be translated. IP Office makes this translation using gateways and gatekeepers.

With IP telephony you connect an IP telephone to an IP PBX through a LAN. There are two basic types of IP telephones:

- A physical telephone, which looks very similar to a standard telephone, referred to as a “hardphone”
- A software application, referred to as a “softphone”, which runs on the user’s PC, allowing them to use a headset and microphone to make and receive calls anywhere they an and IP connection.

Quality of Service considerations

When making use of IP telephony, there are a number of data centric considerations such as which data types have priority on the IP network when there is contention. This is set with IP/TCP quality of service and should not be ignored. In situations where LAN bandwidth is limited, a quality of service capable LAN switch should be used to ensure voice packets are transmitted with the required priority on the network. If not, the conversation carried over IP appears as broken up due to delays or has unacceptable delays introduced in the conversation causing latency and jitter. With IP hardphones there is the need for Power over Ethernet (PoE), or local phone power supplies to be provided to the telephones as the IP telephones are not powered by IP Office.

Voice compression channels

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. IP Office systems use voice compression channels to make the conversion. These channels support the common IP audio codecs G.711, G.723 and G.729a.

The System Status Application can be used to display voice compression channel usage. Within the **Resources** section it displays the number of channel in use. It also displays how often there have been insufficient channels available and the last time such an event occurred.

Table 1: Voice compression channels

Call type	Voice compression channel usage
IP device to non-IP device	Requires a voice compression channel for the duration of the call. If no channel is available, busy indication is returned to the caller.

Table continues…

Página2141 de 3226.

Call type	Voice compression channel usage
IP device to IP device	Call progress tones (for example dial tone, secondary dial tone, etc) do not require voice compression channels with the following exceptions: • Short code confirmation, ARS camp on and account code entry tones require a voice compression channel. • Devices using G723 require a voice compression channel for all tones except call waiting. When a call is connected: • If the IP devices use the same audio codec no voice compression channel is used. • If the devices use differing audio codecs, a voice compression channel is required for each.
Non-IP device to non-IP device	No voice compression channels are required.
Music on hold played to IP device	Provided from the TDM bus and therefore requires a voice compression channel when played to an IP device.
Conference resources and IP devices	Managed by the conference chip which is on the TDM bus. Therefore, a voice compression channel is required for each IP device involved in a conference. This includes services that use conference resources such as call listen, intrusion, call recording and silent monitoring
Page call to IP device	Uses G729a for page calls, therefore only requiring one channel but also only supporting pages to G729a capable devices.
Voicemail services and IP devices	Treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.
Fax calls	These are voice calls but with a slightly wider frequency range than spoken voice calls. IP Office only supports fax across IP between IP Office systems with the Fax transport option selected. It does not currently support T38.
T38 fax calls	IP Office supports T38 fax on SIP trunks and SIP extensions. Each T38 fax call uses a VCM channel. Within a Small Community Network, a T38 fax call can be converted to a call across an H323 SCN lines using the IP Office Fax Transport Support protocol. This conversion uses 2 VCM channels. In order use T38 Fax connection, the Equipment Classification of an analog extension connected to a fax machine can be set Fax Machine. Additionally, a new short code feature Dial Fax is available.

Note:

T3 IP devices must be configured to 20 ms packet size for the above conditions to apply. If left configured for 10 ms packet size, a voice compression channel is needed for all tones and for non-direct media calls.

H.323 signaling protocol

IP Office IP telephony systems use open standards. Digital IP telephones, gateways and gatekeepers support the H.323 standard and it is this that allows devices from different

Página2142 de 3226.

manufacturers to work together. IP Office also supports an optional integral gateway, Voice Compression Modules (VCMs) and gatekeeper functionality.

IP Office uses the H.323 signaling protocol using the following architectural components:

IP telephones	H.323 service endpoint devices that support audio calls. Other types of H.323 devices can support video as part of H.323.
Gateways	Provide media translation to allow calls to be made to non-H.323 devices, for instance an analog telephone or the public network to connect with a H.323 device.
Gatekeepers	Control the call processing and security for H.323 devices.
Multipoint Connection Units (MCUs)	Control conferences by adding together media streams.

These elements form an H.323 zone which is analogous to a PABX. Each zone has a single gatekeeper to control call distribution, call control and the resource management. On power-up, IP telephones, gateways and MCUs make registration requests to a gatekeeper which then authenticates (accepts or rejects) the request to become a member of the zone. Once accepted, a telephone wishing to make a call sends a call set-up message to the gatekeeper which then determines how to route the call and will then send an alert to the called telephone, or if the call is to a non-H.323 telephone establish the call via a Gateway within the zone.

Session Initiation Protocol trunking

IP Office uses Session Initiation Protocol (SIP) trunks to allow users to take advantage of telephony services offered by internet service providers (ISPs). In many cases, telephony services offer substantial savings in comparison to traditional exchange lines. To help enable the SIP Service Provider, Avaya offers a SIP Compliance Testing Program (GSSCP) that will validate the operation of IP Office with the ISPs SIP trunk offering. For more information about Avaya's SIP Compliance Testing Program (GSSCP), see https://www.devconnectprogram.com/site/global/compliance_testing/overview/index.gsp.

IP Office allows all users, regardless of their phone type, to make and receive SIP calls. SIP trunks are handled like any other line on IP Office, affording all the call routing and toll control needed to manage inbound and outbound calls.

SIP trunks require provisioning of voice compression channels through the installation of VCM modules within the control unit. A license for the maximum required number of simultaneous SIP calls is also needed. Up to 128 simultaneous calls are supported.

IP Office also supports the T38 protocol which allows Fax over IP.

There are several possible network topologies for SIP trunk systems, as shown in the following diagrams:

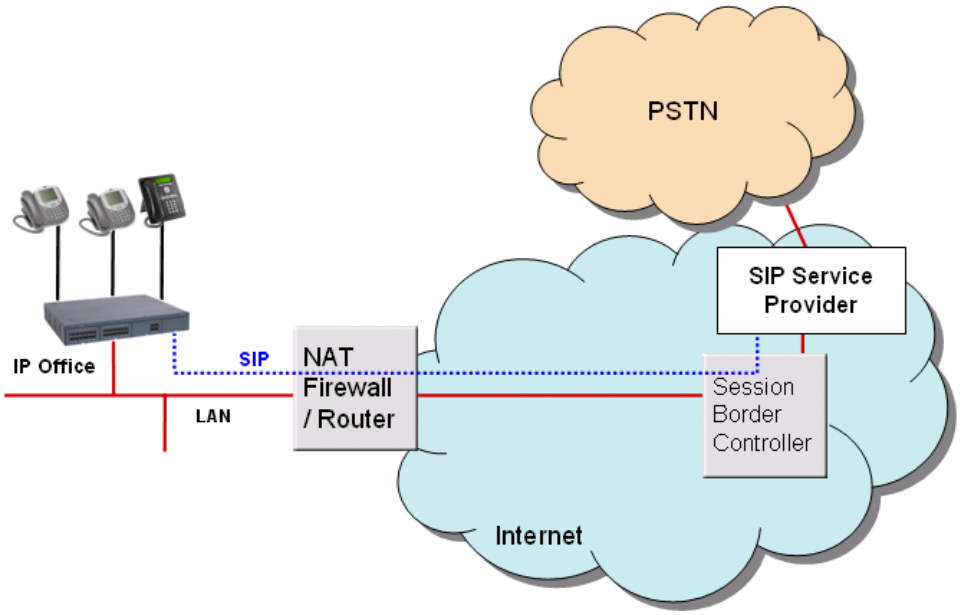


Figure 5: Service provider with Avaya Session Border Controller for Enterprise (recommended)

To make this configuration secure, the IP Office firewall is set to drop all packets except SIP.

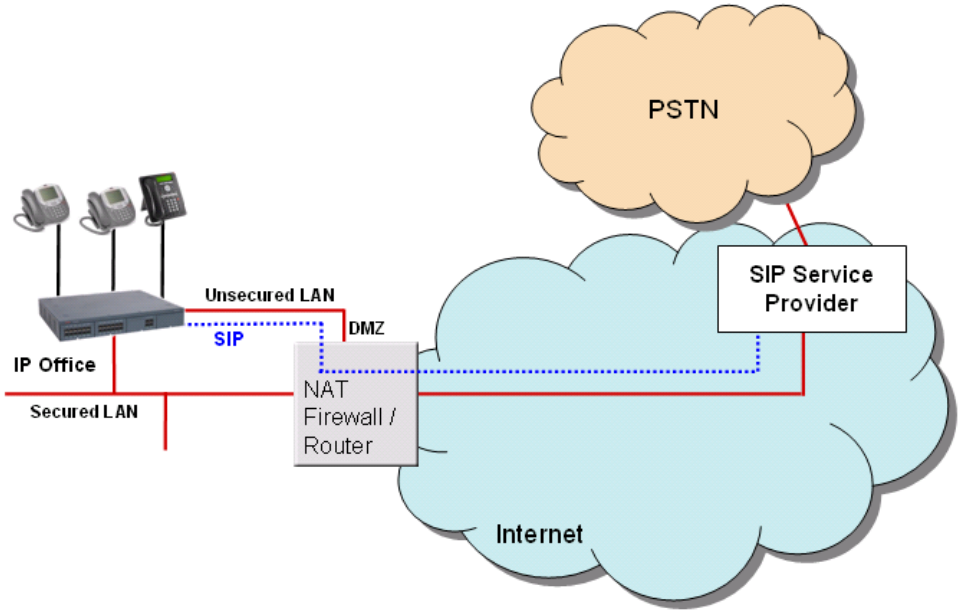


Figure 6: Direct connection from the second Ethernet port to the internet through a DMZ port on the router

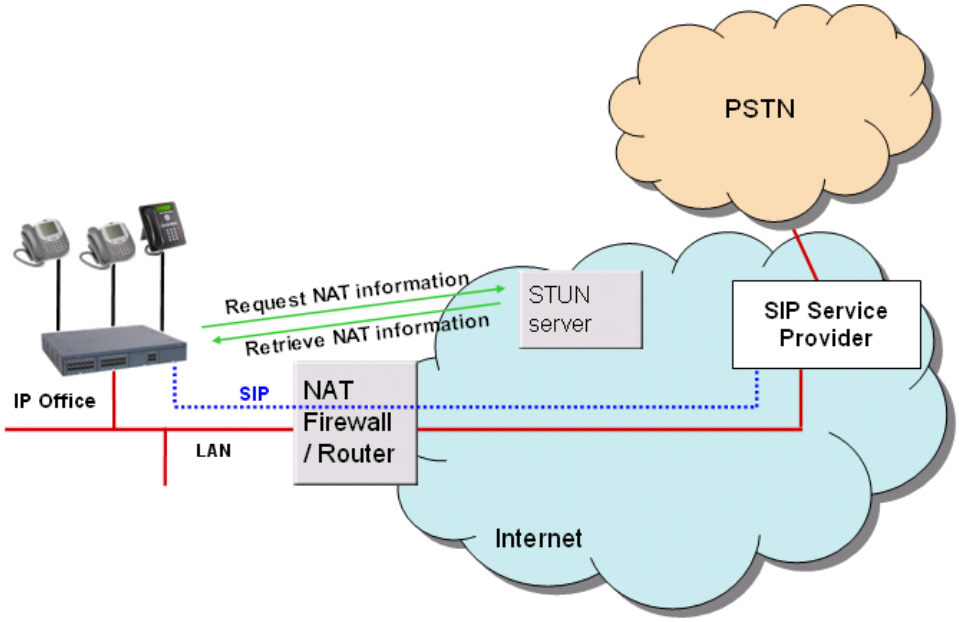


Figure 7: Connection to ITSP over NAT using third-party STUN servers

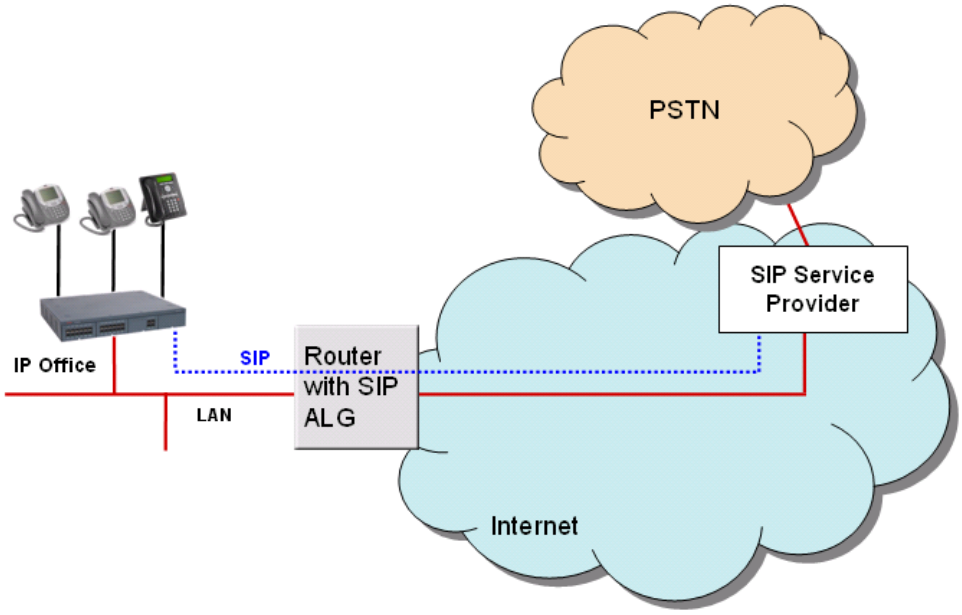


Figure 8: Connection to ITSP through router with ALG to resolves NAT issues

SIP servers

IP Office SIP endpoint implementation is built on two major SIP components: SIP server components SIP endpoint user agent applications.

SIP servers provide SIP endpoint support to allow full interoperability between SIP endpoints, other IP telephones based on H.323, digital and analog telephones as well as IP Office trunks (analog, digital or SIP-based).

Página2145 de 3226.

SIP servers provide centralized information and enablement services in a SIP ecosystem. The core SIP servers and their functions are summarized here. IP Office provides the features of the following two servers for voice and fax communication.

- **Registrar server**

  When SIP IP telephones come online, they need to make sure that others are aware that they're available to take and make calls. The Registrar authenticates and registers the IP phone (often directly related to a specific user) when it comes online, and then stores information on the telephones logical identities.

- **Proxy server**

  A proxy server takes SIP requests, processes them, and passes them downstream while sending responses upstream to other SIP servers or devices. A proxy server may act as both a server and a client, and can modify a SIP request before passing it along. A proxy is involved only in the setup and teardown of a communication session. After user agents establish a session, communications occur directly between the parties.

Functionality of the following two SIP servers are generally available by IP Office using existing IP Office functionality. Therefore, while functionality is provided, for example, allowing hot desking in a small community network, a consistent methodology between SIP and non-SIP endpoints is used to deliver those features

- **Location service**

  As users roam, the network needs to be continually aware of their locations. The location service is a database that keeps track of users and their locations. The location service gets its input from the registrar server and provides key information to the proxy and redirect servers. IP Office provides hot desking support, delivering a similar functionality but working consistently between SIP and non SIP endpoints.

- **Redirect server**

  If users are not in their home domains, sessions bound for them needs to be redirected to them.

  The redirect server maps a SIP request destined for a user to the device closest to the user. In IP Office, call forwarding and Follow me functionality is used to provide again consistent functionality between all type of endpoints.

SIP endpoint user agents

SIP endpoints, such as SIP telephones, cell phones, PDAs, or workstations, use user agent (UA) applications to provide the interface between the users and the SIP network.

SIP endpoint support is fully integrated into IP Office. No other components are needed. SIP endpoints require VCM module capacity like any other IP phone.

SIP extensions function like any other IP Office extension. IP Office provides the following functionality:

- Make and receive calls to any other extension, independent of type of extension.

Página2146 de 3226.

- Deliver end-to-end media. During calls between two SIP extensions or a SIP extension and an Avaya IP telephone, IP Office transmits audio end-to-end for basic telephone calls. Conferencing requires a VCM resource.
- Use short codes and authorization codes.
- Transmit in band call progress tones.
- Register endpoint using authentication with username and password.
- Support Auto-create. Successful endpoint registration uses a third-party license.
- Several extensions can register on one IP address, each using a license. This enables the connection of SIP terminal adapters with more than one analog port, giving a different extension number to each port.

Computer Telephony Integration

Computer Telephony Integration (CTI) bridges the gap between the telephone system and business applications. With IP Office, this is achieved with the IP Office CTI Link, a CTI middleware product and software developers kit (SDK).

On IP Office, CTI is delivered through adherence to open standards. This gives businesses access to a wide range of third-party solutions, addressing vertical markets, and designed to meet their requirements. For developers, migrating their offering from other platforms to IP Office is quick and easy, and the advanced CTI features that IP Office offers makes it easy to demonstrate full integration, and more business benefits.

IP Office provides two levels of CTI interoperability:

CTI Link Lite	Free of charge and provides all the functionality required to support the vast majority of applications, including screen-popping, and many third-party products.
CTI Link Pro	Provides enhanced functionality, including the ability to control multiple telephones and gives access to advanced call center operation.

Because IP networking is integrated into the IP Office system, all CTI is done through the LAN. This introduces additional points of failure, as well as relying on non-standard interfaces and handsets. On IP Office, all devices can be used with CTI.

Supported CTI interfaces

IP Office supports the following interfaces:

TAPILink Lite	Provides first-party CTI support for Microsoft TAPI 2.1 and TAPI 3.0, so each PC can control or monitor one telephone. The software components are supplied with the IP Office system on the User CD, and do not required a license key for use. The specification requires that a certain amount of core functionality is implemented, and additionally defines a series of optional functionality that switch vendors may also implemented.

Página2147 de 3226.

TAPILink Pro	Provides third-party CTI support for TAPI 2.1 and 3.0. These components are identical to their first-party equivalent; the presence of the CTI Link Pro RFA license key (which can be purchased in the usual way for products) enables this additional functionality. TAPILink Pro provides all of the features and functionality of TAPILink Lite, but additionally provides third party CTI operation. This means that a single server can control and monitor any number of telephone devices. In addition, TAPILink Pro provides the ability to monitor and control groups. This allows an application to be notified when a call enters a queue, and can also redirect it to another location.
TAPI-WAV driver	Provides software-based support for voice processing. The TAPI-WAV driver is for use with TAPI 2.1 only; for TAPI 3.0, IP Office supports the Media Service Provider (MSP) interface, defined by Microsoft in TAPI 3.0. This functionality will only work in conjunction with CTI Link Pro and also requires TAPI-WAV licenses. Each license enables 4 ports of voice processing.
DevLink Pro	Provides a real-time event stream in addition to the SMDR interface provided in IP Office SMDR. The real-time event stream takes the form of a call record, which is issued whenever the state of any endpoint of a call changes (typically there are two end points on a call, but for some circumstances, such as conference calls, intruded calls there may be more).
IP Office SMDR	Provides an interface to obtain SMDR events. A comma-separated record is issued for each call, when the call is completed. This interface is designed for call accounting and call billing applications. The IP Office SMDR can be output direct from the IP Office control unit to a designated IP address and port.
IP Office Software Development Kit	This toolkit is delivered on a single CD, containing the developer documentation for TAPILink Lite, TAPILink Pro, DevLink Lite and DevLink pro, as well as pre-compiled programs for exploring TAPI 2.1 and 3.0. In addition, example source code is included, making it easy for developers to become familiar with IP Office CTI interfaces. The Developer Connection Program (DevConnect) is the Avaya developer partner program, and is designed for third-party companies who are creating a product for sale, and who wish to receive technical support. Membership of the program is at the sole discretion of Avaya. DevConnect members pay an annual fee, for which they receive technical support directly from Avaya. In addition, Avaya will perform interoperability testing between IP Office and the member's product, and may also create opportunities for joint marketing, including exhibitions, use of Avaya's logo, and other benefits. More information on the DevConnect program can be found at http://www.devconnectprogram.com.
Centralized CTI WebService API	Provides a more open platform to allow third-parties to add value and build out solutions. Supports distributed (SE/SCN) environment and, therefore, is not limited to nodal like TAPI. It does have a dependency on Avaya one-X® Portal access for the users. When creating a new user in IP Office, it does not require a restart.

Página2148 de 3226.

SSI over Web Services	Provides system monitoring information of SSI over a read-only REST web service available over https only. Realtime call data and call control are not available via this interface, but they will be made available via the DevConnect program. This feature already has several areas instrumented but the data is for SSA and delivered over the Proprietary SSI interface, and there is a small set of data available on SNMP. It does not require a license.

Open APIs/SDKs

With Release 10.1, IP Office supports a new Management API/SDK to address the needs of “Easy Button” setups. Enhancements to cover more areas, specifically what the legacy "XO" Configuration Web Services covers so that the legacy API can be made End Of Life. Management API provides a REST-based API Interface to the third-party application developers for consuming IP Office configuration objects.

- Provides all capabilities of currently supported IP Office configuration services (XO services).
- Request and response are in XML and JSON format.
- Provides Read/Write access to privileged service users only.
- No separate license is required for accessing the APIs.

Components

Hardware components

IP Office control unit

IP Office control unit (IP500 V2) is a stackable unit with an optional 19" rack mounting kit and an optional wall mounting kit for smaller configurations.

The IP500 V2 control unit is compatible with all IP500 base extension and Voice Compression Module (VCM) cards as well as all external IP500 expansion modules.

The IP500 V2 control unit has 4 slots for the insertion of IP500 base cards. The slots are numbered 1 to 4 from left to right. Normally they can be used in any order, however if the capacity for a particular type of card is exceeded, the card in the rightmost slot will be disabled. Each base card includes an integral front panel with ports for cable connections. Typically the first 8 ports on the left are for connection of extension devices. The 4 ports on the left are used for connection of trunks if a trunk daughter card is added to the base card.

The control unit provides the following functionality:

Página2149 de 3226.

Maximum extensions	Up to 384 extensions.
Conference parties	128 as standard but maximum 64 in any individual conference. Silence suppression is applied to conferences with more than 10 parties.
Trunk cards	Up to 4. Any combination of trunk daughter cards.
Voice compression channels	Up to 148 channels using up to VCM and combination cards.
Voicemail channels	Up to 250 voicemail/recording channels supported on the Primary server. For Select deployments, the Secondary server can also support up to 250 voicemail/recording channels.
Locales	Supported in the following countries: Argentina, Australia, Bahrain, Belgium, Brazil, Canada, Chile, China, Colombia, Customize, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Italy, Japan, Korea, Kuwait, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Norway, Oman, Pakistan, Peru, Poland, Portugal, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, United Kingdom, United States, Venezuela.
Power supply	Internal power supply unit.
Mounting	Free-standing, rack mounted or wall mounted (requires mounting kits).
Memory	Maximum configuration file size: 2048 KB.

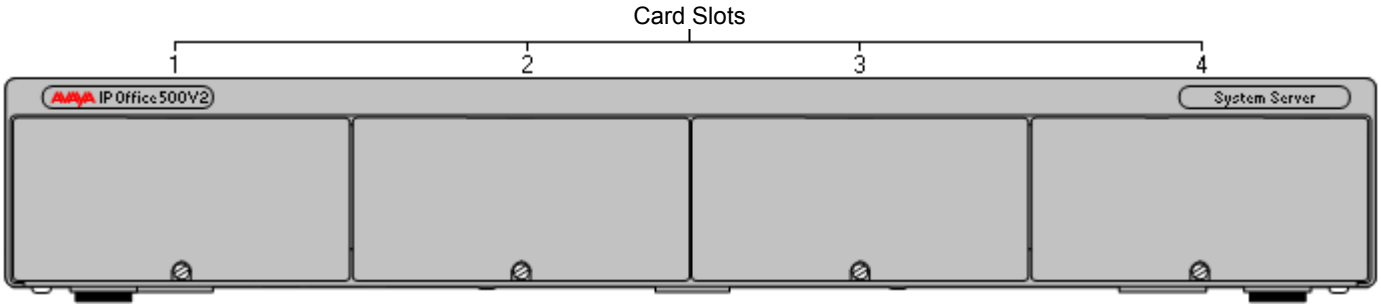


Figure 9: IP500 V2 front view

Página2150 de 3226.

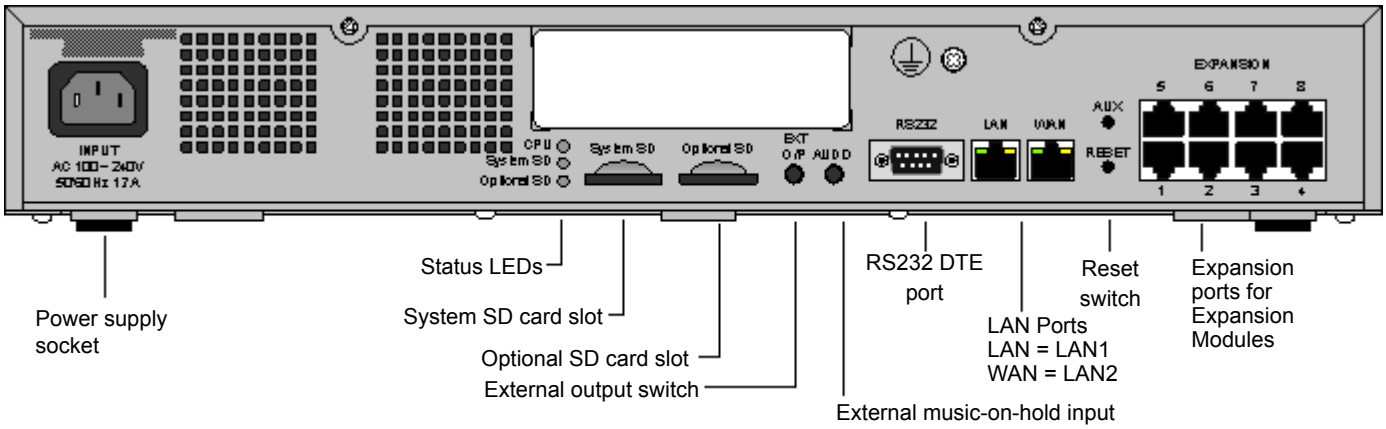


Figure 10: IP500 V2 rear view

Feature keys

The serial number of the feature key SD card fitted to the IP Office control unit is used as the basis for all licenses issued for that IP Office system and is used to regularly validate the licenses. If the feature key SD card is removed, over the next few hours licensed features will stop operating.

Pulse code modulation encoding

Pulse code modulation (PCM) is a method for encoding voice as data. In telephony, two methods PCM encoding are widely used, a-law and µ-law (also called mu-law or u-law). Typically µ-law is used in North America and a few other locations while a-law by the rest of the world. As well as setting the correct PCM encoding for the region, the a-law or µ-law setting of IP Office when it is first started affects a wide range of regional defaults relating to line settings and other values.

Base cards

The following base cards are available:

Table 2: IP500 V2 base cards

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
Digital Station (DS8)	3	Ports 1–8: Digital stations With trunk card: Ports 9–12: Central Office lines	Selected Avaya 2400, 5400 and 9500 series phones T3 phones (EMEA only) 3810 wireless phones (North America only) **Note:** 4400 series phones are not supported on this card. They are supported on external expansion module DS ports. 4100, 7400, M series and T series phones use the TCM8 Digital Station card.

Table continues…

Página2151 de 3226.

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
Analog Phone 2	4	Ports 1–2: Analog stations With trunk card: Ports 9–12: Trunk connections	Analog phones
Analog Phone 8	4	Ports 1–8: Analog stations With trunk card: Ports 9–12: Trunk connections	Analog phones
Digital Station (TCM8)	4	Ports 1–8: BST digital stations With trunk card: Ports 9–12: Central Office lines	Norstar®/BCM phones BST series phones Global M series phones Digital Mobility Controllers (DMCs) 7406e Wireless Telephones Digital Audio Conferencing Unit
Voice Compression Module (VCM V2)	2	Ports 1–8: Not present With trunk card: Ports 9–12: Central Office lines	VoIP calls including IP extensions or IP trunks. Up to 128 voice compression channels depending on the codec used. The IP500V2 control unit supports up to 148 voice compression channels, using the card plus voice compression ports on the Combination card.
ATM Combination (ATM V2)	2	Ports 1–6: Digital stations Ports 7–8: Analog stations Ports 9–12: Central Office lines 10 voice compression channels. Codec support is G.711, G729a and G.723 with 64ms echo cancellation. G.722 is supported by release 8.0 and higher.	Avaya digital phones except 3800 and 4400 series phones Analog phones Preinstalled trunk cards

Table continues…

Página2152 de 3226.

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
BRI Combination	2	Ports 1–6: Digital stations Ports 7–8: Analog stations Ports 9–10: BRI trunk ports (4 BRI channels) 10 voice compression channels. Codec support is G.711, G729a and G.723 with 64ms echo cancellation. G.722 is supported by IP Office Release 8.0 and higher.	Avaya digital phones except 3800 and 4400 series phones (DS type not TCM) Analog phones Preinstalled trunk cards
Unified Communications Module (UCM V2)	1		Requires separate Preferred Edition license. Not supported on Server Edition. More than 200 users when running Voicemail Pro only. Up to 200 users when running Voicemail Pro and Avaya one-X® Portal for IP Office. 50 simultaneous Avaya one-X® Portal for IP Office users. No trunk cards
ETR6	3	Ports 1–6: ETR stations With ATM4: Ports 7–8: Power Failure Transfer Ports 9–12: Central Office lines	Not supported on Server Edition. PARTNER ACS phone ATM4, PRI/T1, or PARTNER mode µ-law SD cards (North America only)

Trunk cards

Trunk cards can be fitted to existing base cards to provide support for trunk ports. The trunk card uses the ports provided on the base card for cable connection. Each trunk card comes with spacer pegs for installation and port identification labels.

Note:

These cards are used for PSTN/FXS gateways with IP Office for Linux.

Página2153 de 3226.

Tip:

In systems with both Analog Phone 8 base cards and analog trunk cards, combining the two types are recommended because it provides analog power failure support for one trunk per extension (not applicable to the Analog Phone 2 base card).

Table 3: IP500 V2 trunk cards

Trunk card	Maximum per system	Works with these base cards	Description
Analog (V2)	4	ETR6 DS8 TCM8 Analog Phone 2/8	4 analog loop start trunks V.32 modem for remote access 1 power failure extension to trunk connection on Phone 8 cards

Table continues…

Página2154 de 3226.

Trunk card	Maximum per system	Works with these base cards	Description
Universal PRI (PRI-U)	4	ETR6 DS8 TCM8 Analog Phone 2/8 VCM	Up to 2 PRI trunk connections. The card is available in single and dual port variants. The card can be configured for E1 PRI, T1 robbed bit, T1 PRI or E1R2 PRI trunks. Supports primary rate digital trunks. On each card, 8 channels per interface are enabled by default. This means that the single PRI has 8 channels enabled, while the dual PRI has 8 channels enabled on each of the two circuits. Further channels may be enabled by the purchase of additional licenses in 2-channel or 8-channel increments. Available in single and dual version. The single variant can support up to 24 T1 channels or up to 30 E1 channels. The dual variant can support up to 48 T1 channels or 60 E1 channels. Configurable for T1, E1, E1R2 MFC use, depending on territory. Includes an integrated CSU/DSU: • CSU allows trunks to be put into loop-back mode for testing purposes. This can be set manually, using the monitor application, or automatically from a Central Office sending a Line Loop Back (LLB) pattern. • DSU allows the T1 trunk to be shared between data and voice services. Includes diagnostics capabilities: visual indicators to show service state and physical test points to monitor traffic. Supports mobility features: Mobile Call Control and one-X Mobile clients
BRI (Euro ISDN)	4	DS8 TCM8 Analog Phone 2/8 VCM	Up to 4 BRI trunk connections, each trunk providing 2B+D digital channels. Available in 2 (4 channels) and 4 (8 channels) options. Supports mobility features: Mobile Call Control and one-X Mobile clients.

External expansion modules

External expansion modules can be used with the IP500 V2 control unit.

Página2155 de 3226.

Analog phone expansion modules

On analog ports, call information is sent while the phone is ringing, and cannot be updated during a call or set on an outbound call (the phone may do a local match but this is not controlled by IP Office). The primary purpose of displays is to give information about incoming calls. Where the caller display standard chosen supports the delivery of text (extension name) as well as the number, both are delivered.

An analog extension port can be set for external paging operation. It does not operate like a normal extension and is connected to external equipment through an isolation device (can also be used as an MoH source). The port will always be busy so it cannot be called directly and can only be accessed by using a paging feature. When not receiving a page, the port will remain silent. When being paged, the page tone is sent before the speech path is opened.

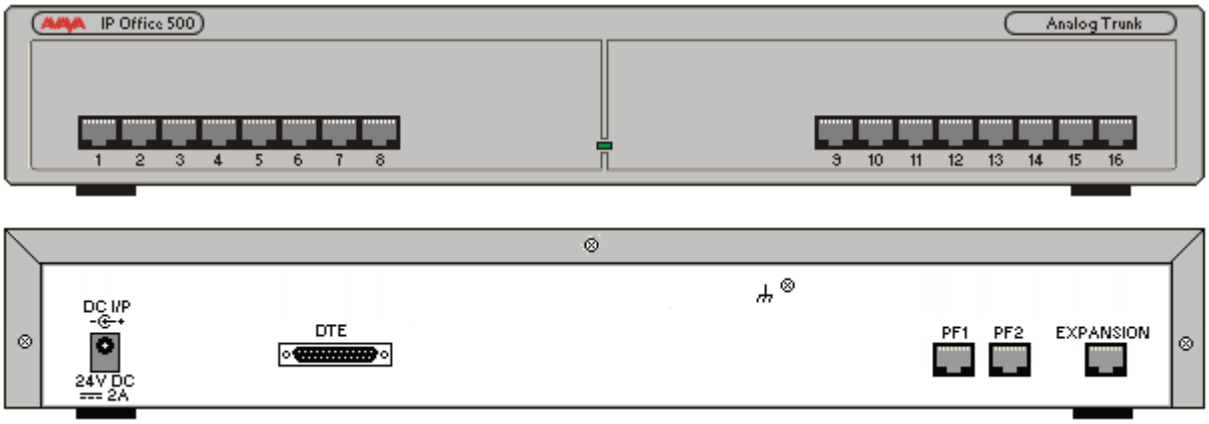
For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.

Expansion module	Telephones supported	Interfaces supported
Analog Phone 16	16 analog stations with calling line presentation	DTMF signaling (No rotary or Loop Disconnect) Time Break Recall (No Earth Recall) Message Waiting Indication (MWI): 51V Stepped, 81V, 101V and Line Reversal and Bellcore FSK
Analog Phone 30	30 analog stations with calling line presentation	

Analog trunk modules

This type of module can be used to add 16 additional analog trunks to an IP500 V2 system. The module supports both loop-start and ground-start trunks. The module also provides two powerfail ports for direct connection of analog phones to the first two analog trunks.

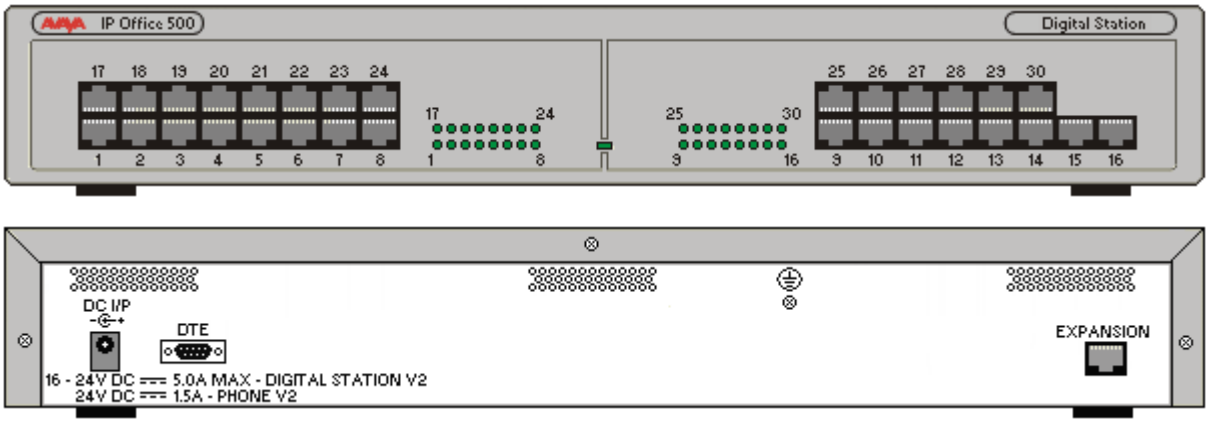
Basic Edition systems only support a single ATM16 expansion module. For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.



Expansion module	Description	Interfaces supported
ATM16	16 analog trunks	Loop-start Ground start

Digital station expansion modules

For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.



Expansion module	Telephones supported	Description
DS16A	Norstar®/BCM telephones	16 digital station ports
DS30A	BST series telephones Global M series telephones Digital Mobility Controllers (DMCs) 7406e Wireless Telephones Digital Audio Conferencing Unit	30 digital station ports
DS16B, DS16B2[1]	Avaya telephones	16 digital station ports
DS30B, DS30B2[1]	Either DS or TCM mode supporting the telephones connected to either the DS8 or the TCM8 cards.	30 digital station ports

Application server

The IP Office Application Server provides reliability, scalability and processing power for larger scale IP Office deployments. It is an external, rack mounted server that provides scalability for larger installations and multisite deployments not currently supported with the Unified Communications Module (UCM V2).

The IP Office Application Server is a single installation of selected IP Office™ Platform applications running on Linux. The Linux operating system is included as part of the installation. However, installation requires minimal Linux knowledge due to the inclusion of a web based management interface to allow the server to be managed remotely via web browser.

[1] DS16B2 and DS30B2 are supported on 10.1, 9.1 SP 12, and 10.0 SP5 onwards.

Página2157 de 3226.

The IP Office Application Server hosts the following applications:

- Management Services
- one-X Portal for IP Office
- Voicemail Pro
- Web License Manager (WebLM)
- Web Manager
- Optional Services
  - Media Manager
  - Web Collaboration
  - WebRTC Gateway

WebRTC gateway configuration guidelines

Use the following guidelines when configuring a WebRTC gateway:

- Define WebRTC SIP extensions on the:
  - SIP server that is part of the WebRTC gateway configuration.
  - Primary server if this is part of the deployment topology.
- With IP500 V2 deployments, WebRTC should be enabled on the Application server.

Gateway limitations

The WebRTC gateway does not support resiliency.

Avaya Session Border Controller for Enterprise

An session border controller acts a router between the enterprise and carrier service, allowing only authorized sessions to pass through the connection point (border). The Avaya Session Border Controller for Enterprise (SBCE) delivers security to a SIP-based Unified Communications network.

For information on the SBCE, see *Avaya Session Border Controller for Enterprise Overview and Specification*.

For information on deploying the SBCE with IP Office, see “Configuring the Avaya Session Border Controller for IP Office Remote Workers” in either

- *Administering Avaya IP Office™ Platform with Web Manager*
- *Administering Avaya IP Office™ Platform with Manager*

Phones

IP Office supports multiple telephone solutions:

- IP telephones

Página2158 de 3226.

- Digital telephones
- ETR telephones
- Analog telephones
- Wireless telephones
- Third-party SIP endpoints such as, desktop telephones, softphones and conferencing speakerphones

For detailed specifications, see specific telephone information on the Avaya Support site at http://support.avaya.com.

Related links

Remote phone support on page 39
Accessing Avaya DevConnect Application Notes on page 134
Using the Avaya InSite Knowledge Base on page 134
Phone interoperability on page 95

Remote phone support

IP phones using NAT router

IP Office supports remote 9600 Series IP phones with the H.323 FW which resides behind a NAT router to IP Office. The configuration does not require any VPN concentrator equipment. Remote 9600 H.323 IP phones can connect to IP Office even if it is located behind a NAT router. The phones are authenticated in the same way as phones in the private network. IP Office determines that a phone is located outside the private network and relays the VOIP RTP traffic to ensure it transverses the NAT router.

Note:

H.323 signaling and the media traffic is not encrypted.

To reach IP Office from the remote private network, remote H.323 IP phones need to be configured to the public IP address of the NAT router hosting the IP Office. Configurable ports need to be forwarded to IP Office. IP Office requires a valid public IP address be configured and the public IP address can be statically configured or dynamically discovered via a STUN server. The Remote Worker feature requires the Essential Edition license which provides 4 remote worker seats. Enable the Remote Worker feature using IP Office Manager. Additional remote worker capability is available with the Teleworker User or Power User licenses and a Preferred Edition license.

VPN phones

VPN phones provide secure communication over public ISP networks to IP Office at the company headquarters. It is a software-only product that runs on 5610/5620/5621 or 4610/21 IP phones. In combination with one of these phones and the most popular VPN gateway products, the software extends enterprise telephony to remote locations. VPN functionality is supported on 9600 IP phones, and does not require a separate software load. VPN phone has been tested with a number of VPN-gateways from major vendors like Cisco or Juniper as well as with smaller VPN-access devices from companies like Adtran, Kentrox, Netgear, and SonicWall. Refer to the Avaya Support website for a list of available application notes on VPN-gateways tested with each line of phones.

Página2159 de 3226.

SIP phones using Avaya SBCE

The Avaya Session Border Controller for Enterprise (Avaya SBCE) sits on the edge of customer's network with both internal and external IP interfaces. Using these IP interfaces, Avaya SBCE functions as the gateway for SIP traffic into and out of the network. When used internally, SIP clients register to the IP Office directly. When used externally, the SIP clients connect to the Avaya SBCE. This is achieved using Split DNS, which automatically resolves the FQDNs to the internal IP address of the IP Office or the public IP address of the Avaya SBCE depending on where the clients are currently located. Apart from acting as a gateway, Avaya SBCE also provides protection against any external SIP-based attacks. For privacy over the public internet, the public side of the Avaya SBCE facing the remote workers must be configured to use the recommended values of TLS for signaling and SRTP for media encryption, as long as they are supported by the endpoints.

IP Office applications

User applications

The following sections provide an overview of the applications intended for end users.

Avaya one-X® Mobile

Avaya one-X® Mobile is an application that mobile users use to connect to IP Office.

Avaya one-X® Mobile works in call-back telephony mode. For example, when a user initiates a call from the client, IP Office initiates a call to the caller's mobile device and then dials the destination. This mode offers cost savings to users in countries where incoming voice calls are free or for users who have a cheaper unlimited voice plan as compared with a data plan.

The one-X Mobile Preferred mobility client also works in Voice over IP (VoIP) mode. In the VoIP mode, the client makes calls over Wi-Fi/3G/4G data networks. The client, using its underlying SIP stack, registers with IP Office over the data network and functions as an office extension.

Users in countries where incoming calls are charged will see a significant cost savings in the VoIP mode especially when on Wi-Fi networks. The availability of both call-back and VoIP modes on the mobility client will enable users to toggle between the modes based on their network connections. This will empower end-users to make a choice of the appropriate mode based on their voice and data plan as well as the availability and quality of their data connection (WiFi/3G/4G). For example,

- The user can choose the call-back mode when he or she doesn't have Wi-Fi access and the 3G data connection is not providing good quality for voice.
- The user can choose the VoIP mode when he or she has access to a mobile hotspot where a Wi-Fi data connection is available or when the 3G or 4G data connection is good.

One one-X Mobile Preferred mobility client supports VoIP mode on both iOS and Android devices. VoIP mode is available with the Power User profile. Users with Mobile Worker profiles can only

Página2160 de 3226.

use call-back mode. VoIP mode does not require an IP endpoint license. The following features are available:

- Ring-tone selection
- High bandwidth or narrowband codec selection based on the network connection available
- Bluetooth headset audio control on VoIP calls
- Conference screen
- Contact phone number selection
- Voicemail priority indicator
- Swipe support for instant messaging on home screen
- Group action support
- Emoticons
- CLID lookup in contacts for calls
- Send voicemail as WAV in email
- Enable or disable mobile twinning (simultaneous ring)
- Enable or disable DND (send all calls)
- Call log combined with voicemails in the event history
- Call monitoring to see and interact with all calls
- VoIP mode dial plan
- Transfer calls as a third-party call controller (3PCC)

Avaya one-X® Portal for IP Office

Avaya one-X® Portal for IP Office provides users control of their telephone from a networked PC. Use this application with any extension; analog, digital or any IP telephone, wired or wireless, that is available as part of the Office Worker, Power User or Teleworker user licenses.

Avaya one-X® Portal for IP Office is a server-based application that the user accesses via web browser.

For Telecommuter mode, One-X applications require answer supervision and disconnect detection for proper functioning. As a result, the one-X applications will not work with trunks that do not support answer supervision and disconnect detection.

Note:

one-X applications function on trunk types such as PRI, BRI, and SIP, however, they will not function on E1R2, T1 RBS and analog loop start trunks.

System administrators can control if Avaya one-X® Portal for IP Office can be accessed over a secure protocol only, recommended for hosted deployments to provide “secure only” access. The other option is to allow users to access the client over a secure and unsecure protocol (HTTP/HTTPS). The client application forces users to change their passwords and voicemail passcodes to meet the complexity settings configured by the administrator.

Página2161 de 3226.

Through gadgets, Avaya one-X® Portal for IP Office provides the following features:

- Call information
- Call and conference control
- Presence and instant messaging notifications, monitoring and archiving
- Contact import and export
- XMPP groups displayed in the **System Directory** tab
- Dial to user's own bridge and invite other users to join
- Conference call and other meeting scheduling including port reservations, email support and automatic report creation — available within the Outlook interface
- One-click web conferencing hosting and single sign-on joining web conferences as a participant

Avaya Equinox™ for IP Office

Avaya Equinox™ for IP Office is a SIP-based Unified Communications (UC) client that provides users with real time collaboration capabilities and enables business users to easily manage their day-to-day communications from a single interface. IP Office supports the following operating systems:

- Desktop:
  - Windows
  - macOS
- Mobile phone:
  - Android: From a mobile phone, tablet, or an Avaya Vantage™ device
  - iOS

Note:

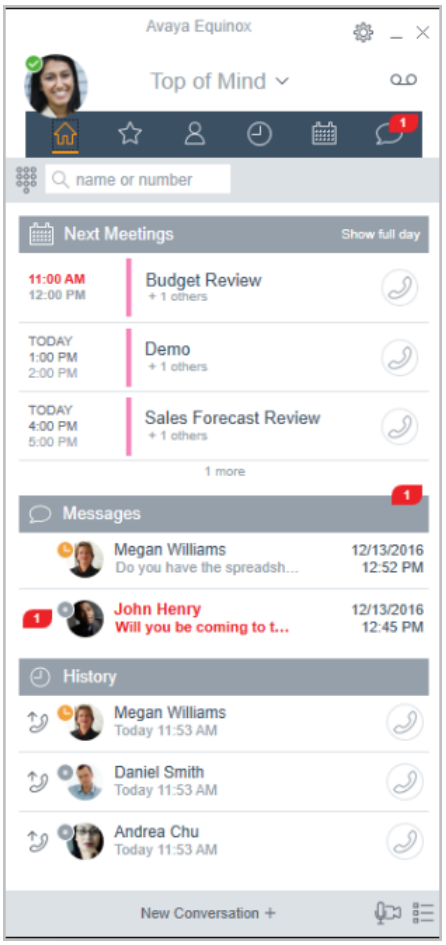
In Avaya Vantage™ Release 2.0.1, the K165 and K175 devices support the Avaya Equinox™ client. The K155 device does not support the Avaya Equinox™ client.

Avaya Equinox™ is a common cross-platform client. The client capabilities vary depending on the platform it is registered with. The supported features in Avaya Equinox™ for IP Office are:

- Top of Mind Home Screen
  - Next meetings showing local calendar schedule or Exchange Web Service/Office 365
  - Local Call History
  - Messages
  - Start Meetings/Launch Spaces dashboard
- Top of Mind Lite Option for Mobile phones
- IP Office directory and local contacts
- Messaging through Avaya Spaces

Página2162 de 3226.

- Presence through IP Office server
- Local call history
- Dialpad with Redial
- Desktop integration with Microsoft Outlook and Browsers
- Softphone client audio and video calls
- Shared control of an associated IP Office deskphone.



Avaya Equinox™ registers with IP Office server as a SIP softphone for audio and video calling, and telephony features. The following features are supported:

- Point to point audio and video calls (make, receive, and end)
- Multiple call handling (incoming and outgoing)
- Hold and retrieve (audio and video calls)
- Transfer (blind and consultative)
- Consult conferencing
- Escalate audio to video call
- Share control with supported desk phones in the Avaya Equinox™ desktop client

Página2163 de 3226.

- Avaya Equinox™ on Avaya Vantage™
- Presence and directory integration with Avaya Equinox™ on Avaya Vantage™
- Enter DTMFs during a call

Avaya Equinox™ client on Avaya Vantage™ supports the following features:

- Making outgoing calls.
- Handling incoming calls.
- Putting call on hold and resuming the call.
- Muting and unmuting a call.
- Transferring a call.
- Escalating an audio call to video call and de-escalating video call to audio call.
- Entering DTMF digits using the keypad.
- Access your local contacts
- Access your IP Office contacts by using IP Office directory.
- Manage your presence status and presence status messages.

Avaya Equinox™ for IP Office limitations:

- CTI Control — Avaya Equinox™ for IP Office cannot be controlled through other applications such as Avaya Contact Center Select, IP Office Contact Center, or IP Office SoftConsole.
- Branch worker — Avaya Equinox™ for IP Office does not support failover between Avaya Aura® core and IP Office Branch.
- For Instant Messaging, Avaya Equinox™ for IP Office depends on the availability of Avaya Spacesbasic account in the Cloud.
- The Avaya Equinox™ client accesses Avaya Equinox® Meetings Online using HTTPS, from within the Equinox Meetings tab of the client. The Avaya Equinox™ client can access local on-premise Equinox Conferencing in the same way using HTTPS, that is, if the access URL is configured under Equinox Meetings. However, if the Avaya Equinox™ client accesses local on-premise Equinox Conferencing through SIP trunks, audio and video will be available but not sharing or conference roster. The same applies for accessing Scopia over SIP trunks too. Even when Avaya Equinox™ client accesses local on-premise IP Office Meet Me Conferencing, audio will be available but not sharing or conference roster.

Avaya IP Office Web Client

Avaya IP Office Web Client is a WebRTC application that provides various communication capabilities. The client takes advantage of WebRTC Gateway resiliency improvements delivered in R11.0 and is supported on Server Edition and IP500 V2. Users must have Office Worker or Power User license to use the Avaya IP Office Web Client features. The client is supported in the following environments:

- Google Chrome browsers on Windows OS
- Google Chrome browsers on macOS
- Standalone client on Windows OS

Página2164 de 3226.

Avaya IP Office Web Client provides the following features:

- Point to point audio and video calls
- Access to Voicemail access
- Call logs
- Conferencing:
  - Ad-hoc Conference by merging calls
  - Starting or joining an IP Office Meet Me Conference
  - Accessing IP Office Web Collaboration
- Point-to-point Instant Messaging and Presence by integrating with Avaya one-X® Portal for IP Office
- Click-to-call using Google Chrome extension
- Single-Sign-On (SSO) support for Avaya one-X® Portal for IP Office and IP Office Web Collaboration
- System Directory and Favorites (Personal Directory)

Avaya Communicator

Avaya Communicator is a collaboration software client that delivers an innovative interface for real time communications for Windows and on the iPad. It enables users to handle phone calls, instant messages, conferencing, web collaboration, presence, enterprise contacts and e-mail, all from a single interface. Avaya Communicator delivers the intuitive graphic design of spotlights, media menu, notification bar, and contact cards.

Avaya Communicator for IP Office communicates with both IP Office and Avaya one-X® Portal to provide communication and collaboration features. Telephony features such as make/receive calls, hold/unhold, mute/unmute, DTMF, MWI etc. are provided by IP500 V2 and UC features such as IM, presence, and enterprise contacts are provided by the Avaya one-X® Portal server.

If Avaya one-X® Portal server is unavailable, either due to licensing restriction or connectivity issues, the Avaya Communicator client will work in a telephony-only mode providing only telephony features. Interoperability with Avaya Session Border Controller for Enterprise allows the Flare Communicator client to be used by users with the Remote Worker profile and register with IP Office without requiring a VPN connection.

Avaya Communicator provides the following features:

- Add participants using dial-pad or drag and drop
- Mute and unmute all or a subset of participants
- Lock and unlock the conference
- Place conference in lecture mode
- Enable and disable entry and exit tones
- Drop all or some participants from the conference
- End the conference

- Enable and disable continuation to allow the conference continue after the moderator drops
- Promote participants to moderator
- Create ad-hoc conferences by merging P2P calls
- Authorization and account codes (Windows only)
- Hold timeout reminder (Windows only)
- Compact user experience
- TSL/SRTP support
- Contact filtering
- Web conferencing integration
- Unsupervised transfer
- Auto-answer
- Simultaneous mode
- Password change
- Account codes
- Auto configuration (iOS only)
- Bluetooth and headset device support and selection (iOS only)
- Interoperability with Scopia (Radvision XT5000)

Note:

Avaya Communicator does not support recording and active speaker indicator.

Avaya Communicator for iPad

Avaya Communicator for iPad integrates voice, video, presence, instant messaging, directories into one unified interface over Wi-Fi or 3G cellular and VPN connections.

Avaya Communicator is a software-only solution that can be easily downloaded from the Apple iTunes Store supporting iPad2, iPad3, iPad4, iPad Mini (with and without retina display), iPad Air both Wi-Fi and 3G models and the following iOS versions: 6.1.x, 7.0.x, 7.1.x, and 8.0.x.

Note:

Avaya Communicator is not supported on iOS 6.0.x.

With Avaya Communicator, IP Office users can use iPad devices for:

- Easy access to the real-time communications tools they rely on every day (phone, presence, IM, etc.)
- Blending real-time communications and business processes, such as mobile sales
- Taking advantage of Wi-Fi and 3G connectivity for cost-saving VoIP
- Secure signaling over TLS and secure media exchange over SRTP in cloud environments

Página2166 de 3226.

- As a web conferencing moderator, the ability to share white board and documents
- Changing passwords
- Auto-answer support
- Unsupervised transfers
- Auto configuration services using a configuration profile hosted on a web server by email address or URL
- Bluetooth and headset device support and selection
- System directory search
- Add/delete members from a team (XMPP Group)
- Search the system directory and add to a team or personal contact
- Radvision XT5000 support for point-to-point video calls

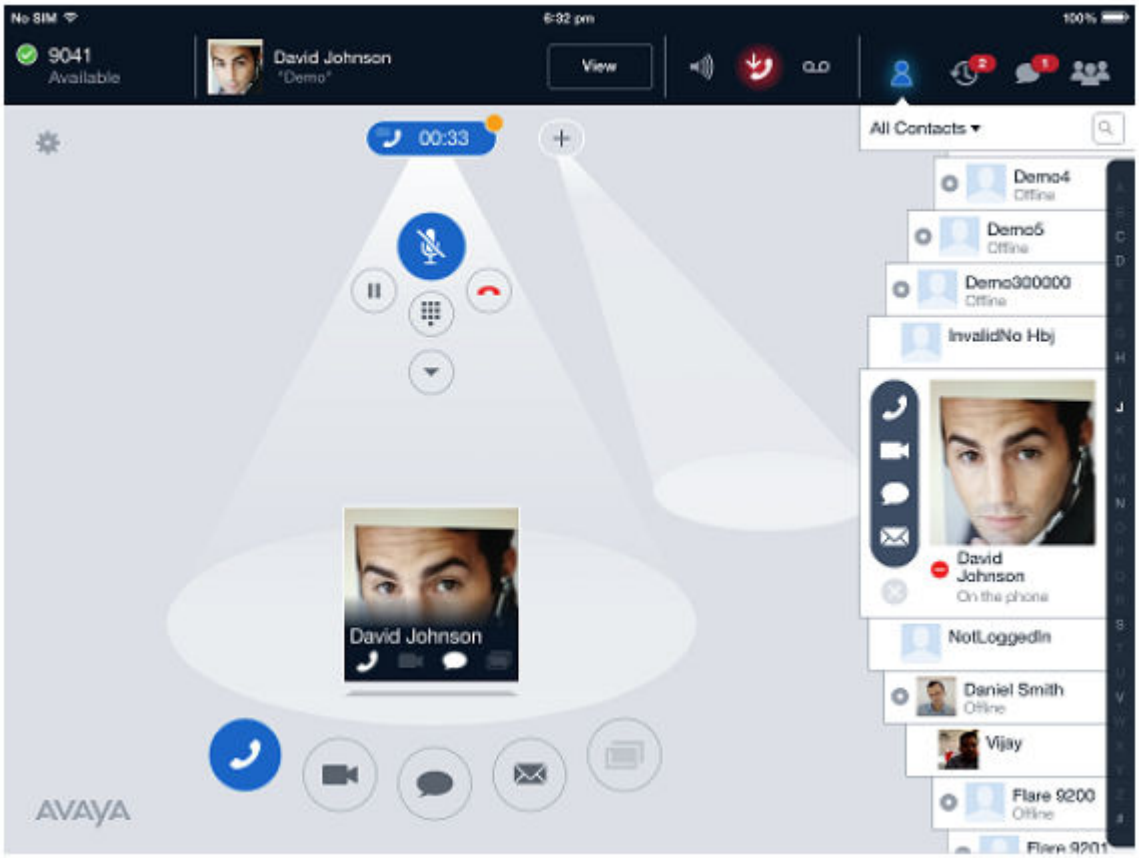


Figure 11: Avaya Communicator for iPad

Avaya Communicator for Windows

Avaya Communicator for Windows integrates voice, presence, instant messaging and directories into one unified offering for Windows laptops and desktops over a LAN connection.

Avaya Communicator provides the following features:

- Compact mode occupying less screen real estate

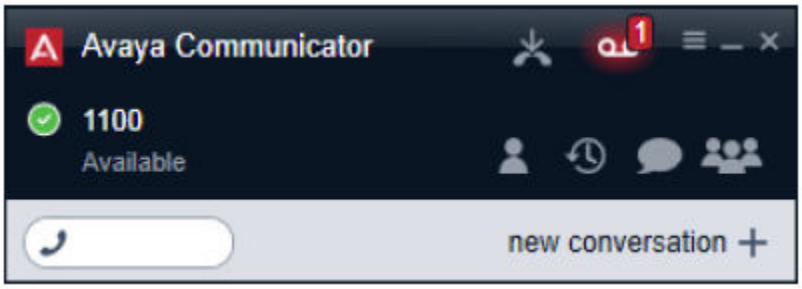


Figure 12: Avaya Communicator for Windows compact view

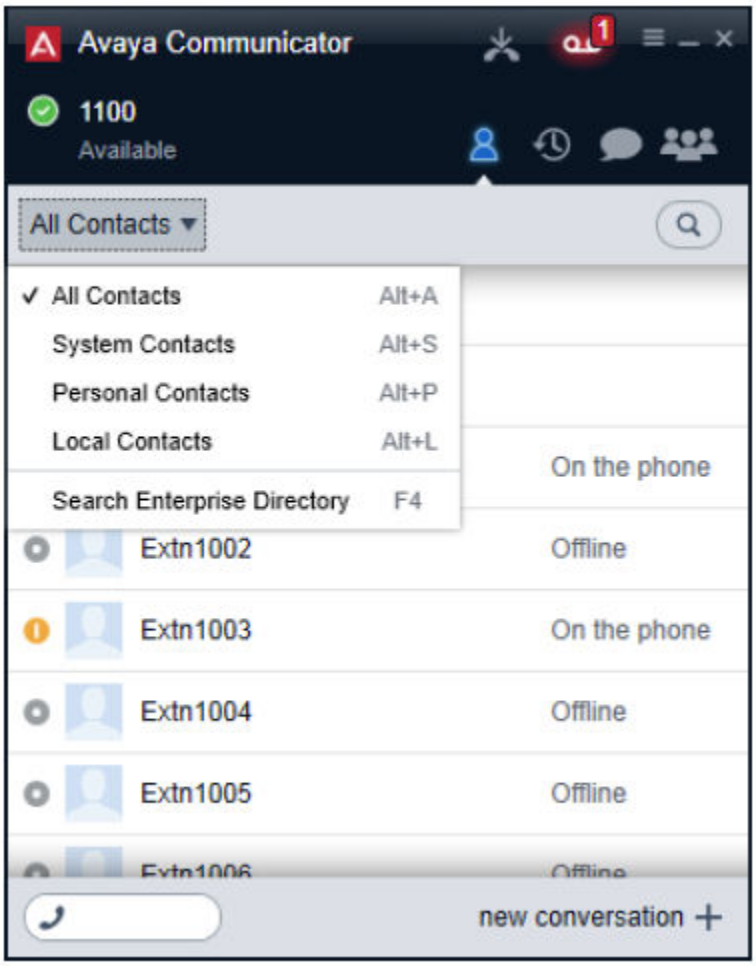


Figure 13: Avaya Communicator for Windows full view

- Secure signaling over TLS and secure media exchange over SRTP for cloud environments
- Contact filtering according to criteria and choosing to view only system, local, or personal contacts

Página2168 de 3226.

- Web conferencing integration
- Unsupervised transfers
- Auto-answer
- Simultaneous mode for interfaces to one-X Portal, Outlook and Salesforce
- Password changing
- Account codes

SoftConsole

SoftConsole is the PC-based Windows receptionist application for IP Office. It can be purchased with the Receptionist user license.

SoftConsole provides enterprise receptionists and operators with call information and call actions to simplify call handling and instant messaging. With SoftConsole, users see the status of other users and adjust basic telephony settings of other users, such as forwarding numbers. Avaya recommends using phones that support Auto Answer. Users can use instant messaging features provided by Avaya one-X® Portal, if available.

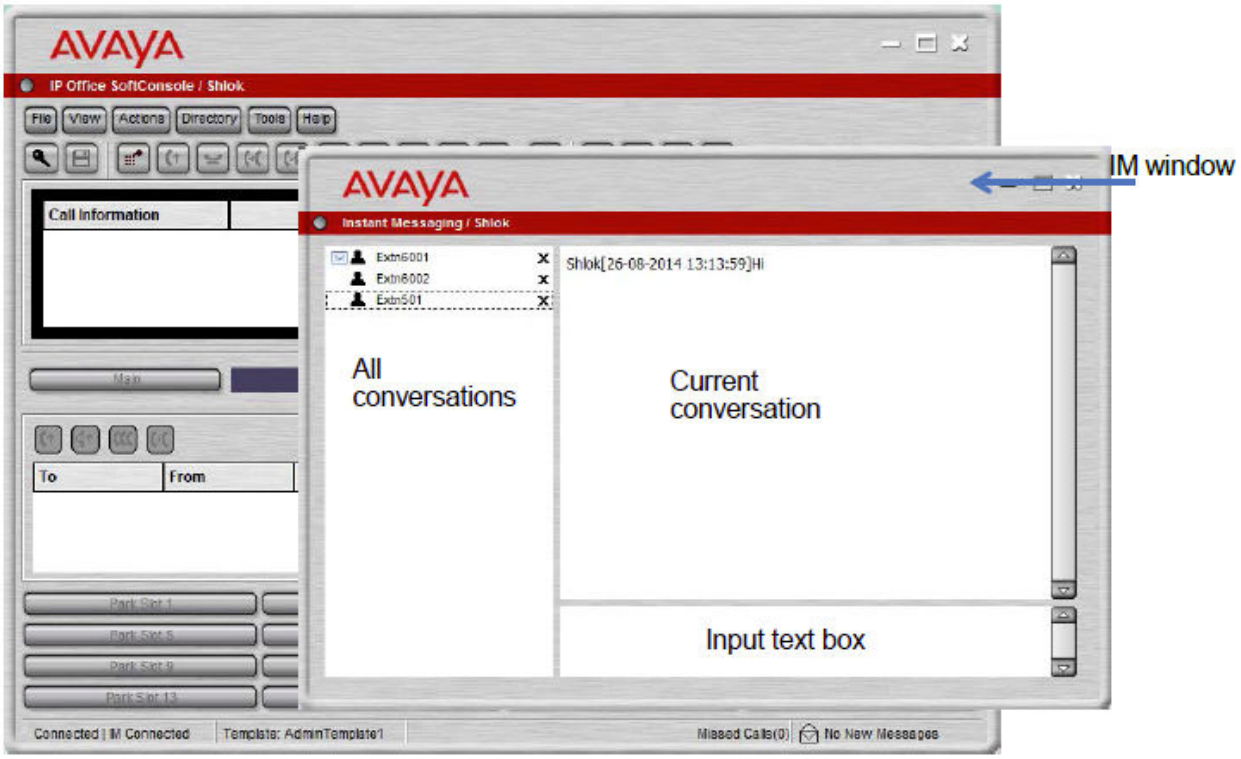


Figure 14: SoftConsole instant messaging window

WebSocket communication allows SoftConsole clients to communicate with IP Office and Avaya one-X® Portal. The WebSocket protocol is bidirectional between the client and the server. As the communication is done over port 80 or 443 (same port used for HTTP), there are no issues with firewall traversal. In a hosted environment, WebSocket communication provides security.

Página2169 de 3226.

SoftConsole can be minimized in the Windows system tray when not in use, but will pop up on the screen when a call is received. Sound and media files can be associated with calls. If this feature is used, the PC requires a sound card and speakers.

SoftConsole supports the following features:

- Answering calls
- Making outgoing calls
- Supervised and unsupervised transfers
- Transfer calls to voicemail
- Hold and park calls
- Monitoring queues and answering queue calls
- Using and viewing conference rooms
- Conferencing held calls
- Adding users to a conference
- Adding text to a call
- Door release
- Intrude
- Sending text messages
- Paging
- Recording calls
- Sending email
- Using dial pad
- Multiple language support, users can select language

Embedded Voicemail

In environments like retail or home office, where space, noise or cost considerations rule out using a PC for voicemail, Embedded Voicemail provides basic voicemail services. Embedded Voicemail is on the IP500 V2 control unit and does not require a separate voicemail server.

Embedded Voicemail is available with IP Office Essential Edition. No additional licenses are required.

Voicemail Pro

Voicemail Pro is provided with IP Office Preferred Edition and is an advanced messaging and call flow application for IP Office systems. Voicemail Pro can handle 40 (up to 250/500 on Server Edition/ Server Edition Select) simultaneous calls depending on license and system settings. Each user has the option of turning their voicemail on or off. When on, the system automatically answers their telephone when they are not available to take a call, plays a personal greeting, and records a message.

Página2170 de 3226.

When a message has been left, the user will see a message-waiting lamp lit on their telephone and can press a retrieval button to collect their messages.

Voicemail Pro can also ring the user to deliver any new messages. Voicemail messages are time and date stamped and the caller's number recorded. Voicemail Pro can be configured to delete read messages automatically, unless the user chooses to save the message permanently.

Voicemails can be collected remotely by dialing into the Voicemail Pro server. If the number the user is dialing from is recognized (home number or mobile/cell phone for example), the user will listen to their voicemail straight away. If the source number is not recognized, the user will be prompted for a mailbox number and a PIN code for that mailbox, before they can listen to their voicemail. Users have the ability to set and change their own PIN codes.

When a voicemail needs to be forwarded to other users, Voicemail Pro provides many options:

- Voicemails can be forwarded to another mailbox, or group of mailboxes
- Recipients can add their comments to the voicemail before forwarding to another mailbox or mailboxes.
- Voicemails can be forwarded as email WAV attachments.

All options are available in a choice of languages; both spoken voice prompts and graphical programming interfaces and have the choice of IP Office TUI and INTUITY emulation TUI.

Conferencing

Users can place calls on hold and a create a conference using either the telephone or desktop applications. Additional conference members may be added, however a single conference may not have more than 64 members (with IP500 V2 only and more on Server Edition).

For ad-hoc conferencing, the system requires as many digital trunks/VoIP channels as external participants (as well as Preferred Edition for Meet-Me conferences). The system supports 128 conferencing channels on the IP500 V2, allowing multiple conferences of any size from 3 to 64 parties. The system support 42 3-party conferences, 2 64-party conferences or any combination in between. Meet-Me capabilities require Preferred Edition for direct dial into a conference bridge with PIN code security. In an SCN network, only one centralized Preferred Edition license is required to host Meet-Me conferences at any of the sites. Conference IDs are also shared across the SCN sites.

The following conference channel capacities are available:

Table 4: Conferencing channel capacities

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
HP DL120 Dell R210	128	128	414	414
HP DL360	256	256	825	825
Dell R620	256	512	825	825

Table continues…

Página2171 de 3226.

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
OVA	256	512	825	825
IP500V2	128	128	128	128

To initiate a conference, users dial the direct number allocated to the conference bridge, type in the PIN (require Preferred Edition and Voicemail Pro) if required. For ad-hoc conferences with a few participants, users can easily set up immediate conferences by calling all parties and bringing them to the conference bridge. With Avaya one-X® Portal for IP Office, the originator of the conference can keep control: the Caller ID number (and the associated name if recognized) of each participant is displayed. If required, they can selectively hang-up a specific participant. The system plays a single beep on entry and a double beep on exit. The owner of the conference may use their extension number as the conference ID. The owner of the conference has control of the conference with the ability to mute and drop calls of participants. All participants will hear the system Music on Hold (MOH) until the owner joins, and will hear MOH when the owner drops. Note that any internal party has the option to view and drop participants (not just the conference originator).

Users can record a personalized greeting for a conference (requires Preferred Edition and Voicemail Pro).

Users can record the conference using Avaya one-X® Portal for IP Office, digital or IP display phone or a short code (requires Preferred Edition and Voicemail Pro). To prevent unauthorized access to the conference bridge, PIN codes, Caller ID number screening as well as time and date profiles can be set-up using Voicemail Pro. One user can manage the conferencing bridge facility from any location.

Conferencing has the following restrictions:

- Only two calls connecting through analog trunks are permitted in any single conference.
- Each external caller requires a digital trunk/VoIP channel (for example 1 T1 allows 23/24 external parties, 1 E1 allows 30 parties and a fully licensed VCM-64 allows 64 parties).
- There are no limits on the mix of internal and external calls in conference, but if all internal participants disconnect from the conference bridge, the external participants can be disconnected automatically by the system for added security (configurable system setting).
- System features such as call intrusion, call recording and silent monitoring all use conference resources, as does automatic recording if enabled. When any of these features are active the number of slots available for conference parties is reduced. For example, a conference call between 3 parties and being recorded will use 4 conference slots.

Meet-Me conferencing

Meet-Me conferencing enables multiple callers to talk in an audio conference. Callers can be on-site personnel as well as external parties whether field-based engineers, sales staff on the road, customers or suppliers. Conference calls can be planned in advance or established ad-hoc as and when required.

Página2172 de 3226.

Video collaboration

IP Office provides Bring Your Own Device (BYOD) and HD room system support for video collaboration.

IP Office supports video collaboration with data sharing through Avaya Scopia® desktop and mobile applications when using Radvision MCU or Video Collaboration for IP Office. Flare clients can also participate in multiparty video conferences. Avaya Scopia® connects to IP Office as a SIP endpoint using an Avaya IP license.

Avaya Video Collaboration for IP Office provides the following features:

- Direct integration including a common dial plan with IP Office
- “Virtual conference room” for up to eight participants with click-to-join capabilities form any standards-based room system, desktop or mobile device
- Freely distributed desktop and mobile video clients for PCs, Macs and most popular iOS and Android devices, enabling people inside and outside an organization to easily join a video meeting
- Low bandwidth HD multiparty video conferencing with data collaboration using native SIP/H.323
- Automatic firewall transversal to engage with participants outside the network

The following diagram shows the topology of IP Office deployed with video endpoints.

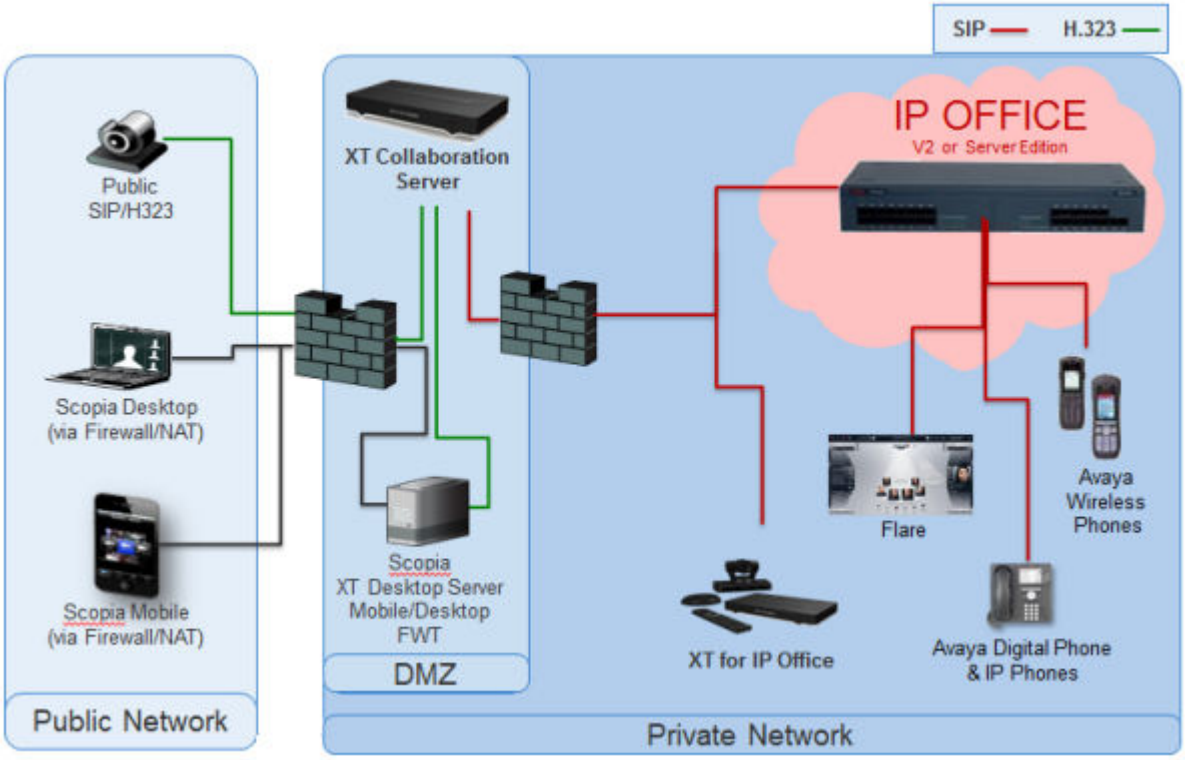


Figure 15: Video endpoints

Collaboration Agent

Collaboration Agent is an application that provides web collaboration and conferencing tools. Users with Avaya Aura® Conferencing accounts and invited guests can use the tools to manage conferences and participate and collaborate in conferences.

Conference participants can join conferences by logging in to Collaboration Agent and dialing in to the audio bridge assigned to the conference. Participants can also use the integrated audio and video feature of Collaboration Agent. Participants can use the Collaboration Agent tools to boost productivity and track action items even after the conference ends. Conference moderators can:

- Record all aspects of conferences.
- Record and edit meeting minutes.
- Create and distribute meeting reports based on the meeting minutes.

Collaboration Agent features

In Collaboration Agent, the participants and moderators can perform multiple tasks such as:

- View a list of other participants.
- Virtually raise a hand and seek permission to speak.
- Send messages.
- Annotate shared content.
- Record or edit minutes.
- Set the entry and exit tones.
- Dial out to other users and the users to the conference.
- Disconnect participants.
- Promote participants to the moderator role.
- Invite more participants to join an active conference.

During the conference, participants can view the following information in Collaboration Agent:

- The participants who joined only on the audio bridge
- The participants active on web collaboration
- The participant currently speaking
- The current presenter

Optional features

The following features are optional and must be enabled by the system administrator:

- Starting conferences before moderators join.
- Integrated video
- Promoting all participants to the presenter role so that all participants can share content
- Dialing out from Collaboration Agent to connect users to conferences
- Conference recording

Página2174 de 3226.

Avaya Spaces

Avaya Spaces is a cloud-based team collaboration and meeting application. It seamlessly integrates voice, video, tasks, sharing, and more into your browser or the Spaces application. Each IP Office user is entitled to a free Avaya Spaces Basic account that includes the following team collaboration activities through Avaya Equinox™ client:

- Creation of Spaces for managing ongoing projects: You can use the Spaces area in the dashboard to start a new conversation. In fact, the first time you start using Avaya Spaces, you can view the option to create your own Space. You can invite participants to your Space by entering their email addresses. You can set different permissions for each participant based on the type of actions you want them to be able to take within your Space. If you have many Spaces, you can categorize the frequently used ones as favorites.
- VoIP audio confererencing with up to five participants.
- Limited file sharing (up to 1–GB)
- Point to point video calls, escalate your chats with audio or video.
- Exchange instant messages with other users by using Avaya Spaces Direct Messaging.
- Join a Spaces meeting.

Avaya Equinox® Meetings Online

Avaya Equinox® Meetings Online offers an optional, subscription service for multi-party Unified Communications, that is, audio, video, and web collaboration. The service provides an Over The Top (OTT) virtual meeting room with audio and video conferencing, content sharing, chat and meeting moderation. Users can access the service through desktop, mobile, and video room system as well as audio dial in; third party video room system interoperability is also supported.

Installation and administration applications

The following sections provide an overview of the installation and administration related applications.

IP Office Manager

Use the Manager to manage IP Office standalone systems or systems in a small community network (SCN). Manager tracks system configuration changes, manages upgrades, and configuration imports and exports.

IP Office has a built-in audit trail that tracks changes to the system configuration, and who has made them. Manager can display the audit trail to assist with problem resolution. The audit trail records the last 15 changes in the configuration and records the following elements:

- Configuration Changed - For configuration changes, the log will report at a high level on all configuration categories (users, hunt group...) that have been changed.
- Configuration Erased
- Configuration merged
- Reboot - user instigated reboot

Página2175 de 3226.

- Upgrade
- Cold Start
- Warm Start
- Write at HH:MM - This is when the administrator saved the configuration via the schedule option
- Write with Immediate Reboot
- Write with Reboot When Free

IP Office Manager is also used for maintenance functions such as:

- Upgrade to the IP Office system software
- Ability to send software over an IP network link to a system and have it validated before committing to the upgrade
- Backwards compatibility with systems from Release 2.1 onwards to allow a single management application
- Importing and Exporting IP Office configuration information in ACSII-CSV files.

Server Edition Manager

Server Edition Manager supports complete centralized administration for Server Edition Primary, Server Edition Secondary, and Server Edition Expansion Systems. Manager also provides IP Office telephony and Unified Communications features.

Manager enables management of all the components within the solution for activities such as:

- Single point of configuration for IP Office and voicemail
- Simple initial installation wizard
- Overview of the system with inventory and status
- Common settings consolidated to the Server Edition Primary
- Integrated Voicemail Proclient, System Status Application, and Linux Platform settings access
- Supports online, offline administration, and configuring a complete solution
- Template operations
- Centralized configuration and template storage
- Administrator account management utility
- Retains existing IP Office expertise
- Context sensitive help

Even though Manager is a Windows application, Manager can be installed directly from the Web administration portal of Server Edition Primary server. This enables you to use any Windows personal computer that has any IP Office Manager that is pre-installed immediately.

Using Manager, the administrator can create templates for many management items such as users, extensions, Hunt Groups, and Lines. The administrator can then create any new item using

Página2176 de 3226.

the default settings or the template. You can create multiple users and extensions using one template.

Call Routing Support:

- Full IP Office ARS and dial plan support
- Default routing simplifies configuration
- Solution wide auto line group numbering
- Common incoming call routes provide resilience
- Resilient Hunt Groups

Offline Operation:

- Complete solution can be created and/or managed offline if required
- Can still manage when some deices offline
- On/offline configuration sync options to harmonize as required

Solution Management:

- Complete solution view with status and inventory
- Users and Hunt Groups are solution wide
- Centralized User Rights, feature short codes, Time Profiles, Incoming Call Routes, and Account Codes
- Permits advanced per-device configuration if desired
- All configurations stored on primary server
- Solution wide system directory
- Easy management of central and per-device licenses

Resilience management:

- You can manage every device locally for ‘rainy day’ events
- You can manage the solution through a secondary server when the primary server fails or in a split WAN setup
- On/Offline configuration sync options to harmonize as required

Add or Remove Devices:

- Single process for addition or removal of device
- Built-in Initial Configuration Utility (ICU) to simplify adding a new device
- Common configuration items from primary server is auto populated
- Can configure before you install a new device

Validation :

- Configuration validation on read and any change.
- Solution wide validations

Página2177 de 3226.

Template:

- Create a local and centralized template from an existing Line, Extension, User, Hunt Group, Time Profile, Firewall Profile, IP Route and Service entries
- Recreate multiple Extension and Users from one template

Remote access:

- Supports access from service through SSL VPN

Security:

- Single Sign On to all except one-X Portal administration

Web Manager

Web Manager is a browser-based management tool designed to simplify the installation and maintenance process and provides access to most, but not all, IP Office configuration settings. Web Manager eliminates the need to have windows operating system because it can run on any device that supports standard browsers.

Granular access:

Web Manager provides service users with access to entire configuration objects if the service user has the configuration access. However, large customers who have multiple service users roles or customers having deployments in the cloud environment need to have granular configuration access for different service users. Hosting partners will be able to build an account for customer or re-seller with limited permissions. These permissions shall restrict the customer or re-seller from performing activities that affects service of the system.

Configuration dashboard:

The Dashboard is a simplified version of the existing IP Office Web Manager and is presented to the administrators when a fresh single-node IP Office system is installed. The Dashboard consists of minimum required set of configuration fields to set up the system. The full setup can be performed anytime afterwards.

IP Office Media Manager

IP Office Media Manager is a native IP Office application to archive, store, search, playback, download, audit, and delete IP Office call recordings. The Operation, Administration, and Management of (OAM) of the application is integrated within the IP Office solution, for example, IP Office Web Manager.

Media Manager obtains the recordings from the IP Office Voicemail Pro application through a pre-configured hand-off directory. Media Manager moves the recordings from the hand-off directory to an additional hard disk partition on the Server Edition Primary or Application Server and then archives the recordings to a storage location configured by the administrator. The archiving location can be a Network-Attached Storage (NAS), a local DVD drive, or cloud storage. For cloud storage, Media Manager supports only Google Drive in this release.

Media Manager is licensed on a system basis. Apart from a new IP Office Release 11.0 and later Media Manager license, the application also works with an earlier Contact Recorder license, for customers upgrading from an earlier IP Office version. Media Manager allows a 90–day trial period before licensing is enforced.

Contact Recorder is not supported in IP Office Release 11.0 and later and is not part of IP Office Release 11.0 and later software. However, Media Manager supports migration of Contact Recorder data to IP Office Release 11.0 and later.

Media Manager is available as part of the IP Office Server Edition and Application Server software image. The application runs on the standard Linux distribution supported by IP Office Server Edition and Application Server platforms. The software is installed as a standard Linux RPM only on the Server Edition Primary server or the Application Server in case of IP500 V2 deployments. The application is not supported on UCM or Windows platforms. The management interface is web-based and all popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Internet Explorer are supported.

Media Manager in IP Office Release 11.0 Feature Pack 4 supports deleting or recordings and keeping track of usage of recordings through the Audit trail feature. The Audit trail feature helps you in keeping track of the activities around the recordings in the library. Using this feature, you can find out the users who have:

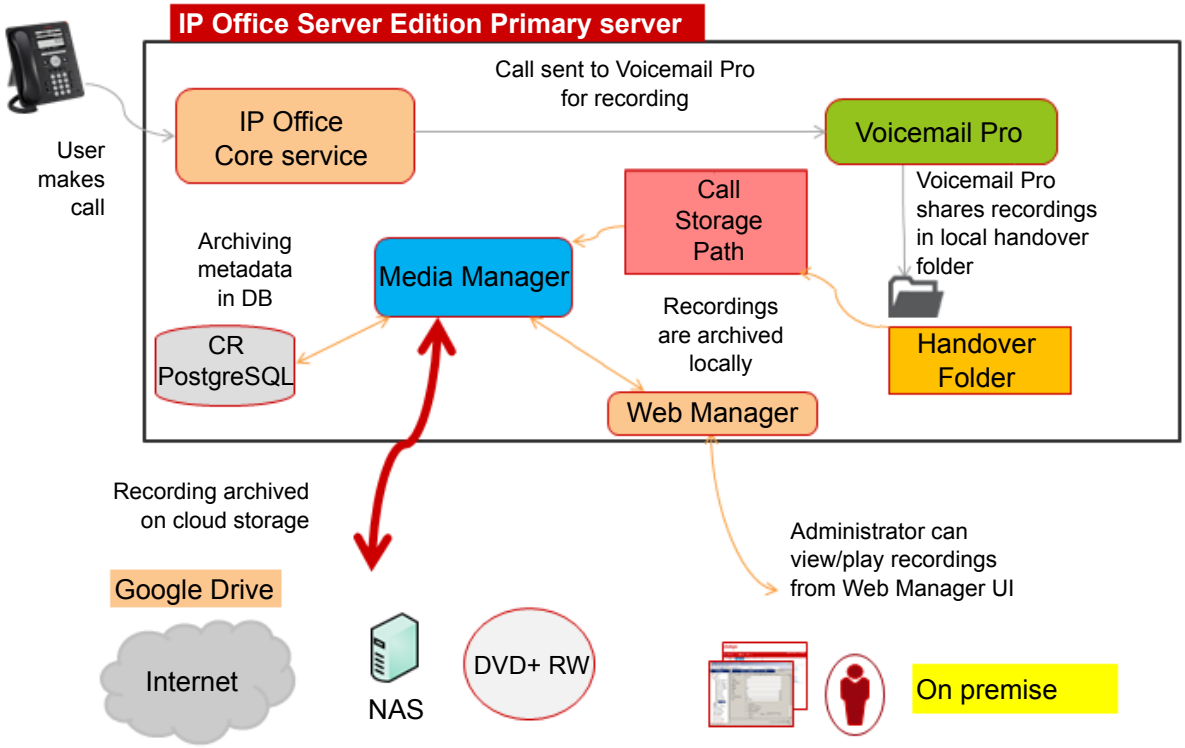
- Searched a recording
- Replayed a recording
- Downloaded a recording
- Deleted a recording

For each event, Media Manager displays the user name, date, time, and the type of user action. The Audit trail is maintained for a predefined number of days and can be modified. By default the Audit trail data is available for 180 days.

Media Manager is available as part of the IP Office Server Edition and Application Server software image. The application runs on the standard Linux distribution supported by IP Office Server Edition and Application Server platforms. The software is installed as a standard Linux RPM only on the Server Edition Primary server or the Application Server in case of IP500 V2 deployments. The application is not supported on UCM or Windows platforms. The management interface is web-based and all popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Internet Explorer are supported.

A standard IP Office Server Edition deployment:

Página2179 de 3226.



Availability of Contact Recorder features in Media Manager

The search capabilities in Media Manager has been enhanced for the administrators and the users.

Functionality	Description	Availability in Contact Recorder	Availability in Media Manager
Search by administrator	Search by administrators using Target Number, Skills, Agent, and Call ID	Yes	Yes
Search through Web Self-Admin	Search by users using the search filters Target Number, Skills, Agent, and Call ID	Yes	Yes
Web Self-Admin search results	A maximum of 100 results are displayed.	Yes	Yes
Call sets	Facility to save search results for retrieving in the future.	Yes	No
Email	Attaching recordings to emails.	Yes	No

Table continues…

Functionality	Description	Availability in Contact Recorder	Availability in Media Manager
Bulk Export	Exporting multiple recordings and the related details	Yes	Yes
Owner	Available as a search option.	No	Yes
Audit Trail	Audit can be performed to track the use of call recordings.	Yes	Yes
Windows Domain Authentication	-	Yes	No

Solution Management Application

IP Office Manager and Web Manager use the Solution Management Application (SMA) to access the system configuration.

SMA resides on the primary or secondary server. Settings are available for remote access and Server Edition Central Access. Central Access communicates with the primary or secondary server rather than to each node individually. Avaya requires Central Access for a hosted environment and recommends it for non-hosted environments with more than 32 nodes.

SoftConsole Administrator mode

System administrators can start SoftConsole in administrator mode. When run in this mode, there is no access to the telephony functions.

SoftConsole administrator mode enables users to configure the following functions:

- Create and edit user profiles
- Amend the length of call notes
- Create and edit templates
- Remove or display the interface panels

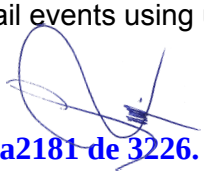
SNMP Management Console

Simple Network Management Protocol (SNMP) is an industry standard designed to allow the management of data equipment from different vendors using a single Network Manager application. The Network Manager periodically polls equipment to solicit a response, if no response is received an alarm is raised. In addition to responding to polls, IP Office monitors the state of its Extensions, Trunk cards, Expansion Modules and Media cards so that if an error is detected IP Office will notify the Network Manager.

As the IP Office platform comprises many applications, the core software notifies SNMP events from both Voicemail Pro and Embedded Voicemail to warn of approaching storage capacity limits.

IP Office sends email notifications directly to the email server; no additional PC client is needed.

On customer sites where SNMP management is not available, IP Office can email events using up to 3 email addresses each containing a different set of alarms.



The following system event categories can be chosen for email notification, if installed on the system:

- Generic
- Trunk lines
- Embedded Voicemail Card
- VCM
- Expansion modules
- Applications
- License
- Phone change
- CSU Loop-Back

IP Office has been tested against CastleRock's SNMPc-EE™ and HP's Network Node Manager (part of the OpenView application suite).

System Status Application (SSA)

The System Status Application (SSA) is a diagnostic tool for system managers and administrators to monitor and check the status of IP Office systems locally or remotely. SSA shows both the current state of an IP Office system and details of any problems that have occurred. The information reported is a combination of real-time events, historical events, status and configuration data to assist fault finding and diagnosis. SSA provides real-time status, historic utilization and alarm information for ports, modules and expansion cards on the system. SSA connects to all variants of IP Office using an IP connection that can be remote or local. Modem connections at 14.4kbps or above are supported for remote diagnostics.

SSA provides information on the following:

Alarms	SSA displays all alarms which are recorded within IP Office for each device in error. The number, date and time of the occurrence is recorded. The last 50 alarms are stored within IP Office to avoid need for local PC.
Call Details	Information on incoming and outgoing calls, including call length, call ID and routing information.
Extensions	SSA details all extensions (including device type and port location) on the IP Office system. Information on the current status of a device is also displayed. SSA shows IP Extensions that were registered but no longer available and IP extensions that are configured but have not been registered after last re-boot. This helps to spot phones that are Idle, disconnected, or are misconfigured. SSA also shows quarantined phones and blacklisted extensions and IP addresses.

Página2182 de 3226.

Trunks	IP Office trunks and connections (VoIP, analog and digital) and their current status are displayed. For VoIP trunks, QoS information is also displayed (e.g. round trip delay, jitter and packet loss).
System Resources	IP Office includes central resources that are utilized to perform various functions. Diagnosing these resources is often critical to the successful operation of the system. This includes details on resources for VCM, Voicemail and conferencing.
QoS Monitoring	QoS Parameters from connected calls, such as jitter and roundtrip delay, are monitored.

SSA can be launched independently or from IP Office Manager and there can be up to two (2) SSA clients connected to an IP Office unit at one time.

Note: SSA is not a configuration tool for IP Office systems.

SysMonitor

Use SysMonitor to troubleshoot IP Office from both local (LAN) and remote locations (WAN).

Select the protocols and interfaces to monitor and diagnose through a graphical interface. Capture traces directly to the screen or as a log file for later analysis. Color code different traces to improve the clarity in large files. The utility also captures system alarms and displays the activity log of the last 20 alarms that have occurred.

Cloud Operations Manager

Cloud Operations Manager is an administration tool that allows a simplified way of multi-customer management with a focus on cloud-based systems. The tool enables management of IP Office Server Edition systems and provides the following capabilities:

- Single Unified Management portal capable of managing up to 3000 IP Office systems.
- Dashboard that displays error conditions, ongoing system activities, and system health
- Grouping of systems based on versions and tags for accessing similar systems at the click of a button
- Displays all connected systems such as Primary, Secondary, Expansions, and open applications
- Ability to centrally manage IP Office software upgrades and patching across multiple system and versions
- Role-based administration: Cloud Operations Manager has its own service users with access to complete or selective customers IP Office. No granular feature level access is available in Release 11.0.
- Provides facility to launch Native IP Office Management applications. Uses need to log in to the applications separately after the application is launched. Launching of IP Office Contact Center, Avaya Contact Center Select, and Avaya Workforce Optimization Select are not supported in Release 11.0.

Página2183 de 3226.

- Alarms for Configuration, Services, Trunks, Link, and Security by Severity type
- Alarms for status of IP Office systems indicating whether they are online of offline
- Alarms indicating status of various applications

Data Migration Manager (DMM)

The Data Migration Manager (DMM) facilitates migration from BCM and Norstar systems to IP Office. There are three steps in the migration process: extract, convert and apply.

DMM migrates:

- Announcements and greetings
- Voicemail messages
- Extract Call Pilot configuration

Contact center applications

The following sections provide an overview of the contact center applications.

For general information about:

- IP Office Contact Center, see *Avaya IP Office Contact Center Feature Description*.
- Avaya Contact Center Select, see *Avaya Contact Center Select Solution Description*.

IP Office Contact Center overview

Note:

IP Office Contact Center goes End of Sale for new systems in September 2019.

Avaya is the market leader in call center technology, and IP Office Contact Center can take your business to a new level. IP Office Contact Center provides integrated contact center capabilities specifically designed for businesses supporting between 5 and 250 contact center agents and supervisors.

IP Office Contact Center provides the following features and characteristics:

- All-in-one customer service solution that delivers consistent service to customers across multiple media channels and locations. IP Office Contact Center includes a user interface (UI) on Microsoft Windows and a web interface supported on various browsers.
- Fast implementation with minimum disruption to the business. IP Office Contact Center also includes an automatic synchronization feature for configuration. This feature can be enabled and disabled as needed during implementation.
- Access to Agent UI functionality, including call control, from a SalesForce (SFDC) plug-in or SAP CRM connector.
- Email and chat capabilities on the Windows and Web UI.
- Inbound and outbound voice calls with telephony and dialer capabilities.
- Skills-based routing.

Página2184 de 3226.

- Address book access so agents can quickly find the contact information they need to make calls and send emails.
- Real time and historical reporting for all media channels.
- Interactive Voice Response (IVR) and Task Flow Editor scripts.
- User profile and agent group privilege configuration to determine which features are available to users of the interface. Administrators must assign privileges and create agent groups.
- Access to a web-based administration portal. You can use the administration portal to perform configuration, maintenance, monitoring, and management tasks. You can also upload certificates, collect logs, and download email archives and the IP Office Contact Center User Interface for Windows. Advanced administration tasks must be performed in the IP Office Contact Center User Interface for Windows. You cannot perform administration tasks with the IP Office Contact Center Web User Interface.
- Access to a wallboard that displays IP Office Contact Center statistics. For more information about Wallboard, see *Using Avaya IP Office Contact Center Wallboard*.
- Option to easily integrate chat functionality into a web page. For more information, see *Avaya IP Office Contact Center Email and Chat Services Task Based Guide*.
- Optional integration with call recording applications, such as IP Office Media Manager. Calls are recorded with Voicemail Pro and the details of the complete recording are stored in the database of the call recording application. You can search for and manage recordings using a web browser.
- Optional interoperability with Avaya Workforce Optimization Select, which is a stand-alone product that does not currently integrate with IP Office Contact Center UIs or applications.
- Media Resource Control Protocol (MRCP) integration, which provides support for text to speech (TTS) and automatic speech recognition.

Avaya Contact Center Select overview

Avaya Contact Center Select is a context-sensitive, collaborative, voice and multimedia contact center solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform.

Avaya Contact Center Select uses industry-standard SIP and CTI interfaces to integrate with IP Office. This integration gives Avaya Contact Center Select access to and control of a wide range of IP Office phones and features. Customers integrating Avaya Contact Center Select with IP Office gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility.

Avaya Agent Desktop is a single-interface client application used by Avaya Contact Center Select agents to assist customers. Avaya Contact Center Select agents use Agent Desktop software to respond to customer voice and multimedia contacts. Agent Desktop supports a range of IP Office phones and a wide variety of multimedia contact types.

By default, Avaya Contact Center Select connections and Web Services use secure TLS communication. The Avaya Contact Center Select Certificate Management tool makes it easier to manage security certificates.

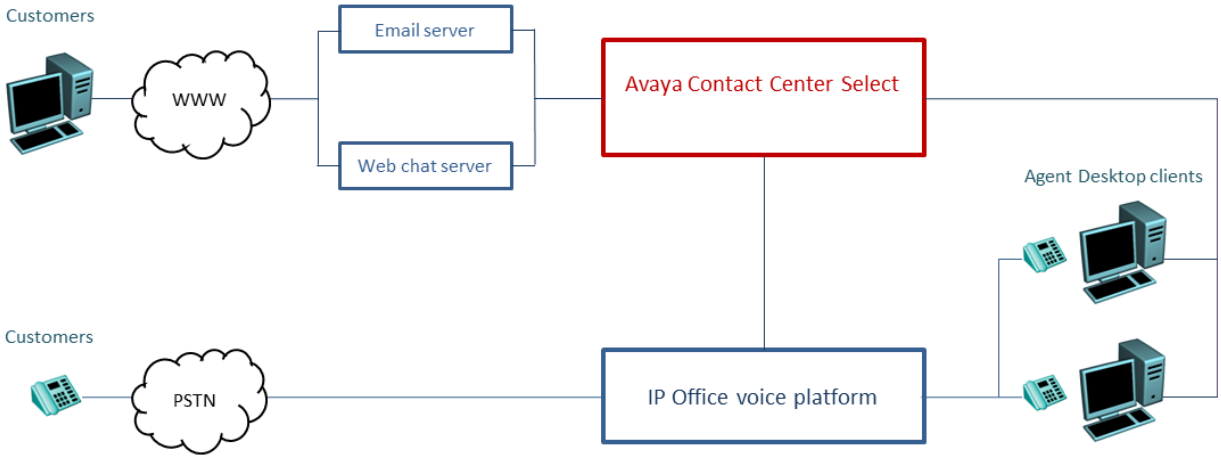


Figure 16: Typical contact center solution using voice and multimedia Avaya Contact Center Select and the Avaya IP Office voice phone system

Avaya Contact Center Select provides a feature-rich voice and multimedia solution with integrated routing and reporting for small to midsize enterprises. Avaya Contact Center Select provides unified contact center and IP Office phone user account management for agents and supervisors. Voice-enabled agents and supervisors created in Avaya Contact Center Select are automatically added to IP Office. Avaya Contact Center Select synchronizes user (agent and supervisor) information between Avaya Contact Center Select and IP Office.

Página2186 de 3226.

Chapter 3: Solution specifications

Reference configurations

IP Office is sold in different editions, reference configurations, and deployment scenarios to meet different customer requirements. The editions build on one another to offer advanced functionality, including presence, instant messaging, web collaboration, and Microsoft software integration.

The following sections summarize IP Office editions and other configuration options. These sections do not provide complete reference configuration details for every IP Office option. Separate Reference Configuration documents are available for IP Office Server Edition, IP Office Branch, Powered by Avaya Cloud solutions, and IP Office Contact Center.

IP Office editions

IP Office Basic Edition

IP Office Basic Edition is intended for small and growing enterprises that need higher productivity with a professional touch. Businesses can increase capacity as needed.

IP Office Basic Edition provides basic telephony features such as:

- 64 trunk capacity: analog, PRI/T1, and SIP
- Key system operation
- 64 party conferencing capacity
- Automated Attendant
- Multiple language support
- Call forwarding
- Caller ID
- Dial by name
- Breakout to reception
- Integrated voicemail:
  - Maximum of 6 concurrent calls to voicemail with approximately 25 hours of storage
  - Message control including Save, Delete, Forward, Repeat, Rewind, Fast Forward, and Skip Message

Página2187 de 3226.

- Visual voicemail
- Message time and date stamping

Modes of operation

IP500V2 control units are supplied with no installed firmware or configuration. When first powered up, the control unit loads and installs the necessary firmware from the system SD card installed in it. It creates a default configuration matching the card installed in the control unit and external expansion modules attached to it. IP500V2 control units can operate in a number of modes. The initial mode is determined by the type of system SD card.

Mode	SD card
IP Office Basic Edition Quick mode	• a-law telephony PBX system operation. • µ-law telephony key system operation.
IP Office Basic Edition - PARTNER Mode	Defaults to a-law telephony PARTNER mode operation.
IP Office Basic Edition - NORSTAR Mode	Defaults to µ-law telephony NORSTAR mode operation.

Basic Edition runs on the IP500V2 control unit. An SD is required and is installed in the rear of the control unit, providing operating software, feature keys, and licenses. An optional SD card can be installed in the optional SD card slot, providing redundant backup and system upgrade capabilities.

Table 5: Supported base cards

Basic Edition supports following base cards:

Base card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
Combination analog	4	4
Combination BRI		2
ETR6	3	
DS8	3	3
TCM8	4	4
Phone 2	4	4
Phone 8	4	4

Table 6: Supported trunk cards

Basic Edition supports the following trunk cards:

Trunk card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
ATM4	4	4
PRI/T1	1	
PRI/E1		1

Table continues…

Página2188 de 3226.

Trunk card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
BRI4		4
BRI8		1

Expansion modules

Basic Edition supports the following expansion modules:

- DS16A
- DS16B
- DS16B2
- ATM16
- Phone 16
- Phone 30
- DS30A
- DS30B
- DS30B2

Note:

DS16B2 and DS30B2 digital station modules are supported on IP Office Release 10.1, Release 9.1 SP12, and 10.0 SP5 onwards.

IP Office Essential Edition

IP Office Essential Edition provides the same features as Basic Edition as well as the following:

- Mobile call control with one number access and simultaneous ringing on mobile devices
- Up to 4 remote workers through an internet connection and an Avaya 9600 series IP phone
- 24 hour access with customized voicemail greetings for each staff member
- Voicemail:
  - Maximum of 6 concurrent calls to voicemail
  - Send voicemails to email
  - Up to 25 hours of voicemail storage (with 6 ports)
  - Up to 40 automated attendants with a maximum of 6 concurrent calls
- Multiple language support
- Up to 128 party audio conference bridge with 64 in any one conference

Note:

Basic Edition is not a prerequisite for Essential Edition or Preferred Edition, and is not stacked under Essential Edition.

Página2189 de 3226.

IP Office Preferred Edition

IP Office Preferred Edition provides intelligent call routing, messaging, call handling and application integration.

In addition to the features provided with Essential Edition, IP Office Preferred Edition provides the following:

- Scalable voicemail:
  - Up to 40 simultaneous calls
  - Send a voicemail to all employees, a department, or a team
  - Address messages by extension or by name
  - Voicemail messages can “find” users to alert them a message is waiting
- Secure conferencing for up to 128 parties with 64 per conference
- Automated call routing with an unlimited number of automatic attendants that can be customized for time of day, day of week or other variables as well as to recognize callers and deliver personalized messages
- Call recording for incoming and outgoing calls that can be sent to voicemail or email inboxes as WAV files

Components

- IP500 V2 control unit
- Ethernet attached PC running the supported version of Windows Server
- Ethernet attached PC configured with Application Server software
- IMAP mail client (Outlook) for voicemail synchronization in email and browser-based access to voicemail
- Digital trunks and channels to support users
- IP Office supported telephones

IP Office Server Edition

IP Office Server Edition provides IP Office telephony capabilities, unified communications, mobility, and collaboration. It also provides high availability, ease of use, and low total cost of ownership (TCO). Targeted at the midsize enterprise, IP Office Server Edition supports up to 150 sites, 3000 users, and comprehensive resilience.

IP Office Server Edition Solution provides the following:

- A single Server Edition Primary server provides IP Office, Voicemail Pro, and Avaya one-X® Portal for IP Office.
- A Server Edition Secondary server increases the capacity and provide resilience.
- Expansion systems, which provide additional capacity, support analog or digital interfaces, and remote locations.
- A Select IP Office Server Edition Solution provides additional capacity.
- Support for an existing IP500 V2 control unit optimized for a hybrid of analog/TDM and IP deployments, or a Linux server optimized for IP only deployments.

Página2190 de 3226.

- Users and extensions can be configured on the IP Office Server Edition server or the Server Edition Expansion System.
- Software distribution includes the various user and administration applications such as IP Office Manager, SSA, Voicemail Pro, and IP Office SoftConsole.
- Components can be in the same location or in different locations.
- Optionally configure a separate application server dedicated to Avaya one-X® Portal to provide more user capacity than the Server Edition Primary supports.
- Add additional servers and expansion systems any time.

.

Topology

IP Office Server Edition is based on a double star network topology that provides comprehensive features and their management, enables ease of use, installation, and administration. The overall solution provides a flexible and modular architecture starting with a single server and you can scale up the number of users and locations by networking multiple servers. The components automatically act as a single logical unit and you can administer the components from a single console through an integrated management system.

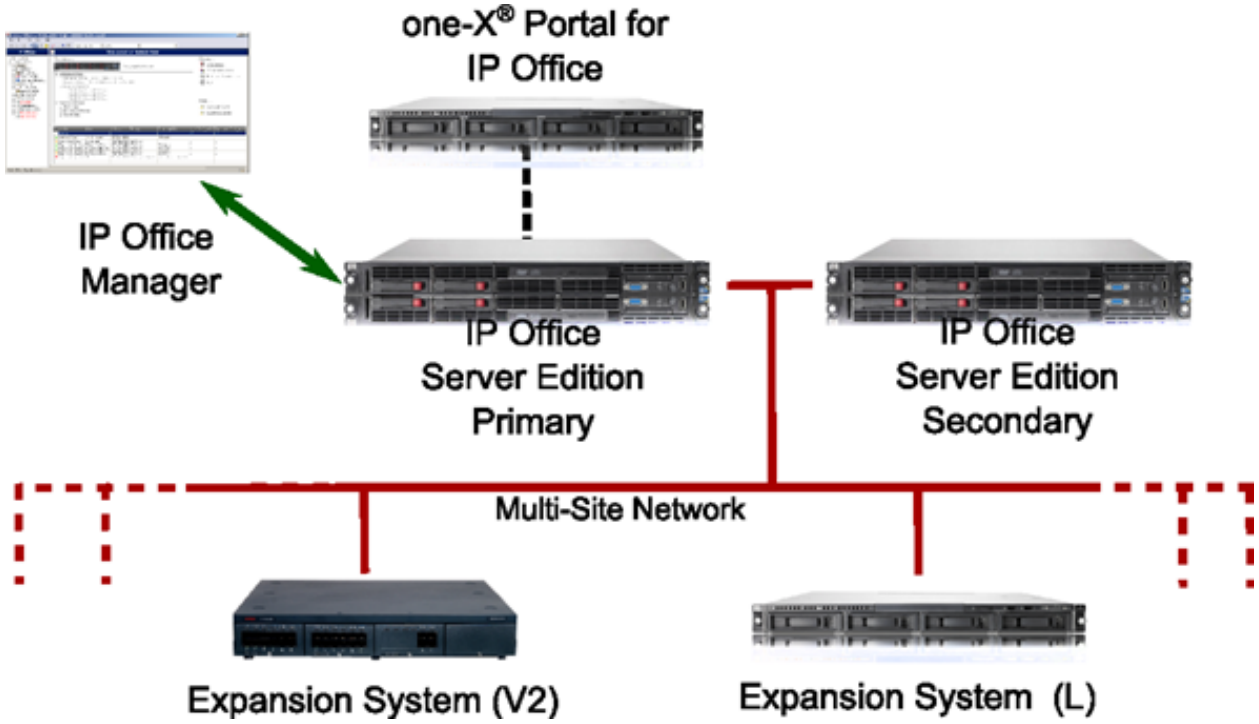


Figure 17: IP Office Server Edition topology

Deployment models

Centralized IP only	One primary server located at the customer headquarters

Página2191 de 3226.

Centralized IP analog and digital	One primary server and one expansion server located at the customer headquarters
Distributed IP only	One primary server located at the customer headquarters and one secondary server located at a remote location
Distributed IP analog and digital	One primary server and one expansion system located at the customer headquarters and one expansion system located at each remote site
Virtualized environment	Customer-provided software and hardware VMware vSphere platform with IP Office Server Edition and application server OVA ignited as a primary, secondary, expansion or application server.

Components

Component	Server options	Description
Server Edition Primary server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Software distribution includes: • IP Office Server Edition • Voicemail Pro • Avaya one-X® Portal for IP Office • IP Office Manager • System Status Application (SSA) • SoftConsole
Server Edition Secondary server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component to support resilience either centrally or at a remote site.
Server Edition Expansion System	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component to support remote locations. Up to 148 expansion systems provide additional capacity, support analog or digital interfaces, and local trunks at remote sites. Can be set up either centrally or at a remote site. **Note:** In a cloud environment, the IP500 V2 expansion system provides support for analog and digital endpoints.

Table continues…

Página2192 de 3226.

Component	Server options	Description
Server Edition Expansion System	IP500 V2	Optional component to support remote locations and as a gateway. Can be an existing IP500 V2 or IP Office Server Edition server. Can be set up either centrally or at a remote site.
Avaya one-X® Portal for IP Office application server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component. You can optionally configure a separate application server dedicated to Avaya one-X® Portal to provide more Power User capacity above the maximum that Server Edition Primary supports.

Virtualized environment components

Avaya provides a virtualized equivalent to the IP Office Server Edition and applications server packaged as a single OVA ready for installation on vSphere supported host hardware from a PC. The OVA is available as a download from Avaya or on an orderable DVD. Once deployed, it can be ignited as a primary, secondary, expansion or applications server.

Other deployment options

You can also deploy IP Office in:

- An enterprise branch environment (Centralized IP Office branch) or a Distributed Branch environment).

  You can deploy an IP Office system as a standalone branch or connect it to the Avaya Aura® network. A CS 1000 branch environment is also supported.
- A Cloud environment with the Powered by Avaya offers.

Contact center options are also available.

IP Office as an enterprise branch overview

You can deploy IP Office as an enterprise branch to provide a communications solution that is adaptable to meet the growing needs of an enterprise branch network while providing investment protection of the installed hardware platform and phones. You can implement an IP Office enterprise branch on an IP Office Standard Mode, Essential, or Preferred system. The IP Office system can be installed as an independent, standalone branch, or be connected to the Avaya Aura® network and migrated to a Distributed, Centralized, or Mixed enterprise branch to provide specific features and applications to meet the needs of individual employees in each branch location.

In addition to centralized SIP endpoints or centralized analog devices configured as ATA, IP Office can concurrently support other IP and TDM endpoints for a community of Centralized users and IP Office users in the same branch. Ideal for enterprises wanting applications deployed in customer

Página2193 de 3226.

data centers or in the branch, an IP Office Branch can effectively deliver a range of communication tools without complex infrastructure and administration.

IP Office is also supported in an Avaya Communication Server 1000 (CS 1000) branch environment. Only the Distributed enterprise branch option is supported. IP Office can be deployed as a new branch in an existing CS 1000 configuration with the addition of Avaya Aura® Session Manager to which IP Office connects through the SM Line for branch connectivity. Providing phone investment protection, IP Office can also be deployed as a replacement for Business Communications Manager (BCM) or Norstar in a branch office and connect to CS 1000 through Avaya Aura® Session Manager. IP Office cannot operate as a survivable gateway to CS 1000 endpoints as similar to Survivable Remote Gateway (SRG).

Topology

The IP Office Branch solution provides the flexibility to support independent, stand-alone IP Office branches as well as IP Office branches connected to an Avaya Aura® system. The Branch solution also supports CS 1000 integration. The following deployment options are available for the solution architecture:

- **Stand-alone IP Office branch option**: Independent IP Office systems are deployed within the network. These IP Office systems are not connected to each other or to anything else in the network. With this option, IP Office Branches are not connected to an Avaya Aura® system and users cannot access any Avaya Aura® services.
- **Distributed enterprise branch deployment option**: All users in this deployment option are IP Office users. These IP Office users obtain telephony services from the local IP Office and not from Avaya Aura®. The IP Office systems in this deployment option can be connected to Avaya Aura® Session Manager and administrators can obtain Centralized management services through Avaya Aura® System Manager. The enterprise can choose to connect IP Office users in this deployment option to an IP Office voice mail system, Embedded Voicemail or Voicemail Pro, or a Centralized voice mail system, such as Avaya Aura® Messaging or Avaya Modular Messaging. IP Office users in this deployment also have access to some Centralized Avaya Aura® applications and services.

  With the Distributed branch deployment option, you can also connect CS 1000 to IP Office in the branch through Avaya Aura® Session Manager. Users still obtain telephony services from the local IP Office, but can use Avaya CallPilot® as their voice mail system. When connected to CS 1000, IP Office and CS 1000 interoperate as peers through Avaya Aura® Session Manager.
- **Centralized enterprise branch deployment option**: All users in the enterprise are Centralized users.

  Centralized users register to Avaya Aura® Session Manager and obtain telephony services from the Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. If WAN connectivity to Avaya Aura® Session Manager is lost, the user automatically gets basic telephony services from the local IP Office. The telephony features provided by IP Office in survivability mode is limited compared to the features that are normally provided to the Centralized phone.

  Centralized users must be configured on the Avaya Aura® Session Manager, Communication Manager, and IP Office. A Centralized user must be configured on the Avaya Aura® Session

Página2194 de 3226.

Manager and Avaya Aura® Communication Manager as a SIP user. On IP Office, the Centralized user must have either a SIP extension, an analog extension, or an analog fax device.

- **Mixed enterprise branch deployment option**: An enterprise branch with both Centralized users and IP Office users. Centralized users and IP Office users obtain the same telephony services described above. All users in this deployment option must use a Centralized voice mail system: Avaya Aura® Messaging or Avaya Modular Messaging.

The deployment options in the Branch solution allow you to start off with stand-alone IP Office systems and then slowly evolve the solution architecture into a Centralized environment as your enterprise grows.

The following image shows the topology of the solution architecture with the deployment options described above. This image does not show CS 1000 in the Distributed branch deployment.

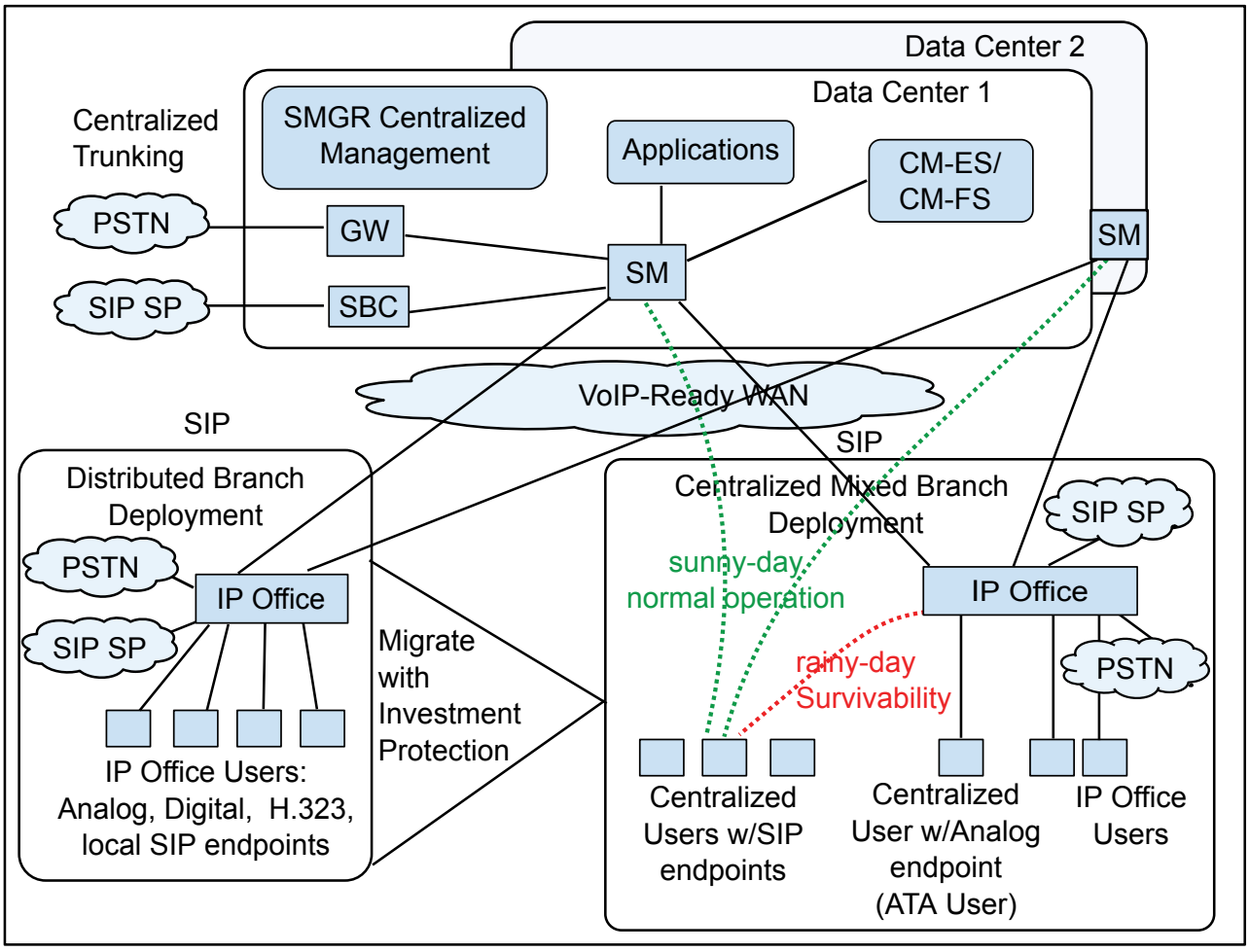


Figure 18: Topology of solution architecture

Powered by Avaya Cloud overview

The Powered by Avaya Cloud solution enables you, the BP or provider, to sell core IP Office and, optionally IP Office Contact Center or Avaya Contact Center Select, features to small and medium

Página2195 de 3226.

enterprise users. With Powered by Avaya, you install and host the product instances in a Cloud data center at your site.

The existing Powered by Avaya Cloud solution enables you, the BP or provider, to sell core IP Office and, optionally IP Office Contact Center or Avaya Contact Center Select, Telephony and Unified Communications (UC) features to users in small and medium enterprises. With the new IP Office Cloud offer, the optional IP Office Contact Center and Avaya Contact Center Select components are not supported. Hybrid Cloud functionality, Voicemail Pro, and Media Manager are also not supported in the new IP Office Cloud offer. This offer currently uses Embedded Voicemail as its voice mail system.

With the existing Powered by Avaya offer, you install and host the product instances in a Cloud data center. The new IP Office Cloud is hosted in a Google Cloud environment with one IP Office cluster per provider.

Key benefits of the Cloud solution include the following:

- Reduction in operational costs for the enterprise by reducing the IT complexity of equipment maintenance.
- Reduction in service delivery costs for the BP through virtualization and shared infrastructure.
- Programmatic interface to support license installations, configure centralized licensing, or delete a license file.
- Automated billing with Avaya One Source Cloud Services.
- Flexibility to change your Avaya One Source Cloud Services order anytime. You can add or remove users anytime. You can update your order to add or remove the optional IP Office Contact Center and Avaya Contact Center Select programs as needed.
- Support for IP500 V2 expansion systems at the enterprise site with Hybrid Cloud. This does not apply to the new IP Office Cloud offer.
- Support for resiliency with High Availability (HA).

Powered by Avaya topology

Powered by Avaya supports the following deployment models:

- Public Network: This deployment model uses a public over-the-internet connection between the Cloud data center and the enterprise premises. All users connecting over the Public Network are considered Remote Workers.
- Private Network: This deployment model requires an MPLS or site-to-site VPN connection between the Cloud data center and the enterprise premises.

Página2196 de 3226.

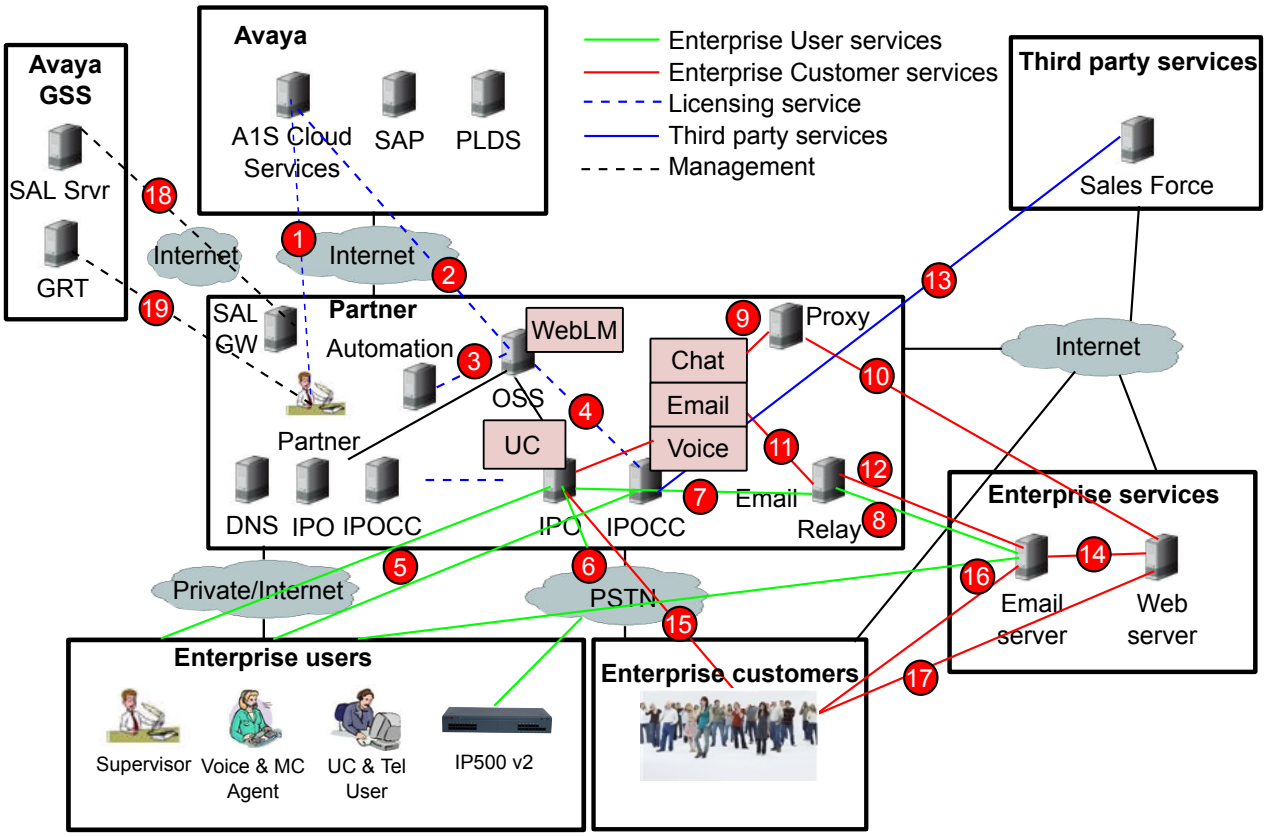


Figure 19: Powered by Avaya topology

Contact center reference configurations

IP Office Contact Center deployment options

IP Office Contact Center can be deployed using the following deployment configurations and options:

Configuration	Deployment options	Agents and trunks
IP Office Contact Center with IP500V2	IP500V2, IP Office Contact Center server, and an application server	Up to 30 agents on SIP and digital trunks.
IP Office Contact Center with IP Office Server Edition	IP Office Server Edition server and IP Office Contact Center server *and/or* a Linux expansion server (optional) *or* Hosted as a service in a cloud environment	Up to 250 agents on SIP trunks. Only 125 agents can be deployed on each Linux expansion node.

Table continues…

Página2197 de 3226.

Configuration	Deployment options	Agents and trunks
IP Office Contact Center with IP Office Server Edition and IP500V2 expansion	IP Office Server Edition server, IP500V2 expansion server, and IP Office Contact Center server	Up to 250 agents on SIP and digital trunks. Only 30 agents can be deployed on each IP500V2 node.
IP Office Contact Center with IP Office Server Edition in a distributed environment	IP Office Server Edition server, IP500V2 expansion server, IP Office Contact Center server, and a Linux expansion in a distributed environment	Up to 250 agents on SIP and digital trunks. Up to 30 agents can be deployed on each IP500V2 node, and up to 125 agents can be deployed on each Linux expansion node. Agents and trunks are distributed on any expansion server.

Detailed IP Office Contact Center topologies are shown in the following documents:

- *Avaya IP Office Contact Center Feature Description*
- *Avaya IP Office Contact Center Reference Configuration*

Avaya Contact Center Select reference configurations

Avaya Contact Center Select is a feature-rich contact center solution that provides skill-based routing for customer voice and multimedia contacts. Avaya Contact Center Select provides extensive tools for agent management, real-time and historical reporting, and graphical tools to create contact flows and treatment rules. It provides license management, networking, and Open Interfaces Web Services. Customers integrating Avaya Contact Center Select with the IP Office platform gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility.

At deployment time, Avaya Contact Center Select automatically launches a simple configuration wizard to rapidly deploy a functional contact center solution. It is preloaded with sample users, skillsets, and contact center parameters. Use this sample data to rapidly commission the solution and make the first routed customer call and email contact.

Avaya Contact Center Select supports the following routed contact types:

- Voice
- Email
- Outbound
- Web communications (Web chat)
- SMS text messages
- Fax messages
- Scanned documents
- Voice mail messages
- Social Networking

Página2198 de 3226.

Avaya Contact Center Select also supports peer-to-peer Instant Messaging. To support the email-based contact types, you must add an email server to your solution. To support the Web communications contact type, you must add a Web communications server to your solution.

Avaya Contact Center Select provides a simplified voice prompt management utility. The contact center supervisor can perform prompt management work without requiring administrator access to the Avaya Contact Center Select server. Avaya Contact Center Select provides a number of status monitoring utilities to monitor the integration points with IP Office.

Contact Center Manager Administration is a browser-based configuration and reporting interface for Avaya Contact Center Select. Avaya Contact Center Select supervisors use Contact Center Manager Administration to configure contact center resources, agents, skillsets, contact flows, components, and activities. Contact Center Manager Administration provides historical and real-time reporting about the contact center.

User data synchronization

Avaya Contact Center Select provides unified administration for contact center agents and IP Office users. The users (agents and agent-supervisors) that you configure in Avaya Contact Center Select are automatically mirrored to the connected IP Office.

When you create an agent in Avaya Contact Center Select, a matching user account is created in IP Office. When you modify agent details in Avaya Contact Center Select, the corresponding IP Office user details are automatically updated. However, if you delete an agent in Avaya Contact Center Select, the corresponding IP Office user is not deleted. Synchronization works in one direction — from Avaya Contact Center Select to IP Office. The IP Office administrator can manually force data synchronization from Avaya Contact Center Select.

Topology

In a contact center solution using Avaya Contact Center Select and an IP Office telephone system, the following network and connectivity topology considerations apply:

- The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.
- Each Avaya Contact Center Select connects to a single IP Office Server Edition Primary server. Alternatively, each Avaya Contact Center Select can connect to a single IP Office 500V2 Standard Mode with an Advanced Edition license.
- A Small Community Network (SCN) is a system of networked IP Office systems that can, among other features, share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select. Avaya Contact Center Select connects to the IP Office Server Edition Primary server of the SCN. To support an IP Office SCN, Avaya Contact Center Select must connect to an IP Office Server Edition Primary server in that SCN network.
- The Avaya Contact Center Select server and the connected IP Office telephone system must be located in the same campus location.
- Each supervisor client computer communicates with the Avaya Contact Center Select server. The supervisor uses the Contact Center Manager Administration Web interface to configure agents and run reports. The agent supervisor uses the Avaya Agent Desktop software to handle customer calls, to accept emergency or supervisor calls from agents and to observe calls or Web communication contacts. Each voice-enabled supervisor with Agent Desktop requires an associated IP Office telephone.

Página2199 de 3226.

- Each agent client computer communicates with the Avaya Contact Center Select server. The agent uses Agent Desktop to handle customer voice and multimedia contacts. Each voice-enabled agent requires an associated IP Office telephone.

Avaya Contact Center Select supports the following deployment options:

- Avaya Contact Center Select DVD
- Avaya Contact Center Select VMware
- Avaya Contact Center Select hardware appliance
- Avaya Contact Center Select Business Continuity

For more information about Avaya Contact Center Select deployment options, refer to *Avaya Contact Center Select Solution Description*.

Related links

Reference configurations on page 67
Avaya Contact Center Select DVD on page 80
Avaya Contact Center Select and VMware on page 81
Avaya Contact Center Select hardware appliance on page 82
Avaya Contact Center Select Business Continuity on page 83

Avaya Contact Center Select DVD

The Avaya Contact Center Select DVD contains the contact center application software. The DVD deployment option supports Platform Vendor Independence (PVI). PVI gives the customer the flexibility to purchase a server that meets the Avaya Contact Center Select server requirements and conforms to the customer's own corporate standards.

Avaya Contact Center Select supports a range of PVI server specifications, each specification supporting a specified maximum agent capacity and call rate. This range of PVI specifications gives the customer the flexibility to use the minimum hardware to meet their solutions requirements while allowing for future expansions.

The Avaya Contact Center Select DVD deployment option does not require VMware resources or infrastructure, which keeps Total Cost of Ownership (TCO) and solution complexity to the minimum.

Página2200 de 3226.

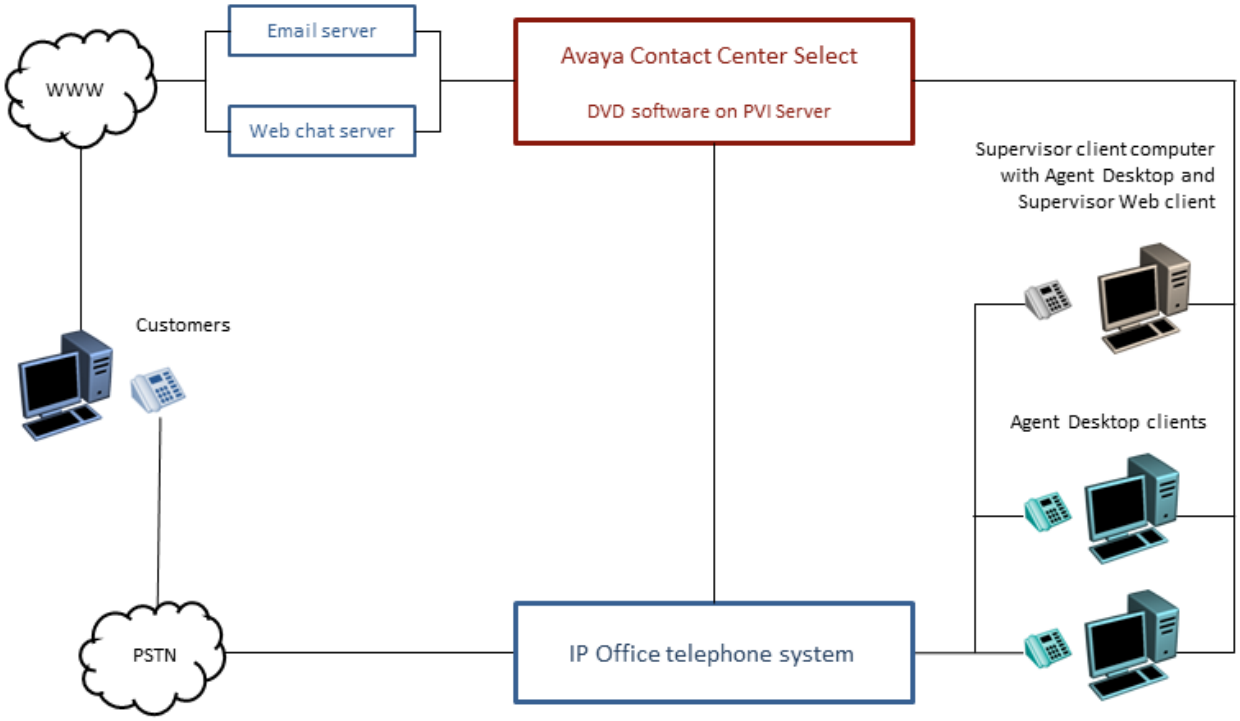


Figure 20: Typical Avaya Contact Center Select DVD deployment

To use the Avaya Contact Center Select DVD deployment option, the customer must provide the following:

- Server hardware that meets one of the Avaya Contact Center Select PVI specifications: Entry-level, Mid-range, or High-end.
- Microsoft Windows 2012 R2 Standard or Datacenter Edition operating system and license.

For more information about the Avaya Contact Center Select DVD option, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select and VMware

Avaya Contact Center Select supports VMware virtualization for increased productivity, flexibility and efficiency. All Avaya Contact Center Select deployment options support the virtualized IP Office Server Edition OVA on VMware.

Avaya Contact Center Select offers a software appliance package that consists of the following components:

- Avaya Contact Center Select virtual machine
- Avaya Aura® Media Server OVA
- Avaya WebLM OVA

Deploy these virtual machines and IP Office to build a virtualized and scalable contact center solution.

Página2201 de 3226.

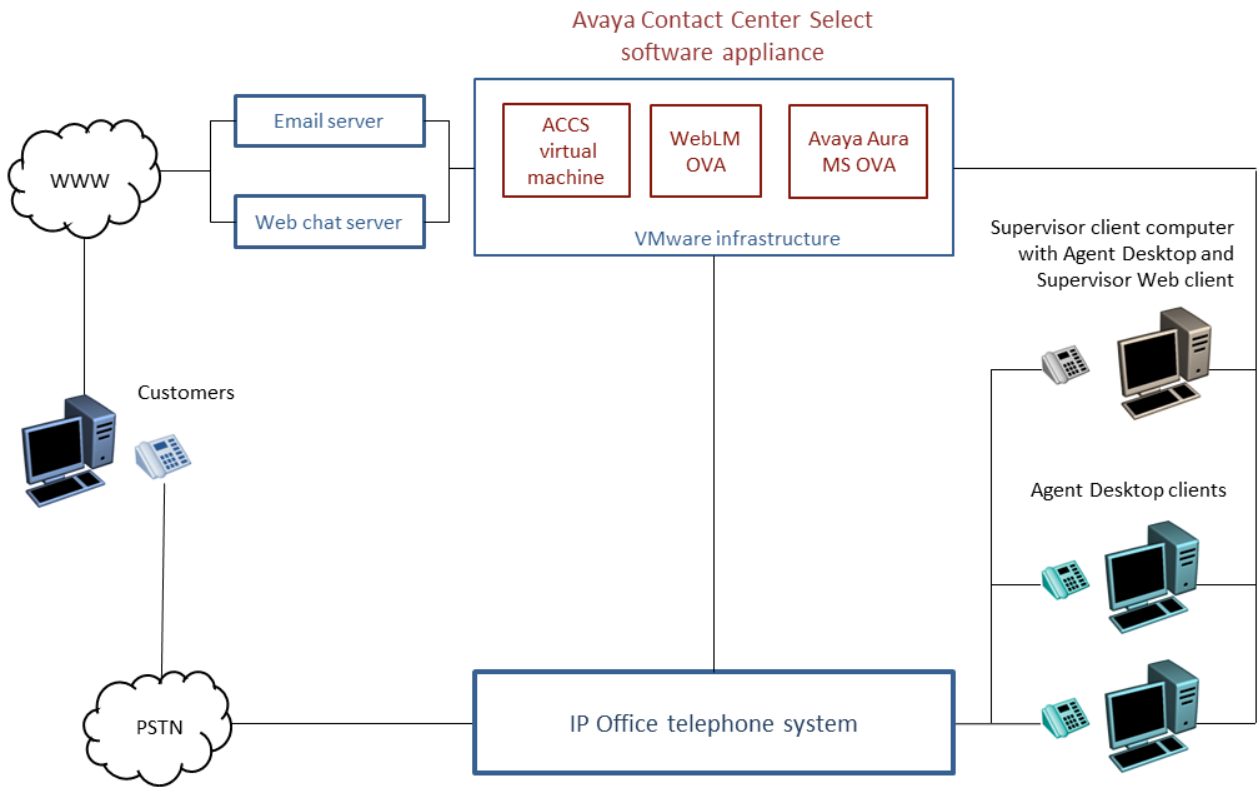


Figure 21: Typical Avaya Contact Center Select and VMware solution

Avaya Contact Center Select is a collection of applications providing real-time call control, multimedia handling, and statistical reporting. Deploy Avaya Contact Center Select on an enterprise-grade VMware virtual environment. Avaya recommends that you apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a virtualization infrastructure.

Avaya Contact Center Select supports VMware ESXi. VMware vCenter software is not required; however it is supported and it is useful for Avaya Contact Center Select in multi-host contact center environments.

For more information about Avaya Contact Center Select and VMware, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select hardware appliance

The Avaya Contact Center Select hardware appliance is a physical rack-mount server with the Avaya Contact Center Select application software already loaded and partially preconfigured. Avaya supplies the server hardware and a license for the Microsoft Windows 2012 R2 Standard Edition operating system.

The Avaya Contact Center Select hardware appliance server delivers speedy and simplified contact center deployment.

Página2202 de 3226.

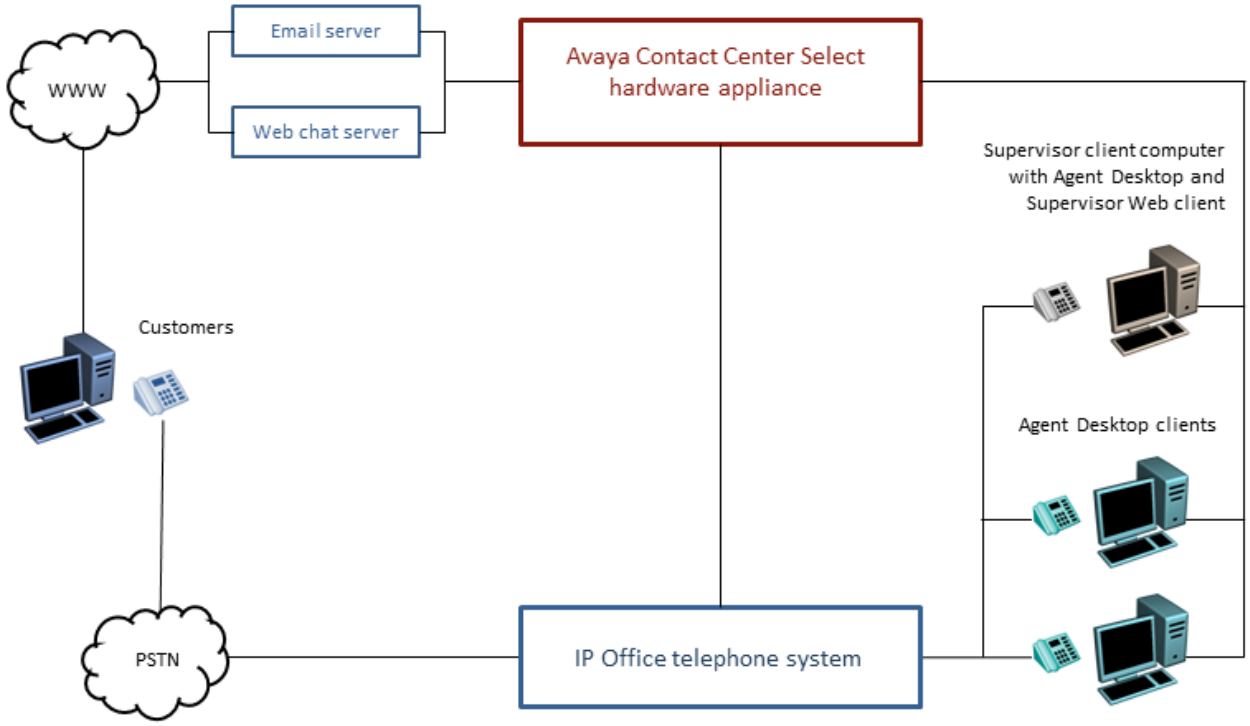


Figure 22: Typical Avaya Contact Center Select hardware appliance solution

After the basic telephony and email features are working, you can then configure more multimedia contacts, multiplicity, custom prompts, and other enhanced features and functions to improve your customer's experience.

The hardware appliance server supplied by Avaya is optimized to provide all of the real-time computational and logging resources required by Avaya Contact Center Select. The hardware appliance supports the Avaya Contact Center Select maximum agent and call rate capacity.

Avaya provides the Microsoft Windows operating system product key for the hardware appliance. The product key is displayed on a sticker attached to the top of the Avaya Contact Center Select hardware appliance server.

For more information about the Avaya Contact Center Select hardware appliance, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select Business Continuity

Business Continuity is an Avaya Contact Center Select licensed feature. Avaya Contact Center Select solutions that support Business Continuity have two Avaya Contact Center Select servers. One server, called the active server, processes customer contacts. The other server, called standby or Remote Geographic Node, shadows the active server. If the active server fails, the other Avaya Contact Center Select server can take over contact processing. This feature provides Avaya Contact Center Select redundancy, data resiliency, and disaster recovery.

To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active

Página2203 de 3226.

and standby servers. Avaya Contact Center Select agents are also supported in domains with a two-way trust relationship with the Avaya Contact Center Select server domain.

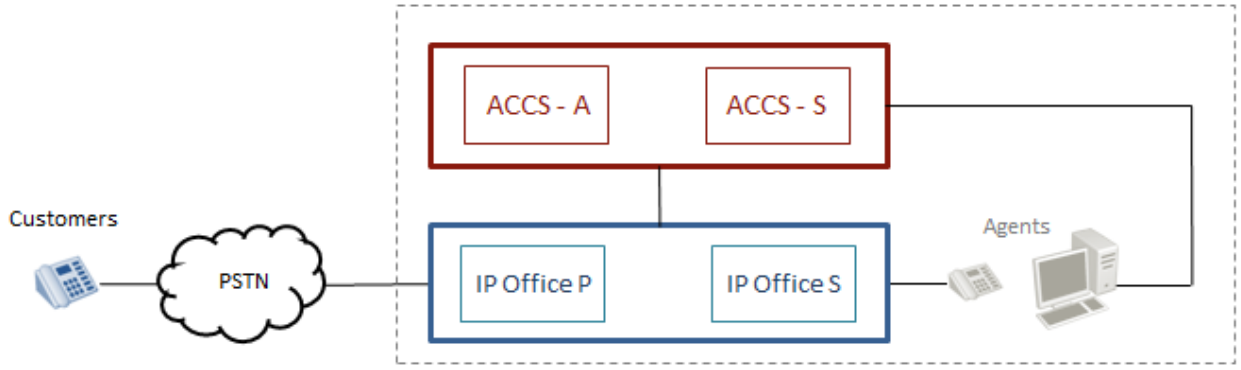


Figure 23: Avaya Contact Center Select Business Continuity with IP Office resilience

IP Office Server Edition solutions support voice platform resilience when an IP Office Secondary Server is added to the solution. Avaya Contact Center Select supports this IP Office resilience feature.

All Avaya Contact Center Select deployment options, DVD, VMware, and Hardware Appliance, support Contact Center Business Continuity and IP Office resilience. Avaya Contact Center Select Business Continuity adds additional resource requirements, topology, network connectivity, and domain layout considerations to the solution.

For more information, refer to *Avaya Contact Center Select Business Continuity*.

Hardware and software options

Hardware options

Server, base card, trunk card, and expansion module hardware options are available depending on the edition required:

- Dell PowerEdge™ R210 or R620
- Hewlett Packard ProLiant DL120 G7 or DL360 G7
- Avaya IP500 V2

Software options

IP Office acts as a server for a variety of applications, including:

- Avaya Communicator for IP Office supported on Windows and iPad devices
- Avaya one-X® Mobile for IP Office
- Avaya one-X® Portal for IP Office

Página2204 de 3226.

- Lync Integration for IP Office
- IP Office SoftConsole
- IP Office Media Manager
- Avaya Equinox™ client for IP Office
- Avaya IP Office Web Client

IP Office can also be deployed with other components. You can deploy IP Office with Radvision or other video endpoints. You can also use IP Office Branch solution offer to connect IP Office branches to the Avaya Aura® infrastructure, allowing users to leverage core Avaya Aura® applications and services including centralized dial plans, voice mail, management, and licensing.

Related links

Accessing Avaya DevConnect Application Notes on page 134
Interoperability on page 93

Server specifications

The following tables list the minimum server specifications for the IP Office Server Edition Solution:

Server option	Large server #1	Large server #2	Large server #3
Chassis	Dell R630 1U	Dell R620 1U	HP DL360G7 1U
Processor	2 x E5-2620v3, 2.4 GHz	2 x E5-2630, 2.3 GHz	2 x E5620, 2.4 GHz
Memory (RAM)	32 GB	32 GB	12 GB
Hard disk drive	2 x 600 GB	2 x 600 GB	2x 300 GB, 10K
RAID	RAID 1 Hot swap	RAID 1 Hot swap	RAID 1 Hot swap
RAID Controller	H730	H710	P410i
Power Supplies	2x 750W AC Hot swap	2x 495W AC Hot swap	2x 460W AC Hot swap
NICS	6x GB full duplex	4x GB full duplex	4 Port, Motherboard
Optical Drive	1x DVD +/- RW	1x DVD +/- RW	1x DVD+/-RW, SATA, INTERNAL
PCI Type	2 x8 Gen2 Slots (PCIe)	2 x8 Gen2 Slots (PCIe)	1-LP X8 PCIe & 1-FL/FH X16 PCIe Riser

Server option	Small server #1	Small server #2	Small server #3
Chassis	HP DL120G7 1U	Dell R210 1U	Dell R220 1U
Processor	1 x E3-1220, 3.1 GHz	1 x E3-1220, 3.1 GHz	1 x E3-1220, 3.1 GHz
Memory (RAM)	12 GB	12 GB	16 GB
Hard disk drive	1x 250 GB, 7.5K	1x 250 GB, 7.5K	1x 500 GB, 7.2K
RAID	RAID 0 (none)	RAID 0 (none)	RAID 0 (none)

Table continues…

Página2205 de 3226.

Server option	Small server #1	Small server #2	Small server #3
RAID Controller	P212, 256 MB	On board	On board
Power Supplies	1 x 400 W AC	1 x 502 W AC	1 x 250 W AC
NICS	2 Port, Motherboard	2 Port, Motherboard	2 Port, Motherboard
Optical Drive	1x DVD+/-RW, SATA, INTERNAL	1x DVD+/-RW, SATA, INTERNAL	1x DVD+/-RW, SATA, INTERNAL
PCI Type	1-HL/LP X8 PCIe & 1-FL/FH X16 PCIe Riser	1 x16 Gen2 Slots (PCIe)	1 x16 Gen2 Slots (PCIe)

Note:

In some geographies, where 12 GB of RAM is not a standard Dell option use 16 GB RAM.

Server Combinations and Usage

- The Server Edition Primary and Server Edition Secondary must be on the same platform. This constraint applies equally to virtual servers. It is possible to mix native and virtual central servers, but the resources allocated to the virtual environment should match the native server.
- Virtualised and native servers can be mixed in the same Server Edition solution in any role, provided the Server Edition Primary and Server Edition Secondary are the same as indicated above.
- It is possible to use the Unified Communication / Application Server R210 / DL120 is / R220 servers as this is the same hardware and software as the Server Edition R210 / DL120 / R220 servers. If the server is installed with theServer Edition software, it will be supported by Avaya.
- You cannot set up a Server Edition Expansion System(L) in the Standard IP Office mode of operation in the IP Office Server Edition Solution.
- You cannot re-provision a Server Edition server without a complete reinstall. For example, you cannot convert a primary server to a secondary or expansion system.
- You cannot set up a Server Edition Expansion System (L) in the Standard IP Office mode of operation in the IP Office Server Edition Solution. You cannot convert a Server Edition Expansion System (V2) to a Server Edition Primary or Server Edition Secondary server.
- The use of any external Voicemail Pro server (either Linux or Windows) is not supported.
- The use of an external Avaya one-X® Portal server not running Server Edition software, and not running on a supported server, is not supported.

  Note:

  Salesforce (SFDC) has been removed from Avaya one-X® Portal.

Página2206 de 3226.

Operating system and browser support

Windows Operating System

Table 7: Windows Editions and Service Packs

Operating System*	Service Pack	Edition
Windows 7	SP1	Professional, Enterprise, Ultimate
Windows 8.1	N/A	Professional, Enterprise
Windows 10	N/A	Professional (SMB), Enterprise
Windows Server 2012	N/A	Standard
Windows Server 2012 R2	N/A	Standard
Windows Server 2016	N/A	Standard, Essentials

* Windows Server 2008 R2 (64-bit) is not supported from Release 10.1.

Table 8: Windows Support – Server Components

Server	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
Preferred Edition server (Voicemail Pro) Standalone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Preferred Edition server with UMS	No	No	No	No	No	No	Yes	Yes
Preferred Edition server with Campaigns	No	No	No	No	No	No	Yes	Yes
Preferred Edition server with IMS	No	No	No	No	No	No	No	No
Preferred Edition server with MAPI service for Voicemail Pro on Linux	Yes	Yes	No	No	No	No	Yes	Yes
Avaya one-X® Portal for IP Office server	No	No	No	No	No	No	Yes	Yes
TAPI first-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI third-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

Página2207 de 3226.

Server	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
TAPI WAV[2]	Yes	No	Yes	No	Yes	No	No	No

* Windows 8.1 is the replacement/Service Pack for Windows 8.0. Therefore, we no longer support Windows 8.0.

Table 9: Windows Support – Thick Client Apps

Application	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
Preferred Edition client	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Office SoftConsole	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
IP Office Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SysMonitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System Status Application	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI first-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI WAV[3]	Yes	No	Yes	No	Yes	No	No	No
Avaya Equinox™ for Windows	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Avaya Communicator for Windows	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Avaya one-X® Portal plug-in for Microsoft Outlook	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Call Assistant	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Plug-in for Microsoft Lync 2013/Skype for Business[4]	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Table continues…

[2] TAPI WAV is not recommended for new designs and is not supported on a 64-bit OS.
[3] TAPI WAV is not recommended for new designs and is not supported on a 64-bit OS.
[4] Plug-in for Microsoft Lync 2010 is not supported from Release 10.1.

Página2208 de 3226.

Application	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
Web Conferencing [5]	Yes	Yes	Yes	Yes	Yes	Yes	No	No
IP Office Web Client	Yes	Yes	Yes	Yes	Yes	Yes	No	No

* Windows 8.1 is the replacement/service pack for Windows 8.0. Therefore, we no longer support Windows 8.0.

macOS Operating System

Table 10: macOS Support – Thick Client Apps

Application	macOS 10.8 (Mountain Lion)	macOS 10.9 (Mavericks)	macOS 10.10 (Yosemite)	macOS 10.11 (El Capitan)	macOS 10.12 (Sierra)	macOS 10.13 (High Sierra)
Web Conferencing [6]	Yes	Yes	Yes	Yes	Yes	
Avaya Equinox™ for Mac	No	No	No	Yes	Yes	Yes

Browsers

Table 11: Supported Browsers

Application	Internet Explorer 10*	Internet Explorer 11	Edge	Firefox	Chrome	Safari 8	Safari 9	Safari 10
Voicemail Pro Campaigns	Yes	Yes	Yes	No	No	No	No	No
Voicemail Pro UMS WebMail	Yes	Yes	Yes	No	No	No	No	No
Avaya one-X® Portal for IP Office client	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Web Conferencing[7]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Table continues…

[5] Includes Adobe Flash and Java Applet for sharing.
[6] Includes Adobe Flash and Java Applet for sharing.
[7] Includes Adobe Flash and Java Applet for sharing.

Application	Internet Explorer 10*	Internet Explorer 11	Edge	Firefox	Chrome	Safari 8	Safari 9	Safari 10
Web Manager and Web Control Page	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
D100 DECT Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP DECT R4 Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Avaya Communicator for Web	No	Yes	No	No	Yes	No	No	No
IP Office Media Manager	Yes	Yes	Yes	Yes	Yes	No	No	No
Avaya IP Office Web Client	No	No	No	No	Yes	No	No	No

* Only on Windows Server 2012; however, Server 2012 R2 supports Internet Explorer 11.

Other Apps

Table 12: Microsoft Exchange

Application	Exchange 2010	Exchange 2013	Exchange 2016
Voicemail Pro UMS	Yes	Yes	Yes
Avaya one-X® Portal for IM and Presence	Yes	Yes	Yes

Table 13: Microsoft Outlook

Application	Outlook 2010	Outlook 2013	Outlook 2016
Voicemail Pro IMS	No	No	No
TAPI (for dialing)	Yes	Yes	Yes
Voicemail Pro UMS with IMAP	Yes	Yes	Yes
Avaya one-X® Portal Outlook Plug-in[8]	Yes	Yes	Yes

[8] For Outlook 2013 and later, the contact screen popping feature is not supported.

Página2210 de 3226.

Virtualization

Table 14: Virtualization support

Hypervisor	IP Office Server Edition	IP Office Partner-Hosted
VMware ESXi 5.1	Yes	Yes
VMware ESXi 5.5 U2+	Yes	Yes
VMware ESXi 6.0	Yes	Yes
VMware ESXi 6.5	Yes	Yes
VMware ESXi 6.7	Yes	Yes
Microsoft HyperV on Server 2012 R2	Yes	Yes
Microsoft HyperV on Server 2016	Yes	Yes
KVM	No	Yes
Amazon AWS	Yes	Yes

Note:

Google KVM is supported on QEMU with CentOS version 6 and 7 in case of Powered by Avaya (hosted) solution and not supported for CPE. For more information, see *Deploying Powered by Avaya for Business Partners guide*.

Customer-provided PC requirements

The following customer-provided PC requirements for applications are the minimum required.

IP Office Manager

IP Office Manager is used to access all parts of the configuration. Different levels of access can be defined to control which parts of the configuration the IP Office Manager user can view and alter. IP Office Manager is also used to upgrade the software files on the system. IP Office Manager acts as a TFTP server from which some Avaya telephones can request new software.

RAM	Standard Edition: 4 GB Server Edition: 6 GB Select Server Edition: 8 GB
Hard disk free space	1 GB
Processor	Standard Edition: Core i3 Server Edition: Core i5 Select Server Edition: Core i5
Operating system	Operating system and browser support on page 88

Página2211 de 3226.

Additional software	.NET Framework 4.0: Installed with the software if not already installed.

IP Office SysMonitor

RAM	128 MB
Hard disk free space	10 GB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 88

IP Office System Status Application

RAM	256 MB
Hard disk free space	1.4 GB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 88
Additional software	Sun Java Virtual Machine Web Browser: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

TAPI

RAM	64 MB
Hard disk free space	50 MB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 88
Additional software	Web Browser: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

Página2212 de 3226.

Virtual environment requirements

Ensure you have the following:

- VMware vSphere client software for management (vSphere ESXi software and virtualized instances running on a single host server)

  Note:

  vCenter software is not required, however might be useful for multi-host server environments.

- Host hardware supporting VMware vSphere and IP Office Server Edition resource requirements and specifications to meet configuration needs.

VMWare ESXi support:

- IP Office Server Edition and IP Office Contact Center support VMWare ESXi 5.1 and 5.5 U2.
- IP Office Contact Center supports VMWare ESXi 6.0. IP Office Server Edition supports VMWare ESXi 6.0 for only versions 10.0 and later.

  For more information about IP Office Contact Center support and specifications, see *Avaya IP Office Contact Center Reference Configuration*.

Note:

ESXi 4.x is no longer supported.

Additional hypervisor support:

Hypervisor support is now extended to:

- Microsoft Hyper-V
- AWS (for Amazon Web Services): An AMI (Amazon Machine Image) is provided that can perform Auto Ignition and ICU based on User Data set in AWS. The AMI will behave similar to the existing Google Compute Image. Consult the instance types that Amazon EC2 supports on the Amazon AWS website.

  In Amazon Dashboard, you need to select Launch Instance under Create Instance. Select Community AMIs and search for Avaya IP Office.
- KVM (for Kernel-based Virtual Machine)

Interoperability

Interoperability means that two systems can communicate with an interface in each system to handle the communication. Compatibility means that two components in the same environment are compatible with each other if they run or reside in the environment without adversely affecting the behavior of the other.

For detailed information about IP Office interoperability and supported releases, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=IP+Office+Platform.

Página2213 de 3226.

Avaya product interfaces

IP Office includes an interface to the following Avaya products:

- Avaya Aura®
- Avaya Contact Center Select
- Avaya Aura® Messaging
- Avaya CallPilot®
- Avaya Cloud Video Phase
- Avaya Communicator for Windows
- Avaya Communicator for iPad
- Avaya Equinox™
- Avaya one-X® Communicator
- Avaya Session Border Controller for Enterprise
- Avaya Business Communications Manager
- Avaya Communication Server 1000
- Avaya Modular Messaging
- Avaya Scopia®
- Secure Access Link
- Avaya Aura® Experience Portal

ISDN interfaces

EU interfaces:

- BRI: RJ45 sockets. ETSI T-Bus and S-Bus interfaces to CTR3 for Pan European connection
- PRI E1: RJ45 socket. ETSI T-Bus interface to CTR4 for Pan European connection
- PRI T1/J1: RJ45 socket: FCC Part 68/JATE connection

USA interfaces:

- PRI T1 service: Ground Start (GS) - Default, E&M, 56 K data for 5ESS, 56/64/64 restricted for 4ESS
- PRI ISDN switch support: 4ESS, 5ESS, DMS-100, DMS-250 (includes conformance to ANSI T1.607 and Bellcore Special Report SR4287, 1992)
- PRI ISDN Services: AT&T Megacom 800, AT&T WATS (4ESS), AT&T SDS Accunet 56 Kbps and 64 Kbps (4ESS), AT&T Multiquest (4ESS)

Related links

Phone interoperability on page 95
IP Office and Avaya Aura Communication Manager interoperability on page 99
BCM and IP Office interoperability on page 100
Accessing Avaya DevConnect Application Notes on page 134
Product compatibility on page 133
Hardware and software options on page 84

Página2214 de 3226.

Phone interoperability

The following table summarizes the phone interoperability comparison by IP Office edition.

Table 15: Generally available phones

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
Analog deskphones:			
POTS	Yes	Yes	No
1000 Series Video phones:			
1010, 1020, 1030, 1040 (Lifesize)	No	Yes	No
1400 Series : DS Digital phones – IP Office and Communication Manager			
1403, 1408, 1416	Yes	Yes	No
DBM32	Yes	Yes	No
1600 Series : IP (H.323) phones – IP Office and Communication Manager			
1603, 1603SW, 1603SW–i, 1608, 1608–i, 1616, 1616–I	No	Yes	Yes
2400 Series: DS Digital phones – IP Office and Communication Manager			
2402D, 2410D, 2420	Yes	Yes	No
EU24	Yes	Yes	No
3600 Series: WiFi H.323 – IP Office and Communication Manager			
3641, 3645	No	Yes	Yes
3700 Series: DECT – IP Office and Communication Manager			
3720, 3525, 3730, 3735, 3745, 3749	No	Yes	Yes
9500 Series: DS digital – IP Office only			
9504, 9508	Yes	Yes	No
BM12	Yes	Yes	No
9600 Series: IP H.323 – IP Office and Communication Manager			
9620L, 9620C, 9630, 9640G, 9650, 9650C	No	Yes	Yes
SBM24 with 96x0	No	Yes	Yes
9608, 9611, 9621, 9641, J169, J179	No	Yes	Yes
BM12	No	Yes	Yes
B100 Series Conference Phones:			
B149, B159	Yes	Yes	No

Table continues…

Página2215 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
B179 SIP	No	Yes	Yes
D100/D160 DECT Phones:			
D160	Yes	Yes	Yes
E100 Series IP Phones:			
E129	No	Yes	Yes
E159	No	Yes	Yes
E169	No	Yes	Yes
H100 Series Video Collaboration Stations:			
H175	No	Yes	Yes
Avaya J100 Series IP Phones:			
Avaya J139 IP Phone	No	Yes	No
Avaya J169 IP Phone	No	Yes	No
Avaya J179 IP Phone	No	Yes	No
Softphone:			
Avaya Communicator Windows	No	Yes	Yes
Avaya Communicator iPad	No	Yes	Yes
Avaya Equinox™	No	Yes	Yes

Table 16: Generally available NORSTAR/BCM phones

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
1100 Series SIP phones: BCM Unistim migration			
1120E, 1140E	No	Yes	Yes
BM LED and paper labels	No	Yes	Yes
BM LCD	No	Yes	Yes
1200 Series SIP phones: BCM Unistim migration			
1220, 1230	No	Yes	Yes
BCM paper	No	Yes	Yes
BCM LCD	No	Yes	Yes
NORSTAR/BCM Digital phones:			

Table continues…

Página2216 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
T7000, T7100, T7208, T7316, T7316E	Yes	Yes	No
T24 Key Module	Yes	Yes	No
M7100(N), M7208(N), M7310(N), M7310BLF, M7324(N)[9]	Yes	Yes	No
CAP Key Module	Yes	Yes	No
NORSTAR/BCM Digital Conference Phone	Yes	Yes	No
Nortel Digital Mobility phones:			
T7406, T7406E	Yes	Yes	No
7420, 7430, 7434, 7439, 7440, 7449	Yes	Yes	No
4135, 4136, 4145, 4146, 4145EX, 4146EX	Yes	Yes	No

Avaya has tested the following phones for interoperability with IP Office. These phones may not support all features. If the phone is past its Avaya Manufacturer Support Period, issue resolution is limited to those already fixed.

Table 17: Supported Avaya phones no longer for sale

Note:

Supported in this context means the phones have been tested by Avaya for interoperability with IP Office. Older phone models may not support new features if the phone model is outside of the Avaya Manufacturer Support period. If there is a software update related to the Release 11.0, a software fix will not be provided for Phones that are outside of the Avaya Manufacturing Support period. Phones “No Longer supported” are outside of the Avaya Manufacturing Support period and are not covered under Avaya Maintenance offers (End of Service Support and End of Maintenance Support)

1. OSX 10.9 Mavericks is last OS version supported for Video Softphone for MAC. That client is no longer available on either of 10.x or 11.0 software for same reason. Avaya Communicator for Web, Avaya IP Office Web Client, and Avaya Equinox™ are available for Mac users on IP Office Release 11.0.
2. Digital and analog phones are supported with Server Edition or Select as indicated using the IP500 V2 as an expansion module.

[9] Only the global version of the M7000 Series phones are supported. The non-global versions are not supported and can be identified by the contrast levels; the global version has 9 contrast levels and the non-global version has only 4 contrast levels.

Página2217 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
ETR phones: Analog Feature Phone, PARTNER and IP Office			
“Refreshed” 34, 18 and 6 button display	Yes	No	No
“Euro” 34 and 18 button display	Yes	No	No
“Euro” 18 and 6 button display	Yes	No	No

Related links

Interoperability on page 93
Phone availability on page 98
Accessing Avaya DevConnect Application Notes on page 134
Using the Avaya InSite Knowledge Base on page 134
Phones on page 38

Phone availability

Phones available worldwide

The Avaya phones listed below are the recommended phones for use with IP Office. These phones are sold worldwide in every country where IP Office is available.

For detailed specifications, see specific phone information on the Avaya Support site at http://support.avaya.com.

Digital phone models	IP phone models
1403	1603
1408	1608
1416	1616
9504	9608
9508	9611
	9621
	9641
	Avaya J169 IP Phone
	Avaya J179 IP Phone
	Avaya J139 IP Phone

Phones only available in certain countries

In addition to the phones listed above, the following Avaya phones are available in certain countries and regions.

Página2218 de 3226.

Digital/Analog phone models	IP phones
2402	9620L/9620C
2410	9630G/9640/9640G
2420	9650/9650C
3810 Wireless	3720 DECT R4 Wireless Handset
EU24/EU24BL DSS Unit	3725 DECT R4 Wireless Handset
	3730 DECT R4 Wireless Handset
	3735 DECT R4 Wireless Handset
	3745 DECT R4 Wireless Handset
	3749 DECT R4 Wireless Handset
	3641 Wireless (WiFi) phone
	3645 Ruggedized Wireless (WiFi) phone
	D100

Related links

Phone interoperability on page 95

IP Office and Avaya Aura® Communication Manager interoperability

IP Office uses H.323 protocol for trunks between the nodes and the Avaya Aura® Communication Manager. Centralized voicemail for all IP Office systems in the SCN network and all phones are supported on the individual call servers. Advanced call handling features are available between the IP Office nodes. This interface works on Essential and Preferred Editions.

Supported phones include:

- Avaya IP phones (H.323)
- Avaya digital phones
- BCM 7000 series digital phones
- BCM 1100/1200 series IP phones (SIP)
- DECT R4 phones
- Analog phones

These features allow for simple networking needs between IP Office remote branches to an Avaya Aura® Communication Manager at the main site.

Página2219 de 3226.

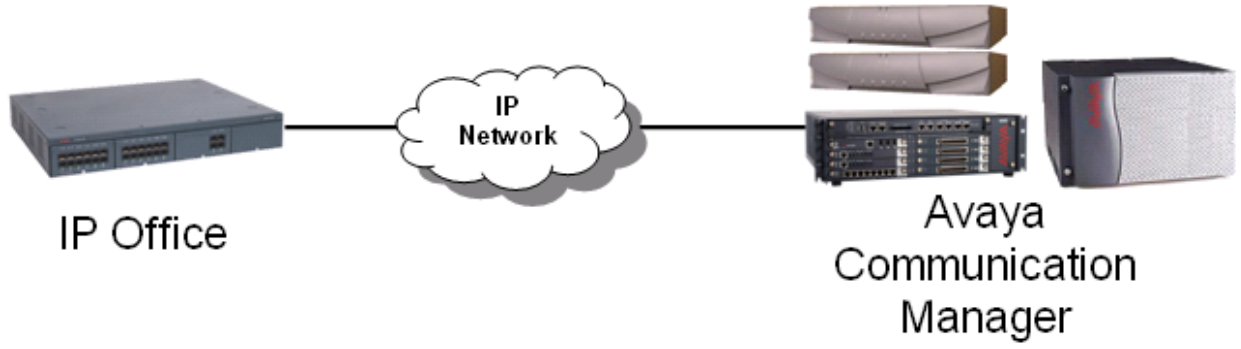


Figure 24: VoIP networking using H.323

Q.SIG provides the following supplementary services which are also available between IP Office and Avaya Aura® Communication Manager equipped with the relevant RFA licenses:

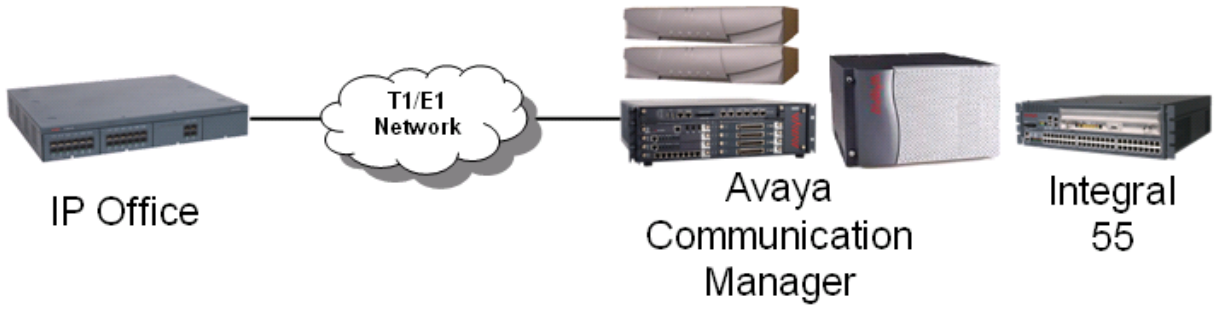


Figure 25: Q.SIG networking using T1/E1 links (TDM)

Related links

Interoperability on page 93

BCM and IP Office interoperability

The SIP interoperability support between IP Office and BCM50/450 allows customers to migrate a network of BCM, step-by-step, to an IP Office SCN or Server Edition network.

Protocol support	IP Office to BCM: SIP BCM to BCM: SIP or SIP/MCDN IP Office to IP Office H.323: SCN or SIP
	Note: It is not possible to connect IP Office and BCM through the MCDN or SCN protocol directly.
IP Office platform requirements	Release 8.1 or higher, Essential, Preferred or Server Editions

Página2220 de 3226.

BCM platform requirements	BCM50 or BCM450 6.0
Centralized voicemail	IP Office with a centralized Voicemail Pro system in the SCN network BCM with a centralized voicemail within the BCM MCDN network. **Note:** Centralized Voicemail across IP Office and BCM systems is not supported.
Phones	All phones supported on the individual call servers and releases including Avaya IP Phone (H.323), Avaya Digital phones, BCM 7000 Series Digital phones, BCM1100/1200 Series IP Phones (SIP), DECT R4 and Analog phones.
Features	Advanced feature set of IP Office SCN available between the IP Office and BCM. MCDN features are also available between the IP Office and BCM. The standard SIP features are supported.

Related links

Interoperability on page 93

Security specification

The Avaya Product Security Support Team (PSST) responds to ongoing security vulnerabilities for all Avaya Products. For more information, see *Avaya Product Security Vulnerability Response Policy* and *Avaya Security Vulnerability Classification* at the Avaya Support website at https://support.avaya.com/security.

Default security

The IP Office software security engine is supplied by Mocana Corporation. For more information, see https://www.mocana.com.

Security features are built-in into the software platform. These features consist of:

- Integrated firewall to prevent Denial of Service (DoS) attacks
- Secure connections to ensure the privacy and integrity of transmitted information including:
  - TSL on administration interfaces
  - HTTPS client
  - HTTPS server
  - IPSec
  - SIP-TLS

Página2221 de 3226.

- SSL/VPN
- VMPro/Exchange MAPI integration (TLS)

For detailed information about SSL/VPN remote access, see *Deploying Avaya IP Office™ Platform SSL VPN Services* and *Avaya IP Office™ Platform Port Matrix* at the Avaya Support website.

Configurable security

Configurable security settings include the following features:

- Encryption and message authentication
- Configuring integrated firewall settings
- Digital certificates
- Prevention of tool fraud by restricting user privileges and using security policy configuration to manage account credentials and access control

See *Avaya IP Office™ Platform Security Guidelines* for more information.

Network security

Network security leverages resources such as VLANs and firewalls available on the enterprise network and includes:

- External firewall configuration
- Separate of network functionality by creating separate VLAN groups and security zones
- Hardening of Layer 2 (data link layer) and Layer 3 (Network layer) by configuring SNMP trap destinations, syslog entries, and an IPSec VPN.
- SSL/VPN remote access

Operational security

Ongoing operational security to maintain a secure system includes:

- Patching
- Logging and monitoring
- Virus protection

Related links

Platform and application security details on page 102

Platform and application security details

For additional information on security, see *Avaya IP Office™ Platform Security Guidelines*

Platform

- The IP Office for Linux operating system is based on Red Hat Enterprise Linux that is further hardened for defaults, packages, and users.
- The operating system of Server Edition Expansion System (L) is developed for IP Office. The operating system is simple, stable, and reliable.

Página2222 de 3226.

- The operating system of Server Edition Expansion System (V2) is developed for IP Office. The operating system is simple, stable, and reliable.
- Components that are secure:
  - Software security engine for all the components.
  - Hardware security engine for Office Server Edition Expansion System (V2).
  - Internal Access Control Engine polices for external service requests and internal applications.

Manager

- Transport Layer Security (TLS) secures the communications between IP Office Manager and IP Office and insecure ciphers are disabled.
- Provides Role based user access control (RBAC).
- Provides comprehensive user account and password controls.
- You can enable a PKI Trust domain.
- The system generates warnings messages if administrative passwords are set to default. The system sends alarms or login failure.
- The system records all the accesses in the audit trail.
- You can disable unused services and ports such as HTTP.

Administration user accounts

The administration user accounts can be controlled for:

- Password complexity
- Previous password history (administrative accounts only)
- Change password on next login
- Idle lockout and login failure lockout
- Time and date the account expires (administrative accounts only)

Single sign-on (SSO)

- Administration credentials to log in to Linux Platform settings are securely transferred to Manager, SSA,Voicemail Pro client.
- All administrative logins on all IP Office components including Voicemail Pro and Avaya one-X® Portal for IP Office use security settings of IP Office.
- Server user management feature in Web Manager synchronizes administrative user credentials with all components of IP Office including Voicemail Pro and Avaya one-X® Portal for IP Office in IP Office Server Edition Solution.

Audit trail

- Each IP Office system maintains an audit trail of access and configuration change.
- Linux Platform settings also maintains an audit trail.
- The IP Office system displays the audit trail in IP Office Server Edition Manager and SSA.
-

Página2223 de 3226.

Public Key Infrastructure (PKI)

- IP Office supports X.509 certificates
- The Server Edition Primary and the Application server support an integrated Certificate Authority (CA)
- The Trusted Certificate Store can be configured and Identity certificate is available.
- The system performs a Certificate Signing Request (CSR) through Simple Certificate Enrollment Protocol (SCEP).
- The system creates a self-signed Identity certificate that can be copied to all HTTPS/TLS interfaces.
- Flexible controls to enforce Trust domain on specific services. Extended trust controls for PKI .
- Web Management Console,Voicemail Pro and Avaya one-X® Portal for IP Office on Linux support X.509 certificates, but not PKI.

LAN

- The servers and expansion systems are thoroughly tested for resistance to Denial of Service and other attacks
- Server Edition Expansion System (V2) supports a configure able Firewall
- Time profiles on Server Edition Expansion System (V2) only
- Static NAT and NAPT in Server Edition Expansion System (V2)
- ICMP Filtering
- L2TP/PPP VPN on Server Edition Expansion System (V2) only
- PAP or CHAP password exchange
- Idle or quota timeout
- IPSec VPN on Server Edition Expansion System (V2) only

Endpoints

- Username and PIN or password or login code are in the IP Office configuration, and you can administer these through IP Office Server Edition Manager
- You can use HTTP or HTTPS for settings and firmware upgrades
- You cannot make calls unless you are logged in

Call barring

- You can configure flexible call barring controls using login name or account code to allow internal, local, national or international calls on the basis of every user and system.
- You cannot use speed dials, transfers, forwarding, and conferences to bypass controls.
- You can enable trunk to trunk calls using IP Office Server Edition Manager. Trunk to trunk calls are disabled by default.
- SIP trunk configuration for incoming calls must match URIs..
- You can use SMDR (CDR) to create a record of all calls.

Voicemail Pro client

- You can enforce user login with Personal Identification Number (PIN) and configure complexity for the PIN.
- You can enforce PIN change when the user logs in for the first time.
- Idle timeout.

Related links

Security specification on page 101

Port assignments

Details of the range of ports used by IP Office and IP Office applications are found at https://support.avaya.com/products/.

DTE port	9 way D-type D-Type female connector: V.24/V.28
Analog trunk ports	RJ45 sockets: Loop Start/Ground Start (regionally dependant)
Power fail ports	RJ45 sockets: 2x sockets for ATM16 and 1x sockets for ATM4
ISDN data rates	BRI: B-channel 64 Kbps or 56 Kbps, D-channel 16 Kbps
Analog phone ports	• RJ45 sockets • REN: 2. (External Bell via POT port: REN = 1) • Off Hook Current: 25 mA. • Ring Voltage: 40 V (nominal) RMS.
LAN	RJ45 sockets. Auto-negotiating 10/100 BaseT Ethernet (10/100 Mbps)
Audio	• 3.5 mm stereo jack socket. Input impedance 10 K/channel. • Maximum AC signal - 200 mV rms.
External output port	• 3.5 mm stereo jack socket. Switching capacity 0.7 A. • Maximum Voltage - 55V DC. On state resistance 0.7. • Short circuit current 1 A. Reverse circuit current capacity 1.4 A.
Embedded voice memory	IP500V2: 512 MB compact flash memory (SD) card for voicemail

Página2225 de 3226.

Typical upgrade paths

Upgrading IP500 V2 platforms

Customers can migrate to the latest release by purchasing an upgrade license or under the terms of their IP Office Support Services support contract, as applicable. Customers migrating to the latest release will be required to have an IP500 V2 control unit or supported servers with Server Edition. IP500 base cards, trunk cards and expansion modules are supported with IP500 V2 control unit and may migrate to the V2 control unit. Licenses will require a dongle swap to move from the IP500 key card to the IP500 V2 SD card.

For systems using the IP500 V2 with any software release prior to 8.1.1.0, a two-stage upgrade process is required to cope with the increased size of the 9.1 binary file. Upgrade to 8.1.1.0 or any 9.0 version before attempting the upgrade to 9.1.

Ensure that the systems do not contain unsupported hardware. Upgrade them if necessary prior to upgrading the software. Install upgrade licenses prior to the upgrade.

Use the Manager Upgrade Wizard to display the software currently present on the SD card and the new versions available for upgrade.

IP400 hardware will no longer be supported, including IP400 series internal cards, expansion modules and trunk cards listed below:

IP400 VCM cards	VCM4
	VCM8
	VCM16
	VCM24
	VCM30
IP400 modules and station cards	Digital Station V1: 16 and 30 port variants
	Phone V1: 8, 16 and 30 port variants
	So8: ETSI BRI SO support
IP400 cards	Analog Trunk Card Uni (ATM4U)
	Analog Trunk Cards (ATM4)
	BRI Trunk Cards
	T1 PRI Trunk Cards
	E1 PRI Trunk Cards
	E1R2 PRI Trunk Cards

The following IP400 trunk and station modules will continue to be supported in the current release.

IP400 expansion modules	Analog trunk 16
	Digital Station V2: 16 and 30 port variants

Página2226 de 3226.

Phone V2: 16 and 30 port variants

Upgrading Server Edition

Upgrade Server Edition primary, secondary and expansion systems using the iso image burned to a DVD or USB. Install upgrade licenses prior to upgrading. There are two options available:

Upgrading to IP Office Select

Existing Server Edition licenses need to be migrated by purchasing a new set of Select PLDS licenses.

Upgrading Application Server

The upgrade process for the Application Server is the same as for IP Office Server Edition.

Upgrading UCM

Upgrade UCM using a USB2 memory Key with new software or the Web Manager ISO upgrade process.

Upgrading Windows server applications

Download the latest windows applications and copy to the server or burn to a DVD.

Upgrading networked systems

In previous releases, networking was achieved using H.323 lines configured with supplementary services set to SCN. From 9.1 and later, these lines will be migrated to IP Office Lines.

Replacing Customer Call Reporter

Advanced Edition and Customer Call Reporter (CCR) are no longer available for sale. Additionally, existing Advanced Edition customers will need to migrate their CCR to IP Office Contact Center via purchase of the IP Office Contact Center solution prior to upgrading. However, CCR will continue to be sold and supported on the previous release consistent with Avaya lifecycle support policy.

Avaya will provide CCR customers with a clear path to move to IP Office Contact Center. Further, as a result of this change, Preferred Edition will now come with the Voicemail Pro database and Visual Basic Scripting (these were previously part of Advanced Edition).

Ordering process

Software applications are orderable by Avaya Partners from their Avaya Authorized Distributor. Avaya Partners must contact their respective distributors directly to purchase all IP Office software applications. Each distributor implements a customized IP Office software purchasing and distribution process for its network of Avaya Partners. These distributor specific internal processes are not covered by this document.

BCM with CS1000 to IP Office migration

This configuration allows migrating a network of BCM and CS1000 to IP Office step-by-step by adding IP Office systems to it.

Protocol support	IP Office to BCM: SIP

Página2227 de 3226.

	IP Office to CS1000: SIP IP Office to IP Office: SIP or H323 - SCN Networking BCM to BCM: SIP or SIP/MCDN BCM to CS1000: SIP or SIP/MCDN **Note:** Only UDP will be supported and not TCP. IP Office to CS1000 using H.323 or PRI trunks is not supported.
IP Office platform requirements	Release 8.1 or higher, Essential, Preferred or Server Editions
BCM platform requirements	BCM50 or BCM450 6.0
CS1000 platform requirements	CS1000 7.5 with NRS
Centralized voicemail	Centralized Voicemail for all IP Office systems in the SCN network. BCM systems may use centralized voicemail of the CS1000. IP Office systems cannot use centralized voicemail of CS1000.
Phones	All phones supported on the individual call servers and releases including Avaya IP Phone (H.323), Avaya Digital phones, BCM 7000 Series digital phones, BCM1100/1200 Series IP phones (SIP), DECT R4 phones, and Analog phones.

IP Office Branch migration

Migration roadmap and limitations

You can upgrade from a B5800 Branch Gateway to the current release of IP Office, or from a previous release of IP Office to the current release of IP Office. The upgrade process for the IP Office Branch solution varies depending on how the architecture is deployed.

If the B5800 Branch Gateway or IP Office release you are upgrading from is connected to the Avaya Aura® infrastructure and uses Avaya Aura® System Manager for centralized management, use Avaya Aura® System Manager to upgrade the firmware and software for the system.

If the architecture is deployed in a stand-alone IP Office branch environment with no centralization or connection to the Avaya Aura® network, you must use IP Office Manager for upgrades. From IP Office Manager, you can perform an upgrade using the upgrade wizard or the System SD card.

Página2228 de 3226.

For procedures on how to perform System Manager or IP Office Manager upgrades for your Branch solution, see *Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*.

Licenses

Many solutions, applications, and features on IP Office systems are licensed and only operate when a valid license is detected. This includes features within IP Office applications connected to the IP Office system.

This section describes the license requirements for IP Office features. For information and procedures on managing licenses, see “Applying Licenses” in the following documents:

- *Administering Avaya IP Office™ Platform with Manager*
- *Administering Avaya IP Office™ Platform with Web Manager*

Ports, channels, and users

Some licenses enable a number of ports, channels, or users. Depending on the particular license, each supported instance can be consumed either when it is configured for use or when it is actually being used. When no further instances of a license are available, further use of the licensed feature is not allowed.

Multiple licenses can be added to give a higher number of supported ports, channels, or users. However, licenses above the capacity supported by the particular IP Office control unit will not work.

PLDS licensing

IP Office uses the Avaya Product Licensing and Delivery System (PLDS) to manage licenses. PLDS is an online, web-based tool for managing license entitlements and electronic delivery of software and related license files. PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads. You can access PLDS from http://plds.avaya.com/.

PLDS license files

Licenses are delivered from PLDS with license files. A PLDS license file is generated for installing on a specific machine. There are two deployment options:

- PLDS Nodal license files are generated for and installed on particular IP Office nodes.
- PLDS WebLM license files are generated for and installed on a WebLM server that can license multiple IP Office nodes.

WebLM centralized licensing is supported in IP Office Server Edition and in IP Office Branch deployments, but not in non-Branch deployments of IP Office Standard mode.

Página2229 de 3226.

PLDS host ID

Each PLDS license file must be created with the PLDS host ID of the system where the license file is to be loaded. PLDS Nodal license files are machine specific and you must specify the host ID in the **PLDS host ID** field in IP Office Manager or Web Manager.

IP500 V2 systems: You can find the PLDS host ID in the **Licensing** tab of IP Office Manager and Web Manager. The PLDS host ID is made of the two digits “11”, followed by the 10 digit feature key serial number printed on the IP Office SD card. If the SD card is changed, the PLDS host ID will also change.

IP Office Linux servers: The PLDS host ID can be found on the server labeling, the server packaging label, and the system ignition Login screen. The PLDS host ID is derived from the system ID. If the system ID changes, the PLDS host ID will also change.

WebLM: The WebLM host ID is the Mac address of the WebLM server. In a virtual environment, the WebLM host ID is a virtual Mac address that starts with the letter “V”. The WebLM host ID must be used when generating a PLDS license file for the WebLM server in order to implement a centralized licensing scheme for multiple IP Office systems. The WebLM host ID can be found on the server labeling, the server packaging label, the system ignition Login screen, and through the WebLM management interface.

Web License Manager (WebLM)

The Web License Manager (WebLM) is a web-based application for managing licenses. If you use the WebLM server running on the IP Office server, then you can use IP Office Web Manager to log in to the WebLM server by selecting **Applications** > **Web License Manager**. WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on (SSO).

Note:

- WebLM license management is supported for Server Edition deployments and for Enterprise Branch deployments using the System Manager WebLM server. It is not supported for Standard Mode systems.
- When upgrading from a previous release, all systems must be running the same software level. IP Office Server Edition does not support mixed versioning.

For more information on WebLM, see *Administering standalone Avaya WebLM*.

Migration of ADI licenses

ADI licenses are no longer supported as of Release 10.0. New licenses must be obtained from PLDS.

Using the One Source Configurator (OSC), all ADI licenses from previous releases are upgraded to PLDS. The **License Migration** option in IP Office Manager can be used to extract license information about the system, and this information can then be uploaded to OSC. After the information is extracted, IP Office Manager signs the file so it cannot be modified.

Página2230 de 3226.

PLDS license creation

The PLDS license must be created with the PLDS host ID of the system where the license will be loaded. If the licenses are loaded locally on the IP Office, then the PLDS host ID is available in IP Office Manager or Web Manager. For IP500 V2, it is also the Feature Key number on the SD card, which starts with “11”. If the PLDS file is loaded on a WebLM server, then the host ID is available on the WebLM interface under **Server Properties**.

For more information about migrating IP Office licenses to PLDS, see *Administering Avaya IP Office™ Platform with Manager* or *Administering Avaya IP Office™ Platform with Web Manager*.

Virtual licenses

As part of the migration process, the following virtual licenses are provided as actual PLDS licenses only through the XML migration process:

- Virtual Essential Edition
- Virtual Preferred Edition for systems with a UCMv1 module
- Virtual Avaya IP endpoints for systems with:
  - VCM32/64 v1 modules that provided 12 Avaya IP endpoints
  - Legacy VCM channel migration licenses
- Additional virtual Voicemail Pro ports for Server Edition

  Te PLDS licensing system adds two Voicemail Pro ports to any Server Edition or Server Edition Select license.

Customers with older systems (IP500 V1 / IP406 V2 / IP412 at release 6.0 or later) can upgrade through A1S Configurator BOM upload and ADI license validation process. Any virtualized licenses on these older systems will not carry forward and must be purchased as new.

Note:

The legacy Windows soft phone is not supported in IP Office Release 11.0 and will not function. The previous virtual licenses provided when upgrading are no longer provided in release 11.0. Avaya Equinox™ for Windows is the replacement. The Teleworker license enables the use of the Avaya Equinox™ for Windows. In earlier releases, this was only available with Office Worker and Power User.

Server Edition Centralized and Nodal licensing

Before release 10, Server Edition deployments used nodal licensing. This type of licensing can still be used in release 10 and higher. However, it is expected that most deployments will prefer to centralize license management using the Avaya Web License Management (WebLM) server. The WebLM server is automatically installed on the Server Edition Primary server. For newly installed systems, centralized licensing is the default configuration.

All systems in the Server Edition solution must use the same **License Source**.

Nodal licensing

With nodal licensing, license files must be installed on each node in the system. For some licensed features, the required license can be installed on the Server Edition Primary server and

used by all nodes in the system. However, for other licensed features, the required license must be installed on the node where the feature is used.

Centralized licensing

As of release 10, you can use the WebLM server running on the Server Edition Primary server to fully centralize license management. With centralized license management, all licenses are contained in a single PLDS file uploaded to WebLM. All nodes in the solution obtain their licenses from WebLM.

The IP Office Secondary server and Expansion systems can be configured to request licenses directly from the WebLM server, or to use a proxy option. When configured to use the proxy option, the license requests are sent through the IP Office Primary server, which proxies the requests to the WebLM server. The Primary server does not allocate licenses, but only acts as a proxy.

Systems using nodal licensing can be converted to use centralized licensing. Since PLDS license files are generated using the host ID of the server where they reside, you must regenerate the license file using the host ID of the WebLM server that will host the license file.

Centralized license distribution

When the license source is WebLM, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features. Editable fields can be used to:

- Request additional licenses from the WebLM server.
- Remove licenses from the IP Office node to apply them elsewhere.

Important:

When reallocating licenses, always reduce the number on the IP Office node where they are currently applied before applying them on another node. If you exceed the number of licenses available, you will receive an error message.

Distribution after conversion from Nodal to Centralized licensing

- If the IP Office node needs any of the following licenses, then you must manually configure the respective **Reserved Licenses** editable fields. This will allow the IP Office node to request the licenses from the WebLM server.
  - **VMPro Recordings Administrators**
  - **VMPro TTS Professional**
  - **CTI Link Pro**

Extension Reserved license setting: When the license source is **Local**, the setting **Extension** > **VoIP** > **Reserve License** is set to **None**. Switching the license source to WebLM changes the setting to **Reserve Avaya IP endpoint license**. If required, you must manually change this setting to **Reserve 3rd party endpoint license** or **Both**.

License allocation in WebLM

You can use WebLM to view the licenses used by each node in IP Office Server Edition. In the WebLM navigation pane on the left, click **Licensed Products**. The Acquired licenses table displays information about the licenses acquired for each client ID. In IP Office, the WebLM client ID for each node is displayed on the license Remote Server page.

Página2232 de 3226.

Nodal license distribution

When the **License Source** is **Local**, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features.

Nodal licensing for a Server Edition solution is based on a combination of licensing done through the Server Edition Primary server plus some server-specific licenses. All the user specific and system specific licenses can be managed from the Server Edition Primary server that also acts as a licensing server. Licenses are entered into the configuration of the Server Edition Primary server and are based on the system ID of that server.

Where a license is used to enable features, such as SIP Trunk channels, on other systems, the Server Edition Primary server only allocates those licenses to other systems after it has met its own license needs.

When another system loses connection to the Server Edition Primary server, any license requirements based on those licenses entered in the Server Edition Primary server's configuration are supported for a grace period of 30 days.

Other server specific licenses are entered into the configuration of the server requiring the feature and are based on the System ID of that system.

License	Primary server	Server-specific
Server Edition	Yes	No
Avaya IP endpoints	Yes	No
Third-party IP endpoints	Yes	No
SIP trunk channels	Yes	No
IP500 universal PRI channels	No	Yes
Additional voicemail ports [3]	Yes	No
Web Collaboration	No	Yes
UMS Web Services [1]	No	Yes
Office Worker	Yes	No
Power User	Yes	No
Office Worker to Power User upgrade	Yes	No
Receptionist	No	Yes
CTI Link Pro	No	Yes
Messaging TTS Pro [3]	Yes	No
Voicemail Pro Recording Administrator [2] [3]	Yes	No
WAV User	No	Yes
IPSec tunneling	No	Yes

1. UMS Web Service licenses are for Hunt Groups only.
2. The Voicemail Pro Recording Administrator license refers to Contact Store. Only one license is required for a Server Edition network.

Página2233 de 3226.

3. For deployments with dual Voicemail Pro servers, Messaging TTS Pro, Voicemail Pro Recording Administrator, and Additional voicemail ports licenses must be on the Secondary Server.

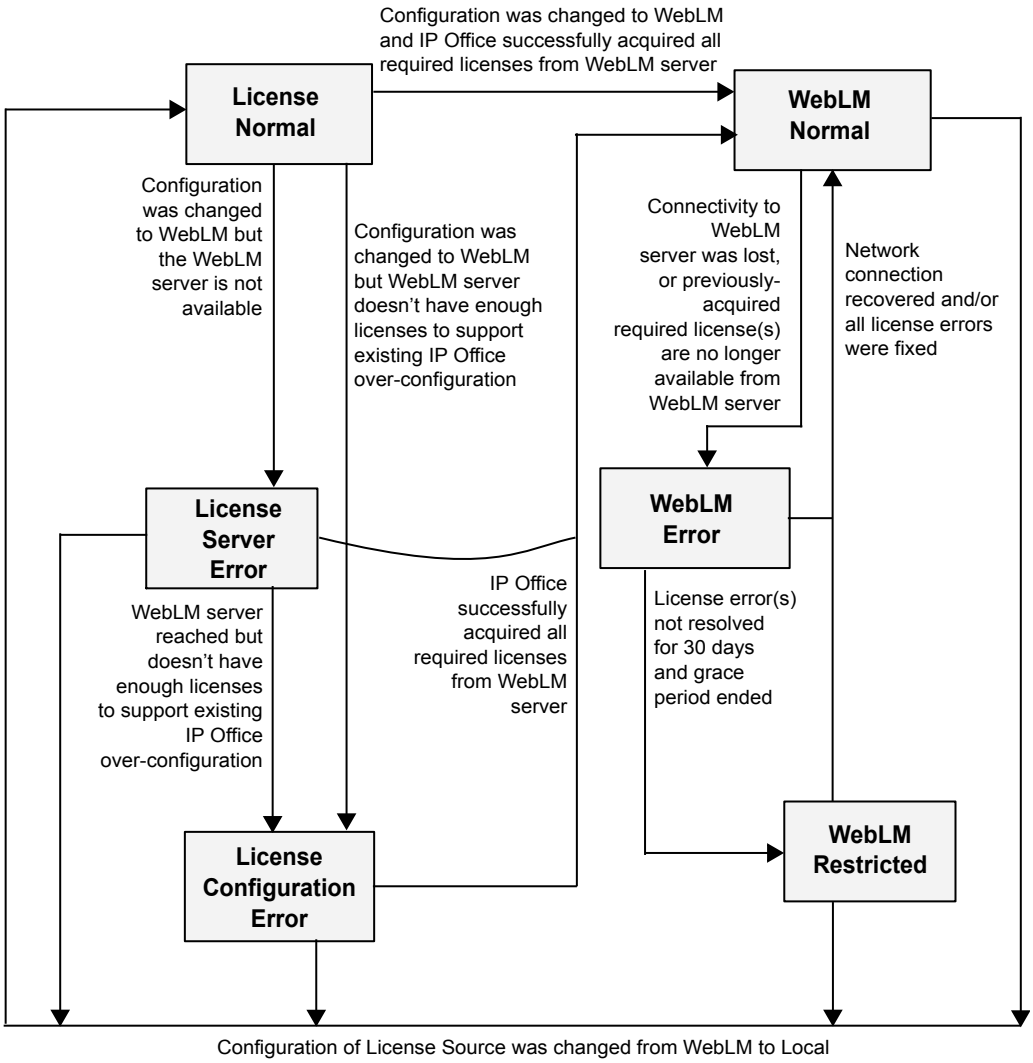
WebLM licensing

License modes

The following are the IP Office license modes when you are using WebLM licensing. The license mode is displayed in IP Office Manager, Web Manager, and System Status Application (SSA).

Mode	Description
License Normal	WebLM licensing is not configured. Traditional Nodal licensing. No grace period. Over-configuration is allowed.
License Server Error	Configuration was changed to WebLM, but the WebLM server is not available. No grace period. Until the problem is resolved, IP Office is unlicensed and unusable similar to traditional Nodal licensing if no licenses are installed.
License Configuration Error	Configuration was changed to WebLM and the WebLM server is available, but it doesn't have enough licenses to support the existing IP Office configuration. No grace period. Until the problem is resolved, IP Office is unlicensed and unusable similar to traditional Nodal licensing if no licenses are installed. Licenses must be added to the WebLM license file or IP Office configuration must be modified to correct over-configuration.
WebLM Normal	IP Office is configured for WebLM licensing, the WebLM server is available and IP Office successfully acquired all the licenses required to support all of its configured features. New licenses are acquired for newly-configured features, and over-configuration of licensed features is prevented if licenses cannot be acquired. IP Office periodically renews its acquired licenses. Failure to renew will lead to the WebLM Error mode with grace period.
WebLM Error	IP Office is configured for WebLM licensing and was previously in WebLM Normal mode. But IP Office now cannot renew or re-acquire all the licenses required to support all of its configured features. Over configuration of licensed features is prevented if licenses cannot be acquired. IP Office keeps operating for a 30-day grace period based on its existing configuration (lost licenses are replaced with virtual grace licenses).
WebLM Restricted	IP Office was in the WebLM Error mode, but the 30-day grace period has expired and the problems for this error have not been resolved. Unlicensed features will stop working (virtual grace licenses are deleted). Any configuration of IP Office is not allowed, except configuration changes that reduce the licensing errors.

License mode state transitions



WebLM licensing configuration

In WebLM licensing, licenses must fully support the IP Office configuration. Over-configuration is not allowed. IP Office, based on its configuration, requests the required licenses from the WebLM server.

For some types of licenses, such as for users, extensions, receptionists, and web collaboration, the type and quantity of required licenses is determined by the configuration of the respective items. For example, the User and Extension records in the IP Office configuration. These quantities are displayed in read-only fields in the 'Reserved Licenses' list in the IP Office Configuration License > Remote Server tab.

For other types of licenses, such as for SIP trunk sessions and Voicemail Pro ports, the quantity of required licenses must be configured explicitly. These quantities have to be configured in editable fields in the Reserved Licenses list in the IP Office Configuration License > Remote Server tab.

Página2235 de 3226.

Licensing configuration warnings and alarms

License Configuration Error mode

- IP Office goes into the License Configuration Error mode when you change the IP Office License Source from “Local” to “WebLM” and it is under-licensed or over-configured.

  In this mode, IP Office is unlicensed and unusable. This mode is a transition error state and not supported as a steady state. Try to avoid entering into this mode and, if it happens, fix the errors immediately.
- Installed systems with traditional licensing may be under-licensed or over-configured. If they are upgraded to version 10.0 and migrated using WebLM licensing without acquiring the additional needed licenses or removing the over-configuration, then the installed systems goes into the License Configuration Error mode after migration.

  To help avoid this problem, warnings are given by the IP Office Manager License Migration Tool. If IP Office has over-configuration relative to its existing old licenses, the License Migration Tool displays a warning and also includes detailed warning information in the License Migration information file.
- If IP Office is in the License Configuration Error mode, Systems Status Application (SSA) alarms page shows alarms indicating the cause of the problem.

  If you encounter this mode, review the SSA alarm errors and resolve them by acquiring the missing required licenses or by modifying the IP Office configuration so as to not require these licenses.

Other warnings

When the administrator sets the License Source to “WebLM”, IP Office Manager and IP Office Web Manager display a warning advising the administrator to check and verify that sufficient licenses are available on the WebLM server.

WebLM user and IP Endpoint licensing

IP endpoint licenses

When IP Office uses WebLM licensing, each configured H.323 or SIP extension requires a license and IP Office requests the required licenses from the WebLM server. Sufficient licenses are required for all the configured H.323 and SIP extensions and not only for the maximum number of concurrently-registered extensions. This is consistent with WebLM licensing for users and receptionists.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of extensions with a small number of licenses to cover only a subset of the extensions registering at the same time. For example, configuring three extensions with one IP endpoint license to cover only one of the three extensions registering at the same time. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing, and set the **Reserve License** field for the extensions to `None`.

For each configured H.323 or SIP extension, IP Office requests from the WebLM server an Avaya or third-party IP endpoint license, as per the **Reserve License** field of the configured extension record. When IP Office uses WebLM licensing, the **Reserve License** field for each configured H.323 and SIP extension is by default set to Avaya IP endpoint license. This field is editable and the

administrator can change it to a third-party IP endpoint license or to both Avaya and third-party IP endpoints.

Note:

For the **Reserve License** field, the value `None` is not available with WebLM licensing because IP Office must request a license from the WebLM server.

User licenses

When IP Office uses WebLM licensing, sufficient User licenses are required as per the IP Office users configuration and not only for the maximum number of concurrently-registered users. This is consistent with WebLM licensing for IP endpoints and receptionists. IP Office requests from the WebLM server the required User licenses (for example, Power User licenses) as per the user profile of all configured users.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of users with a small number of licenses to cover only a subset of the users registering at the same time. For example, configuring three users with one User license to cover only one of the three users registering at the same time. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing.

Receptionist licenses

When IP Office uses WebLM licensing, Receptionist licenses are required for all users that are configured as Receptionist and not only for the maximum number of users that would run their IP Office SoftConsole application concurrently. This is consistent with WebLM licensing for IP endpoints and users. With WebLM, licenses are required according to the configured objects, and over-configuration and under-licensing are not allowed.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of Receptionist users with a small number of licenses to cover only a subset of the users connecting at the same time using IP Office SoftConsole. For example, configuring three Receptionist users with one Receptionist license to cover only one of the three users connecting at the same time using IP Office SoftConsole. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing.

Auto-create support for users and extensions

When IP Office uses WebLM licensing, you cannot auto-create users and extensions as it is not supported. The administrator must manually configure users and extensions. For DECT extensions, the “Preconfigured” method must be used.

However, auto-create for users and extensions is supported if you use local PLDS license file instead of Centralized WebLM licensing.

Página2237 de 3226.

Basic Edition license for new systems

To upgrade to Release 11.0, the new PLDS R11.0 upgrade runtime license is used in combination with the R11.0 software. Upgrading to IP Office R11.0 from releases prior to R10.0 involves a complete transition to PLDS licenses. To upgrade existing IP Office systems to IP Office R11.0, paid or transactional or entitled Edition R11.0 upgrade or migration licenses are required.

Material code	License	Description
396490	IP OFFICE R11 BASIC EDITION MIG UPGRADE PLDS	R11 Basic Edition starting in PLDS
369472	IP OFFICE R11 BASIC EDITION MIGRATION UPGRADE	ADI or PLDS upgrade to R11 Basic Edition

Customers must also purchase SD cards, which are configured, by default, with Basic Edition.

Customers must obtain this material code, which is merchandisable and does not have to be configured, before ordering IP Office Support Services. This is especially important for customers who already have Basic Edition or for after-market IP Office Support Services purchases, including customers who set up Basic Edition without IP Office Support Services first, but then later choose to get IP Office Support Services. These customers must place a merchandise order for this material code first and then place their after-market purchase of IP Office Support Services and register their equipment for servicing.

Note:

Basic Edition is not a prerequisite for Essential Edition or Preferred Edition, and is not stacked under Essential Edition.

Essential Edition and Preferred Edition licenses

An Essential Edition license is a prerequisite on IP500 V2 systems, and includes mobile twinning for all users and four remote workers.

A Preferred Edition license is a prerequisite for any user profile licenses. In a multisite network, the Preferred Edition license of the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server still requires its own Preferred Edition license for Voicemail Pro operation. For a IP500 V2 system fitted with a Unified Communications Module (UCM V2), the card requires a separate Preferred Edition license.

The Preferred Edition license includes support for 4 messaging ports. The total number of messaging ports supported can be increased by adding additional messaging port licenses, at the time of purchase or later, up to the maximum supported by the particular control unit.

Página2238 de 3226.

Order code	License	Description
396491	IP OFFICE R11 ESSENTIAL EDITION UPGRADE PLDS LIC:DS	Essential Edition (PLDS upgrades)
396474	IP OFFICE R11 ESSENTIAL EDITION MIG UPG LIC:DS	ADI migrations to PLDS and upgrades to R11.0 Essential Edition
396492	IP OFFICE R11 PREFERRED VOICEMAIL PRO UPGRADE PLDS LIC:DS	Preferred Edition (PLDS upgrades)
396476	IP OFFICE R11 PREFERRED VOICEMAIL PRO MIG UPG LIC:DS	ADI migrations to PLDS and upgrades to R11.0 Preferred Edition

Server Edition licenses

A Server Edition license includes:

- Features from Essential Edition
- Features from Preferred Edition
- Centralized Voicemail Pro
- Two ports of Voicemail Pro
- Unlimited multi-site networking channels (IP Office Lines)

A Server Edition license enables:

- Meet-me conferencing
- Advanced messaging
- Automated attendant
- Call recording
- Conditional call routing
- Queue announcements
- Mobile twinning
- Call control
- Call back

One Server Edition license is required for the primary server, the secondary server, and for each Linux or IP500 V2 expansion system. The licenses enable voice networking between systems in the Server Edition network.

Order code	License	Description
PLDS Upgrades (starting PLDS)		
396493	IPO R11 SE/VRTLZD UPG PLDS LIC	Paid Upgrade Code
ADI Migrations to PLDS and upgrade to R11.0		
396480	IP Office R11 SE ADI MIG UPG LIC	Paid Upgrade Code
396478	IPO R11 VRTLZD SE ADI Migration UPG LIC	Paid Upgrade Code
IP Office PLDS upgrades		
396519	IPO-SL 11 SE/VRTLZD UPG PLDS LIC	Paid Upgrade Code

Página2239 de 3226.

Branch licenses

The following table describes key IP Office licenses that are of particular interest to branch deployments.

Display name	Description
Avaya WebLM Model	This license is required by IP Office in branch deployments in order to connect to the WebLM server and use WebLM centralized licensing.
Branch System	This license is required for IP Office in branch deployments. It is used for tracking purpose only.
IP Office Centralized Endpoints license	One license is required for each Centralized user configured on the IP Office with a SIP extension or an analog extension. **Important:** In addition to this IP Office license, each centralized user also requires a license on the central Avaya Aura® system.
SM Trunk Channel	This license is required with sufficient quantity to allow for the maximum number of concurrent SM Line calls to be enabled on the system. The total number of SM Trunk Channel licenses requirements depend on the expected traffic patterns in the particular deployment. **Note:** IP Office also supports SM Line connections to Avaya Aura® Session Manager in other IP Office Server Edition deployments. These connections are not limited to branch deployments.

Small Community Network licenses

In a Small Community Network (SCN), there must be at least one IP Office Preferred Edition. Two are required with resiliency.

The different types of users in an SCN have the same functionality, regardless of where the IP Office Preferred Edition is installed.

In a multisite network, if one or more IP Office Preferred Edition system is installed, then all the IP Office systems in the multisite network will automatically have Preferred licenses as prerequisites for the following user types:

- Power users
- Teleworkers
- Mobile workers
- Office workers

Página2240 de 3226.

Trunk licenses

The tables in this section include all the net new and uplift IP Office PLDS software license material codes. The material codes with indication of R10+ are known as “ANY” codes and can be used for Release 10.0 and later system deployments. The SAP descriptions have been modified to show 10+ for this change, while the material code remains the same. Other codes are R11.0 release specific and contain R11.0 in the description.

SIP trunk sessions

These licenses are used to permit sessions on SIP trunks and SM Lines added to the system. Multiple licenses can be combined for the total number of channels required.

Order code	License	Description
383085	IPO R10+ SIP TRNK 1 LIC	SIP trunk 1 session
307332	IIPO-SL R10+ SIP TRNK 1 LIC	SIP trunk 1 session – Select
383120	IPO R10+ SM LINE SIP TRNK LIC	SM Line session
382917	IPO-SL R10+ SM LINE SIP TRK LIC	IP Office Select SM Line session

IP500 Universal PRI additional channels

The IP500 PRI Universal trunk card (UTC) is available in 1 or 2 port variants, each port supporting a single PRI circuit connection. The ports can be switched between supporting E1, E1R2, or T1 line types as required for the trunk being connected. Each port supports 8 B-channels (“Bearer”) which do not need to be licensed. If additional B-channels are required, they must be licensed through the addition of the licenses below. Multiple licenses can be added to achieve the total number of channels required. D-channels are not subject to licensing. The licenses are consumed by those channels, which are configured as being *in service*, in order of the installed IP500 PRI-U cards.

IP500 Universal PRI additional E1 channels

These licenses are used to enable additional E1 B-channels for IP500 PRI-U cards configured for E1 operation. Each port can support up to 30 B-channels in this mode.

Order code	License	Description
383092	IPO R10+ IP500 E1 ADD 2CH LIC	2 E1 channels
383093	IPO R10+ IP500 E1 ADD 8CH LIC	8 E1 channels
383094	IPO R10+ IP500 E1 ADD 22CH LIC	22 E1 channels
307337	IPO-SL R10+ IP500 E1 ADD 2CH LIC	2 E1 channels – Select
307338	IPO-SL R10+ IP500 E1 ADD 8CH LIC	8 E1 channels – Select
307339	IPO-SL R10+ IP500 E1 22CH LIC	22 E1 channels – Select

IP500 Universal PRI additional E1R2 channels

These licenses are used to enable additional E1R2 B-channels for IP500 PRI-U cards configured for E1R2 operation. Each port can support up to 30 B-channels in this mode.

Página2241 de 3226.

Order code	License	Description
275637	IPO R10 IP500 E1R2 ADD 2CH PLDS LIC	2 E1R2 channels
383096	IPO R10+ IP500 E1R2 ADD 8CH LIC	8 E1R2 channels
383097	IPO R10+ IP500 E1R2 ADD 22CH LIC	22 E1R2 channels
307340	IPO-SL R10+ IP500 E1R2 2CH LIC	2 E1R2 channels – Select
307341	IPO-SL R10+ IP500 E1R2 8CH LIC	8 E1R2 channels – Select
307342	IPO-SL R10+ IP500 E1R2 22CH LIC	22 E1R2 channels – Select

IP500 V2 Universal PRI additional T1 channels

These licenses are used to enable additional T1 B-channels for IP500 PRI-U cards configured for T1 PRI or T1 robbed-bit operation. Each port can support up to 23 B-channels (T1 PRI) or 24 B-channels (T1 robbed bit) in this mode.

Order code	License	Description
383091	IPO R10+ IP500 T1 ADD 2CH LIC	2 T1 channels
307336	IPO-SL R10+ IP500 T1 ADD 2CH LIC	2 T1 channels – Select

IP500 V2 Voice Networking

The use of private voice networking trunks between IP500 V2 control units and other systems requires voice networking channel licenses within the IP500 V2. This applies to H.323 IP trunks configured on the IP500 V2, including IP trunks being used for an IP Office Small Community Network (SCN). A voice networking license is also required for the use of trunks configured for Q.SIG operation. On an H.323 IP trunk, a license instance is consumed for each simultaneous outgoing call. On a Q.SIG trunk, the number of calls is limited by the trunk type rather than available licenses.

Additional licenses can be added to achieve the number of voice networking channels required.

Order code	License	Description
383087	IPO R10+ IP500 VCE NTWK 4 LIC	4 voice networking channels including the Advanced Networking features (distributed groups and hot-desking across Small Community Network)

User licenses

A profile controls whether users can be configured for a number of features. Every user on the system, except users with Basic User profile and non-licensed users, requires one of the user license types.

The table below lists the different user profiles and the features accessible by each profile. Setting a user to a particular profile enables those features by default, but they can be manually disabled if necessary. The number of users that can be configured for each profile is controlled by the user licenses present in the configuration.

Página2242 de 3226.

Except for a Basic User, a Preferred Edition system license is a prerequisite for any user profile licenses. In a multi-site network, the Preferred Edition license for the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server still requires its own Preferred Edition license for Voicemail Pro operation.

Feature		Standard Mode					Server Edition		
	Non-licensed User [1]	Basic User	Office Worker	Teleworker	Mobile Worker	Power User	Basic User	Office Worker	Power User
one-X Portal Services	–	–	Yes	Yes	–	Yes	–	Yes	Yes
Telecommuter options	–	–	–	Yes	–	Yes	–	–	Yes
UMS Web Services	–	–	Yes	Yes	–	Yes	–	Yes	Yes
TTS for Email Reading	–	–	–	–	Yes	Yes	–	–	Yes
Remote Worker [2]	–	–	–	Yes	–	Yes	Yes	Yes	Yes
Avaya Communicator [3]	–	–	Yes	Yes	–	Yes	Yes	Yes	Yes
WebRTC	–	–	Yes	–	–	Yes	–	Yes	Yes
Avaya Equinox™	–	–	Yes	Yes	–	Yes	–	Yes	Yes

User Profile Notes:

1. Non-licensed users can be created on both Standard Mode and Server Edition systems.
2. The system supports users using remote H.323 or SIP extensions. On non-Server Edition systems, up to 4 users are supported as remote extensions without needing to be configured and licensed for a user profile. Additional remote users are supported if licensed and configured for either a **Teleworker** or **Power User** user profile. On Server Edition systems, the remote worker is supported for all user profiles.
3. Supported for advanced Avaya Communicator for IP Office usage if one-X Portal and Voicemail Pro applications are also installed. If otherwise, only basic Avaya Communicator for IP Office usage is supported.
4. Avaya Equinox™ can be used with a Basic User or a Mobile Worker license in conjunction with IP Softphone license but in standard mode only. In such cases, Simultaneous mode, Shared control feature, and Presence support will not be available.

Non-licensed user

A non-licensed user:

- Is allowed dial in access and paging.
- Can be used as a Music on Hold or Analog paging port.
- Can be authenticated to allow remote access for remote administration.
- Can make internal and emergency calls as NoUser.
- Can forward to voice mail box for voice mail box only users.
- Can be used for internal twinning.

Basic users

New users are created as Basic users by default. Basic users can perform hot-desking, make and receive calls, forward calls, and perform mobile twinning.

Basic user licenses are no longer provisioned. For both new systems and upgrades, the **Basic Users** field is greyed out.

Basic user licenses are required only in the Cloud environment.

Office Worker licenses

This option is targeted at users who are working in the office. In conjunction with a wired or wireless Avaya phone, these users are provided with functions to control their communication with a PC. For example, these users can control audio conferences or manage voice mail with an email client (requires a Preferred Edition license).

An Office Worker license enables Avaya Communicator, Avaya Equinox™ for Windows and Mac, and Avaya Communicator for Web. The Office Worker license enables a user to use the Unified Messaging Service (UMS) and Avaya one-X® Portal for IP Office without Telecommuter functionality. The license instances are consumed for each user being configured.

Order code	License	Description
383105	IPO R10+ MOBILE WORKER 5 TRL LIC	5 licenses for Mobile workers
383107	IPO R10+ OFFICE WORKER 5 TRL LIC	5 licenses for Office workers
307347	IPO-SL R10+ OFFICE WORKER 5 TRL LIC	5 users – Select

Teleworker licenses

This option is targeted at users who are working from home or elsewhere with Internet connection to the office. They are provided with the ability to leverage the PLDS or ISDN using Telecommuter mode, without incurring any remote phone charges. Alternatively the new IP Office Video Softphone can be used if the quality of service of the local internet connection is adequate.

Teleworker includes the remote worker capability with the package. An Essential Edition license provides 4 remote worker seats. Customers requiring additional seats will need to purchase the Teleworker solution.

The Teleworker license enables a user to use Avaya Communicator, Avaya Equinox™ for Windows and Mac, and Avaya one-X® Portal for IP Office. UMS functionality for voice mail or email integration is also enabled, providing synchronization with any IMAP email client. The license instances are consumed for each user being configured.

Página2244 de 3226.

Order code	License	Description
383103	IPO R10+ TELEWORKER 5 TRL LIC	5 users

Mobile Worker licenses

This option is targeted at users with mobile devices. For example, field sales and service staff who are often on the road. These users are provided with features, such as one number access and call control as if in the office, enabling them to never miss a call. The Mobile Worker license enables the use of the one-X Mobile Preferred client in callback mode (but not in VoIP mode).

Power User licenses

This option is targeted at key knowledge workers with the need for both Mobile Worker and Teleworker functionality. A Power User license enables Avaya Communicator, Avaya Equinox™ (desktop and mobile), Avaya Communicator for Web, and VoIP mode in one-X Mobile Preferred.

The Power User license enables a user to use Avaya one-X® Portal for IP Office, all mobility features, and UMS. A Power User license is required to enable conference scheduling in Avaya one-X® Portal for IP Office.

The license instances are consumed for each user being configured.

Order code	License	Description
396319	IP Office R11 OFFICE WORKER TO POWER USER 1 UPLIFT LIC	Upgrade from Office Worker to Power User – 1 user
396505	IP OFFICE-SELECT R11 OFFICE WORKER TO POWER USER 1 UPLIFT LIC	Upgrade from Office Worker to Power User – 1 user – Select
396318	IP Office R11 MOBILE TO POWER USER 1 UPLIFT LIC	Upgrade from Mobile Worker to Power User – 1 user
396316	IP Office R11 POWER USER 1 LIC	1 user
396503	IP Office-Select R11 POWER USER 1 LIC	1 user – Select

Receptionist licenses

This option is targeted at operators or receptionists and provides a visual computer interface for call handling and management for multiple sites. Up to 10 Receptionist users are supported on each node. Server Edition supports up to 32 Receptionist users, and Server Edition Select supports up to 50.

The Receptionist license also enables a user to use IP Office SoftConsole, a Windows application intended for receptionists and operators. Up to 4 IP Office SoftConsole clients can run at the same time and be licensed on a single IP Office system. Additional licenses can be added.

Order code	License	Description
307318	IPO-SL R10+ RECEPTS 1 LIC	1 user
382687	IPO R10+ RECEPTIONIST 1 LIC	1 user

Página2245 de 3226.

Centralized User license

In IP Office Branch deployments, where IP Office is deployed as a branch of a central Avaya Aura® system, users with a SIP or analog extension can be configured as Centralized users. Every Centralized user requires a Centralized Endpoint license.

Web Collaboration licenses

Order code	License	Description
383122	IPO R10+ WEB COLLAB USER 1 LIC	1 user
382918	IPO-SL 10+ WEB COLLAB USR 1 LIC	1 user – Select

IP endpoint licenses

All IP endpoints, Avaya and third party, require an endpoint license.

Avaya IP endpoint licenses

All Avaya IP phones, including DECT and Wi-Fi phones, require an Avaya IP Endpoint license and will consume one instance of that license. This does not apply to the Avaya Softphone or Avaya Communicator. Avaya IP phones without a license will still be able to register but will be limited to making emergency calls only. The phone will display `No license available` and `Emergency Calls Only`. If a license becomes available, it will be assigned to any unlicensed DECT handsets first and then to any other unlicensed Avaya IP phone in the order that the phones registered.

Order code	License	Description
307350	IPO-SL R10+ AV IP ENDPT 1 LIC	1 endpoint – Select
383110	IPO R10+ AV IP ENDPT 1 LIC	1 endpoint

Third-party IP endpoint licenses

Non-Avaya IP phones, including SIP or H.323 devices, require a Third Party IP Endpoint license to register to IP Office and will consume one instance of that license.

Order code	License	Description
307323	IPO-SL R10+ 3RD PTY IP END 1 LIC	1 endpoint – Select
383072	IPO R10+ 3RD PTY IP ENDPT 1 LIC	1 endpoint

Trial licenses

Order code	License	Description
396446	IP OFFICE R11 ESSENTIAL EDITION TRIAL LIC	Essential Edition
396448	IP OFFICE R11 PREFERRED VOICEMAIL PRO TRIAL LIC	Preferred Edition

Table continues…

Página2246 de 3226.

Order code	License	Description
383123	IPO R10+ WEB COLLAB 5 TRL LIC	5 Web Collaboration licenses
382919	IPO-SL R10+ WEB COLLAB 5 TRL LIC	5 Web Collaboration licenses — Select
396504	IP OFFICE-SELECT R11 POWER USER 5 TRIAL LIC	5Power User license — Select
396317	IP OFFICE R11 POWER USER 5 TRIAL LIC	5 Power User licenses
383103	IPO R10+ TELEWORKER 5 TRL LIC	5 Teleworker licenses
383105	IPO R10+ MOBILE WORKER 5 TRL LIC	5 Mobile Worker licenses
307347	IPO-SL R10+ OFFICE WORKER 5 TRL LIC	5 Office Worker licenses — Select
383107	IPO R10+ OFFICE WORKER 5 TRL LIC	5 Office Worker licenses
307319	IPO-SL R10+ RECEPTS 5 TRL LIC	5 Receptionist licenses — Select
382688	IPO R10+ RECEPTIONIST 5 TRL LIC	5 Receptionist licenses
307324	IPO-SL 10 3RD PTY IP 5 TRL LIC	Third party IP endpoint trial license — Select
383073	IPO R10 3RDPTY IPENDPT 5 TRL LIC	Third party IP endpoint trial license
382913	IPO-SL R10+ AV IP ENDPT 5 TRL LIC	5 Avaya IP endpoint licenses — Select
383111	IPO R10+ AV IP ENDPT 5 TRL LIC	5 Avaya IP endpoint licenses
383090	IPO R10+ VMPRO UMS 5 TRL LIC	5 Voicemail Pro UMS licenses
307335	IPO-SL R10+ VMPRO UMS 5 TRL LIC	5 Voicemail Pro UMS licenses – Select
383078	IPO R10+ 3RD PTY TTS TRL LIC	Voicemail Pro third party TTS license
383076	IPO R10+ TTS WNDWS TRL LIC	Voicemail Pro Windows TTS license
307327	IPO-SL R10+ TTS PROLINUX TRL LIC	Voicemail Pro Linux TTS license — Select
383080	IPO R10+ TTS PRO LINUX TRL LIC	Voicemail Pro Linux TTS license
307329	IPO-SL R10+ IPSEC VPN TRL LIC	IPSec Tunneling — Select
383082	IPO R10+ IPSEC VPN TRL LIC	IPSec Tunneling
307333	IPO-SL R10+ SIP TRNK 5 TRL LIC	SIP trunk sessions — Select
383086	IPO R10+ SIP TRNK 5 TRL LIC	SIP trunk sessions
383088	IPO R10+ IP500 VCE NTWK 4	IP500 Voice Networking
307321	IPO-SL R10+ CTI TRL LIC	CIT Link Pro — Select
383070	IPO R10+ CTI TRL LIC	CIT Link Pro

Upgrade licenses

To upgrade existing systems to the latest release, upgrade licenses are required. Upgrade licenses are sold separately. Customers can only upgrade to the latest equivalent of their existing Edition.

Página2247 de 3226.

Note:

Upgrading from a previous release of Basic Edition to the latest version of Essential Edition is not a valid upgrade path.

Order code	License	Description
383738	IPO-SL R10+ RECEPTS 1 UPG PLDS LIC	Select Receptionist upgrade
383696	IPO R10+ RECEPTIONIST 1 UPG PLDS LIC	Receptionist upgrade
383739	IPO-SL 10+ CTI UPG PLDS LIC	Select CTI upgrade
383697	IPO R10+ TI UPG PLDS LIC	CTI upgrade
383740	IPO-SL 10+ MPRO 1 UPG PLDS LIC	Select Voicemail Pro upgrade
383698	IPO R10+ VM PRO 1 UPG PLDS LIC	Voicemail Pro upgrade
383741	IPO-SL 10+ 3RDPTY IPEND1 UPG PLDS LIC	Select IP third party endpoint upgrade
383699	IPO R10+ 3RDPTY IPENDPT1 UPG PLDS LIC	IP third party endpoint upgrade
383742	IPO-SL 10+ TAPI WAV 1 UPG PLDS LIC	Select TAPI WAV upgrade
383700	IPO R10+ TAPI WAV 1 UPG PLDS LIC	TAPI WAV upgrade
383702	IPO R10+ 3RD PTY TTS UPG PLDS LIC	Third party TTS upgrade
383744	IPO-SL 10+ IPSEC VPN UPG PLDS LIC	Select IPSec VPN upgrade
383704	IPO R10+ IPSEC VPN UPG PLDS LIC	IPSec VPN upgrade
383747	IPO-SL 10+ VMPRO UMS 1 UPG PLDS LIC	Select Voicemail Pro Unified Messaging Server upgrade
383708	IPO R10+ VM PRO UMS 1 UPG PLDS LIC	Voicemail Pro Unified Messaging Server upgrade
383748	IPO-SL 10+ IP500 T1 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383709	IPO R10+ IP500 T1 CH1 UPG PLDS LIC	IP500 additional channel upgrade
383749	IPO-SL 10+ IP500 E1 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383710	IPO R10+ IP500 E1 CH1 UPG PLDS LIC	IP500 additional channel upgrade
383752	IPO-SL 10+ IP500 E1R2 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383713	IPO R10+ IP500 E1R2 CH1 UPG PLDS LIC	IP500 additional channel upgrade

Table continues…

Página2248 de 3226.

Order code	License	Description
383707	IPO R10+ IP500 VCE NTWK1 UPG PLDS LIC	IP500 voice networking upgrade
383757	IPO-SL 10+ AV IP ENDPT 1 UPG PLDS LIC	Select Avaya IP endpoint upgrade
383722	IPO R10+ SFTPH 1 PLDS UPG LIC	Soft Phone upgrade
383760	IPO-SL 10+ SMLINE SIPTRK UPG PLDS LIC	Select SM Line SIP trunk upgrade
383726	IPO R10+ SM LINE SIPTRNK UPG PLDS LIC	SM Line SIP trunk upgrade
383706	IPO R10+ SIP TRNK 1 UPG PLDS LIC	SIP trunk upgrade
383761	IPO-SL 10+ WEBCOLLB USR1 UPG PLDS LIC	Select Web Collaboration user upgrade
383728	IPO R10+ WEBCOLLAB USER1 UPG PLDS LIC	Web Collaboration user upgrade
383730	IPO R10 ESS ED EVM 1CH UPG PLDS LIC	Essential Edition Embedded Voicemail channel upgrade

Página2249 de 3226.

Chapter 4: Resources

Documentation

See the following related documents on the Avaya Support website at support.avaya.com and the IP Office Knowledge Base at marketingtools.avaya.com/knowledgebase.

Document number	Title	Use this document to:	Audience
Overview			
16–604278	*Avaya IP Office™ Platform Start Here First*	See a list of all the documents related to the solution.	Everyone
Not numbered	*Avaya IP Office™ Platform Feature Description*	Understand the solution features at a high-level.	Everyone
Not numbered	*Avaya IP Office Contact Center Feature Description*	Understand IP Office Contact Center features and capabilities.	Everyone
Planning			
15–604135	*Avaya IP Office™ Platform Server Edition Reference Configuration*	Understand the technical specifications of and plan for IP Office Server Edition deployment.	Sales Engineers Implementation Engineers
15–604253	*Avaya IP Office™ Platform in a Branch Environment Reference Configuration*	Understand the technical specifications of and plan for IP Office in a branch environment deployment.	Sales Engineers Implementation Engineers
Not numbered	*OnAvaya™ and Powered by Avaya Reference Configuration for Business Partners*	Understand the technical specifications of both IP Office Cloud solutions and plan for deployment.	Sales Engineers Implementation Engineers
Not numbered	*Avaya IP Office™ Platform Security Guidelines*	Understand and follow recommended security guidelines.	Sales Engineers Implementation Engineers
Not numbered	*Avaya IP Office Contact Center Reference Configuration*	Understand technical specifications of IP Office Contact Center and plan for deployment.	Sales Engineers Implementation Engineers

Página2250 de 3226.

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Training

Avaya training and credentials are designed to ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website at http://avaya-learning.com/.

The following courses are also available on the Avaya Learning website. After logging in to the website, enter the course code or the course title in the **Search** field.

Course code	Course title
2S00012W	APSS – Small and MidMarket Communications – IP Office™ Platform and Select Overview

Table continues…

Página2251 de 3226.

Course code	Course title
4601W	Avaya IP Office™ Platform — Components
4602W	Avaya IP Office™ Platform — Editions
2S00015O	Small and Midmarket Communications — IP Office — Endpoints
10S00005E	Knowledge Access: Avaya IP Office™ Platform Implementation
5S00004E	Knowledge Access: Avaya IP Office™ Platform Support

Included in all Knowledge Collection Access offers above is a separate area called IP Office Supplemental Knowledge. This floor in the Virtual Campus contains self-directed learning objects, which cover IP Office delta information. This material can be consumed by technicians experienced in IP Office.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Página2252 de 3226.

Additional IP Office resources

You can find information at the following additional resource websites.

Avaya

http://www.avaya.com is the official Avaya website. The front page also provides access to individual Avaya websites for different countries.

Avaya Sales & Partner Portal

http://sales.avaya.com is the official website for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the portal can be customized for specific products and information types that you wish to see and be notified about by email.

Avaya IP Office Knowledge Base

http://marketingtools.avaya.com/knowledgebase provides access to an online, regularly updated version of the IP Office Knowledge Base.

Avaya maintenance, lifecycle and warranty information

Avaya support services complement standard Avaya maintenance, lifecycle and warranty policies that are posted on http://support.avaya.com. For more information, send email to support@avaya.com.

International Avaya User Group

http://www.iaug.org is the official discussion forum for Avaya product users.

Product compatibility

For the latest and most accurate compatibility information go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Related links

Accessing Avaya DevConnect Application Notes on page 134
Interoperability on page 93

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Página2253 de 3226.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya User ID and password.

   The Support page appears.
3. Under **Support by Product**, click **Product-specific support**.
4. Enter the product in **Enter Product Name** text box and press Enter.
5. Select the product from the drop down list and choose the relevant release.
6. Select the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Phones on page 38
Phone interoperability on page 95

Accessing Avaya DevConnect Application Notes

The Avaya DevConnect program conducts testing with service providers to establish compatibility with Avaya products.

Procedure

1. Go to http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp.
2. Sign in or register.
3. Click a timeframe to search within.

   A list of all the application notes for that timeframe appears.

Página2254 de 3226.

4. In the **Search** field, type `IP Office` and press **Enter**.

   A list of relevant Application Notes appear.

Related links

[Phones](#) on page 38
[Phone interoperability](#) on page 95
[Product compatibility](#) on page 133
[Hardware and software options](#) on page 84
[Interoperability](#) on page 93

Página2255 de 3226.

Glossary list

Automatic Route Selection	A feature of some telephone systems in which the system automatically chooses the most cost-effective way to send a toll call.
Busy Hour Call Completions	A measure of dynamic traffic calls that can be completed in an average busy hour.
Communication Manager	A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.
Computer Supported Telecommunications Application (CSTA)	A standard interface for Computer Telephony Integration (CTI) applications, such as voice mail and auto-attendant, to interact with telephony equipment.
Digital Communications Protocol	A proprietary protocol that is used to transmit both digitized voice and digitized data over the same communications link. A Digital Communications Protocol (DCP) link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels and two telephones or data modules.
Directory Enabled Management	An interface that uses Avaya Directory Server to facilitate administration of Modular Messaging from a centralized location.
Distributed Communications System	A proprietary inter-networking protocol from Avaya with which you can configure two or more Avaya-based private communication networks to operate as one, large network.
Domain Name System (DNS)	An Internet Engineering Task Force (IETF) standard for ASCII strings to represent IP addresses. The DNS is a distributed internal directory service used mostly to translate between domain names and IP addresses. Avaya 9600 Series IP Telephones can use DNS to resolve names into IP addresses. In DHCP, TFTP, and HTTP files, DNS names can be used whenever IP addresses are available as long as a valid DNS server is identified first.

Página2256 de 3226.

Dynamic Data Exchange (DDE)	An interprocess communication (IPC) method.
Dynamic Host Configuration Protocol (DHCP)	An Internet Engineering Task Force (IETF) protocol used to automate IP address allocation and management.
Ethernet Routing Switch (ERS)	The Avaya stackable chassis system that provides high-performance, convergence-ready, secure, and resilient Ethernet switching connectivity.
Expansion Interface	A port circuit pack in a port network (PN) that provides the interface between a time-division multiplex (TDM) bus or a packet bus on the PN and a fiber-optic link. Expansion interface (EI) carries circuit-switched data, packet-switched data, network control, timing control, and digital signal-1 (DS1) control. EI in an expansion port network (EPN) also communicates with the master maintenance circuit pack to provide the environmental status and the alarm status of the EPN to the switch processing element (SPE).
Expansion port network	In Intuity Audix Server configurations, a port network (PN) that is connected to the time-division multiplex (TDM) bus and the packet bus of a processor port network (PPN). Control is achieved by indirect connection of the EPN to the PPN by way of a port network link (PNL).
Extension to Cellular access number	The phone number dialed to connect to the Avaya server that is running Communication Manager. The Extension to Cellular access number initiates the process of enabling or disabling Extension to Cellular or changing the station security code.
Federal Communications Commission (FCC)	A United States federal agency that regulates communications such as wire-line communications and the Internet.
Global Technical Services	An Avaya team that answers customer calls about products in Avaya Integrated Management.
Internet Protocol	A connectionless protocol that operates at Layer 3 of the Open Systems Interconnect (OSI) model. Internet Protocol (IP) is used for Internet addressing and routing packets over multiple networks to a final destination. IP works in conjunction with Transmission Control Protocol (TCP), and is identified as TCP/IP.
Local Survivable Processor	A configuration of the S8300 media server in which the server acts as an alternate server or gatekeeper for IP entities such as IP telephones and G700 media gateways. These IP entities use the Local Survivable Processor (LSP) when the IP entities lose connectivity with the primary server.

Página2257 de 3226.

Media gateway	An application-enabling hardware element that is part of a family of such elements. This family includes intra-switch connectivity, control interfaces, port interfaces, and cabinets. Avaya media gateways support both bearer traffic and signaling traffic that is routed between packet-switched networks and circuit-switched networks to deliver data, voice, fax, and messaging capabilities. Media gateways provide protocol conversion, such as IP to ATM to TDM, conferencing, presence, such as on-hook or off-hook, connectivity to private networks and public networks, such as IP, ATM, TDM, and networking, such as QSIG, DCS, ISDN. Media gateways support optional form factors.
Network Address Port Translation	A network routing technique. Network Address Port Translation (NAPT) is used to access systems on the same subnet as an IP Office.
Network Routing Policy	An application for centrally managing SIP routing for Session Manager instances. A routing policy describes how a call is routed: where it comes from, where it's going, what its dial pattern is, what time of day it is routed, and its cost for a particular route.
Novell® eDirectory™	An X.500-compatible directory service software product initially released in 1993 by Novell® for centrally managing access to resources on multiple servers and computers within a given network. Novell® eDirectory™ was formerly known as Novell® Directory Services. It is sometimes referred to as Netware Directory Services. Novell® eDirectory™ is a hierarchical, object-oriented database used to represent certain assets in an organization in a logical tree, including people, positions, servers, workstations, applications, printers, services, and groups.
OFCOM	The United Kingdom Office of Communication for the regulation of telecommunications.
PARTNER® Contact Closure Adjunct	A device that is connected to the chassis of a media gateway and provides contact closures. Contact Closure Adjunct (CCA) closes a relay in response to a dial-in command from the media gateway to operate a door or perform a similar action.
Product Information Presentation System	The Product Information Presentation System (PIPS) reports provide data from the Product Information Expert (PIE), a data mining tool that extracts Avaya customer switch and adjunct configuration information and stores it in a database.
Product Licensing and Delivery System (PLDS)	The Avaya licensing and download website and management system. Avaya Business Partners and customers use this site to obtain ISO image files and other software downloads.
Public Switched Telephone Network (PSTN)	A telephone network that includes many communication technologies such as microwave transmission, satellites, and undersea cables.

Página2258 de 3226.

Remote Feature Activation	A Web-based Avaya application to remotely activate features and increase capacities on the system of a customer by delivering a new license file.
System Manager	A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity.
System Status Application	An IP Office application that shows the status of things such as outgoing calls.
Telecommuter	The configuration where Communication Manager establishes the voice connection to a circuit-switched telephone. Requires two connections: a TCP/IP connection for signaling control and a circuit-switched connection for voice.
Telephony Application Program Interface (TAPI)	A Microsoft® Windows API that enables computers running Windows to use telephony services. TAPI is used for data, FAX, and voice communications. Applications can use TAPI to control telephony functions, such as dial, answer, and hang up.
Telephony Service Provider Interface (TSPI)	A Microsoft-defined interface to the telephony service provider (TSP). Microsoft® Windows comes with an H.323 TSP, an IP conference TSP, a kernel-mode device driver TSP, and a unimodem TSP.

Página2259 de 3226.

Index

A

a-law PCM ... 31
application notes ... 134
application support ... 87
architecture ... 71
auto-create support for users and extensions in WebLM ... 117
Avaya Communicator ... 45
  iPad ... 46
  Windows ... 47
Avaya Contact Center Select
  Business Continuity ... 83
  deployment options ... 80–83
  DVD ... 80
  hardware appliance ... 82
  overview ... 65
  reference configurations ... 78
  topology ... 78, 80–83
  user data synchronization ... 78
  VMware ... 81
Avaya Equinox Meeting Online ... 55
Avaya Spaces overview ... 55

B

base cards ... 31
Basic Edition ... 67
BCM migration ... 100, 107
browser support ... 87

C

CA ... 61
Central Access ... 61
cloud operations manager ... 63
cloud overview ... 75
components ... 72
Computer Telephony Integration ... 27
conference calls ... 51
configuration of WebLM licensing ... 115
  warnings and alarms ... 116
contact center ... 64
control unit ... 29
CTI ... 27
customer-provided PC requirements ... 91

D

data networking ... 18
deployment options ... 67
  Avaya Contact Center Select ... 78, 80–83
  DVD ... 80, 83
deployment options *(continued)*
  hardware appliance ... 82
  VMware ... 81
DevConnect ... 134
DMM ... 64
document changes ... 7

E

Embedded Voicemail ... 50
endpoints ... 126
end user applications ... 40
Equinox for IP Office
  Equinox
    Avaya Equinox ... 42
Essential Edition ... 69
external expansion modules ... 35

F

feature keys ... 31
features ... 13
features overview ... 54

G

gatekeepers ... 22
gateways ... 22
guidelines
  WebRTC ... 38

H

H.323 ... 22
hardware options ... 84

I

InSite Knowledge Base ... 134
interfaces ... 105
interoperability ... 93, 99
IP500 V2 ... 29
iPad ... 46
IP endpoint licenses ... 126
IP endpoint licenses for WebLM ... 116
IP Office applications
  contact center applications ... 64
  installation and administration applications ... 55
  user applications ... 40
IP Office Contact Center
  deployment options ... 77
  topology ... 77

Página2260 de 3226.

ip office editions 10
IP telephony 19

L

License migration
ADI 110
licenses 109
Basic Edition 118
Branch 120
Essential Edition 118
IP endpoints 126
Preferred Edition 118
SCN 120
Server Edition 119
small community network 120
Standard Mode 118
trials 126
trunks 121
upgrades 106, 127
users 122

M

Manager 55
MCUs 22
media manager
overview 58
Meet-Me conferencing 52
Migration
roadmap and limitations 108
Multipoint Connection Units 22

N

new features 11

O

one-X Mobile Preferred 40
one-X Portal for IP Office 41
operating system support 87
options
deployment 73
overview 10, 64, 75
Avaya Contact Center Select 65
Avaya Equinox Meeting Online 55
Avaya Spaces 55
enterprise branch 73
IP Office 73

P

packet-based voice and data networking 18
PCM 31
phones 38
phones *(continued)*
compatibility 95
country availability 98
remote 39
PLDS licensing 109
ports 105
Preferred Edition 70
private circuit switched voice networking 14
product compatibility 133
public voice networking 15
pulse code modulation 31

R

Radvision 53
receptionist licenses for WebLM 117
reference configuration
IP Office Contact Center 77
reference configurations 67, 73
related documents 130
remote phones 39
resource websites 133

S

SCN licenses 120
Scopia 53
SD cards 31
security 101, 102
Server Edition 70
Centralized licensing 111
licenses 119
Nodal licensing 111
Server Edition Manager 56
Session Initiation Protocol 23
SIP 23, 25
SIP endpoint user agents 26
SMA 61
SNMP Management Console 61
SoftConsole 49
SoftConsole administration 61
software options 84
Solution Management Application 61
solution specification 85
specifications
port interfaces 105
SSA 62
Standard Mode 118
support 133
SysMonitor 63

T

telephones 38
topology 14, 71, 74
Avaya Contact Center Select 78, 80–83

Página2261 de 3226.

topology *(continued)*
BP-hosted 76
Business Continuity 83
DVD 80
hardware appliance 82
Partner Powered 76
VMware 81
training 131
trials 126
trunk cards 33
trunks
licenses 121

U

upgrade licenses 127
upgrades 106
user licenses 122
user licenses for WebLM 117

V

VCMs 22
Video Collaboration Solution 53
video conferencing 53
videos 132
virtual environment 93
virtual licenses 111
Voice Compression Modules 22
Voicemail Pro 50
voice networking 14, 15, 18

W

web client
ip office web client
webrtc 44
Web License Manager 110
WebLM 110
WebLM license modes 114
WebLM license mode state transitions 115
WebLM licensing
auto-create support for users and extensions 117
configuration 115
configuration warnings and alarms 116
IP endpoint licenses 116
license modes 114
license mode state transitions 115
receptionist licenses 117
user licenses 117
Web Manager 58
WebRTC 38

Página2262 de 3226.

Avaya IP Office™ Platform Solution Description

Release 11.0.4
May 2019

© 2018-2019, Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order with a default of one (1) Cluster if not stated. “Cluster” means a group of Servers and other resources that act as a single system.

Enterprise License (EN). End User may install and use each copy or an Instance of the Software only for enterprise-wide use of an unlimited number of Instances of the Software as indicated on the order or as authorized by Avaya in writing.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

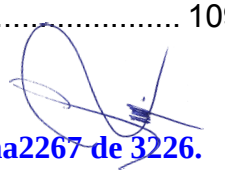
The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 7
Purpose 7
Change history 7
Chapter 2: Avaya IP Office™ Platform overview 10
IP Office editions 10
New in this release 11
Features 13
Topology 14
Networking 14
Private circuit switched voice networking 14
Public voice networking 15
Packet-based voice and data networking 18
Internet protocol telephony 19
Computer Telephony Integration 27
Components 29
Hardware components 29
Phones 38
IP Office applications 40
Chapter 3: Solution specifications 67
Reference configurations 67
IP Office editions 67
Other deployment options 73
Hardware and software options 84
Server specifications 85
Operating system and browser support 87
Customer-provided PC requirements 91
Virtual environment requirements 93
Interoperability 93
Phone interoperability 95
IP Office and Avaya Aura® Communication Manager interoperability 99
BCM and IP Office interoperability 100
Security specification 101
Platform and application security details 102
Port assignments 105
Typical upgrade paths 106
BCM with CS1000 to IP Office migration 107
IP Office Branch migration 108
Licenses 109
PLDS licensing 109



Página2267 de 3226.

Migration of ADI licenses 110
Server Edition Centralized and Nodal licensing 111
Basic Edition license for new systems 118
Essential Edition and Preferred Edition licenses 118
Server Edition licenses 119
Branch licenses 120
Small Community Network licenses 120
Trunk licenses 121
User licenses 122
IP endpoint licenses 126
Trial licenses 126
Upgrade licenses 127
Chapter 4: Resources 130
Documentation 130
Finding documents on the Avaya Support website 131
Training 131
Viewing Avaya Mentor videos 132
Additional IP Office resources 133
Product compatibility 133
Support 133
Using the Avaya InSite Knowledge Base 134
Accessing Avaya DevConnect Application Notes 134
Glossary list 136

Página2268 de 3226.

Chapter 1: Introduction

Purpose

This document describes IP Office from a holistic perspective focusing on the strategic, enterprise, and functional views of the architecture. This document also includes a high-level description of solution specifications and available reference configurations.

Change history

The following table describes major changes made in this document for each release.

Issue	Release date	Summary of changes
Release 11.0 FP4	February 2019	• Updated the What's new topic with the Release 11.0 FP4 features. • Updated Avaya Equinox™ topic to add content on Shared Control and Avaya Vantage™ support. • Updated Avaya one-X® Portal topic to add serviceability enhancements. • Updated the licensing information. • Updated the supported browsers section. • Updated Media Manager section to add new features supported in IP Office Release 11.0 FP4. • Listed VMWare ESXi 6.7 as a supported Hypervisor.

Table continues…

Página2269 de 3226.

Issue	Release date	Summary of changes
Release 11.0	May 2018	• Updated the What's new topic with the Release 11.0 features. • Removed references to IP Office Integrated Contact Reporter. • Removed references to IP Office Video SoftPhone as it is not supported in Release 11.0 • Added content about the following applications: - Cloud Operations Manager - Avaya Equinox™ client for IP Office - Avaya IP Office Web Client • Updated the Web Manager section to add content about Configuration Dashboard. • Updated Media Manager section to add new features supported in IP Office Release 11.0. • Added J169 and J179 phones to the phone interoperability and availability sections.
Release 10.1, Issue 1	June 2017	• Updated the "New in this release" section. • Added information about two new applications: IP Office Integrated Contact Reporter and IP Office Media Manager • Added information about additional hypervisor support in the "Virtual environment requirements" section • Added information about two new DECT phones: 3730 and 3735 • Added information about a new Management API/SDK, and two new CTI interfaces: Centralized CTI WebService API and SSI over Web Services • Added information about two new expansion modules: DS16B2 and DS30B2 • Added granular access information in the "Web Manager" section • Added extension information in the "System Status Application (SSA)" section • Updated the "Operating system and browser support" section

Table continues…

Página2270 de 3226.

Issue	Release date	Summary of changes
Release 10.0, Issue 1	July 2016	• Updated the “New in this release” section. • Replaced 3740 DECT handset references with 3745 DECT. • Updated Avaya Contact Center Select content. • Made the following major licensing updates: - Added more contextual information. - Updated license names and their associated codes. - Reorganized Server Edition licensing content. - Added Basic Edition licenses. - Clarified basic user license support.
Release 9.1, Issue 01.18	February 2016	This document was created to replace the *Avaya IP Office Product Description*.

Página2271 de 3226.

Chapter 2: Avaya IP Office™ Platform overview

The Avaya IP Office™ Platform is a cost-effective telephony system that supports a mobile, distributed workforce with voice and video on virtually any device. IP Office is an integrated, modular communications solution that scales up to 3000 extensions and 150 sites in a multisite network with resiliency. Match a deployment model to infrastructure needs from simple appliances to virtualized software in a data center with options in between. Improve customer experience and contact center agent efficiency with powerful, affordable multichannel functionality for voice, email and web chat. The solution combines collaboration software plus multichannel contact centers, networking, security and video.

IP Office provides a hybrid PBX with both Time Division Multiplexing (TDM) and IP telephony with trunk support, used in either mode or both concurrently. IP Office has data capabilities built-in, providing IP routing, switching and firewall protection, between LAN and WAN (LAN2).

In addition to basic telephony services and voicemail, IP Office offers both hard phone and soft phone options. Soft phone applications are designed to provide flexibility for remote workers and to allow workers to access telephony services, such as making and receiving calls, voicemail, and call forwarding from their computer or mobile device.

IP Office editions

IP Office also offers advanced features such as audio and video conferencing and voice over IP to meet the evolving needs of small, medium, and large enterprises.

IP Office is available in many deployment models based on the size of the enterprise and the features required using one or all the following elements:

- Virtualized IP Office software running in a virtual machine
- Dedicated server
- IP Office 500 V2 (IP500 V2) control unit

Página2272 de 3226.

Edition	Platform	Business size (users)	Addresses business needs
Basic Edition	IP500 V2	Less than 25	Simple telephony and messaging capabilities only
Essential Edition	IP500 V2	20–99	Simple telephony and messaging capabilities plus IP telephony with essential mobility
Preferred Edition	IP500 V2	21–250	Essential Edition capabilities plus unified communications with preferred mobility
Server Edition	Linux Server, IP500 V2 and Linux Expansion	100 — 2000	Preferred Edition on a software-based solution.
IP Office Select	Linux Server, IP500 V2 and Linux Expansion	100 — 3000	Preferred Edition on a software-based solution with increased scale and resiliency.
Server Edition or IP Office Select with Virtualized Software	Virtualized	100 — 2000 (or) 100 — 3000	Preferred Edition on a software-based solution with increased scale and resiliency.
Server Edition or IP Office Select hosted in Cloud	Cloud (Powered by Avaya)	100–2000 (or) 25–3000	Preferred Edition on a software-based solution with increased scale and resiliency.

IP Office Essential Edition and Preferred Edition are also referred to as IP Office Standard Mode. Each edition builds upon the next to offer additional functionality.

New in this release

IP Office™ Platform Release 11.0 Feature Pack 4 offers the following new features and capabilities:

Note:

Features are available worldwide unless otherwise specified. Not all features are supported on all platforms and phones. See the descriptions for details.

Fallback twinning

With this feature, IP Office redirects calls to the users twinned mobile number when the primary extensions are unreachable even if mobile twinning is disabled. This feature provides a mechanism for failing over to an external device such as mobile and PSTN if a customer site supporting IP Office phones, loses connectivity with the Cloud data center. The following two short codes are available for disabling and enabling mobile Fallback twinning:

- **Set Fallback Twinning Off**: To disable Fallback twinning

Página2273 de 3226.

- **Set Fallback Twinning On**: To enable Fallback twinning

IP Office Media Manager enhancements

The following features have been added to IP Office Media Manager:

- Delete recordings
- Audit trail: Administrators can keep track of the usage of recording files in IP Office Media Manager. The following type of usage of a recording can be tracked using this feature:
  - Delete
  - Download
  - Replay
  - Search

Security enhancements for registration of SIP devices

The new security enhancements enable administrators to allow or disallow registration of SIP devices in IP Office based on their User Agent strings. Administrators can use the configuration settings to add, modify, or remove SIP User Agent strings to SIP UA Blacklist, SIP UA Whitelist, and IP Whitelist. Subsequently, the **Allowed SIP User Agents** setting can be used to select which SIP User Agents are allowed for registering with IP Office.

Automatic user synchronization with Avaya Spaces

IP Office R 11.0 FP4 system users and user details created for Avaya Equinox™ can be automatically synchronized with Avaya Spaces server. To use and receive additional Avaya Spaces features, the details of users configured for Avaya Equinox™ need matching users configured on the Avaya Spaces server. The synchronization can be done manually or automatically.

Default extension password

The default extension password or PIN is different than the user password and is much stronger with a minimum of nine digits. IP Office R11.0 FP4 deployments provide for an auto-generated default extension PIN of 10 digits, which can be viewed and modified later. An eye icon next to the **Default Extension Password** field in the user interface can be used to view the existing default extension password.

Avaya Equinox™ support on Avaya Vantage™

Avaya Equinox™ is supported on Avaya Vantage™ phones K165 and K175 in IP Office R 11.0 FP4 deployments.

Route incoming SIP trunk calls based on an optional SIP header

IP Office can be configured to use the optional **P-Called-Party** header in incoming SIP message for call routing. IP Office reads the `P-Called-Party ID` header in the SIP message and routes the incoming SIP calls based on it.

SIP and H.323 Registrars disabled by default

To secure IP Office R 11.0 FP4 from vulnerabilities, the **H.323 Gatekeeper Enable** and **SIP Registrar Enable** fields are disabled by default. Whenever a new H.323 or SIP extension is added and the corresponding registrar is not enabled, IP Office system displays an error message and prompts to enable the fields. When resiliency support is enabled on an IP Office Line in systems having IP extensions and the systems do not have the corresponding registrars enabled,

Página2274 de 3226.

IP Office system displays an error message and prompts administrators to enable the corresponding registrars.

Avaya Equinox™ shared control

Avaya Equinox™ can now be used in shared control mode with desk phones. The shared control feature is available even when the Avaya Equinox™ client and desk phones are registered on different systems within the same network.

Conference Join

Conference Join feature allows two separate conferences to be joined into one single conference that contains all the previous participants of both the earlier conferences. Once the conferences have been joined it is not possible to revert to the two separate conferences again.

JEM 24 button module support on Avaya J169/J179 IP Phone

Avaya J169/J179 IP Phone can support up to three JEM24 button modules. Each JEM24 has 24 dual-LED buttons with adjacent button label display. The button LEDs are used to indicate the status of the button feature whilst pressing the button is used to access the feature. A single JEM24 supports 72 programmable button slots. These are arranged in 3-pages, with pages accessed using the module's page scroll button. When multiple modules are connected to a phone, each module only supports a single page of 24 programmable button slots.

The modules automatically match the display settings of the phone to which they are connected - color with Avaya J179 IP Phone or greyscale with Avaya J169 IP Phone, font size, background image, screen saver. The button modules are powered though the phone. For more information, see the *IP Office Platform R11.0 J100 Series Telephone User Guide*.

Avaya J139 IP Phone

IP Office support for Avaya J139 IP Phone. Avaya J139 IP Phone is an advanced SIP desk phone that supports IP Office interactive menus and button programming. Avaya J139 IP Phone does not support all the advanced knowledge worker and contact center features that are available in Avaya J169 IP Phone and Avaya J179 IP Phone phones. For more information, see the *IP Office Platform R11.0 J100 Series Telephone User Guide*.

Serviceability enhancements in Avaya one-X® Portal

Avaya one-X® Portal supports a number of serviceability features such as displaying count of logged-in sessions, user avatar, option to block client versions, option to track repeated failed login attempts, and option to clear all sessions of a user.

Simplified Web Self-Administration

The enhanced interface is focused on simplifying the configuration and make it easier for non-technical users and provides a three step self-guided wizard for setting up the basic account. By default the new capability, that is running the wizard, is enabled for all users but the administrator can disable the capability or modify as required.

Features

See *Avaya IP Office™ Platform Feature Description* for detailed feature descriptions.

Página2275 de 3226.

Topology

There are many options for IP Office topology. For detailed information about all the deployment scenarios, see the related *Reference Configuration* documents for each deployment scenario.

Figure 1: IP Office systems connected to a single IP Office Manager endpoint

Networking

Private circuit switched voice networking

Where leased line circuits are used within a private networking scenario, these E1 or T1 interfaces are typically configured to use Q.SIG signaling between sites.

Q.SIG provides a level of voice feature transparency between PBXs and is the favored signaling standard within multiple vendor and international voice networks. The IP Office E1 or T1 module terminates a QSIG connection with a 120 ohm RJ45 interface.

Página2276 de 3226.

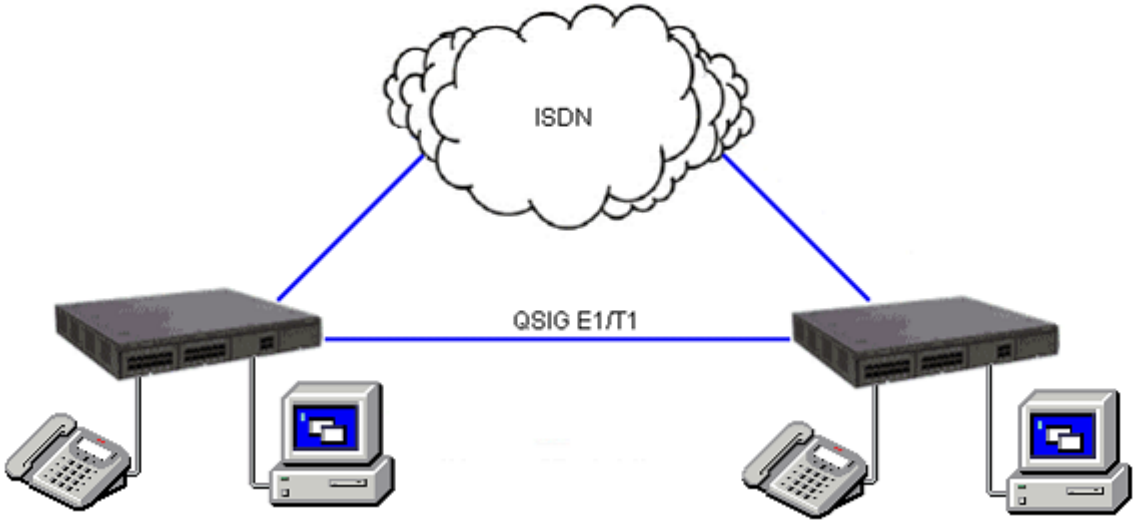


Figure 2: Circuit switched voice networking

IP Office supports the following Q.SIG services across this network:

Simple Telephony Call/Basic Call	ETS300 171/172
Circuit Switched Data Call/Basic Call	ETS300 171/172
Called/Calling Line ID Presentation	ETS300 173
Called/Calling Name Presentation	(SS-CNIP, SS-CONP, SS-CNIR) ETS300 237/238
Message Waiting	(SS-MWI) EN301 260/255
Transfer	(SS-CT) ETS 300 260/261

Public voice networking

IP Office supports a range of trunks and signaling modes for connection to the public switched telephone network (Central Office). Some of these lines are only available in certain territories; please check with your distributor for local availability. Primary rate trunks are available with either a single (24/30 channels) or dual trunk (48/60 channels).

ISDN Primary Rate (ETSI CTR4)

Service is provided by IP500V2 Universal PRI cards. ISDN Primary Rate provides 30 x 64K PCM speech channels over an E1 circuit and one signaling channel. Signaling Conforms to the ETSI Q. 931 standard with Cyclic Redundancy error Checking (CRC).

The following supplementary services are supported:

Página2277 de 3226.

Calling Line Identification Presentation (CLIP)	Provides the telephone number of the incoming call.
Calling Line Identification Restriction (CLIR)	Prevents the telephone number of the IP Office being presented on an outbound call.
Direct Dialing In (DDI)	Where the exchange provides the last x digits of the dialed number on an incoming call. This allows IP Office to route the call to different users or services.
Sub-addressing	Allows the transmission/reception of up to 20 digits, additional to any DDI/DID or CLIP information, for call routing and identification purposes.

IP Office supports the following features on both PRI and BRI trunks.

Note:

Feature availability depends on the ISDN service provider for which there may be charges.

Malicious Call Identification (MCID)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600) Short codes and button programming features are available so that users can trigger this activity at the ISDN exchange when required. This feature is NOT available on standard ISDN DSS1 telephones.
Advice of Charge (AOC)	(T3 digital and IP telephones only; Phone Manager) Advice of charge during a call (AOC-D) and at the end of a call (AOC-E) is supported for outgoing ISDN calls other than Q.SIG. The call cost is displayable on T3 telephones for call accounting purposes. IP Office allows configuration of call cost currency and a call cost mark-up for each user.
Call Completion to Busy Subscriber (CCBS)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, DECT telephones; Phone Manager) CCBS can be used where provided by the ISDN service provider. It allows a callback to be set on external ISDN calls that return busy. It can also be used by incoming ISDN calls to a busy user. This feature is not available on standard ISDN DSS1 telephones.
Partial Rerouting (PR)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, DECT telephones; Phone Manager) When forwarding a call on an ISDN channel to an external number using another ISDN channel, partial rerouting informs the ISDN exchange to perform the forward, thus freeing the channels to IP Office. This feature is not available on standard ISDN DSS1 telephones and it is not supported on Q.SIG.

Página2278 de 3226.

Explicit Call Transfer (ECT)	(Typically used by a third-party application) ECT is supported on the S0 interface. A Call to an S0 Endpoint can be transferred to any other device such as an analog, digital or IP endpoint or to any trunk. The normal usage of this feature is by a third party application connected through one or more S0 interfaces to IP Office. One example is the VoiceDirector, an automatic call assistant.

ISDN Basic Rate (ETSI CTR3)

Service is provided by IP500 V2 BRI cards. ISDN Basic Rate provides 2 x 64K PCM speech channels and one signaling channel using Q.931 signaling and CRC error checking. Both point to point and point to multipoint operation is supported. Multipoint lines allow multiple devices to share the same line; however point-to-point is the preferred mode.

Basic Rate supports all the services that are supported on the primary rate version with the addition of Multiple Subscriber Number. This service is usually mutually exclusive with the DDI/DID service and provides up to 10 numbers for routing purposes, very similar to DDI/DID.

E1R2 channel associated signaling

Service is provided by IP500 V2 Universal PRI cards.

The IP500 Universal PRI card configured as PRI E1R2 supports a single or dual RJ45 network connection. Each card provides channels that can be configured for MFC, Pulse or DTMF dialing dependent on the requirements of the network.

North American T1 Primary Rate

Service is provided by IP500 V2 Universal PRI cards. T1 Primary Rate provides up to 24 64K channels over a 1.54M circuit. Each channel of the T1 trunk can be independently configured (channelized) to support the following signaling emulations with handshake types of immediate, delay or wink.

- Loop-Start
- Ground-Start
- E&M Tie Line
- E&M DID
- E&M Switched 56K
- DID - Channels configured for DID/DDI support incoming calls only. The carrier or Central Office will provide the last x digits that were dialed to be used for call routing.
- Wink-Start

IP Office T1 trunks support both DNIS and ANI services, where available from the central office.

Dialed Number Identification String (DNIS)	Provides a string of digits to IP Office depending on the number dialed by the incoming caller. This string can then be used to route callers to individual extensions, groups or services.
Automatic Number Identification (ANI)	Provides IP Office with a number identifying who the caller is. This may then be used for routing or computer telephony applications.

T1 trunk cards incorporate an integral CSU/DSU, eliminating the need for an external unit. The CSU function allows the trunk to be put in loop-back mode for testing purposes. This can be set

Página2279 de 3226.

manually, using the monitor application, or automatically from a Central Office sending a Line Loop Back (LLB) pattern. The DSU function allows the T1 trunk to be shared between data and voice services.

North American Primary Rate Interface (PRI)

Service is provided by the IP500V2 Universal PRI cards. IP Office supports Primary Rate ISDN trunks on 5ESS or DMS100 central office switches provided by AT&T, Sprint, WorldCom and other Local Telcos. Channels can be pre-configured for the supported services or negotiated on a call-by-call basis.

Special services can be configured to route calls to local operators or pre-subscribed carriers for both national and international calls (SSS). Alternate carriers can also be selected through the configuration of IP Office Transit Network Selection (TNS) tables.

IP Office also supports the Calling Name and Number service over Primary Rate Trunks (NI2).

Analog trunks

Loop start	Loop start trunks are available on the IP Office Analog Trunk cards installed within the IP Office control unit, or on the Analog Trunk 16-port expansion modules (ATM16). The first two trunks on the ATM16 are automatically switched to power fail sockets in the event of power being interrupted. Powerfail is also available on the trunk card when fitted to a combination or phone card. They conform to the TIA/EIA-646-B standard. The loop start trunks also support incoming caller line identification (ICLID) conforming to GR-188-CORE and GR-31-CORE standards. IP Office can use this information to route calls or provide it to computer applications to display additional information about the caller.
Ground start	Ground Start trunks are only available on the ATM16, configured through IP Office Manager. The first two trunks on the module are automatically switched to power fail socket in the event of power being interrupted. They conform to ANSI T1.401 and TIA/EIA-646-B standards. Not available in all territories.

Packet-based voice and data networking

IP Office supports data network use for voice communication, called voice over IP (VoIP).

IP Office supports networked voice and data communications with the following services:

- Built-in IP router
- One link for voice and data networking
- Common access to the Internet; share files and send e-mails to other sites
- Support for RIP-2 protocol for dynamic data routing; IPSec VPN, firewall and NAT (Network Address Translation) and for security; Centralized management and proactive fault management via SNMP.

IP Office supports IP packet-based voice networking between sites through VoIP across the campus LAN or VoIP across the public network.

Página2280 de 3226.

In a factory or campus environment, voice calls can sent over 10/100 Mbps LAN connections on systems equipped with optional Voice Compression Modules (VCM). IP Office supports Diffserve by appropriately marking both RTP packets and signalling packets to facilitate network bandwidth management.

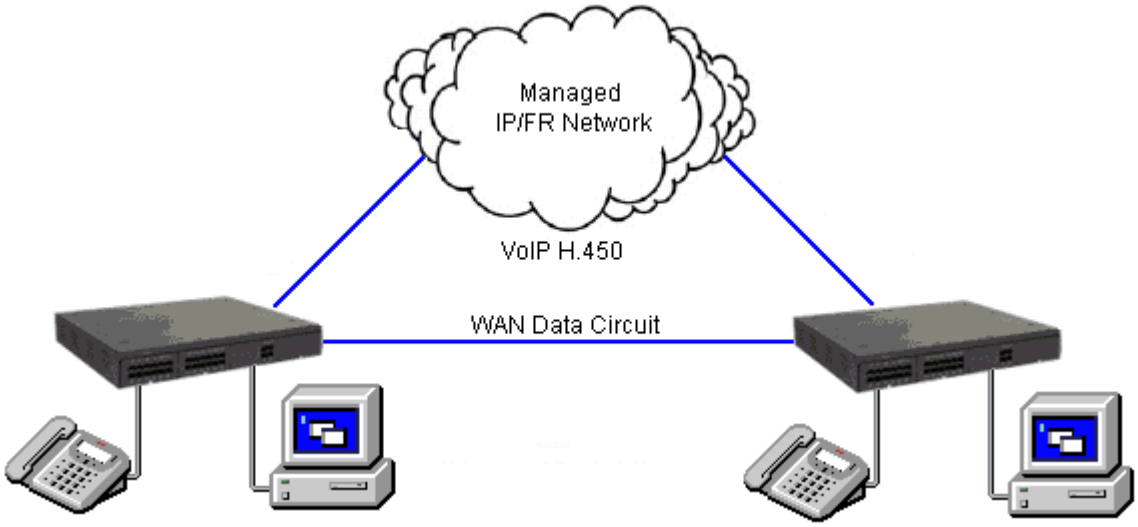


Figure 3: VoIP networking across IP network or WAN

IP Office can realize the benefits of Q.931 and H.450 supplementary service support across a public connection where an appropriate QoS connection can be established.

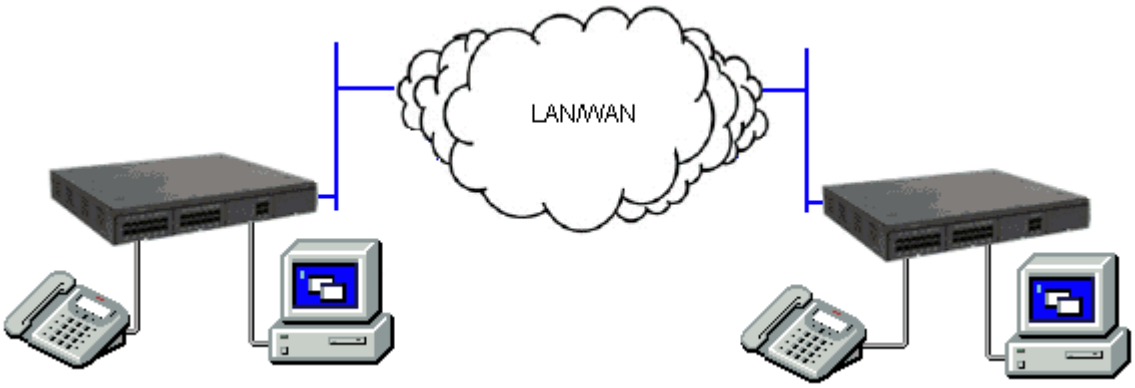


Figure 4: VoIP networking across the LAN

Internet protocol telephony

Internet Protocol (IP) refers to the type of rules that the network uses to send and receive signals. IP telephony converts voice communications into data packets. Conveniently, it runs on Ethernet LAN (local area network) technology. IP telephony unites a company's many locations, including mobile workers, into a single converged communications network.

IP Office is a converged telephony system; it combines aspects of traditional PABX telephony systems and IP data and telephony systems. IP Office supports PSTN, SIP, POTs, digital time

Página2281 de 3226.

division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist.

IP Office connects to the PSTN and to IP trunks providing a “hybrid” PABX function - where both legacy and future technologies can be used together to minimize operating costs and optimize business communications through both voice and data. The converged functionality works on multiple levels:

- Individual phone users can control the operation of their phone through applications running on their PC.
- Data traffic can be routed from the LAN interface to a telephony trunk interface.
- Voice traffic can be routed across internal and external data links. This option is referred to as voice over IP (VoIP).

Voice over IP (VoIP) and network assessments

Voice over IP (VoIP) means voice transmitted over a packet data network. VoIP is often referred to as IP telephony because it uses the internet protocols to make possible enhanced voice communications wherever IP connections exist.

The VoIP mode of operation can include external SIP trunks, IP trunks between customer systems and/or H.323 or SIP IP telephones for users. In either case the following factors must be considered:

- The IP Office control unit must be fitted with voice compression channels. These are used whenever an IP device (trunk or extension) needs to communicate with a non-IP device (trunk or extension) or to a device that uses a different codec.
- A network assessment is a mandatory requirement for all systems using VoIP. For support issues with VoIP, Avaya may request access to the network assessment results and may refuse support if those are not available or satisfactory.

A network assessment would include a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies, and setting voice quality objectives.
- The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support H.323, DHCP, TFTP and jitter buffers in H.323 applications.

An outline of the expected network assessment targets is:

Test	Minimum assessment target
Latency	Less than 150 ms
Packet loss	Less than 3%
Duration	Monitor statistics once every minute for a full week

Signaling protocols

In order to make use of VoIP, IP Office uses signaling protocols called H.323 and Session Initiation Protocol (SIP), to establish end-to-end connections for the voice path through an IP network. This

Página2282 de 3226.

connection ensures that each end is able to transmit and receive voice and provides the network addressing for end-to-end packet transmission. IP Office also connects the different technologies by translating the signals they use. For example an analog telephone can connect to a VoIP destination. This connection requires both the signaling and voice transmission to be translated. IP Office makes this translation using gateways and gatekeepers.

With IP telephony you connect an IP telephone to an IP PBX through a LAN. There are two basic types of IP telephones:

- A physical telephone, which looks very similar to a standard telephone, referred to as a “hardphone”
- A software application, referred to as a “softphone”, which runs on the user’s PC, allowing them to use a headset and microphone to make and receive calls anywhere they an and IP connection.

Quality of Service considerations

When making use of IP telephony, there are a number of data centric considerations such as which data types have priority on the IP network when there is contention. This is set with IP/TCP quality of service and should not be ignored. In situations where LAN bandwidth is limited, a quality of service capable LAN switch should be used to ensure voice packets are transmitted with the required priority on the network. If not, the conversation carried over IP appears as broken up due to delays or has unacceptable delays introduced in the conversation causing latency and jitter. With IP hardphones there is the need for Power over Ethernet (PoE), or local phone power supplies to be provided to the telephones as the IP telephones are not powered by IP Office.

Voice compression channels

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. IP Office systems use voice compression channels to make the conversion. These channels support the common IP audio codecs G.711, G.723 and G.729a.

The System Status Application can be used to display voice compression channel usage. Within the **Resources** section it displays the number of channel in use. It also displays how often there have been insufficient channels available and the last time such an event occurred.

Table 1: Voice compression channels

Call type	Voice compression channel usage
IP device to non-IP device	Requires a voice compression channel for the duration of the call. If no channel is available, busy indication is returned to the caller.

Table continues…

Página2283 de 3226.

Call type	Voice compression channel usage
IP device to IP device	Call progress tones (for example dial tone, secondary dial tone, etc) do not require voice compression channels with the following exceptions: • Short code confirmation, ARS camp on and account code entry tones require a voice compression channel. • Devices using G723 require a voice compression channel for all tones except call waiting. When a call is connected: • If the IP devices use the same audio codec no voice compression channel is used. • If the devices use differing audio codecs, a voice compression channel is required for each.
Non-IP device to non-IP device	No voice compression channels are required.
Music on hold played to IP device	Provided from the TDM bus and therefore requires a voice compression channel when played to an IP device.
Conference resources and IP devices	Managed by the conference chip which is on the TDM bus. Therefore, a voice compression channel is required for each IP device involved in a conference. This includes services that use conference resources such as call listen, intrusion, call recording and silent monitoring
Page call to IP device	Uses G729a for page calls, therefore only requiring one channel but also only supporting pages to G729a capable devices.
Voicemail services and IP devices	Treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.
Fax calls	These are voice calls but with a slightly wider frequency range than spoken voice calls. IP Office only supports fax across IP between IP Office systems with the Fax transport option selected. It does not currently support T38.
T38 fax calls	IP Office supports T38 fax on SIP trunks and SIP extensions. Each T38 fax call uses a VCM channel. Within a Small Community Network, a T38 fax call can be converted to a call across an H323 SCN lines using the IP Office Fax Transport Support protocol. This conversion uses 2 VCM channels. In order use T38 Fax connection, the Equipment Classification of an analog extension connected to a fax machine can be set Fax Machine. Additionally, a new short code feature Dial Fax is available.

Note:

T3 IP devices must be configured to 20 ms packet size for the above conditions to apply. If left configured for 10 ms packet size, a voice compression channel is needed for all tones and for non-direct media calls.

H.323 signaling protocol

IP Office IP telephony systems use open standards. Digital IP telephones, gateways and gatekeepers support the H.323 standard and it is this that allows devices from different

Página2284 de 3226.

manufacturers to work together. IP Office also supports an optional integral gateway, Voice Compression Modules (VCMs) and gatekeeper functionality.

IP Office uses the H.323 signaling protocol using the following architectural components:

IP telephones	H.323 service endpoint devices that support audio calls. Other types of H.323 devices can support video as part of H.323.
Gateways	Provide media translation to allow calls to be made to non-H.323 devices, for instance an analog telephone or the public network to connect with a H.323 device.
Gatekeepers	Control the call processing and security for H.323 devices.
Multipoint Connection Units (MCUs)	Control conferences by adding together media streams.

These elements form an H.323 zone which is analogous to a PABX. Each zone has a single gatekeeper to control call distribution, call control and the resource management. On power-up, IP telephones, gateways and MCUs make registration requests to a gatekeeper which then authenticates (accepts or rejects) the request to become a member of the zone. Once accepted, a telephone wishing to make a call sends a call set-up message to the gatekeeper which then determines how to route the call and will then send an alert to the called telephone, or if the call is to a non-H.323 telephone establish the call via a Gateway within the zone.

Session Initiation Protocol trunking

IP Office uses Session Initiation Protocol (SIP) trunks to allow users to take advantage of telephony services offered by internet service providers (ISPs). In many cases, telephony services offer substantial savings in comparison to traditional exchange lines. To help enable the SIP Service Provider, Avaya offers a SIP Compliance Testing Program (GSSCP) that will validate the operation of IP Office with the ISPs SIP trunk offering. For more information about Avaya's SIP Compliance Testing Program (GSSCP), see https://www.devconnectprogram.com/site/global/compliance_testing/overview/index.gsp.

IP Office allows all users, regardless of their phone type, to make and receive SIP calls. SIP trunks are handled like any other line on IP Office, affording all the call routing and toll control needed to manage inbound and outbound calls.

SIP trunks require provisioning of voice compression channels through the installation of VCM modules within the control unit. A license for the maximum required number of simultaneous SIP calls is also needed. Up to 128 simultaneous calls are supported.

IP Office also supports the T38 protocol which allows Fax over IP.

There are several possible network topologies for SIP trunk systems, as shown in the following diagrams:

Página2285 de 3226.

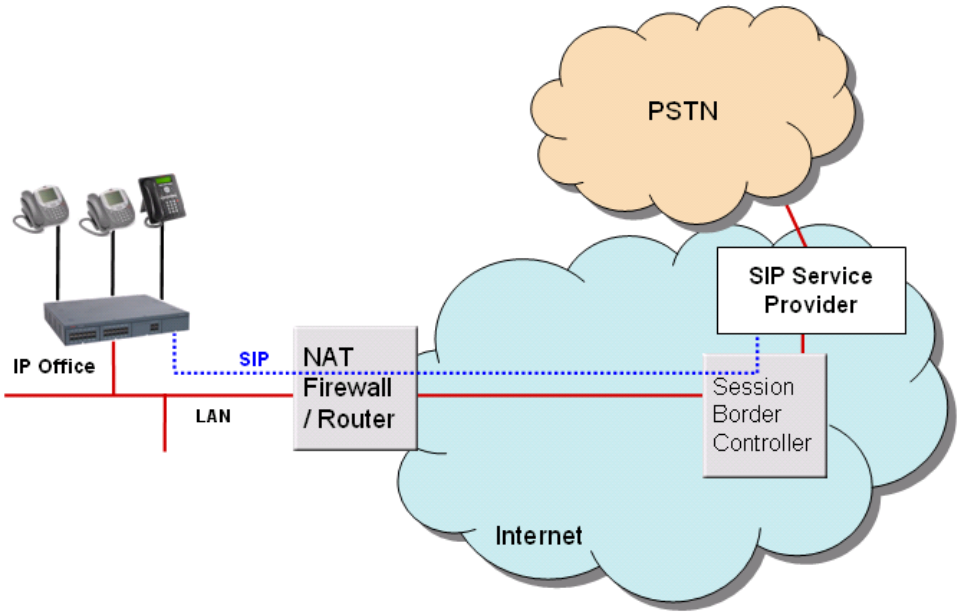


Figure 5: Service provider with Avaya Session Border Controller for Enterprise (recommended)

To make this configuration secure, the IP Office firewall is set to drop all packets except SIP.

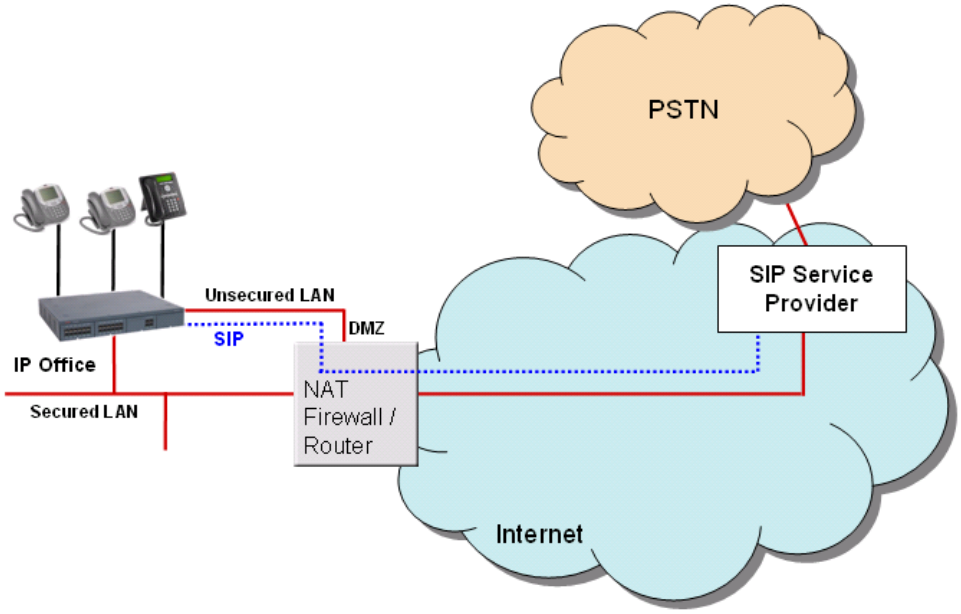


Figure 6: Direct connection from the second Ethernet port to the internet through a DMZ port on the router

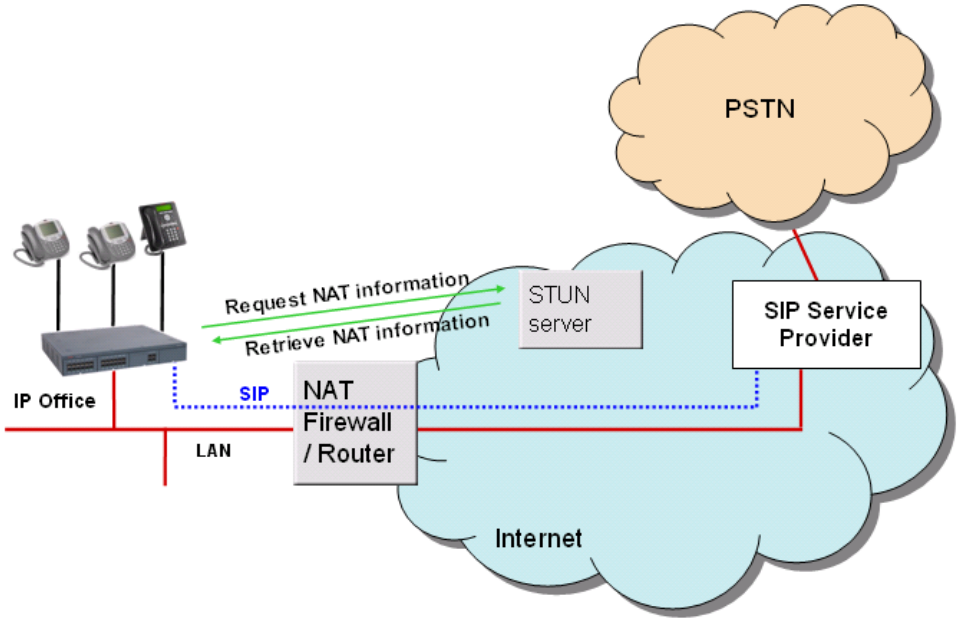


Figure 7: Connection to ITSP over NAT using third-party STUN servers

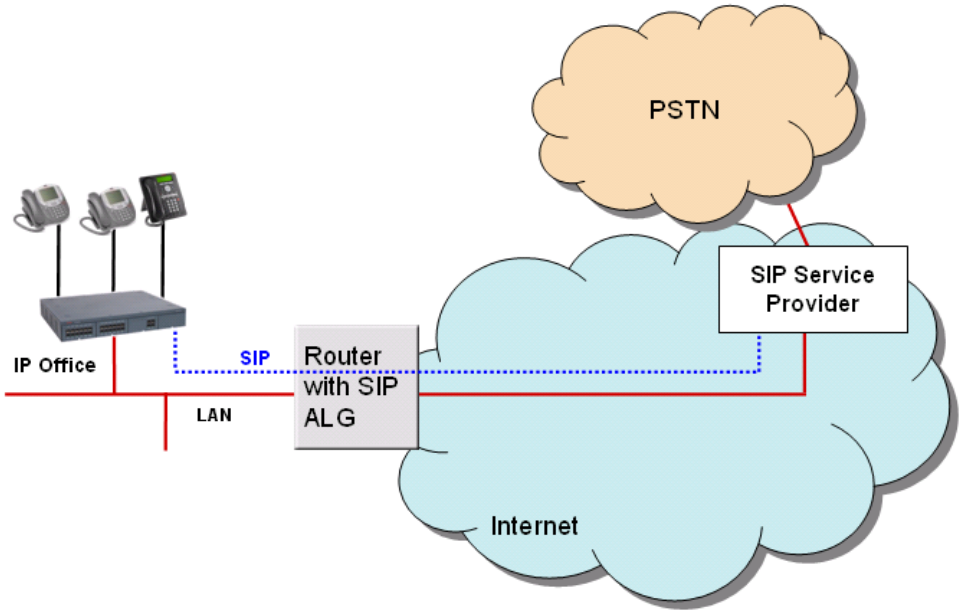


Figure 8: Connection to ITSP through router with ALG to resolves NAT issues

SIP servers

IP Office SIP endpoint implementation is built on two major SIP components: SIP server components SIP endpoint user agent applications.

SIP servers provide SIP endpoint support to allow full interoperability between SIP endpoints, other IP telephones based on H.323, digital and analog telephones as well as IP Office trunks (analog, digital or SIP-based).

Página2287 de 3226.

SIP servers provide centralized information and enablement services in a SIP ecosystem. The core SIP servers and their functions are summarized here. IP Office provides the features of the following two servers for voice and fax communication.

- **Registrar server**

  When SIP IP telephones come online, they need to make sure that others are aware that they're available to take and make calls. The Registrar authenticates and registers the IP phone (often directly related to a specific user) when it comes online, and then stores information on the telephones logical identities.

- **Proxy server**

  A proxy server takes SIP requests, processes them, and passes them downstream while sending responses upstream to other SIP servers or devices. A proxy server may act as both a server and a client, and can modify a SIP request before passing it along. A proxy is involved only in the setup and teardown of a communication session. After user agents establish a session, communications occur directly between the parties.

Functionality of the following two SIP servers are generally available by IP Office using existing IP Office functionality. Therefore, while functionality is provided, for example, allowing hot desking in a small community network, a consistent methodology between SIP and non-SIP endpoints is used to deliver those features

- **Location service**

  As users roam, the network needs to be continually aware of their locations. The location service is a database that keeps track of users and their locations. The location service gets its input from the registrar server and provides key information to the proxy and redirect servers. IP Office provides hot desking support, delivering a similar functionality but working consistently between SIP and non SIP endpoints.

- **Redirect server**

  If users are not in their home domains, sessions bound for them needs to be redirected to them.

  The redirect server maps a SIP request destined for a user to the device closest to the user. In IP Office, call forwarding and Follow me functionality is used to provide again consistent functionality between all type of endpoints.

SIP endpoint user agents

SIP endpoints, such as SIP telephones, cell phones, PDAs, or workstations, use user agent (UA) applications to provide the interface between the users and the SIP network.

SIP endpoint support is fully integrated into IP Office. No other components are needed. SIP endpoints require VCM module capacity like any other IP phone.

SIP extensions function like any other IP Office extension. IP Office provides the following functionality:

- Make and receive calls to any other extension, independent of type of extension.

Página2288 de 3226.

- Deliver end-to-end media. During calls between two SIP extensions or a SIP extension and an Avaya IP telephone, IP Office transmits audio end-to-end for basic telephone calls. Conferencing requires a VCM resource.
- Use short codes and authorization codes.
- Transmit in band call progress tones.
- Register endpoint using authentication with username and password.
- Support Auto-create. Successful endpoint registration uses a third-party license.
- Several extensions can register on one IP address, each using a license. This enables the connection of SIP terminal adapters with more than one analog port, giving a different extension number to each port.

Computer Telephony Integration

Computer Telephony Integration (CTI) bridges the gap between the telephone system and business applications. With IP Office, this is achieved with the IP Office CTI Link, a CTI middleware product and software developers kit (SDK).

On IP Office, CTI is delivered through adherence to open standards. This gives businesses access to a wide range of third-party solutions, addressing vertical markets, and designed to meet their requirements. For developers, migrating their offering from other platforms to IP Office is quick and easy, and the advanced CTI features that IP Office offers makes it easy to demonstrate full integration, and more business benefits.

IP Office provides two levels of CTI interoperability:

CTI Link Lite Free of charge and provides all the functionality required to support the vast majority of applications, including screen-popping, and many third-party products.

CTI Link Pro Provides enhanced functionality, including the ability to control multiple telephones and gives access to advanced call center operation.

Because IP networking is integrated into the IP Office system, all CTI is done through the LAN. This introduces additional points of failure, as well as relying on non-standard interfaces and handsets. On IP Office, all devices can be used with CTI.

Supported CTI interfaces

IP Office supports the following interfaces:

TAPILink Lite Provides first-party CTI support for Microsoft TAPI 2.1 and TAPI 3.0, so each PC can control or monitor one telephone. The software components are supplied with the IP Office system on the User CD, and do not required a license key for use. The specification requires that a certain amount of core functionality is implemented, and additionally defines a series of optional functionality that switch vendors may also implemented.

Página2289 de 3226.

TAPILink Pro	Provides third-party CTI support for TAPI 2.1 and 3.0. These components are identical to their first-party equivalent; the presence of the CTI Link Pro RFA license key (which can be purchased in the usual way for products) enables this additional functionality. TAPILink Pro provides all of the features and functionality of TAPILink Lite, but additionally provides third party CTI operation. This means that a single server can control and monitor any number of telephone devices. In addition, TAPILink Pro provides the ability to monitor and control groups. This allows an application to be notified when a call enters a queue, and can also redirect it to another location.
TAPI-WAV driver	Provides software-based support for voice processing. The TAPI-WAV driver is for use with TAPI 2.1 only; for TAPI 3.0, IP Office supports the Media Service Provider (MSP) interface, defined by Microsoft in TAPI 3.0. This functionality will only work in conjunction with CTI Link Pro and also requires TAPI-WAV licenses. Each license enables 4 ports of voice processing.
DevLink Pro	Provides a real-time event stream in addition to the SMDR interface provided in IP Office SMDR. The real-time event stream takes the form of a call record, which is issued whenever the state of any endpoint of a call changes (typically there are two end points on a call, but for some circumstances, such as conference calls, intruded calls there may be more).
IP Office SMDR	Provides an interface to obtain SMDR events. A comma-separated record is issued for each call, when the call is completed. This interface is designed for call accounting and call billing applications. The IP Office SMDR can be output direct from the IP Office control unit to a designated IP address and port.
IP Office Software Development Kit	This toolkit is delivered on a single CD, containing the developer documentation for TAPILink Lite, TAPILink Pro, DevLink Lite and DevLink pro, as well as pre-compiled programs for exploring TAPI 2.1 and 3.0. In addition, example source code is included, making it easy for developers to become familiar with IP Office CTI interfaces. The Developer Connection Program (DevConnect) is the Avaya developer partner program, and is designed for third-party companies who are creating a product for sale, and who wish to receive technical support. Membership of the program is at the sole discretion of Avaya. DevConnect members pay an annual fee, for which they receive technical support directly from Avaya. In addition, Avaya will perform interoperability testing between IP Office and the member's product, and may also create opportunities for joint marketing, including exhibitions, use of Avaya's logo, and other benefits. More information on the DevConnect program can be found at http://www.devconnectprogram.com.
Centralized CTI WebService API	Provides a more open platform to allow third-parties to add value and build out solutions. Supports distributed (SE/SCN) environment and, therefore, is not limited to nodal like TAPI. It does have a dependency on Avaya one-X® Portal access for the users. When creating a new user in IP Office, it does not require a restart.

Página2290 de 3226.

SSI over Web Services	Provides system monitoring information of SSI over a read-only REST web service available over https only. Realtime call data and call control are not available via this interface, but they will be made available via the DevConnect program. This feature already has several areas instrumented but the data is for SSA and delivered over the Proprietary SSI interface, and there is a small set of data available on SNMP. It does not require a license.

Open APIs/SDKs

With Release 10.1, IP Office supports a new Management API/SDK to address the needs of “Easy Button” setups. Enhancements to cover more areas, specifically what the legacy "XO" Configuration Web Services covers so that the legacy API can be made End Of Life. Management API provides a REST-based API Interface to the third-party application developers for consuming IP Office configuration objects.

- Provides all capabilities of currently supported IP Office configuration services (XO services).
- Request and response are in XML and JSON format.
- Provides Read/Write access to privileged service users only.
- No separate license is required for accessing the APIs.

Components

Hardware components

IP Office control unit

IP Office control unit (IP500 V2) is a stackable unit with an optional 19" rack mounting kit and an optional wall mounting kit for smaller configurations.

The IP500 V2 control unit is compatible with all IP500 base extension and Voice Compression Module (VCM) cards as well as all external IP500 expansion modules.

The IP500 V2 control unit has 4 slots for the insertion of IP500 base cards. The slots are numbered 1 to 4 from left to right. Normally they can be used in any order, however if the capacity for a particular type of card is exceeded, the card in the rightmost slot will be disabled. Each base card includes an integral front panel with ports for cable connections. Typically the first 8 ports on the left are for connection of extension devices. The 4 ports on the left are used for connection of trunks if a trunk daughter card is added to the base card.

The control unit provides the following functionality:

Página2291 de 3226.

Maximum extensions	Up to 384 extensions.
Conference parties	128 as standard but maximum 64 in any individual conference. Silence suppression is applied to conferences with more than 10 parties.
Trunk cards	Up to 4. Any combination of trunk daughter cards.
Voice compression channels	Up to 148 channels using up to VCM and combination cards.
Voicemail channels	Up to 250 voicemail/recording channels supported on the Primary server. For Select deployments, the Secondary server can also support up to 250 voicemail/recording channels.
Locales	Supported in the following countries: Argentina, Australia, Bahrain, Belgium, Brazil, Canada, Chile, China, Colombia, Customize, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Italy, Japan, Korea, Kuwait, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Norway, Oman, Pakistan, Peru, Poland, Portugal, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, United Kingdom, United States, Venezuela.
Power supply	Internal power supply unit.
Mounting	Free-standing, rack mounted or wall mounted (requires mounting kits).
Memory	Maximum configuration file size: 2048 KB.

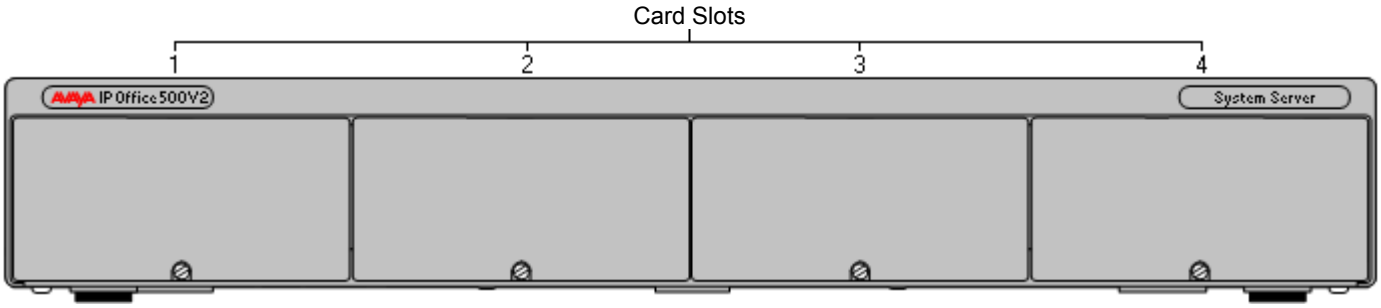


Figure 9: IP500 V2 front view

Página2292 de 3226.

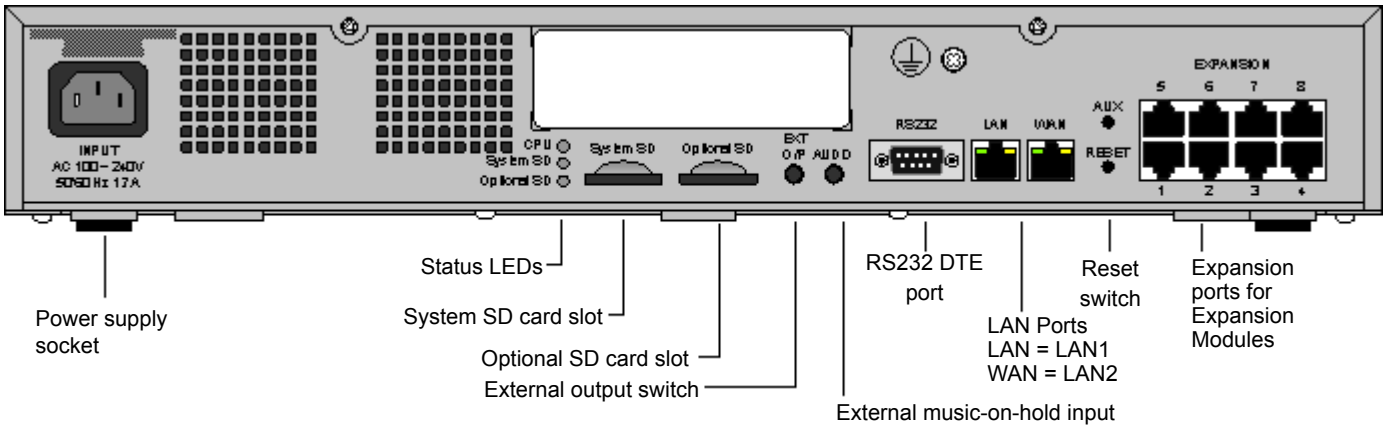


Figure 10: IP500 V2 rear view

Feature keys

The serial number of the feature key SD card fitted to the IP Office control unit is used as the basis for all licenses issued for that IP Office system and is used to regularly validate the licenses. If the feature key SD card is removed, over the next few hours licensed features will stop operating.

Pulse code modulation encoding

Pulse code modulation (PCM) is a method for encoding voice as data. In telephony, two methods PCM encoding are widely used, a-law and µ-law (also called mu-law or u-law). Typically µ-law is used in North America and a few other locations while a-law by the rest of the world. As well as setting the correct PCM encoding for the region, the a-law or µ-law setting of IP Office when it is first started affects a wide range of regional defaults relating to line settings and other values.

Base cards

The following base cards are available:

Table 2: IP500 V2 base cards

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
Digital Station (DS8)	3	Ports 1–8: Digital stations With trunk card: Ports 9–12: Central Office lines	Selected Avaya 2400, 5400 and 9500 series phones T3 phones (EMEA only) 3810 wireless phones (North America only) **Note:** 4400 series phones are not supported on this card. They are supported on external expansion module DS ports. 4100, 7400, M series and T series phones use the TCM8 Digital Station card.

Table continues…

Página2293 de 3226.

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
Analog Phone 2	4	Ports 1–2: Analog stations With trunk card: Ports 9–12: Trunk connections	Analog phones
Analog Phone 8	4	Ports 1–8: Analog stations With trunk card: Ports 9–12: Trunk connections	Analog phones
Digital Station (TCM8)	4	Ports 1–8: BST digital stations With trunk card: Ports 9–12: Central Office lines	Norstar®/BCM phones BST series phones Global M series phones Digital Mobility Controllers (DMCs) 7406e Wireless Telephones Digital Audio Conferencing Unit
Voice Compression Module (VCM V2)	2	Ports 1–8: Not present With trunk card: Ports 9–12: Central Office lines	VoIP calls including IP extensions or IP trunks. Up to 128 voice compression channels depending on the codec used. The IP500V2 control unit supports up to 148 voice compression channels, using the card plus voice compression ports on the Combination card.
ATM Combination (ATM V2)	2	Ports 1–6: Digital stations Ports 7–8: Analog stations Ports 9–12: Central Office lines 10 voice compression channels. Codec support is G.711, G729a and G.723 with 64ms echo cancellation. G.722 is supported by release 8.0 and higher.	Avaya digital phones except 3800 and 4400 series phones Analog phones Preinstalled trunk cards

Table continues…

Página2294 de 3226.

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
BRI Combination	2	Ports 1–6: Digital stations Ports 7–8: Analog stations Ports 9–10: BRI trunk ports (4 BRI channels) 10 voice compression channels. Codec support is G.711, G729a and G.723 with 64ms echo cancellation. G.722 is supported by IP Office Release 8.0 and higher.	Avaya digital phones except 3800 and 4400 series phones (DS type not TCM) Analog phones Preinstalled trunk cards
Unified Communications Module (UCM V2)	1		Requires separate Preferred Edition license. Not supported on Server Edition. More than 200 users when running Voicemail Pro only. Up to 200 users when running Voicemail Pro and Avaya one-X® Portal for IP Office. 50 simultaneous Avaya one-X® Portal for IP Office users. No trunk cards
ETR6	3	Ports 1–6: ETR stations With ATM4: Ports 7–8: Power Failure Transfer Ports 9–12: Central Office lines	Not supported on Server Edition. PARTNER ACS phone ATM4, PRI/T1, or PARTNER mode μ-law SD cards (North America only)

Trunk cards

Trunk cards can be fitted to existing base cards to provide support for trunk ports. The trunk card uses the ports provided on the base card for cable connection. Each trunk card comes with spacer pegs for installation and port identification labels.

Note:

These cards are used for PSTN/FXS gateways with IP Office for Linux.

Página2295 de 3226.

Tip:

In systems with both Analog Phone 8 base cards and analog trunk cards, combining the two types are recommended because it provides analog power failure support for one trunk per extension (not applicable to the Analog Phone 2 base card).

Table 3: IP500 V2 trunk cards

Trunk card	Maximum per system	Works with these base cards	Description
Analog (V2)	4	ETR6 DS8 TCM8 Analog Phone 2/8	4 analog loop start trunks V.32 modem for remote access 1 power failure extension to trunk connection on Phone 8 cards

Table continues…

Página2296 de 3226.

Trunk card	Maximum per system	Works with these base cards	Description
Universal PRI (PRI-U)	4	ETR6 DS8 TCM8 Analog Phone 2/8 VCM	Up to 2 PRI trunk connections. The card is available in single and dual port variants. The card can be configured for E1 PRI, T1 robbed bit, T1 PRI or E1R2 PRI trunks. Supports primary rate digital trunks. On each card, 8 channels per interface are enabled by default. This means that the single PRI has 8 channels enabled, while the dual PRI has 8 channels enabled on each of the two circuits. Further channels may be enabled by the purchase of additional licenses in 2-channel or 8-channel increments. Available in single and dual version. The single variant can support up to 24 T1 channels or up to 30 E1 channels. The dual variant can support up to 48 T1 channels or 60 E1 channels. Configurable for T1, E1, E1R2 MFC use, depending on territory. Includes an integrated CSU/DSU: • CSU allows trunks to be put into loop-back mode for testing purposes. This can be set manually, using the monitor application, or automatically from a Central Office sending a Line Loop Back (LLB) pattern. • DSU allows the T1 trunk to be shared between data and voice services. Includes diagnostics capabilities: visual indicators to show service state and physical test points to monitor traffic. Supports mobility features: Mobile Call Control and one-X Mobile clients
BRI (Euro ISDN)	4	DS8 TCM8 Analog Phone 2/8 VCM	Up to 4 BRI trunk connections, each trunk providing 2B+D digital channels. Available in 2 (4 channels) and 4 (8 channels) options. Supports mobility features: Mobile Call Control and one-X Mobile clients.

External expansion modules

External expansion modules can be used with the IP500 V2 control unit.

Página2297 de 3226.

Analog phone expansion modules

On analog ports, call information is sent while the phone is ringing, and cannot be updated during a call or set on an outbound call (the phone may do a local match but this is not controlled by IP Office). The primary purpose of displays is to give information about incoming calls. Where the caller display standard chosen supports the delivery of text (extension name) as well as the number, both are delivered.

An analog extension port can be set for external paging operation. It does not operate like a normal extension and is connected to external equipment through an isolation device (can also be used as an MoH source). The port will always be busy so it cannot be called directly and can only be accessed by using a paging feature. When not receiving a page, the port will remain silent. When being paged, the page tone is sent before the speech path is opened.

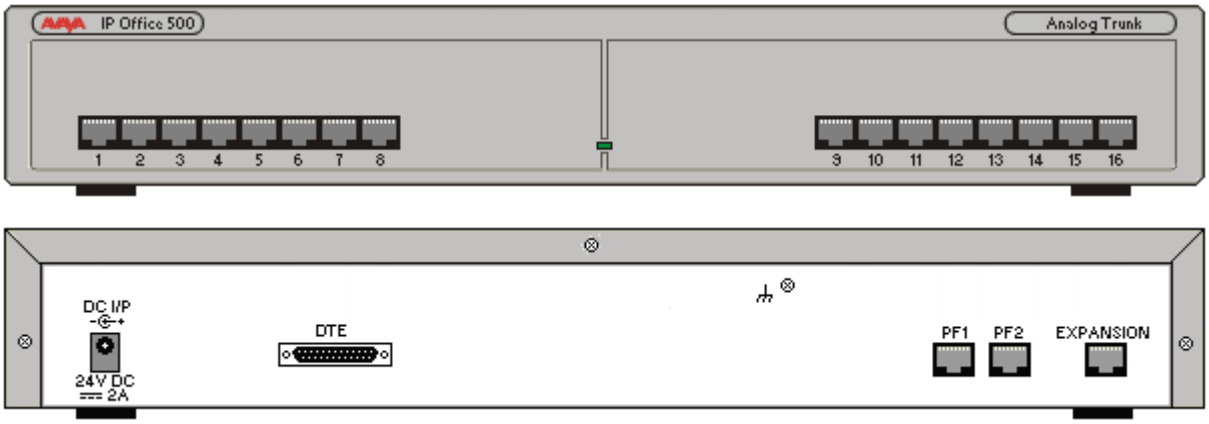
For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.

Expansion module	Telephones supported	Interfaces supported
Analog Phone 16	16 analog stations with calling line presentation	DTMF signaling (No rotary or Loop Disconnect) Time Break Recall (No Earth Recall) Message Waiting Indication (MWI): 51V Stepped, 81V, 101V and Line Reversal and Bellcore FSK
Analog Phone 30	30 analog stations with calling line presentation	

Analog trunk modules

This type of module can be used to add 16 additional analog trunks to an IP500 V2 system. The module supports both loop-start and ground-start trunks. The module also provides two powerfail ports for direct connection of analog phones to the first two analog trunks.

Basic Edition systems only support a single ATM16 expansion module. For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.

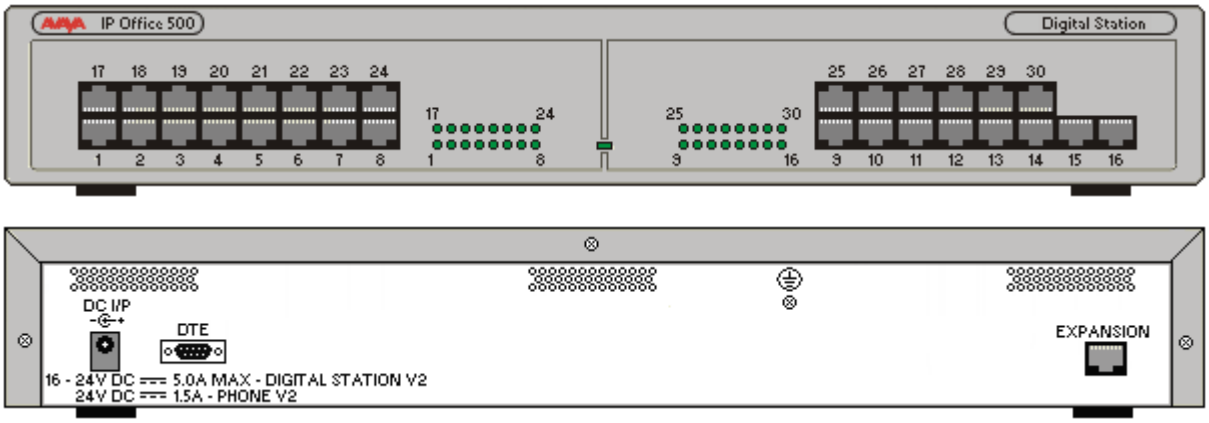


Expansion module	Description	Interfaces supported
ATM16	16 analog trunks	Loop-start Ground start

Página2298 de 3226.

Digital station expansion modules

For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.



Expansion module	Telephones supported	Description
DS16A	Norstar®/BCM telephones	16 digital station ports
DS30A	BST series telephones Global M series telephones Digital Mobility Controllers (DMCs) 7406e Wireless Telephones Digital Audio Conferencing Unit	30 digital station ports
DS16B, DS16B2[1]	Avaya telephones	16 digital station ports
DS30B, DS30B2[1]	Either DS or TCM mode supporting the telephones connected to either the DS8 or the TCM8 cards.	30 digital station ports

Application server

The IP Office Application Server provides reliability, scalability and processing power for larger scale IP Office deployments. It is an external, rack mounted server that provides scalability for larger installations and multisite deployments not currently supported with the Unified Communications Module (UCM V2).

The IP Office Application Server is a single installation of selected IP Office™ Platform applications running on Linux. The Linux operating system is included as part of the installation. However, installation requires minimal Linux knowledge due to the inclusion of a web based management interface to allow the server to be managed remotely via web browser.

[1] DS16B2 and DS30B2 are supported on 10.1, 9.1 SP 12, and 10.0 SP5 onwards.

Página2299 de 3226.

The IP Office Application Server hosts the following applications:

- Management Services
- one-X Portal for IP Office
- Voicemail Pro
- Web License Manager (WebLM)
- Web Manager
- Optional Services
  - Media Manager
  - Web Collaboration
  - WebRTC Gateway

WebRTC gateway configuration guidelines

Use the following guidelines when configuring a WebRTC gateway:

- Define WebRTC SIP extensions on the:
  - SIP server that is part of the WebRTC gateway configuration.
  - Primary server if this is part of the deployment topology.
- With IP500 V2 deployments, WebRTC should be enabled on the Application server.

Gateway limitations

The WebRTC gateway does not support resiliency.

Avaya Session Border Controller for Enterprise

An session border controller acts a router between the enterprise and carrier service, allowing only authorized sessions to pass through the connection point (border). The Avaya Session Border Controller for Enterprise (SBCE) delivers security to a SIP-based Unified Communications network.

For information on the SBCE, see *Avaya Session Border Controller for Enterprise Overview and Specification*.

For information on deploying the SBCE with IP Office, see “Configuring the Avaya Session Border Controller for IP Office Remote Workers” in either

- *Administering Avaya IP Office™ Platform with Web Manager*
- *Administering Avaya IP Office™ Platform with Manager*

Phones

IP Office supports multiple telephone solutions:

- IP telephones

Página2300 de 3226.

- Digital telephones
- ETR telephones
- Analog telephones
- Wireless telephones
- Third-party SIP endpoints such as, desktop telephones, softphones and conferencing speakerphones

For detailed specifications, see specific telephone information on the Avaya Support site at http://support.avaya.com.

Related links

Remote phone support on page 39
Accessing Avaya DevConnect Application Notes on page 134
Using the Avaya InSite Knowledge Base on page 134
Phone interoperability on page 95

Remote phone support

IP phones using NAT router

IP Office supports remote 9600 Series IP phones with the H.323 FW which resides behind a NAT router to IP Office. The configuration does not require any VPN concentrator equipment. Remote 9600 H.323 IP phones can connect to IP Office even if it is located behind a NAT router. The phones are authenticated in the same way as phones in the private network. IP Office determines that a phone is located outside the private network and relays the VOIP RTP traffic to ensure it transverses the NAT router.

Note:

H.323 signaling and the media traffic is not encrypted.

To reach IP Office from the remote private network, remote H.323 IP phones need to be configured to the public IP address of the NAT router hosting the IP Office. Configurable ports need to be forwarded to IP Office. IP Office requires a valid public IP address be configured and the public IP address can be statically configured or dynamically discovered via a STUN server. The Remote Worker feature requires the Essential Edition license which provides 4 remote worker seats. Enable the Remote Worker feature using IP Office Manager. Additional remote worker capability is available with the Teleworker User or Power User licenses and a Preferred Edition license.

VPN phones

VPN phones provide secure communication over public ISP networks to IP Office at the company headquarters. It is a software-only product that runs on 5610/5620/5621 or 4610/21 IP phones. In combination with one of these phones and the most popular VPN gateway products, the software extends enterprise telephony to remote locations. VPN functionality is supported on 9600 IP phones, and does not require a separate software load. VPN phone has been tested with a number of VPN-gateways from major vendors like Cisco or Juniper as well as with smaller VPN-access devices from companies like Adtran, Kentrox, Netgear, and SonicWall. Refer to the Avaya Support website for a list of available application notes on VPN-gateways tested with each line of phones.

Página2301 de 3226.

SIP phones using Avaya SBCE

The Avaya Session Border Controller for Enterprise (Avaya SBCE) sits on the edge of customer's network with both internal and external IP interfaces. Using these IP interfaces, Avaya SBCE functions as the gateway for SIP traffic into and out of the network. When used internally, SIP clients register to the IP Office directly. When used externally, the SIP clients connect to the Avaya SBCE. This is achieved using Split DNS, which automatically resolves the FQDNs to the internal IP address of the IP Office or the public IP address of the Avaya SBCE depending on where the clients are currently located. Apart from acting as a gateway, Avaya SBCE also provides protection against any external SIP-based attacks. For privacy over the public internet, the public side of the Avaya SBCE facing the remote workers must be configured to use the recommended values of TLS for signaling and SRTP for media encryption, as long as they are supported by the endpoints.

IP Office applications

User applications

The following sections provide an overview of the applications intended for end users.

Avaya one-X® Mobile

Avaya one-X® Mobile is an application that mobile users use to connect to IP Office.

Avaya one-X® Mobile works in call-back telephony mode. For example, when a user initiates a call from the client, IP Office initiates a call to the caller's mobile device and then dials the destination. This mode offers cost savings to users in countries where incoming voice calls are free or for users who have a cheaper unlimited voice plan as compared with a data plan.

The one-X Mobile Preferred mobility client also works in Voice over IP (VoIP) mode. In the VoIP mode, the client makes calls over Wi-Fi/3G/4G data networks. The client, using its underlying SIP stack, registers with IP Office over the data network and functions as an office extension.

Users in countries where incoming calls are charged will see a significant cost savings in the VoIP mode especially when on Wi-Fi networks. The availability of both call-back and VoIP modes on the mobility client will enable users to toggle between the modes based on their network connections. This will empower end-users to make a choice of the appropriate mode based on their voice and data plan as well as the availability and quality of their data connection (WiFi/3G/4G). For example,

- The user can choose the call-back mode when he or she doesn't have Wi-Fi access and the 3G data connection is not providing good quality for voice.
- The user can choose the VoIP mode when he or she has access to a mobile hotspot where a Wi-Fi data connection is available or when the 3G or 4G data connection is good.

One one-X Mobile Preferred mobility client supports VoIP mode on both iOS and Android devices. VoIP mode is available with the Power User profile. Users with Mobile Worker profiles can only

Página2302 de 3226.

use call-back mode. VoIP mode does not require an IP endpoint license. The following features are available:

- Ring-tone selection
- High bandwidth or narrowband codec selection based on the network connection available
- Bluetooth headset audio control on VoIP calls
- Conference screen
- Contact phone number selection
- Voicemail priority indicator
- Swipe support for instant messaging on home screen
- Group action support
- Emoticons
- CLID lookup in contacts for calls
- Send voicemail as WAV in email
- Enable or disable mobile twinning (simultaneous ring)
- Enable or disable DND (send all calls)
- Call log combined with voicemails in the event history
- Call monitoring to see and interact with all calls
- VoIP mode dial plan
- Transfer calls as a third-party call controller (3PCC)

Avaya one-X® Portal for IP Office

Avaya one-X® Portal for IP Office provides users control of their telephone from a networked PC. Use this application with any extension; analog, digital or any IP telephone, wired or wireless, that is available as part of the Office Worker, Power User or Teleworker user licenses.

Avaya one-X® Portal for IP Office is a server-based application that the user accesses via web browser.

For Telecommuter mode, One-X applications require answer supervision and disconnect detection for proper functioning. As a result, the one-X applications will not work with trunks that do not support answer supervision and disconnect detection.

Note:

one-X applications function on trunk types such as PRI, BRI, and SIP, however, they will not function on E1R2, T1 RBS and analog loop start trunks.

System administrators can control if Avaya one-X® Portal for IP Office can be accessed over a secure protocol only, recommended for hosted deployments to provide “secure only” access. The other option is to allow users to access the client over a secure and unsecure protocol (HTTP/HTTPS). The client application forces users to change their passwords and voicemail passcodes to meet the complexity settings configured by the administrator.

Página2303 de 3226.

Through gadgets, Avaya one-X® Portal for IP Office provides the following features:

- Call information
- Call and conference control
- Presence and instant messaging notifications, monitoring and archiving
- Contact import and export
- XMPP groups displayed in the **System Directory** tab
- Dial to user's own bridge and invite other users to join
- Conference call and other meeting scheduling including port reservations, email support and automatic report creation — available within the Outlook interface
- One-click web conferencing hosting and single sign-on joining web conferences as a participant

Avaya Equinox™ for IP Office

Avaya Equinox™ for IP Office is a SIP-based Unified Communications (UC) client that provides users with real time collaboration capabilities and enables business users to easily manage their day-to-day communications from a single interface. IP Office supports the following operating systems:

- Desktop:
  - Windows
  - macOS
- Mobile phone:
  - Android: From a mobile phone, tablet, or an Avaya Vantage™ device
  - iOS

Note:

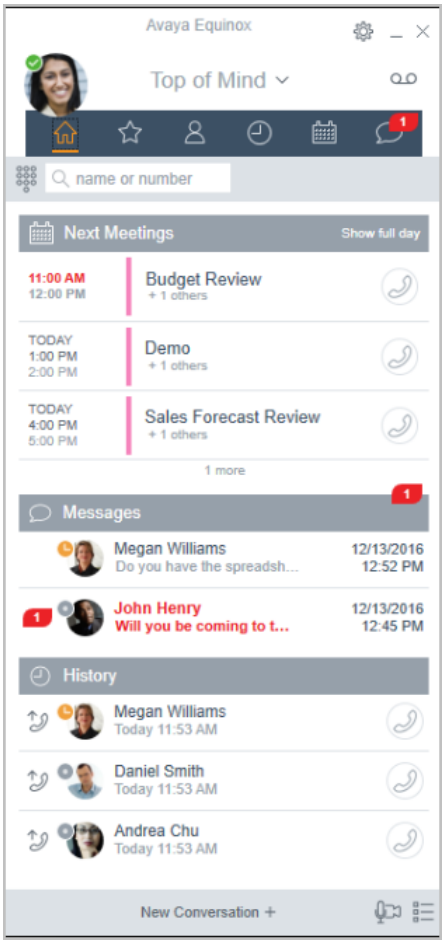
In Avaya Vantage™ Release 2.0.1, the K165 and K175 devices support the Avaya Equinox™ client. The K155 device does not support the Avaya Equinox™ client.

Avaya Equinox™ is a common cross-platform client. The client capabilities vary depending on the platform it is registered with. The supported features in Avaya Equinox™ for IP Office are:

- Top of Mind Home Screen
  - Next meetings showing local calendar schedule or Exchange Web Service/Office 365
  - Local Call History
  - Messages
  - Start Meetings/Launch Spaces dashboard
- Top of Mind Lite Option for Mobile phones
- IP Office directory and local contacts
- Messaging through Avaya Spaces

Página2304 de 3226.

- Presence through IP Office server
- Local call history
- Dialpad with Redial
- Desktop integration with Microsoft Outlook and Browsers
- Softphone client audio and video calls
- Shared control of an associated IP Office deskphone.



Avaya Equinox™ registers with IP Office server as a SIP softphone for audio and video calling, and telephony features. The following features are supported:

- Point to point audio and video calls (make, receive, and end)
- Multiple call handling (incoming and outgoing)
- Hold and retrieve (audio and video calls)
- Transfer (blind and consultative)
- Consult conferencing
- Escalate audio to video call
- Share control with supported desk phones in the Avaya Equinox™ desktop client

Página2305 de 3226.

- Avaya Equinox™ on Avaya Vantage™
- Presence and directory integration with Avaya Equinox™ on Avaya Vantage™
- Enter DTMFs during a call

Avaya Equinox™ client on Avaya Vantage™ supports the following features:

- Making outgoing calls.
- Handling incoming calls.
- Putting call on hold and resuming the call.
- Muting and unmuting a call.
- Transferring a call.
- Escalating an audio call to video call and de-escalating video call to audio call.
- Entering DTMF digits using the keypad.
- Access your local contacts
- Access your IP Office contacts by using IP Office directory.
- Manage your presence status and presence status messages.

Avaya Equinox™ for IP Office limitations:

- CTI Control — Avaya Equinox™ for IP Office cannot be controlled through other applications such as Avaya Contact Center Select, IP Office Contact Center, or IP Office SoftConsole.
- Branch worker — Avaya Equinox™ for IP Office does not support failover between Avaya Aura® core and IP Office Branch.
- For Instant Messaging, Avaya Equinox™ for IP Office depends on the availability of Avaya Spacesbasic account in the Cloud.
- The Avaya Equinox™ client accesses Avaya Equinox® Meetings Online using HTTPS, from within the Equinox Meetings tab of the client. The Avaya Equinox™ client can access local on-premise Equinox Conferencing in the same way using HTTPS, that is, if the access URL is configured under Equinox Meetings. However, if the Avaya Equinox™ client accesses local on-premise Equinox Conferencing through SIP trunks, audio and video will be available but not sharing or conference roster. The same applies for accessing Scopia over SIP trunks too. Even when Avaya Equinox™ client accesses local on-premise IP Office Meet Me Conferencing, audio will be available but not sharing or conference roster.

Avaya IP Office Web Client

Avaya IP Office Web Client is a WebRTC application that provides various communication capabilities. The client takes advantage of WebRTC Gateway resiliency improvements delivered in R11.0 and is supported on Server Edition and IP500 V2. Users must have Office Worker or Power User license to use the Avaya IP Office Web Client features. The client is supported in the following environments:

- Google Chrome browsers on Windows OS
- Google Chrome browsers on macOS
- Standalone client on Windows OS

Página2306 de 3226.

Avaya IP Office Web Client provides the following features:

- Point to point audio and video calls
- Access to Voicemail access
- Call logs
- Conferencing:
  - Ad-hoc Conference by merging calls
  - Starting or joining an IP Office Meet Me Conference
  - Accessing IP Office Web Collaboration
- Point-to-point Instant Messaging and Presence by integrating with Avaya one-X® Portal for IP Office
- Click-to-call using Google Chrome extension
- Single-Sign-On (SSO) support for Avaya one-X® Portal for IP Office and IP Office Web Collaboration
- System Directory and Favorites (Personal Directory)

Avaya Communicator

Avaya Communicator is a collaboration software client that delivers an innovative interface for real time communications for Windows and on the iPad. It enables users to handle phone calls, instant messages, conferencing, web collaboration, presence, enterprise contacts and e-mail, all from a single interface. Avaya Communicator delivers the intuitive graphic design of spotlights, media menu, notification bar, and contact cards.

Avaya Communicator for IP Office communicates with both IP Office and Avaya one-X® Portal to provide communication and collaboration features. Telephony features such as make/receive calls, hold/unhold, mute/unmute, DTMF, MWI etc. are provided by IP500 V2 and UC features such as IM, presence, and enterprise contacts are provided by the Avaya one-X® Portal server.

If Avaya one-X® Portal server is unavailable, either due to licensing restriction or connectivity issues, the Avaya Communicator client will work in a telephony-only mode providing only telephony features. Interoperability with Avaya Session Border Controller for Enterprise allows the Flare Communicator client to be used by users with the Remote Worker profile and register with IP Office without requiring a VPN connection.

Avaya Communicator provides the following features:

- Add participants using dial-pad or drag and drop
- Mute and unmute all or a subset of participants
- Lock and unlock the conference
- Place conference in lecture mode
- Enable and disable entry and exit tones
- Drop all or some participants from the conference
- End the conference

Página2307 de 3226.

- Enable and disable continuation to allow the conference continue after the moderator drops
- Promote participants to moderator
- Create ad-hoc conferences by merging P2P calls
- Authorization and account codes (Windows only)
- Hold timeout reminder (Windows only)
- Compact user experience
- TSL/SRTP support
- Contact filtering
- Web conferencing integration
- Unsupervised transfer
- Auto-answer
- Simultaneous mode
- Password change
- Account codes
- Auto configuration (iOS only)
- Bluetooth and headset device support and selection (iOS only)
- Interoperability with Scopia (Radvision XT5000)

Note:

Avaya Communicator does not support recording and active speaker indicator.

Avaya Communicator for iPad

Avaya Communicator for iPad integrates voice, video, presence, instant messaging, directories into one unified interface over Wi-Fi or 3G cellular and VPN connections.

Avaya Communicator is a software-only solution that can be easily downloaded from the Apple iTunes Store supporting iPad2, iPad3, iPad4, iPad Mini (with and without retina display), iPad Air both Wi-Fi and 3G models and the following iOS versions: 6.1.x, 7.0.x, 7.1.x, and 8.0.x.

Note:

Avaya Communicator is not supported on iOS 6.0.x.

With Avaya Communicator, IP Office users can use iPad devices for:

- Easy access to the real-time communications tools they rely on every day (phone, presence, IM, etc.)
- Blending real-time communications and business processes, such as mobile sales
- Taking advantage of Wi-Fi and 3G connectivity for cost-saving VoIP
- Secure signaling over TLS and secure media exchange over SRTP in cloud environments

Página2308 de 3226.

- As a web conferencing moderator, the ability to share white board and documents
- Changing passwords
- Auto-answer support
- Unsupervised transfers
- Auto configuration services using a configuration profile hosted on a web server by email address or URL
- Bluetooth and headset device support and selection
- System directory search
- Add/delete members from a team (XMPP Group)
- Search the system directory and add to a team or personal contact
- Radvision XT5000 support for point-to-point video calls

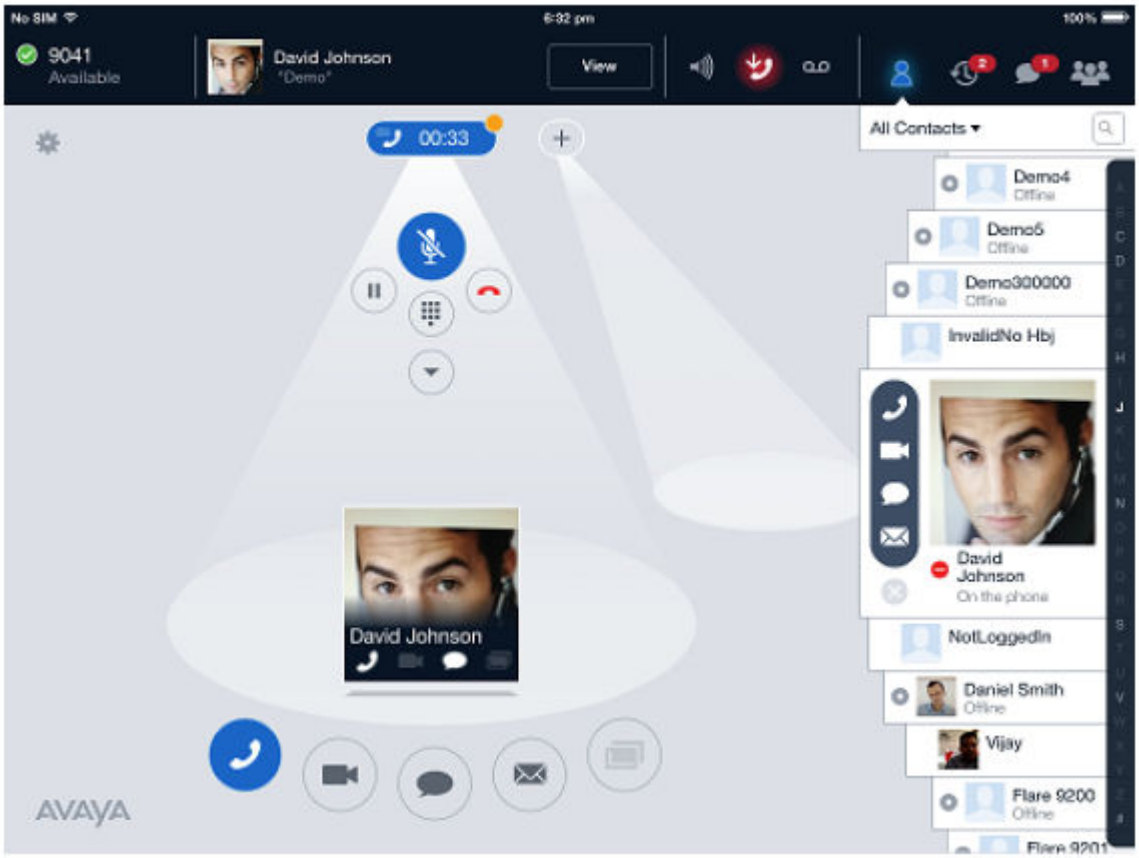


Figure 11: Avaya Communicator for iPad

Avaya Communicator for Windows

Avaya Communicator for Windows integrates voice, presence, instant messaging and directories into one unified offering for Windows laptops and desktops over a LAN connection.

Avaya Communicator provides the following features:

- Compact mode occupying less screen real estate

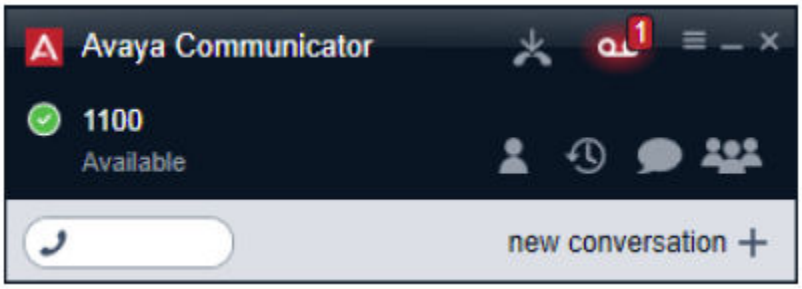


Figure 12: Avaya Communicator for Windows compact view

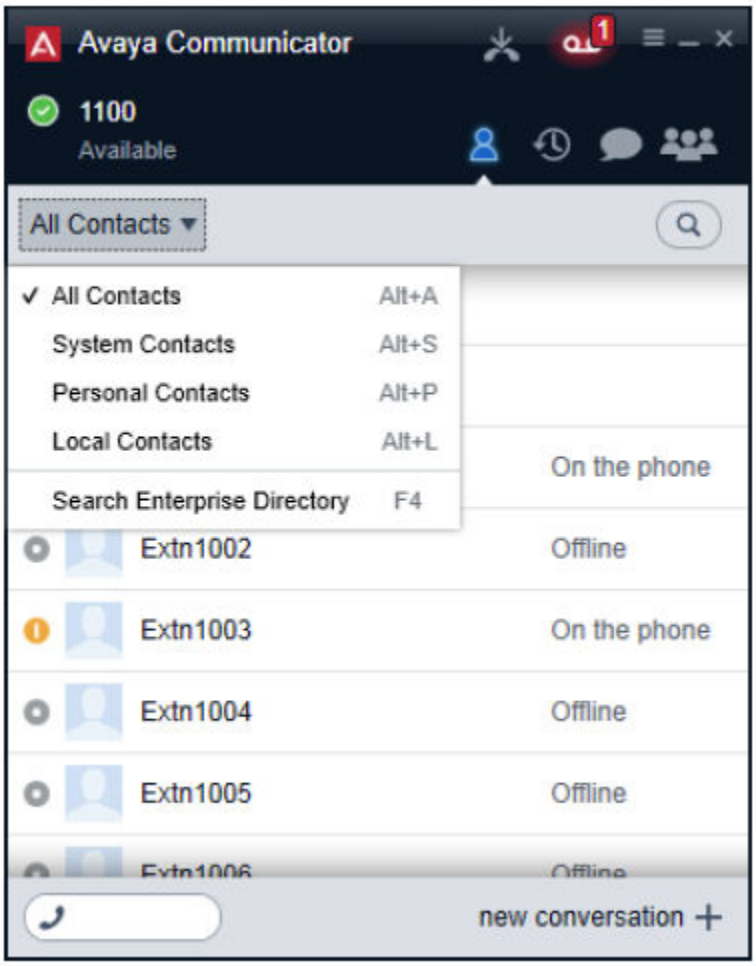


Figure 13: Avaya Communicator for Windows full view

- Secure signaling over TLS and secure media exchange over SRTP for cloud environments
- Contact filtering according to criteria and choosing to view only system, local, or personal contacts

Página2310 de 3226.

- Web conferencing integration
- Unsupervised transfers
- Auto-answer
- Simultaneous mode for interfaces to one-X Portal, Outlook and Salesforce
- Password changing
- Account codes

SoftConsole

SoftConsole is the PC-based Windows receptionist application for IP Office. It can be purchased with the Receptionist user license.

SoftConsole provides enterprise receptionists and operators with call information and call actions to simplify call handling and instant messaging. With SoftConsole, users see the status of other users and adjust basic telephony settings of other users, such as forwarding numbers. Avaya recommends using phones that support Auto Answer. Users can use instant messaging features provided by Avaya one-X® Portal, if available.

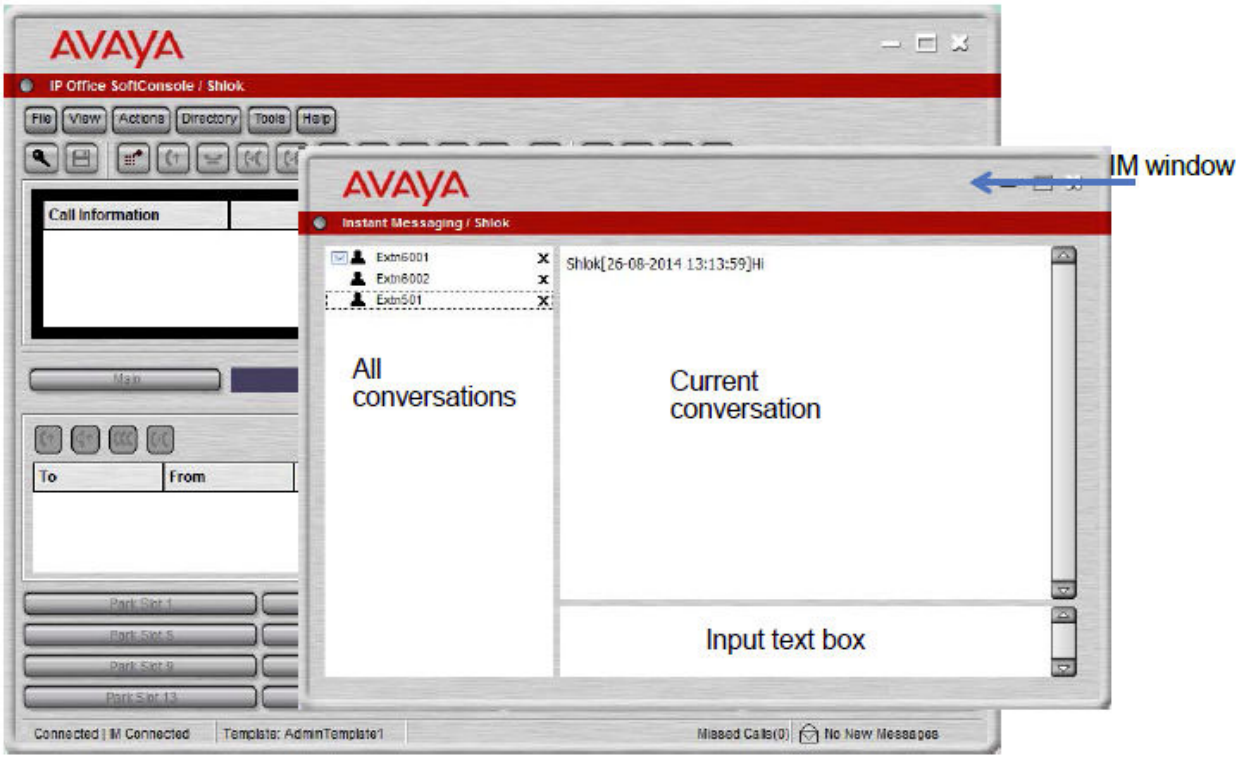


Figure 14: SoftConsole instant messaging window

WebSocket communication allows SoftConsole clients to communicate with IP Office and Avaya one-X® Portal. The WebSocket protocol is bidirectional between the client and the server. As the communication is done over port 80 or 443 (same port used for HTTP), there are no issues with firewall traversal. In a hosted environment, WebSocket communication provides security.

Página2311 de 3226.

SoftConsole can be minimized in the Windows system tray when not in use, but will pop up on the screen when a call is received. Sound and media files can be associated with calls. If this feature is used, the PC requires a sound card and speakers.

SoftConsole supports the following features:

- Answering calls
- Making outgoing calls
- Supervised and unsupervised transfers
- Transfer calls to voicemail
- Hold and park calls
- Monitoring queues and answering queue calls
- Using and viewing conference rooms
- Conferencing held calls
- Adding users to a conference
- Adding text to a call
- Door release
- Intrude
- Sending text messages
- Paging
- Recording calls
- Sending email
- Using dial pad
- Multiple language support, users can select language

Embedded Voicemail

In environments like retail or home office, where space, noise or cost considerations rule out using a PC for voicemail, Embedded Voicemail provides basic voicemail services. Embedded Voicemail is on the IP500 V2 control unit and does not require a separate voicemail server.

Embedded Voicemail is available with IP Office Essential Edition. No additional licenses are required.

Voicemail Pro

Voicemail Pro is provided with IP Office Preferred Edition and is an advanced messaging and call flow application for IP Office systems. Voicemail Pro can handle 40 (up to 250/500 on Server Edition/ Server Edition Select) simultaneous calls depending on license and system settings. Each user has the option of turning their voicemail on or off. When on, the system automatically answers their telephone when they are not available to take a call, plays a personal greeting, and records a message.

Página2312 de 3226.

When a message has been left, the user will see a message-waiting lamp lit on their telephone and can press a retrieval button to collect their messages.

Voicemail Pro can also ring the user to deliver any new messages. Voicemail messages are time and date stamped and the caller's number recorded. Voicemail Pro can be configured to delete read messages automatically, unless the user chooses to save the message permanently.

Voicemails can be collected remotely by dialing into the Voicemail Pro server. If the number the user is dialing from is recognized (home number or mobile/cell phone for example), the user will listen to their voicemail straight away. If the source number is not recognized, the user will be prompted for a mailbox number and a PIN code for that mailbox, before they can listen to their voicemail. Users have the ability to set and change their own PIN codes.

When a voicemail needs to be forwarded to other users, Voicemail Pro provides many options:

- Voicemails can be forwarded to another mailbox, or group of mailboxes
- Recipients can add their comments to the voicemail before forwarding to another mailbox or mailboxes.
- Voicemails can be forwarded as email WAV attachments.

All options are available in a choice of languages; both spoken voice prompts and graphical programming interfaces and have the choice of IP Office TUI and INTUITY emulation TUI.

Conferencing

Users can place calls on hold and a create a conference using either the telephone or desktop applications. Additional conference members may be added, however a single conference may not have more than 64 members (with IP500 V2 only and more on Server Edition).

For ad-hoc conferencing, the system requires as many digital trunks/VoIP channels as external participants (as well as Preferred Edition for Meet-Me conferences). The system supports 128 conferencing channels on the IP500 V2, allowing multiple conferences of any size from 3 to 64 parties. The system support 42 3-party conferences, 2 64-party conferences or any combination in between. Meet-Me capabilities require Preferred Edition for direct dial into a conference bridge with PIN code security. In an SCN network, only one centralized Preferred Edition license is required to host Meet-Me conferences at any of the sites. Conference IDs are also shared across the SCN sites.

The following conference channel capacities are available:

Table 4: Conferencing channel capacities

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
HP DL120 Dell R210	128	128	414	414
HP DL360	256	256	825	825
Dell R620	256	512	825	825

Table continues…

Página2313 de 3226.

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
OVA	256	512	825	825
IP500V2	128	128	128	128

To initiate a conference, users dial the direct number allocated to the conference bridge, type in the PIN (require Preferred Edition and Voicemail Pro) if required. For ad-hoc conferences with a few participants, users can easily set up immediate conferences by calling all parties and bringing them to the conference bridge. With Avaya one-X® Portal for IP Office, the originator of the conference can keep control: the Caller ID number (and the associated name if recognized) of each participant is displayed. If required, they can selectively hang-up a specific participant. The system plays a single beep on entry and a double beep on exit. The owner of the conference may use their extension number as the conference ID. The owner of the conference has control of the conference with the ability to mute and drop calls of participants. All participants will hear the system Music on Hold (MOH) until the owner joins, and will hear MOH when the owner drops. Note that any internal party has the option to view and drop participants (not just the conference originator).

Users can record a personalized greeting for a conference (requires Preferred Edition and Voicemail Pro).

Users can record the conference using Avaya one-X® Portal for IP Office, digital or IP display phone or a short code (requires Preferred Edition and Voicemail Pro). To prevent unauthorized access to the conference bridge, PIN codes, Caller ID number screening as well as time and date profiles can be set-up using Voicemail Pro. One user can manage the conferencing bridge facility from any location.

Conferencing has the following restrictions:

- Only two calls connecting through analog trunks are permitted in any single conference.
- Each external caller requires a digital trunk/VoIP channel (for example 1 T1 allows 23/24 external parties, 1 E1 allows 30 parties and a fully licensed VCM-64 allows 64 parties).
- There are no limits on the mix of internal and external calls in conference, but if all internal participants disconnect from the conference bridge, the external participants can be disconnected automatically by the system for added security (configurable system setting).
- System features such as call intrusion, call recording and silent monitoring all use conference resources, as does automatic recording if enabled. When any of these features are active the number of slots available for conference parties is reduced. For example, a conference call between 3 parties and being recorded will use 4 conference slots.

Meet-Me conferencing

Meet-Me conferencing enables multiple callers to talk in an audio conference. Callers can be on-site personnel as well as external parties whether field-based engineers, sales staff on the road, customers or suppliers. Conference calls can be planned in advance or established ad-hoc as and when required.

Video collaboration

IP Office provides Bring Your Own Device (BYOD) and HD room system support for video collaboration.

IP Office supports video collaboration with data sharing through Avaya Scopia® desktop and mobile applications when using Radvision MCU or Video Collaboration for IP Office. Flare clients can also participate in multiparty video conferences. Avaya Scopia® connects to IP Office as a SIP endpoint using an Avaya IP license.

Avaya Video Collaboration for IP Office provides the following features:

- Direct integration including a common dial plan with IP Office
- “Virtual conference room” for up to eight participants with click-to-join capabilities form any standards-based room system, desktop or mobile device
- Freely distributed desktop and mobile video clients for PCs, Macs and most popular iOS and Android devices, enabling people inside and outside an organization to easily join a video meeting
- Low bandwidth HD multiparty video conferencing with data collaboration using native SIP/H.323
- Automatic firewall transversal to engage with participants outside the network

The following diagram shows the topology of IP Office deployed with video endpoints.

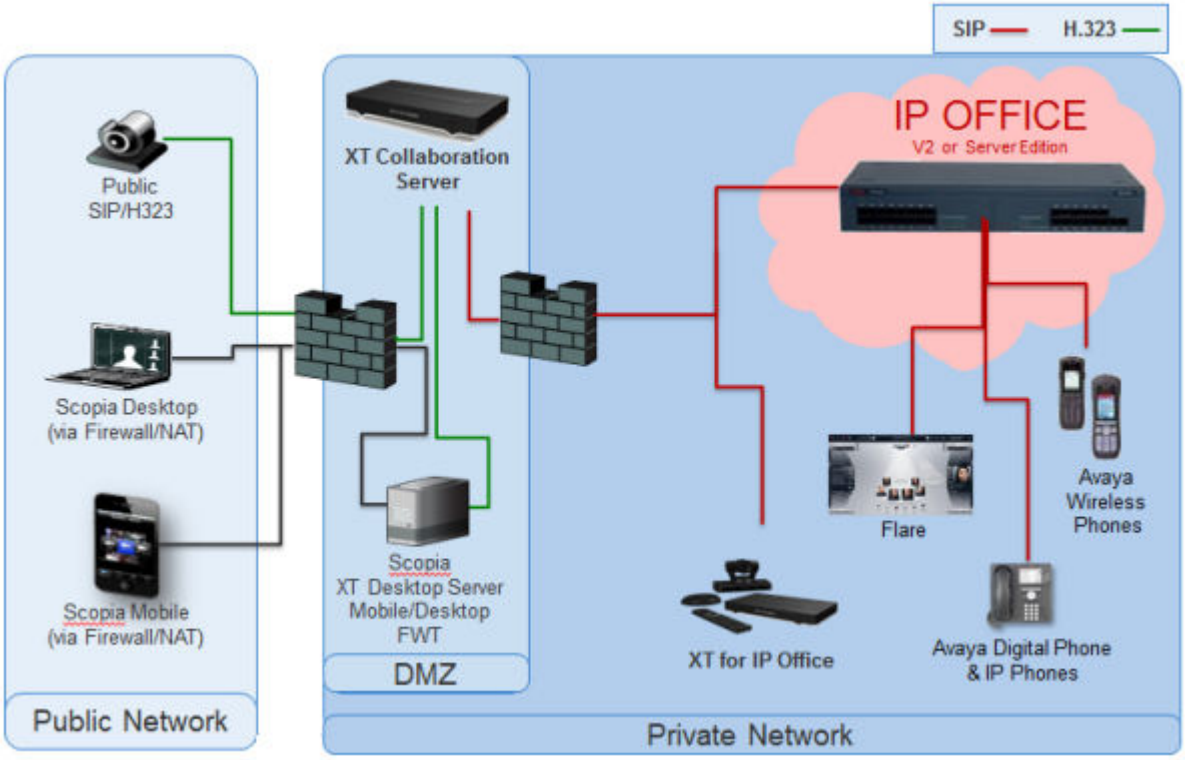


Figure 15: Video endpoints

Página2315 de 3226.

Collaboration Agent

Collaboration Agent is an application that provides web collaboration and conferencing tools. Users with Avaya Aura® Conferencing accounts and invited guests can use the tools to manage conferences and participate and collaborate in conferences.

Conference participants can join conferences by logging in to Collaboration Agent and dialing in to the audio bridge assigned to the conference. Participants can also use the integrated audio and video feature of Collaboration Agent. Participants can use the Collaboration Agent tools to boost productivity and track action items even after the conference ends. Conference moderators can:

- Record all aspects of conferences.
- Record and edit meeting minutes.
- Create and distribute meeting reports based on the meeting minutes.

Collaboration Agent features

In Collaboration Agent, the participants and moderators can perform multiple tasks such as:

- View a list of other participants.
- Virtually raise a hand and seek permission to speak.
- Send messages.
- Annotate shared content.
- Record or edit minutes.
- Set the entry and exit tones.
- Dial out to other users and the users to the conference.
- Disconnect participants.
- Promote participants to the moderator role.
- Invite more participants to join an active conference.

During the conference, participants can view the following information in Collaboration Agent:

- The participants who joined only on the audio bridge
- The participants active on web collaboration
- The participant currently speaking
- The current presenter

Optional features

The following features are optional and must be enabled by the system administrator:

- Starting conferences before moderators join.
- Integrated video
- Promoting all participants to the presenter role so that all participants can share content
- Dialing out from Collaboration Agent to connect users to conferences
- Conference recording

Página2316 de 3226.

Avaya Spaces

Avaya Spaces is a cloud-based team collaboration and meeting application. It seamlessly integrates voice, video, tasks, sharing, and more into your browser or the Spaces application. Each IP Office user is entitled to a free Avaya Spaces Basic account that includes the following team collaboration activities through Avaya Equinox™ client:

- Creation of Spaces for managing ongoing projects: You can use the Spaces area in the dashboard to start a new conversation. In fact, the first time you start using Avaya Spaces, you can view the option to create your own Space. You can invite participants to your Space by entering their email addresses. You can set different permissions for each participant based on the type of actions you want them to be able to take within your Space. If you have many Spaces, you can categorize the frequently used ones as favorites.
- VoIP audio confererencing with up to five participants.
- Limited file sharing (up to 1–GB)
- Point to point video calls, escalate your chats with audio or video.
- Exchange instant messages with other users by using Avaya Spaces Direct Messaging.
- Join a Spaces meeting.

Avaya Equinox® Meetings Online

Avaya Equinox® Meetings Online offers an optional, subscription service for multi-party Unified Communications, that is, audio, video, and web collaboration. The service provides an Over The Top (OTT) virtual meeting room with audio and video conferencing, content sharing, chat and meeting moderation. Users can access the service through desktop, mobile, and video room system as well as audio dial in; third party video room system interoperability is also supported.

Installation and administration applications

The following sections provide an overview of the installation and administration related applications.

IP Office Manager

Use the Manager to manage IP Office standalone systems or systems in a small community network (SCN). Manager tracks system configuration changes, manages upgrades, and configuration imports and exports.

IP Office has a built-in audit trail that tracks changes to the system configuration, and who has made them. Manager can display the audit trail to assist with problem resolution. The audit trail records the last 15 changes in the configuration and records the following elements:

- Configuration Changed - For configuration changes, the log will report at a high level on all configuration categories (users, hunt group...) that have been changed.
- Configuration Erased
- Configuration merged
- Reboot - user instigated reboot

Página2317 de 3226.

- Upgrade
- Cold Start
- Warm Start
- Write at HH:MM - This is when the administrator saved the configuration via the schedule option
- Write with Immediate Reboot
- Write with Reboot When Free

IP Office Manager is also used for maintenance functions such as:

- Upgrade to the IP Office system software
- Ability to send software over an IP network link to a system and have it validated before committing to the upgrade
- Backwards compatibility with systems from Release 2.1 onwards to allow a single management application
- Importing and Exporting IP Office configuration information in ACSII-CSV files.

Server Edition Manager

Server Edition Manager supports complete centralized administration for Server Edition Primary, Server Edition Secondary, and Server Edition Expansion Systems. Manager also provides IP Office telephony and Unified Communications features.

Manager enables management of all the components within the solution for activities such as:

- Single point of configuration for IP Office and voicemail
- Simple initial installation wizard
- Overview of the system with inventory and status
- Common settings consolidated to the Server Edition Primary
- Integrated Voicemail Proclient, System Status Application, and Linux Platform settings access
- Supports online, offline administration, and configuring a complete solution
- Template operations
- Centralized configuration and template storage
- Administrator account management utility
- Retains existing IP Office expertise
- Context sensitive help

Even though Manager is a Windows application, Manager can be installed directly from the Web administration portal of Server Edition Primary server. This enables you to use any Windows personal computer that has any IP Office Manager that is pre-installed immediately.

Using Manager, the administrator can create templates for many management items such as users, extensions, Hunt Groups, and Lines. The administrator can then create any new item using

Página2318 de 3226.

the default settings or the template. You can create multiple users and extensions using one template.

Call Routing Support:

- Full IP Office ARS and dial plan support
- Default routing simplifies configuration
- Solution wide auto line group numbering
- Common incoming call routes provide resilience
- Resilient Hunt Groups

Offline Operation:

- Complete solution can be created and/or managed offline if required
- Can still manage when some deices offline
- On/offline configuration sync options to harmonize as required

Solution Management:

- Complete solution view with status and inventory
- Users and Hunt Groups are solution wide
- Centralized User Rights, feature short codes, Time Profiles, Incoming Call Routes, and Account Codes
- Permits advanced per-device configuration if desired
- All configurations stored on primary server
- Solution wide system directory
- Easy management of central and per-device licenses

Resilience management:

- You can manage every device locally for ‘rainy day’ events
- You can manage the solution through a secondary server when the primary server fails or in a split WAN setup
- On/Offline configuration sync options to harmonize as required

Add or Remove Devices:

- Single process for addition or removal of device
- Built-in Initial Configuration Utility (ICU) to simplify adding a new device
- Common configuration items from primary server is auto populated
- Can configure before you install a new device

Validation :

- Configuration validation on read and any change.
- Solution wide validations

Template:

- Create a local and centralized template from an existing Line, Extension, User, Hunt Group, Time Profile, Firewall Profile, IP Route and Service entries
- Recreate multiple Extension and Users from one template

Remote access:

- Supports access from service through SSL VPN

Security:

- Single Sign On to all except one-X Portal administration

Web Manager

Web Manager is a browser-based management tool designed to simplify the installation and maintenance process and provides access to most, but not all, IP Office configuration settings. Web Manager eliminates the need to have windows operating system because it can run on any device that supports standard browsers.

Granular access:

Web Manager provides service users with access to entire configuration objects if the service user has the configuration access. However, large customers who have multiple service users roles or customers having deployments in the cloud environment need to have granular configuration access for different service users. Hosting partners will be able to build an account for customer or re-seller with limited permissions. These permissions shall restrict the customer or re-seller from performing activities that affects service of the system.

Configuration dashboard:

The Dashboard is a simplified version of the existing IP Office Web Manager and is presented to the administrators when a fresh single-node IP Office system is installed. The Dashboard consists of minimum required set of configuration fields to set up the system. The full setup can be performed anytime afterwards.

IP Office Media Manager

IP Office Media Manager is a native IP Office application to archive, store, search, playback, download, audit, and delete IP Office call recordings. The Operation, Administration, and Management of (OAM) of the application is integrated within the IP Office solution, for example, IP Office Web Manager.

Media Manager obtains the recordings from the IP Office Voicemail Pro application through a pre-configured hand-off directory. Media Manager moves the recordings from the hand-off directory to an additional hard disk partition on the Server Edition Primary or Application Server and then archives the recordings to a storage location configured by the administrator. The archiving location can be a Network-Attached Storage (NAS), a local DVD drive, or cloud storage. For cloud storage, Media Manager supports only Google Drive in this release.

Media Manager is licensed on a system basis. Apart from a new IP Office Release 11.0 and later Media Manager license, the application also works with an earlier Contact Recorder license, for customers upgrading from an earlier IP Office version. Media Manager allows a 90–day trial period before licensing is enforced.

Página2320 de 3226.

Contact Recorder is not supported in IP Office Release 11.0 and later and is not part of IP Office Release 11.0 and later software. However, Media Manager supports migration of Contact Recorder data to IP Office Release 11.0 and later.

Media Manager is available as part of the IP Office Server Edition and Application Server software image. The application runs on the standard Linux distribution supported by IP Office Server Edition and Application Server platforms. The software is installed as a standard Linux RPM only on the Server Edition Primary server or the Application Server in case of IP500 V2 deployments. The application is not supported on UCM or Windows platforms. The management interface is web-based and all popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Internet Explorer are supported.

Media Manager in IP Office Release 11.0 Feature Pack 4 supports deleting or recordings and keeping track of usage of recordings through the Audit trail feature. The Audit trail feature helps you in keeping track of the activities around the recordings in the library. Using this feature, you can find out the users who have:

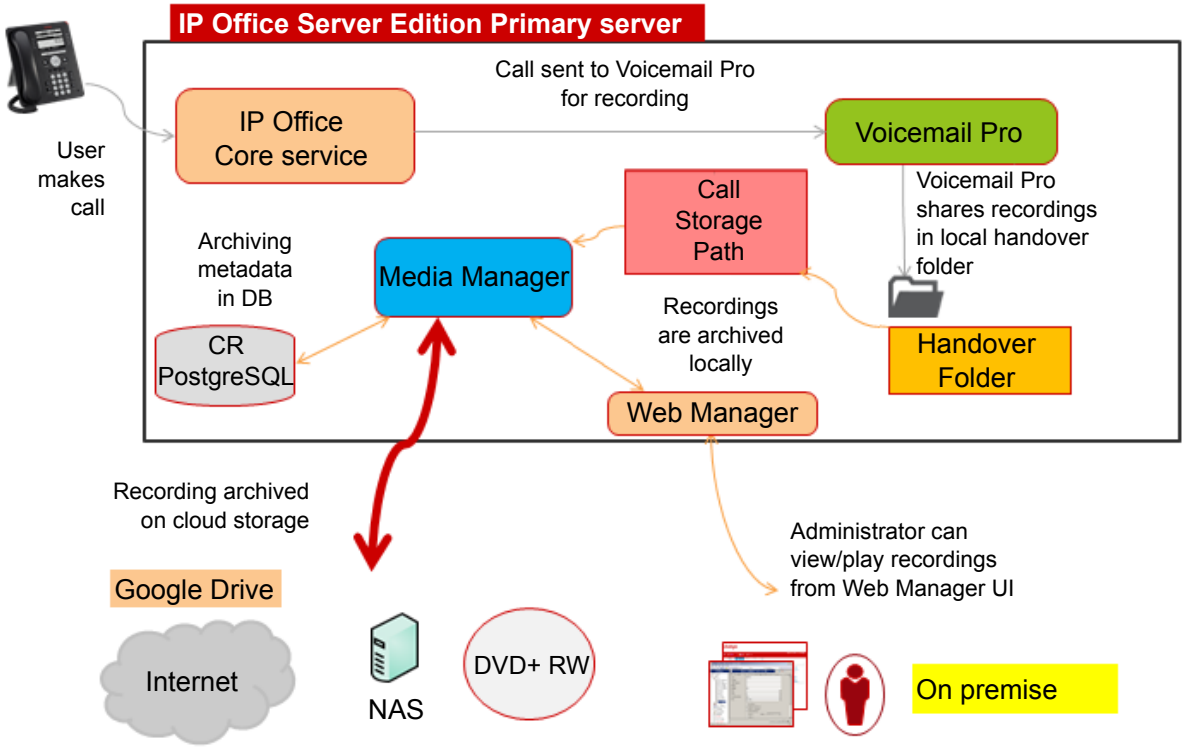
- Searched a recording
- Replayed a recording
- Downloaded a recording
- Deleted a recording

For each event, Media Manager displays the user name, date, time, and the type of user action. The Audit trail is maintained for a predefined number of days and can be modified. By default the Audit trail data is available for 180 days.

Media Manager is available as part of the IP Office Server Edition and Application Server software image. The application runs on the standard Linux distribution supported by IP Office Server Edition and Application Server platforms. The software is installed as a standard Linux RPM only on the Server Edition Primary server or the Application Server in case of IP500 V2 deployments. The application is not supported on UCM or Windows platforms. The management interface is web-based and all popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Internet Explorer are supported.

A standard IP Office Server Edition deployment:

Página2321 de 3226.



Availability of Contact Recorder features in Media Manager

The search capabilities in Media Manager has been enhanced for the administrators and the users.

Functionality	Description	Availability in Contact Recorder	Availability in Media Manager
Search by administrator	Search by administrators using Target Number, Skills, Agent, and Call ID	Yes	Yes
Search through Web Self-Admin	Search by users using the search filters Target Number, Skills, Agent, and Call ID	Yes	Yes
Web Self-Admin search results	A maximum of 100 results are displayed.	Yes	Yes
Call sets	Facility to save search results for retrieving in the future.	Yes	No
Email	Attaching recordings to emails.	Yes	No

Table continues…

Página2322 de 3226.

Functionality	Description	Availability in Contact Recorder	Availability in Media Manager
Bulk Export	Exporting multiple recordings and the related details	Yes	Yes
Owner	Available as a search option.	No	Yes
Audit Trail	Audit can be performed to track the use of call recordings.	Yes	Yes
Windows Domain Authentication	-	Yes	No

Solution Management Application

IP Office Manager and Web Manager use the Solution Management Application (SMA) to access the system configuration.

SMA resides on the primary or secondary server. Settings are available for remote access and Server Edition Central Access. Central Access communicates with the primary or secondary server rather than to each node individually. Avaya requires Central Access for a hosted environment and recommends it for non-hosted environments with more than 32 nodes.

SoftConsole Administrator mode

System administrators can start SoftConsole in administrator mode. When run in this mode, there is no access to the telephony functions.

SoftConsole administrator mode enables users to configure the following functions:

- Create and edit user profiles
- Amend the length of call notes
- Create and edit templates
- Remove or display the interface panels

SNMP Management Console

Simple Network Management Protocol (SNMP) is an industry standard designed to allow the management of data equipment from different vendors using a single Network Manager application. The Network Manager periodically polls equipment to solicit a response, if no response is received an alarm is raised. In addition to responding to polls, IP Office monitors the state of its Extensions, Trunk cards, Expansion Modules and Media cards so that if an error is detected IP Office will notify the Network Manager.

As the IP Office platform comprises many applications, the core software notifies SNMP events from both Voicemail Pro and Embedded Voicemail to warn of approaching storage capacity limits.

IP Office sends email notifications directly to the email server; no additional PC client is needed.

On customer sites where SNMP management is not available, IP Office can email events using up to 3 email addresses each containing a different set of alarms.

Página2323 de 3226.

The following system event categories can be chosen for email notification, if installed on the system:

- Generic
- Trunk lines
- Embedded Voicemail Card
- VCM
- Expansion modules
- Applications
- License
- Phone change
- CSU Loop-Back

IP Office has been tested against CastleRock's SNMPc-EE™ and HP's Network Node Manager (part of the OpenView application suite).

System Status Application (SSA)

The System Status Application (SSA) is a diagnostic tool for system managers and administrators to monitor and check the status of IP Office systems locally or remotely. SSA shows both the current state of an IP Office system and details of any problems that have occurred. The information reported is a combination of real-time events, historical events, status and configuration data to assist fault finding and diagnosis. SSA provides real-time status, historic utilization and alarm information for ports, modules and expansion cards on the system. SSA connects to all variants of IP Office using an IP connection that can be remote or local. Modem connections at 14.4kbps or above are supported for remote diagnostics.

SSA provides information on the following:

Alarms	SSA displays all alarms which are recorded within IP Office for each device in error. The number, date and time of the occurrence is recorded. The last 50 alarms are stored within IP Office to avoid need for local PC.
Call Details	Information on incoming and outgoing calls, including call length, call ID and routing information.
Extensions	SSA details all extensions (including device type and port location) on the IP Office system. Information on the current status of a device is also displayed. SSA shows IP Extensions that were registered but no longer available and IP extensions that are configured but have not been registered after last re-boot. This helps to spot phones that are Idle, disconnected, or are misconfigured. SSA also shows quarantined phones and blacklisted extensions and IP addresses.

Página2324 de 3226.

Trunks	IP Office trunks and connections (VoIP, analog and digital) and their current status are displayed. For VoIP trunks, QoS information is also displayed (e.g. round trip delay, jitter and packet loss).
System Resources	IP Office includes central resources that are utilized to perform various functions. Diagnosing these resources is often critical to the successful operation of the system. This includes details on resources for VCM, Voicemail and conferencing.
QoS Monitoring	QoS Parameters from connected calls, such as jitter and roundtrip delay, are monitored.

SSA can be launched independently or from IP Office Manager and there can be up to two (2) SSA clients connected to an IP Office unit at one time.

Note: SSA is not a configuration tool for IP Office systems.

SysMonitor

Use SysMonitor to troubleshoot IP Office from both local (LAN) and remote locations (WAN).

Select the protocols and interfaces to monitor and diagnose through a graphical interface. Capture traces directly to the screen or as a log file for later analysis. Color code different traces to improve the clarity in large files. The utility also captures system alarms and displays the activity log of the last 20 alarms that have occurred.

Cloud Operations Manager

Cloud Operations Manager is an administration tool that allows a simplified way of multi-customer management with a focus on cloud-based systems. The tool enables management of IP Office Server Edition systems and provides the following capabilities:

- Single Unified Management portal capable of managing up to 3000 IP Office systems.
- Dashboard that displays error conditions, ongoing system activities, and system health
- Grouping of systems based on versions and tags for accessing similar systems at the click of a button
- Displays all connected systems such as Primary, Secondary, Expansions, and open applications
- Ability to centrally manage IP Office software upgrades and patching across multiple system and versions
- Role-based administration: Cloud Operations Manager has its own service users with access to complete or selective customers IP Office. No granular feature level access is available in Release 11.0.
- Provides facility to launch Native IP Office Management applications. Uses need to log in to the applications separately after the application is launched. Launching of IP Office Contact Center, Avaya Contact Center Select, and Avaya Workforce Optimization Select are not supported in Release 11.0.

Página2325 de 3226.

- Alarms for Configuration, Services, Trunks, Link, and Security by Severity type
- Alarms for status of IP Office systems indicating whether they are online of offline
- Alarms indicating status of various applications

Data Migration Manager (DMM)

The Data Migration Manager (DMM) facilitates migration from BCM and Norstar systems to IP Office. There are three steps in the migration process: extract, convert and apply.

DMM migrates:

- Announcements and greetings
- Voicemail messages
- Extract Call Pilot configuration

Contact center applications

The following sections provide an overview of the contact center applications.

For general information about:

- IP Office Contact Center, see *Avaya IP Office Contact Center Feature Description*.
- Avaya Contact Center Select, see *Avaya Contact Center Select Solution Description*.

IP Office Contact Center overview

Note:

IP Office Contact Center goes End of Sale for new systems in September 2019.

Avaya is the market leader in call center technology, and IP Office Contact Center can take your business to a new level. IP Office Contact Center provides integrated contact center capabilities specifically designed for businesses supporting between 5 and 250 contact center agents and supervisors.

IP Office Contact Center provides the following features and characteristics:

- All-in-one customer service solution that delivers consistent service to customers across multiple media channels and locations. IP Office Contact Center includes a user interface (UI) on Microsoft Windows and a web interface supported on various browsers.
- Fast implementation with minimum disruption to the business. IP Office Contact Center also includes an automatic synchronization feature for configuration. This feature can be enabled and disabled as needed during implementation.
- Access to Agent UI functionality, including call control, from a SalesForce (SFDC) plug-in or SAP CRM connector.
- Email and chat capabilities on the Windows and Web UI.
- Inbound and outbound voice calls with telephony and dialer capabilities.
- Skills-based routing.

Página2326 de 3226.

- Address book access so agents can quickly find the contact information they need to make calls and send emails.
- Real time and historical reporting for all media channels.
- Interactive Voice Response (IVR) and Task Flow Editor scripts.
- User profile and agent group privilege configuration to determine which features are available to users of the interface. Administrators must assign privileges and create agent groups.
- Access to a web-based administration portal. You can use the administration portal to perform configuration, maintenance, monitoring, and management tasks. You can also upload certificates, collect logs, and download email archives and the IP Office Contact Center User Interface for Windows. Advanced administration tasks must be performed in the IP Office Contact Center User Interface for Windows. You cannot perform administration tasks with the IP Office Contact Center Web User Interface.
- Access to a wallboard that displays IP Office Contact Center statistics. For more information about Wallboard, see *Using Avaya IP Office Contact Center Wallboard*.
- Option to easily integrate chat functionality into a web page. For more information, see *Avaya IP Office Contact Center Email and Chat Services Task Based Guide*.
- Optional integration with call recording applications, such as IP Office Media Manager. Calls are recorded with Voicemail Pro and the details of the complete recording are stored in the database of the call recording application. You can search for and manage recordings using a web browser.
- Optional interoperability with Avaya Workforce Optimization Select, which is a stand-alone product that does not currently integrate with IP Office Contact Center UIs or applications.
- Media Resource Control Protocol (MRCP) integration, which provides support for text to speech (TTS) and automatic speech recognition.

Avaya Contact Center Select overview

Avaya Contact Center Select is a context-sensitive, collaborative, voice and multimedia contact center solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform.

Avaya Contact Center Select uses industry-standard SIP and CTI interfaces to integrate with IP Office. This integration gives Avaya Contact Center Select access to and control of a wide range of IP Office phones and features. Customers integrating Avaya Contact Center Select with IP Office gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility.

Avaya Agent Desktop is a single-interface client application used by Avaya Contact Center Select agents to assist customers. Avaya Contact Center Select agents use Agent Desktop software to respond to customer voice and multimedia contacts. Agent Desktop supports a range of IP Office phones and a wide variety of multimedia contact types.

By default, Avaya Contact Center Select connections and Web Services use secure TLS communication. The Avaya Contact Center Select Certificate Management tool makes it easier to manage security certificates.

Página2327 de 3226.

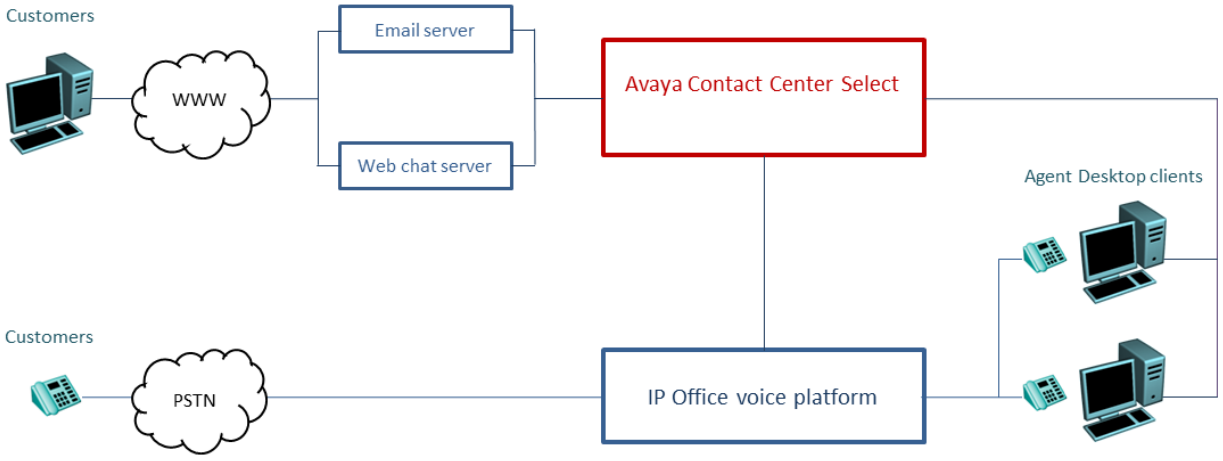


Figure 16: Typical contact center solution using voice and multimedia Avaya Contact Center Select and the Avaya IP Office voice phone system

Avaya Contact Center Select provides a feature-rich voice and multimedia solution with integrated routing and reporting for small to midsize enterprises. Avaya Contact Center Select provides unified contact center and IP Office phone user account management for agents and supervisors. Voice-enabled agents and supervisors created in Avaya Contact Center Select are automatically added to IP Office. Avaya Contact Center Select synchronizes user (agent and supervisor) information between Avaya Contact Center Select and IP Office.

Página2328 de 3226.

Chapter 3: Solution specifications

Reference configurations

IP Office is sold in different editions, reference configurations, and deployment scenarios to meet different customer requirements. The editions build on one another to offer advanced functionality, including presence, instant messaging, web collaboration, and Microsoft software integration.

The following sections summarize IP Office editions and other configuration options. These sections do not provide complete reference configuration details for every IP Office option. Separate Reference Configuration documents are available for IP Office Server Edition, IP Office Branch, Powered by Avaya Cloud solutions, and IP Office Contact Center.

IP Office editions

IP Office Basic Edition

IP Office Basic Edition is intended for small and growing enterprises that need higher productivity with a professional touch. Businesses can increase capacity as needed.

IP Office Basic Edition provides basic telephony features such as:

- 64 trunk capacity: analog, PRI/T1, and SIP
- Key system operation
- 64 party conferencing capacity
- Automated Attendant
- Multiple language support
- Call forwarding
- Caller ID
- Dial by name
- Breakout to reception
- Integrated voicemail:
  - Maximum of 6 concurrent calls to voicemail with approximately 25 hours of storage
  - Message control including Save, Delete, Forward, Repeat, Rewind, Fast Forward, and Skip Message

Página2329 de 3226.

- Visual voicemail
- Message time and date stamping

Modes of operation

IP500V2 control units are supplied with no installed firmware or configuration. When first powered up, the control unit loads and installs the necessary firmware from the system SD card installed in it. It creates a default configuration matching the card installed in the control unit and external expansion modules attached to it. IP500V2 control units can operate in a number of modes. The initial mode is determined by the type of system SD card.

Mode	SD card
IP Office Basic Edition Quick mode	• a-law telephony PBX system operation. • µ-law telephony key system operation.
IP Office Basic Edition - PARTNER Mode	Defaults to a-law telephony PARTNER mode operation.
IP Office Basic Edition - NORSTAR Mode	Defaults to µ-law telephony NORSTAR mode operation.

Basic Edition runs on the IP500V2 control unit. An SD is required and is installed in the rear of the control unit, providing operating software, feature keys, and licenses. An optional SD card can be installed in the optional SD card slot, providing redundant backup and system upgrade capabilities.

Table 5: Supported base cards

Basic Edition supports following base cards:

Base card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
Combination analog	4	4
Combination BRI		2
ETR6	3	
DS8	3	3
TCM8	4	4
Phone 2	4	4
Phone 8	4	4

Table 6: Supported trunk cards

Basic Edition supports the following trunk cards:

Trunk card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
ATM4	4	4
PRI/T1	1	
PRI/E1		1

Table continues…

Página2330 de 3226.

Trunk card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
BRI4		4
BRI8		1

Expansion modules

Basic Edition supports the following expansion modules:

- DS16A
- DS16B
- DS16B2
- ATM16
- Phone 16
- Phone 30
- DS30A
- DS30B
- DS30B2

Note:

DS16B2 and DS30B2 digital station modules are supported on IP Office Release 10.1, Release 9.1 SP12, and 10.0 SP5 onwards.

IP Office Essential Edition

IP Office Essential Edition provides the same features as Basic Edition as well as the following:

- Mobile call control with one number access and simultaneous ringing on mobile devices
- Up to 4 remote workers through an internet connection and an Avaya 9600 series IP phone
- 24 hour access with customized voicemail greetings for each staff member
- Voicemail:
  - Maximum of 6 concurrent calls to voicemail
  - Send voicemails to email
  - Up to 25 hours of voicemail storage (with 6 ports)
  - Up to 40 automated attendants with a maximum of 6 concurrent calls
- Multiple language support
- Up to 128 party audio conference bridge with 64 in any one conference

Note:

Basic Edition is not a prerequisite for Essential Edition or Preferred Edition, and is not stacked under Essential Edition.

Página2331 de 3226.

IP Office Preferred Edition

IP Office Preferred Edition provides intelligent call routing, messaging, call handling and application integration.

In addition to the features provided with Essential Edition, IP Office Preferred Edition provides the following:

- Scalable voicemail:
  - Up to 40 simultaneous calls
  - Send a voicemail to all employees, a department, or a team
  - Address messages by extension or by name
  - Voicemail messages can “find” users to alert them a message is waiting
- Secure conferencing for up to 128 parties with 64 per conference
- Automated call routing with an unlimited number of automatic attendants that can be customized for time of day, day of week or other variables as well as to recognize callers and deliver personalized messages
- Call recording for incoming and outgoing calls that can be sent to voicemail or email inboxes as WAV files

Components

- IP500 V2 control unit
- Ethernet attached PC running the supported version of Windows Server
- Ethernet attached PC configured with Application Server software
- IMAP mail client (Outlook) for voicemail synchronization in email and browser-based access to voicemail
- Digital trunks and channels to support users
- IP Office supported telephones

IP Office Server Edition

IP Office Server Edition provides IP Office telephony capabilities, unified communications, mobility, and collaboration. It also provides high availability, ease of use, and low total cost of ownership (TCO). Targeted at the midsize enterprise, IP Office Server Edition supports up to 150 sites, 3000 users, and comprehensive resilience.

IP Office Server Edition Solution provides the following:

- A single Server Edition Primary server provides IP Office, Voicemail Pro, and Avaya one-X® Portal for IP Office.
- A Server Edition Secondary server increases the capacity and provide resilience.
- Expansion systems, which provide additional capacity, support analog or digital interfaces, and remote locations.
- A Select IP Office Server Edition Solution provides additional capacity.
- Support for an existing IP500 V2 control unit optimized for a hybrid of analog/TDM and IP deployments, or a Linux server optimized for IP only deployments.

Página2332 de 3226.

- Users and extensions can be configured on the IP Office Server Edition server or the Server Edition Expansion System.
- Software distribution includes the various user and administration applications such as IP Office Manager, SSA, Voicemail Pro, and IP Office SoftConsole.
- Components can be in the same location or in different locations.
- Optionally configure a separate application server dedicated to Avaya one-X® Portal to provide more user capacity than the Server Edition Primary supports.
- Add additional servers and expansion systems any time.

.

Topology

IP Office Server Edition is based on a double star network topology that provides comprehensive features and their management, enables ease of use, installation, and administration. The overall solution provides a flexible and modular architecture starting with a single server and you can scale up the number of users and locations by networking multiple servers. The components automatically act as a single logical unit and you can administer the components from a single console through an integrated management system.

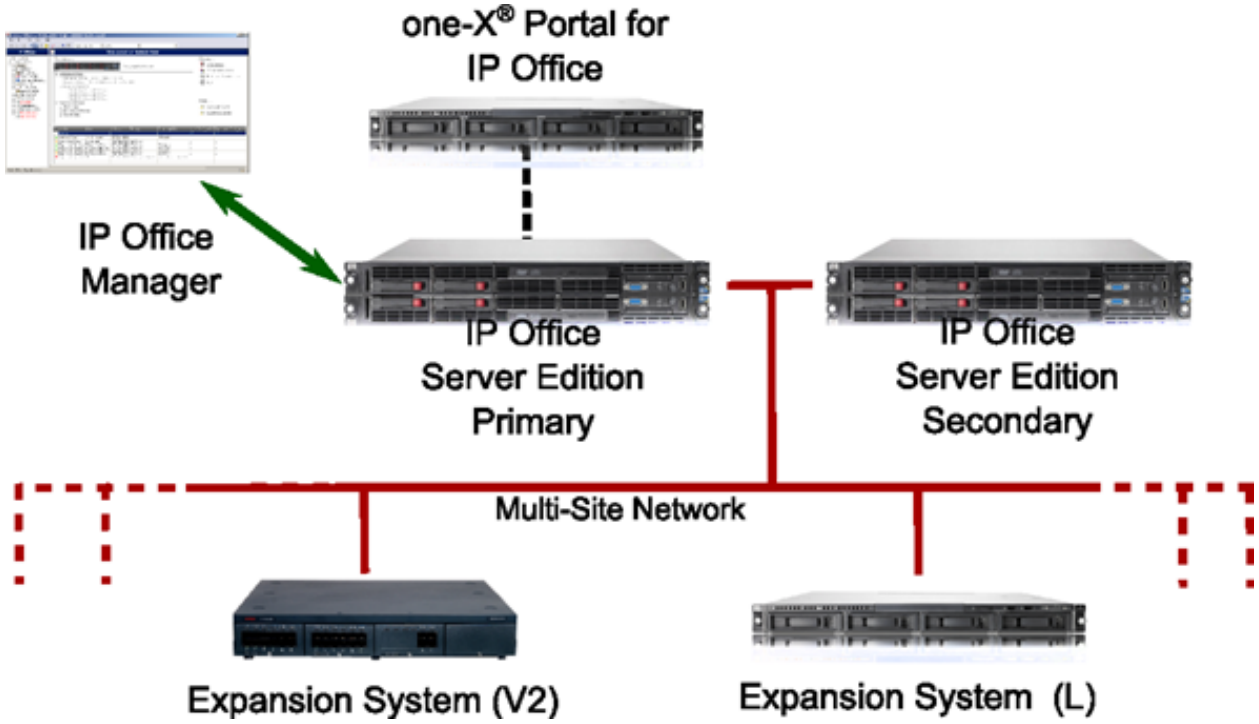


Figure 17: IP Office Server Edition topology

Deployment models

Centralized IP only	One primary server located at the customer headquarters

Página2333 de 3226.

Centralized IP analog and digital	One primary server and one expansion server located at the customer headquarters
Distributed IP only	One primary server located at the customer headquarters and one secondary server located at a remote location
Distributed IP analog and digital	One primary server and one expansion system located at the customer headquarters and one expansion system located at each remote site
Virtualized environment	Customer-provided software and hardware VMware vSphere platform with IP Office Server Edition and application server OVA ignited as a primary, secondary, expansion or application server.

Components

Component	Server options	Description
Server Edition Primary server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Software distribution includes: • IP Office Server Edition • Voicemail Pro • Avaya one-X® Portal for IP Office • IP Office Manager • System Status Application (SSA) • SoftConsole
Server Edition Secondary server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component to support resilience either centrally or at a remote site.
Server Edition Expansion System	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component to support remote locations. Up to 148 expansion systems provide additional capacity, support analog or digital interfaces, and local trunks at remote sites. Can be set up either centrally or at a remote site. **Note:** In a cloud environment, the IP500 V2 expansion system provides support for analog and digital endpoints.

Table continues…

Página2334 de 3226.

Component	Server options	Description
Server Edition Expansion System	IP500 V2	Optional component to support remote locations and as a gateway. Can be an existing IP500 V2 or IP Office Server Edition server. Can be set up either centrally or at a remote site.
Avaya one-X® Portal for IP Office application server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component. You can optionally configure a separate application server dedicated to Avaya one-X® Portal to provide more Power User capacity above the maximum that Server Edition Primary supports.

Virtualized environment components

Avaya provides a virtualized equivalent to the IP Office Server Edition and applications server packaged as a single OVA ready for installation on vSphere supported host hardware from a PC. The OVA is available as a download from Avaya or on an orderable DVD. Once deployed, it can be ignited as a primary, secondary, expansion or applications server.

Other deployment options

You can also deploy IP Office in:

- An enterprise branch environment (Centralized IP Office branch) or a Distributed Branch environment).

  You can deploy an IP Office system as a standalone branch or connect it to the Avaya Aura® network. A CS 1000 branch environment is also supported.
- A Cloud environment with the Powered by Avaya offers.

Contact center options are also available.

IP Office as an enterprise branch overview

You can deploy IP Office as an enterprise branch to provide a communications solution that is adaptable to meet the growing needs of an enterprise branch network while providing investment protection of the installed hardware platform and phones. You can implement an IP Office enterprise branch on an IP Office Standard Mode, Essential, or Preferred system. The IP Office system can be installed as an independent, standalone branch, or be connected to the Avaya Aura® network and migrated to a Distributed, Centralized, or Mixed enterprise branch to provide specific features and applications to meet the needs of individual employees in each branch location.

In addition to centralized SIP endpoints or centralized analog devices configured as ATA, IP Office can concurrently support other IP and TDM endpoints for a community of Centralized users and IP Office users in the same branch. Ideal for enterprises wanting applications deployed in customer

Página2335 de 3226.

data centers or in the branch, an IP Office Branch can effectively deliver a range of communication tools without complex infrastructure and administration.

IP Office is also supported in an Avaya Communication Server 1000 (CS 1000) branch environment. Only the Distributed enterprise branch option is supported. IP Office can be deployed as a new branch in an existing CS 1000 configuration with the addition of Avaya Aura® Session Manager to which IP Office connects through the SM Line for branch connectivity. Providing phone investment protection, IP Office can also be deployed as a replacement for Business Communications Manager (BCM) or Norstar in a branch office and connect to CS 1000 through Avaya Aura® Session Manager. IP Office cannot operate as a survivable gateway to CS 1000 endpoints as similar to Survivable Remote Gateway (SRG).

Topology

The IP Office Branch solution provides the flexibility to support independent, stand-alone IP Office branches as well as IP Office branches connected to an Avaya Aura® system. The Branch solution also supports CS 1000 integration. The following deployment options are available for the solution architecture:

- **Stand-alone IP Office branch option**: Independent IP Office systems are deployed within the network. These IP Office systems are not connected to each other or to anything else in the network. With this option, IP Office Branches are not connected to an Avaya Aura® system and users cannot access any Avaya Aura® services.
- **Distributed enterprise branch deployment option**: All users in this deployment option are IP Office users. These IP Office users obtain telephony services from the local IP Office and not from Avaya Aura®. The IP Office systems in this deployment option can be connected to Avaya Aura® Session Manager and administrators can obtain Centralized management services through Avaya Aura® System Manager. The enterprise can choose to connect IP Office users in this deployment option to an IP Office voice mail system, Embedded Voicemail or Voicemail Pro, or a Centralized voice mail system, such as Avaya Aura® Messaging or Avaya Modular Messaging. IP Office users in this deployment also have access to some Centralized Avaya Aura® applications and services.

  With the Distributed branch deployment option, you can also connect CS 1000 to IP Office in the branch through Avaya Aura® Session Manager. Users still obtain telephony services from the local IP Office, but can use Avaya CallPilot® as their voice mail system. When connected to CS 1000, IP Office and CS 1000 interoperate as peers through Avaya Aura® Session Manager.
- **Centralized enterprise branch deployment option**: All users in the enterprise are Centralized users.

  Centralized users register to Avaya Aura® Session Manager and obtain telephony services from the Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. If WAN connectivity to Avaya Aura® Session Manager is lost, the user automatically gets basic telephony services from the local IP Office. The telephony features provided by IP Office in survivability mode is limited compared to the features that are normally provided to the Centralized phone.

  Centralized users must be configured on the Avaya Aura® Session Manager, Communication Manager, and IP Office. A Centralized user must be configured on the Avaya Aura® Session

Página2336 de 3226.

Manager and Avaya Aura® Communication Manager as a SIP user. On IP Office, the Centralized user must have either a SIP extension, an analog extension, or an analog fax device.

- **Mixed enterprise branch deployment option**: An enterprise branch with both Centralized users and IP Office users. Centralized users and IP Office users obtain the same telephony services described above. All users in this deployment option must use a Centralized voice mail system: Avaya Aura® Messaging or Avaya Modular Messaging.

The deployment options in the Branch solution allow you to start off with stand-alone IP Office systems and then slowly evolve the solution architecture into a Centralized environment as your enterprise grows.

The following image shows the topology of the solution architecture with the deployment options described above. This image does not show CS 1000 in the Distributed branch deployment.

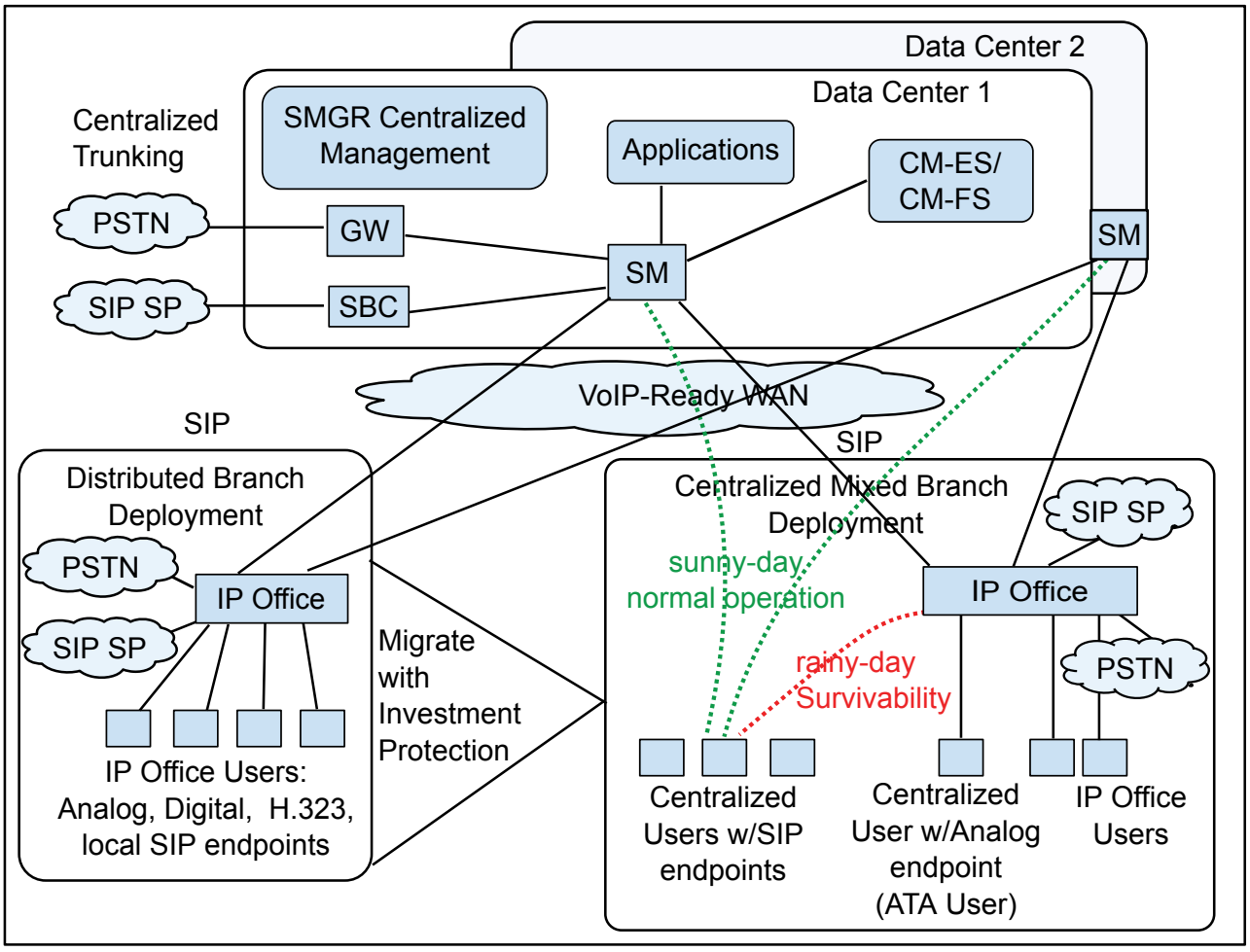


Figure 18: Topology of solution architecture

Powered by Avaya Cloud overview

The Powered by Avaya Cloud solution enables you, the BP or provider, to sell core IP Office and, optionally IP Office Contact Center or Avaya Contact Center Select, features to small and medium

Página2337 de 3226.

enterprise users. With Powered by Avaya, you install and host the product instances in a Cloud data center at your site.

The existing Powered by Avaya Cloud solution enables you, the BP or provider, to sell core IP Office and, optionally IP Office Contact Center or Avaya Contact Center Select, Telephony and Unified Communications (UC) features to users in small and medium enterprises. With the new IP Office Cloud offer, the optional IP Office Contact Center and Avaya Contact Center Select components are not supported. Hybrid Cloud functionality, Voicemail Pro, and Media Manager are also not supported in the new IP Office Cloud offer. This offer currently uses Embedded Voicemail as its voice mail system.

With the existing Powered by Avaya offer, you install and host the product instances in a Cloud data center. The new IP Office Cloud is hosted in a Google Cloud environment with one IP Office cluster per provider.

Key benefits of the Cloud solution include the following:

- Reduction in operational costs for the enterprise by reducing the IT complexity of equipment maintenance.
- Reduction in service delivery costs for the BP through virtualization and shared infrastructure.
- Programmatic interface to support license installations, configure centralized licensing, or delete a license file.
- Automated billing with Avaya One Source Cloud Services.
- Flexibility to change your Avaya One Source Cloud Services order anytime. You can add or remove users anytime. You can update your order to add or remove the optional IP Office Contact Center and Avaya Contact Center Select programs as needed.
- Support for IP500 V2 expansion systems at the enterprise site with Hybrid Cloud. This does not apply to the new IP Office Cloud offer.
- Support for resiliency with High Availability (HA).

Powered by Avaya topology

Powered by Avaya supports the following deployment models:

- Public Network: This deployment model uses a public over-the-internet connection between the Cloud data center and the enterprise premises. All users connecting over the Public Network are considered Remote Workers.
- Private Network: This deployment model requires an MPLS or site-to-site VPN connection between the Cloud data center and the enterprise premises.

Página2338 de 3226.

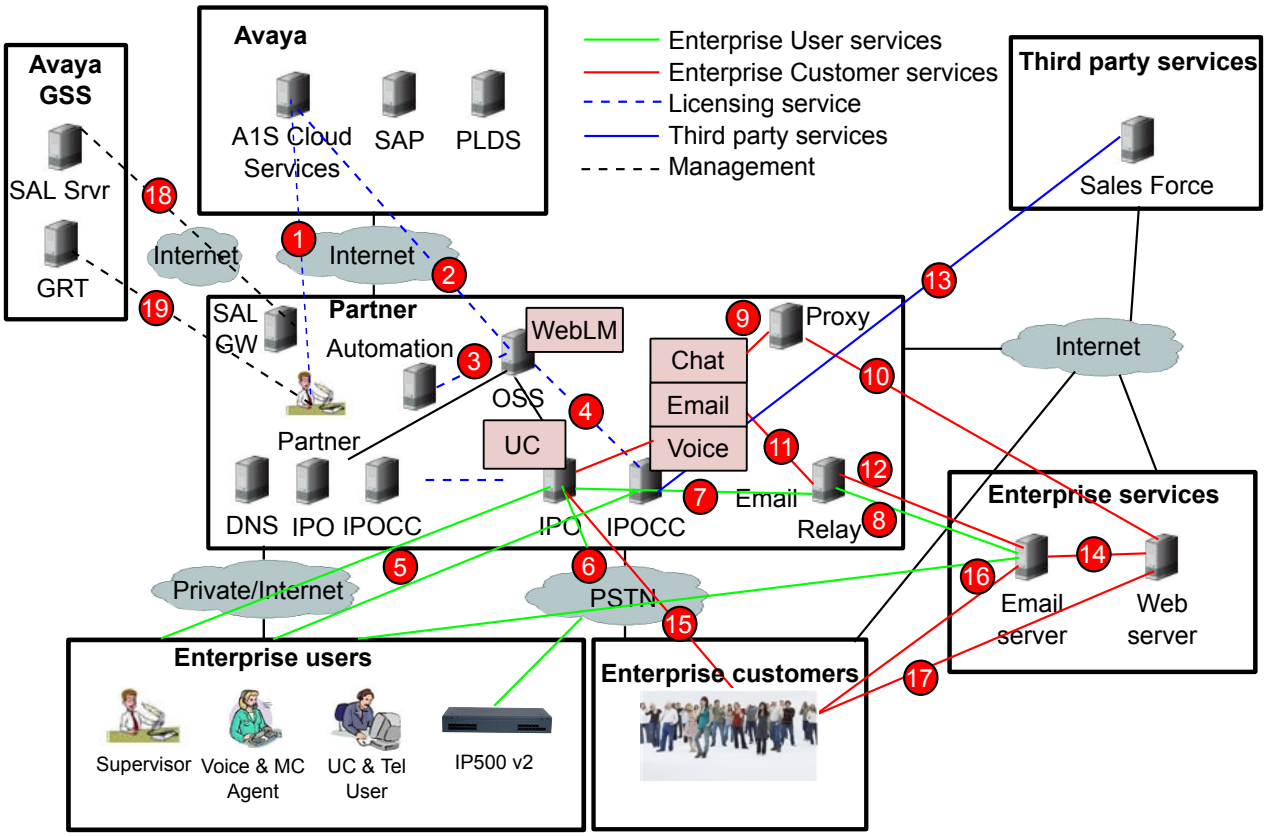


Figure 19: Powered by Avaya topology

Contact center reference configurations

IP Office Contact Center deployment options

IP Office Contact Center can be deployed using the following deployment configurations and options:

Configuration	Deployment options	Agents and trunks
IP Office Contact Center with IP500V2	IP500V2, IP Office Contact Center server, and an application server	Up to 30 agents on SIP and digital trunks.
IP Office Contact Center with IP Office Server Edition	IP Office Server Edition server and IP Office Contact Center server *and/or* a Linux expansion server (optional) *or* Hosted as a service in a cloud environment	Up to 250 agents on SIP trunks. Only 125 agents can be deployed on each Linux expansion node.

Table continues…

Página2339 de 3226.

Configuration	Deployment options	Agents and trunks
IP Office Contact Center with IP Office Server Edition and IP500V2 expansion	IP Office Server Edition server, IP500V2 expansion server, and IP Office Contact Center server	Up to 250 agents on SIP and digital trunks. Only 30 agents can be deployed on each IP500V2 node.
IP Office Contact Center with IP Office Server Edition in a distributed environment	IP Office Server Edition server, IP500V2 expansion server, IP Office Contact Center server, and a Linux expansion in a distributed environment	Up to 250 agents on SIP and digital trunks. Up to 30 agents can be deployed on each IP500V2 node, and up to 125 agents can be deployed on each Linux expansion node. Agents and trunks are distributed on any expansion server.

Detailed IP Office Contact Center topologies are shown in the following documents:

- *Avaya IP Office Contact Center Feature Description*
- *Avaya IP Office Contact Center Reference Configuration*

Avaya Contact Center Select reference configurations

Avaya Contact Center Select is a feature-rich contact center solution that provides skill-based routing for customer voice and multimedia contacts. Avaya Contact Center Select provides extensive tools for agent management, real-time and historical reporting, and graphical tools to create contact flows and treatment rules. It provides license management, networking, and Open Interfaces Web Services. Customers integrating Avaya Contact Center Select with the IP Office platform gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility.

At deployment time, Avaya Contact Center Select automatically launches a simple configuration wizard to rapidly deploy a functional contact center solution. It is preloaded with sample users, skillsets, and contact center parameters. Use this sample data to rapidly commission the solution and make the first routed customer call and email contact.

Avaya Contact Center Select supports the following routed contact types:

- Voice
- Email
- Outbound
- Web communications (Web chat)
- SMS text messages
- Fax messages
- Scanned documents
- Voice mail messages
- Social Networking

Página2340 de 3226.

Avaya Contact Center Select also supports peer-to-peer Instant Messaging. To support the email-based contact types, you must add an email server to your solution. To support the Web communications contact type, you must add a Web communications server to your solution.

Avaya Contact Center Select provides a simplified voice prompt management utility. The contact center supervisor can perform prompt management work without requiring administrator access to the Avaya Contact Center Select server. Avaya Contact Center Select provides a number of status monitoring utilities to monitor the integration points with IP Office.

Contact Center Manager Administration is a browser-based configuration and reporting interface for Avaya Contact Center Select. Avaya Contact Center Select supervisors use Contact Center Manager Administration to configure contact center resources, agents, skillsets, contact flows, components, and activities. Contact Center Manager Administration provides historical and real-time reporting about the contact center.

User data synchronization

Avaya Contact Center Select provides unified administration for contact center agents and IP Office users. The users (agents and agent-supervisors) that you configure in Avaya Contact Center Select are automatically mirrored to the connected IP Office.

When you create an agent in Avaya Contact Center Select, a matching user account is created in IP Office. When you modify agent details in Avaya Contact Center Select, the corresponding IP Office user details are automatically updated. However, if you delete an agent in Avaya Contact Center Select, the corresponding IP Office user is not deleted. Synchronization works in one direction — from Avaya Contact Center Select to IP Office. The IP Office administrator can manually force data synchronization from Avaya Contact Center Select.

Topology

In a contact center solution using Avaya Contact Center Select and an IP Office telephone system, the following network and connectivity topology considerations apply:

- The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.
- Each Avaya Contact Center Select connects to a single IP Office Server Edition Primary server. Alternatively, each Avaya Contact Center Select can connect to a single IP Office 500V2 Standard Mode with an Advanced Edition license.
- A Small Community Network (SCN) is a system of networked IP Office systems that can, among other features, share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select. Avaya Contact Center Select connects to the IP Office Server Edition Primary server of the SCN. To support an IP Office SCN, Avaya Contact Center Select must connect to an IP Office Server Edition Primary server in that SCN network.
- The Avaya Contact Center Select server and the connected IP Office telephone system must be located in the same campus location.
- Each supervisor client computer communicates with the Avaya Contact Center Select server. The supervisor uses the Contact Center Manager Administration Web interface to configure agents and run reports. The agent supervisor uses the Avaya Agent Desktop software to handle customer calls, to accept emergency or supervisor calls from agents and to observe calls or Web communication contacts. Each voice-enabled supervisor with Agent Desktop requires an associated IP Office telephone.

- Each agent client computer communicates with the Avaya Contact Center Select server. The agent uses Agent Desktop to handle customer voice and multimedia contacts. Each voice-enabled agent requires an associated IP Office telephone.

Avaya Contact Center Select supports the following deployment options:

- Avaya Contact Center Select DVD
- Avaya Contact Center Select VMware
- Avaya Contact Center Select hardware appliance
- Avaya Contact Center Select Business Continuity

For more information about Avaya Contact Center Select deployment options, refer to *Avaya Contact Center Select Solution Description*.

Related links

Reference configurations on page 67
Avaya Contact Center Select DVD on page 80
Avaya Contact Center Select and VMware on page 81
Avaya Contact Center Select hardware appliance on page 82
Avaya Contact Center Select Business Continuity on page 83

Avaya Contact Center Select DVD

The Avaya Contact Center Select DVD contains the contact center application software. The DVD deployment option supports Platform Vendor Independence (PVI). PVI gives the customer the flexibility to purchase a server that meets the Avaya Contact Center Select server requirements and conforms to the customer's own corporate standards.

Avaya Contact Center Select supports a range of PVI server specifications, each specification supporting a specified maximum agent capacity and call rate. This range of PVI specifications gives the customer the flexibility to use the minimum hardware to meet their solutions requirements while allowing for future expansions.

The Avaya Contact Center Select DVD deployment option does not require VMware resources or infrastructure, which keeps Total Cost of Ownership (TCO) and solution complexity to the minimum.

Página2342 de 3226.

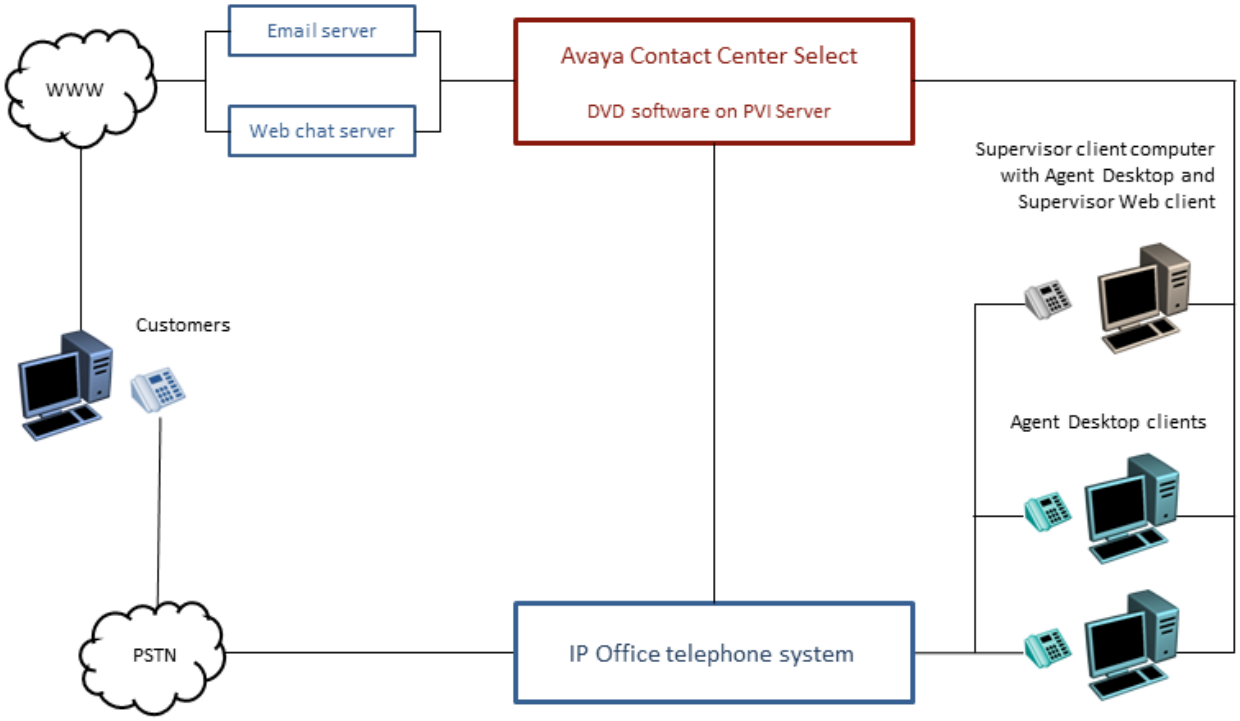


Figure 20: Typical Avaya Contact Center Select DVD deployment

To use the Avaya Contact Center Select DVD deployment option, the customer must provide the following:

- Server hardware that meets one of the Avaya Contact Center Select PVI specifications: Entry-level, Mid-range, or High-end.
- Microsoft Windows 2012 R2 Standard or Datacenter Edition operating system and license.

For more information about the Avaya Contact Center Select DVD option, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select and VMware

Avaya Contact Center Select supports VMware virtualization for increased productivity, flexibility and efficiency. All Avaya Contact Center Select deployment options support the virtualized IP Office Server Edition OVA on VMware.

Avaya Contact Center Select offers a software appliance package that consists of the following components:

- Avaya Contact Center Select virtual machine
- Avaya Aura® Media Server OVA
- Avaya WebLM OVA

Deploy these virtual machines and IP Office to build a virtualized and scalable contact center solution.

Página2343 de 3226.

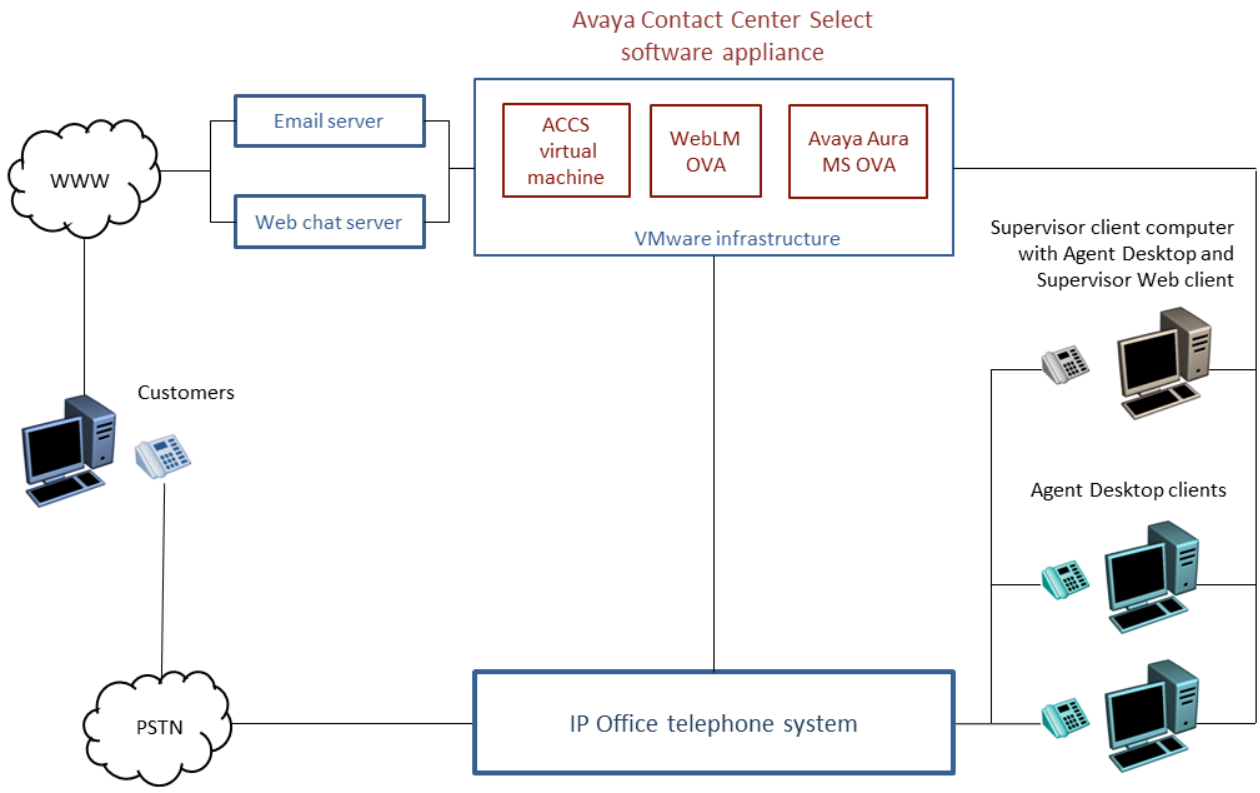


Figure 21: Typical Avaya Contact Center Select and VMware solution

Avaya Contact Center Select is a collection of applications providing real-time call control, multimedia handling, and statistical reporting. Deploy Avaya Contact Center Select on an enterprise-grade VMware virtual environment. Avaya recommends that you apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a virtualization infrastructure.

Avaya Contact Center Select supports VMware ESXi. VMware vCenter software is not required; however it is supported and it is useful for Avaya Contact Center Select in multi-host contact center environments.

For more information about Avaya Contact Center Select and VMware, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select hardware appliance

The Avaya Contact Center Select hardware appliance is a physical rack-mount server with the Avaya Contact Center Select application software already loaded and partially preconfigured. Avaya supplies the server hardware and a license for the Microsoft Windows 2012 R2 Standard Edition operating system.

The Avaya Contact Center Select hardware appliance server delivers speedy and simplified contact center deployment.

Página2344 de 3226.

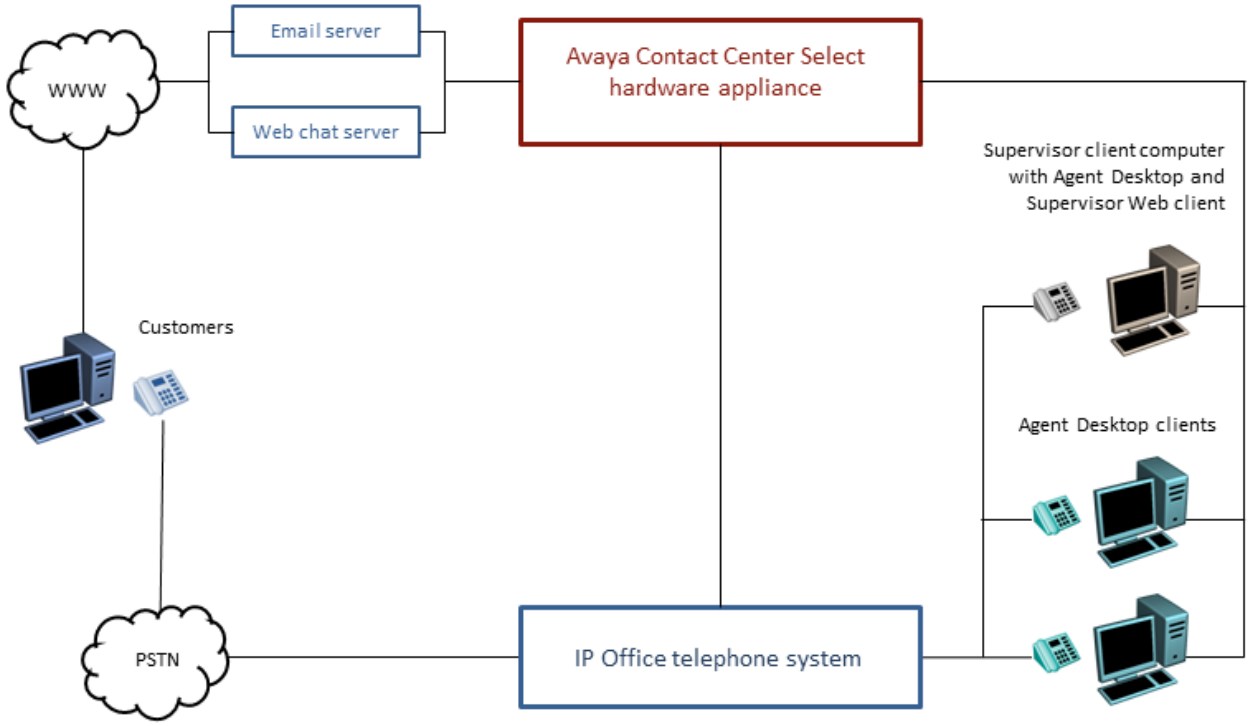


Figure 22: Typical Avaya Contact Center Select hardware appliance solution

After the basic telephony and email features are working, you can then configure more multimedia contacts, multiplicity, custom prompts, and other enhanced features and functions to improve your customer's experience.

The hardware appliance server supplied by Avaya is optimized to provide all of the real-time computational and logging resources required by Avaya Contact Center Select. The hardware appliance supports the Avaya Contact Center Select maximum agent and call rate capacity.

Avaya provides the Microsoft Windows operating system product key for the hardware appliance. The product key is displayed on a sticker attached to the top of the Avaya Contact Center Select hardware appliance server.

For more information about the Avaya Contact Center Select hardware appliance, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select Business Continuity

Business Continuity is an Avaya Contact Center Select licensed feature. Avaya Contact Center Select solutions that support Business Continuity have two Avaya Contact Center Select servers. One server, called the active server, processes customer contacts. The other server, called standby or Remote Geographic Node, shadows the active server. If the active server fails, the other Avaya Contact Center Select server can take over contact processing. This feature provides Avaya Contact Center Select redundancy, data resiliency, and disaster recovery.

To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active

Página2345 de 3226.

and standby servers. Avaya Contact Center Select agents are also supported in domains with a two-way trust relationship with the Avaya Contact Center Select server domain.

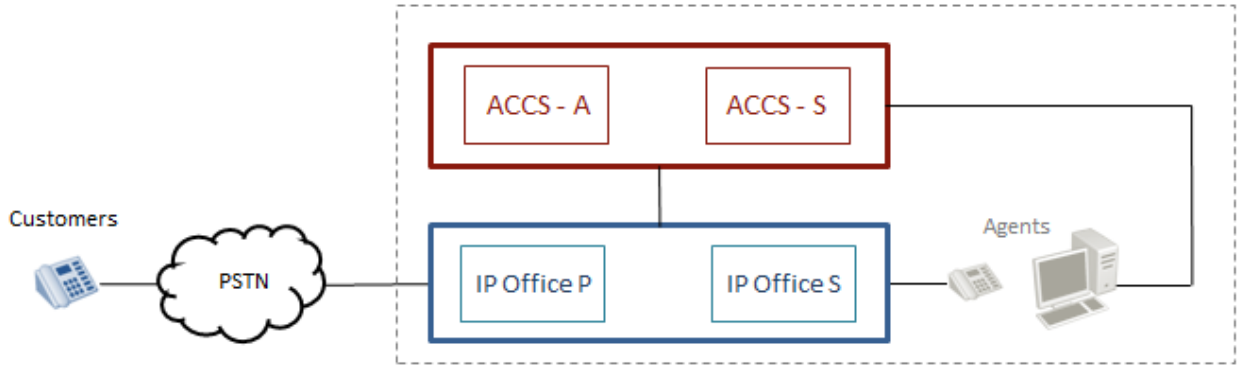


Figure 23: Avaya Contact Center Select Business Continuity with IP Office resilience

IP Office Server Edition solutions support voice platform resilience when an IP Office Secondary Server is added to the solution. Avaya Contact Center Select supports this IP Office resilience feature.

All Avaya Contact Center Select deployment options, DVD, VMware, and Hardware Appliance, support Contact Center Business Continuity and IP Office resilience. Avaya Contact Center Select Business Continuity adds additional resource requirements, topology, network connectivity, and domain layout considerations to the solution.

For more information, refer to *Avaya Contact Center Select Business Continuity*.

Hardware and software options

Hardware options

Server, base card, trunk card, and expansion module hardware options are available depending on the edition required:

- Dell PowerEdge™ R210 or R620
- Hewlett Packard ProLiant DL120 G7 or DL360 G7
- Avaya IP500 V2

Software options

IP Office acts as a server for a variety of applications, including:

- Avaya Communicator for IP Office supported on Windows and iPad devices
- Avaya one-X® Mobile for IP Office
- Avaya one-X® Portal for IP Office

Página2346 de 3226.

- Lync Integration for IP Office
- IP Office SoftConsole
- IP Office Media Manager
- Avaya Equinox™ client for IP Office
- Avaya IP Office Web Client

IP Office can also be deployed with other components. You can deploy IP Office with Radvision or other video endpoints. You can also use IP Office Branch solution offer to connect IP Office branches to the Avaya Aura® infrastructure, allowing users to leverage core Avaya Aura® applications and services including centralized dial plans, voice mail, management, and licensing.

Related links

Accessing Avaya DevConnect Application Notes on page 134
Interoperability on page 93

Server specifications

The following tables list the minimum server specifications for the IP Office Server Edition Solution:

Server option	Large server #1	Large server #2	Large server #3
Chassis	Dell R630 1U	Dell R620 1U	HP DL360G7 1U
Processor	2 x E5-2620v3, 2.4 GHz	2 x E5-2630, 2.3 GHz	2 x E5620, 2.4 GHz
Memory (RAM)	32 GB	32 GB	12 GB
Hard disk drive	2 x 600 GB	2 x 600 GB	2x 300 GB, 10K
RAID	RAID 1 Hot swap	RAID 1 Hot swap	RAID 1 Hot swap
RAID Controller	H730	H710	P410i
Power Supplies	2x 750W AC Hot swap	2x 495W AC Hot swap	2x 460W AC Hot swap
NICS	6x GB full duplex	4x GB full duplex	4 Port, Motherboard
Optical Drive	1x DVD +/- RW	1x DVD +/- RW	1x DVD+/-RW, SATA, INTERNAL
PCI Type	2 x8 Gen2 Slots (PCIe)	2 x8 Gen2 Slots (PCIe)	1-LP X8 PCIe & 1-FL/FH X16 PCIe Riser

Server option	Small server #1	Small server #2	Small server #3
Chassis	HP DL120G7 1U	Dell R210 1U	Dell R220 1U
Processor	1 x E3-1220, 3.1 GHz	1 x E3-1220, 3.1 GHz	1 x E3-1220, 3.1 GHz
Memory (RAM)	12 GB	12 GB	16 GB
Hard disk drive	1x 250 GB, 7.5K	1x 250 GB, 7.5K	1x 500 GB, 7.2K
RAID	RAID 0 (none)	RAID 0 (none)	RAID 0 (none)

Table continues…

Página2347 de 3226.

Server option	Small server #1	Small server #2	Small server #3
RAID Controller	P212, 256 MB	On board	On board
Power Supplies	1 x 400 W AC	1 x 502 W AC	1 x 250 W AC
NICS	2 Port, Motherboard	2 Port, Motherboard	2 Port, Motherboard
Optical Drive	1x DVD+/-RW, SATA, INTERNAL	1x DVD+/-RW, SATA, INTERNAL	1x DVD+/-RW, SATA, INTERNAL
PCI Type	1-HL/LP X8 PCIe & 1-FL/FH X16 PCIe Riser	1 x16 Gen2 Slots (PCIe)	1 x16 Gen2 Slots (PCIe)

Note:

In some geographies, where 12 GB of RAM is not a standard Dell option use 16 GB RAM.

Server Combinations and Usage

- The Server Edition Primary and Server Edition Secondary must be on the same platform. This constraint applies equally to virtual servers. It is possible to mix native and virtual central servers, but the resources allocated to the virtual environment should match the native server.
- Virtualised and native servers can be mixed in the same Server Edition solution in any role, provided the Server Edition Primary and Server Edition Secondary are the same as indicated above.
- It is possible to use the Unified Communication / Application Server R210 / DL120 is / R220 servers as this is the same hardware and software as the Server Edition R210 / DL120 / R220 servers. If the server is installed with theServer Edition software, it will be supported by Avaya.
- You cannot set up a Server Edition Expansion System(L) in the Standard IP Office mode of operation in the IP Office Server Edition Solution.
- You cannot re-provision a Server Edition server without a complete reinstall. For example, you cannot convert a primary server to a secondary or expansion system.
- You cannot set up a Server Edition Expansion System (L) in the Standard IP Office mode of operation in the IP Office Server Edition Solution. You cannot convert a Server Edition Expansion System (V2) to a Server Edition Primary or Server Edition Secondary server.
- The use of any external Voicemail Pro server (either Linux or Windows) is not supported.
- The use of an external Avaya one-X® Portal server not running Server Edition software, and not running on a supported server, is not supported.

Note:

Salesforce (SFDC) has been removed from Avaya one-X® Portal.

Página2348 de 3226.

Operating system and browser support

Windows Operating System

Table 7: Windows Editions and Service Packs

Operating System*	Service Pack	Edition
Windows 7	SP1	Professional, Enterprise, Ultimate
Windows 8.1	N/A	Professional, Enterprise
Windows 10	N/A	Professional (SMB), Enterprise
Windows Server 2012	N/A	Standard
Windows Server 2012 R2	N/A	Standard
Windows Server 2016	N/A	Standard, Essentials

* Windows Server 2008 R2 (64-bit) is not supported from Release 10.1.

Table 8: Windows Support – Server Components

Server	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
Preferred Edition server (Voicemail Pro) Standalone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Preferred Edition server with UMS	No	No	No	No	No	No	Yes	Yes
Preferred Edition server with Campaigns	No	No	No	No	No	No	Yes	Yes
Preferred Edition server with IMS	No	No	No	No	No	No	No	No
Preferred Edition server with MAPI service for Voicemail Pro on Linux	Yes	Yes	No	No	No	No	Yes	Yes
Avaya one-X® Portal for IP Office server	No	No	No	No	No	No	Yes	Yes
TAPI first-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI third-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

Página2349 de 3226.

Server	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
TAPI WAV[2]	Yes	No	Yes	No	Yes	No	No	No

* Windows 8.1 is the replacement/Service Pack for Windows 8.0. Therefore, we no longer support Windows 8.0.

Table 9: Windows Support – Thick Client Apps

Application	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
Preferred Edition client	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Office SoftConsole	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
IP Office Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SysMonitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System Status Application	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI first-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI WAV[3]	Yes	No	Yes	No	Yes	No	No	No
Avaya Equinox™ for Windows	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Avaya Communicator for Windows	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Avaya one-X® Portal plug-in for Microsoft Outlook	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Call Assistant	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Plug-in for Microsoft Lync 2013/Skype for Business[4]	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Table continues…

[2] TAPI WAV is not recommended for new designs and is not supported on a 64-bit OS.
[3] TAPI WAV is not recommended for new designs and is not supported on a 64-bit OS.
[4] Plug-in for Microsoft Lync 2010 is not supported from Release 10.1.

Página2350 de 3226.

Application	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
Web Conferencing [5]	Yes	Yes	Yes	Yes	Yes	Yes	No	No
IP Office Web Client	Yes	Yes	Yes	Yes	Yes	Yes	No	No

* Windows 8.1 is the replacement/service pack for Windows 8.0. Therefore, we no longer support Windows 8.0.

macOS Operating System

Table 10: macOS Support – Thick Client Apps

Application	macOS 10.8 (Mountain Lion)	macOS 10.9 (Mavericks)	macOS 10.10 (Yosemite)	macOS 10.11 (El Capitan)	macOS 10.12 (Sierra)	macOS 10.13 (High Sierra)
Web Conferencing [6]	Yes	Yes	Yes	Yes	Yes	
Avaya Equinox™ for Mac	No	No	No	Yes	Yes	Yes

Browsers

Table 11: Supported Browsers

Application	Internet Explorer 10*	Internet Explorer 11	Edge	Firefox	Chrome	Safari 8	Safari 9	Safari 10
Voicemail Pro Campaigns	Yes	Yes	Yes	No	No	No	No	No
Voicemail Pro UMS WebMail	Yes	Yes	Yes	No	No	No	No	No
Avaya one-X® Portal for IP Office client	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Web Conferencing[7]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Table continues…

[5] Includes Adobe Flash and Java Applet for sharing.
[6] Includes Adobe Flash and Java Applet for sharing.
[7] Includes Adobe Flash and Java Applet for sharing.

Application	Internet Explorer 10*	Internet Explorer 11	Edge	Firefox	Chrome	Safari 8	Safari 9	Safari 10
Web Manager and Web Control Page	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
D100 DECT Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP DECT R4 Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Avaya Communicator for Web	No	Yes	No	No	Yes	No	No	No
IP Office Media Manager	Yes	Yes	Yes	Yes	Yes	No	No	No
Avaya IP Office Web Client	No	No	No	No	Yes	No	No	No

* Only on Windows Server 2012; however, Server 2012 R2 supports Internet Explorer 11.

Other Apps

Table 12: Microsoft Exchange

Application	Exchange 2010	Exchange 2013	Exchange 2016
Voicemail Pro UMS	Yes	Yes	Yes
Avaya one-X® Portal for IM and Presence	Yes	Yes	Yes

Table 13: Microsoft Outlook

Application	Outlook 2010	Outlook 2013	Outlook 2016
Voicemail Pro IMS	No	No	No
TAPI (for dialing)	Yes	Yes	Yes
Voicemail Pro UMS with IMAP	Yes	Yes	Yes
Avaya one-X® Portal Outlook Plug-in[8]	Yes	Yes	Yes

[8] For Outlook 2013 and later, the contact screen popping feature is not supported.

Página2352 de 3226.

Virtualization

Table 14: Virtualization support

Hypervisor	IP Office Server Edition	IP Office Partner-Hosted
VMware ESXi 5.1	Yes	Yes
VMware ESXi 5.5 U2+	Yes	Yes
VMware ESXi 6.0	Yes	Yes
VMware ESXi 6.5	Yes	Yes
VMware ESXi 6.7	Yes	Yes
Microsoft HyperV on Server 2012 R2	Yes	Yes
Microsoft HyperV on Server 2016	Yes	Yes
KVM	No	Yes
Amazon AWS	Yes	Yes

Note:

Google KVM is supported on QEMU with CentOS version 6 and 7 in case of Powered by Avaya (hosted) solution and not supported for CPE. For more information, see *Deploying Powered by Avaya for Business Partners guide*.

Customer-provided PC requirements

The following customer-provided PC requirements for applications are the minimum required.

IP Office Manager

IP Office Manager is used to access all parts of the configuration. Different levels of access can be defined to control which parts of the configuration the IP Office Manager user can view and alter. IP Office Manager is also used to upgrade the software files on the system. IP Office Manager acts as a TFTP server from which some Avaya telephones can request new software.

RAM	Standard Edition: 4 GB Server Edition: 6 GB Select Server Edition: 8 GB
Hard disk free space	1 GB
Processor	Standard Edition: Core i3 Server Edition: Core i5 Select Server Edition: Core i5
Operating system	Operating system and browser support on page 88

Página2353 de 3226.

Additional software	.NET Framework 4.0: Installed with the software if not already installed.

IP Office SysMonitor

RAM	128 MB
Hard disk free space	10 GB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 88

IP Office System Status Application

RAM	256 MB
Hard disk free space	1.4 GB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 88
Additional software	Sun Java Virtual Machine Web Browser: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

TAPI

RAM	64 MB
Hard disk free space	50 MB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 88
Additional software	Web Browser: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

Página2354 de 3226.

Virtual environment requirements

Ensure you have the following:

- VMware vSphere client software for management (vSphere ESXi software and virtualized instances running on a single host server)

  Note:

  vCenter software is not required, however might be useful for multi-host server environments.

- Host hardware supporting VMware vSphere and IP Office Server Edition resource requirements and specifications to meet configuration needs.

VMWare ESXi support:

- IP Office Server Edition and IP Office Contact Center support VMWare ESXi 5.1 and 5.5 U2.
- IP Office Contact Center supports VMWare ESXi 6.0. IP Office Server Edition supports VMWare ESXi 6.0 for only versions 10.0 and later.

  For more information about IP Office Contact Center support and specifications, see *Avaya IP Office Contact Center Reference Configuration*.

Note:

ESXi 4.x is no longer supported.

Additional hypervisor support:

Hypervisor support is now extended to:

- Microsoft Hyper-V
- AWS (for Amazon Web Services): An AMI (Amazon Machine Image) is provided that can perform Auto Ignition and ICU based on User Data set in AWS. The AMI will behave similar to the existing Google Compute Image. Consult the instance types that Amazon EC2 supports on the Amazon AWS website.

  In Amazon Dashboard, you need to select Launch Instance under Create Instance. Select Community AMIs and search for Avaya IP Office.
- KVM (for Kernel-based Virtual Machine)

Interoperability

Interoperability means that two systems can communicate with an interface in each system to handle the communication. Compatibility means that two components in the same environment are compatible with each other if they run or reside in the environment without adversely affecting the behavior of the other.

For detailed information about IP Office interoperability and supported releases, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=IP+Office+Platform.

Página2355 de 3226.

Avaya product interfaces

IP Office includes an interface to the following Avaya products:

- Avaya Aura®
- Avaya Contact Center Select
- Avaya Aura® Messaging
- Avaya CallPilot®
- Avaya Cloud Video Phase
- Avaya Communicator for Windows
- Avaya Communicator for iPad
- Avaya Equinox™
- Avaya one-X® Communicator
- Avaya Session Border Controller for Enterprise
- Avaya Business Communications Manager
- Avaya Communication Server 1000
- Avaya Modular Messaging
- Avaya Scopia®
- Secure Access Link
- Avaya Aura® Experience Portal

ISDN interfaces

EU interfaces:

- BRI: RJ45 sockets. ETSI T-Bus and S-Bus interfaces to CTR3 for Pan European connection
- PRI E1: RJ45 socket. ETSI T-Bus interface to CTR4 for Pan European connection
- PRI T1/J1: RJ45 socket: FCC Part 68/JATE connection

USA interfaces:

- PRI T1 service: Ground Start (GS) - Default, E&M, 56 K data for 5ESS, 56/64/64 restricted for 4ESS
- PRI ISDN switch support: 4ESS, 5ESS, DMS-100, DMS-250 (includes conformance to ANSI T1.607 and Bellcore Special Report SR4287, 1992)
- PRI ISDN Services: AT&T Megacom 800, AT&T WATS (4ESS), AT&T SDS Accunet 56 Kbps and 64 Kbps (4ESS), AT&T Multiquest (4ESS)

Related links

Phone interoperability on page 95
IP Office and Avaya Aura Communication Manager interoperability on page 99
BCM and IP Office interoperability on page 100
Accessing Avaya DevConnect Application Notes on page 134
Product compatibility on page 133
Hardware and software options on page 84

Página2356 de 3226.

Phone interoperability

The following table summarizes the phone interoperability comparison by IP Office edition.

Table 15: Generally available phones

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
Analog deskphones:			
POTS	Yes	Yes	No
1000 Series Video phones:			
1010, 1020, 1030, 1040 (Lifesize)	No	Yes	No
1400 Series : DS Digital phones – IP Office and Communication Manager			
1403, 1408, 1416	Yes	Yes	No
DBM32	Yes	Yes	No
1600 Series : IP (H.323) phones – IP Office and Communication Manager			
1603, 1603SW, 1603SW–i, 1608, 1608–i, 1616, 1616–I	No	Yes	Yes
2400 Series: DS Digital phones – IP Office and Communication Manager			
2402D, 2410D, 2420	Yes	Yes	No
EU24	Yes	Yes	No
3600 Series: WiFi H.323 – IP Office and Communication Manager			
3641, 3645	No	Yes	Yes
3700 Series: DECT – IP Office and Communication Manager			
3720, 3525, 3730, 3735, 3745, 3749	No	Yes	Yes
9500 Series: DS digital – IP Office only			
9504, 9508	Yes	Yes	No
BM12	Yes	Yes	No
9600 Series: IP H.323 – IP Office and Communication Manager			
9620L, 9620C, 9630, 9640G, 9650, 9650C	No	Yes	Yes
SBM24 with 96x0	No	Yes	Yes
9608, 9611, 9621, 9641, J169, J179	No	Yes	Yes
BM12	No	Yes	Yes
B100 Series Conference Phones:			
B149, B159	Yes	Yes	No

Table continues…

Página2357 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
B179 SIP	No	Yes	Yes
D100/D160 DECT Phones:			
D160	Yes	Yes	Yes
E100 Series IP Phones:			
E129	No	Yes	Yes
E159	No	Yes	Yes
E169	No	Yes	Yes
H100 Series Video Collaboration Stations:			
H175	No	Yes	Yes
Avaya J100 Series IP Phones:			
Avaya J139 IP Phone	No	Yes	No
Avaya J169 IP Phone	No	Yes	No
Avaya J179 IP Phone	No	Yes	No
Softphone:			
Avaya Communicator Windows	No	Yes	Yes
Avaya Communicator iPad	No	Yes	Yes
Avaya Equinox™	No	Yes	Yes

Table 16: Generally available NORSTAR/BCM phones

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
1100 Series SIP phones: BCM Unistim migration			
1120E, 1140E	No	Yes	Yes
BM LED and paper labels	No	Yes	Yes
BM LCD	No	Yes	Yes
1200 Series SIP phones: BCM Unistim migration			
1220, 1230	No	Yes	Yes
BCM paper	No	Yes	Yes
BCM LCD	No	Yes	Yes
NORSTAR/BCM Digital phones:			

Table continues…

Página2358 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
T7000, T7100, T7208, T7316, T7316E	Yes	Yes	No
T24 Key Module	Yes	Yes	No
M7100(N), M7208(N), M7310(N), M7310BLF, M7324(N)[9]	Yes	Yes	No
CAP Key Module	Yes	Yes	No
NORSTAR/BCM Digital Conference Phone	Yes	Yes	No
Nortel Digital Mobility phones:			
T7406, T7406E	Yes	Yes	No
7420, 7430, 7434, 7439, 7440, 7449	Yes	Yes	No
4135, 4136, 4145, 4146, 4145EX, 4146EX	Yes	Yes	No

Avaya has tested the following phones for interoperability with IP Office. These phones may not support all features. If the phone is past its Avaya Manufacturer Support Period, issue resolution is limited to those already fixed.

Table 17: Supported Avaya phones no longer for sale

Note:

Supported in this context means the phones have been tested by Avaya for interoperability with IP Office. Older phone models may not support new features if the phone model is outside of the Avaya Manufacturer Support period. If there is a software update related to the Release 11.0, a software fix will not be provided for Phones that are outside of the Avaya Manufacturing Support period. Phones “No Longer supported” are outside of the Avaya Manufacturing Support period and are not covered under Avaya Maintenance offers (End of Service Support and End of Maintenance Support)

1. OSX 10.9 Mavericks is last OS version supported for Video Softphone for MAC. That client is no longer available on either of 10.x or 11.0 software for same reason. Avaya Communicator for Web, Avaya IP Office Web Client, and Avaya Equinox™ are available for Mac users on IP Office Release 11.0.
2. Digital and analog phones are supported with Server Edition or Select as indicated using the IP500 V2 as an expansion module.

[9] Only the global version of the M7000 Series phones are supported. The non-global versions are not supported and can be identified by the contrast levels; the global version has 9 contrast levels and the non-global version has only 4 contrast levels.

Página2359 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
ETR phones: Analog Feature Phone, PARTNER and IP Office			
“Refreshed” 34, 18 and 6 button display	Yes	No	No
“Euro” 34 and 18 button display	Yes	No	No
“Euro” 18 and 6 button display	Yes	No	No

Related links

Interoperability on page 93
Phone availability on page 98
Accessing Avaya DevConnect Application Notes on page 134
Using the Avaya InSite Knowledge Base on page 134
Phones on page 38

Phone availability

Phones available worldwide

The Avaya phones listed below are the recommended phones for use with IP Office. These phones are sold worldwide in every country where IP Office is available.

For detailed specifications, see specific phone information on the Avaya Support site at http://support.avaya.com.

Digital phone models	IP phone models
1403	1603
1408	1608
1416	1616
9504	9608
9508	9611
	9621
	9641
	Avaya J169 IP Phone
	Avaya J179 IP Phone
	Avaya J139 IP Phone

Phones only available in certain countries

In addition to the phones listed above, the following Avaya phones are available in certain countries and regions.

Página2360 de 3226.

Digital/Analog phone models	IP phones
2402	9620L/9620C
2410	9630G/9640/9640G
2420	9650/9650C
3810 Wireless	3720 DECT R4 Wireless Handset
EU24/EU24BL DSS Unit	3725 DECT R4 Wireless Handset
	3730 DECT R4 Wireless Handset
	3735 DECT R4 Wireless Handset
	3745 DECT R4 Wireless Handset
	3749 DECT R4 Wireless Handset
	3641 Wireless (WiFi) phone
	3645 Ruggedized Wireless (WiFi) phone
	D100

Related links

Phone interoperability on page 95

IP Office and Avaya Aura® Communication Manager interoperability

IP Office uses H.323 protocol for trunks between the nodes and the Avaya Aura® Communication Manager. Centralized voicemail for all IP Office systems in the SCN network and all phones are supported on the individual call servers. Advanced call handling features are available between the IP Office nodes. This interface works on Essential and Preferred Editions.

Supported phones include:

- Avaya IP phones (H.323)
- Avaya digital phones
- BCM 7000 series digital phones
- BCM 1100/1200 series IP phones (SIP)
- DECT R4 phones
- Analog phones

These features allow for simple networking needs between IP Office remote branches to an Avaya Aura® Communication Manager at the main site.

Página2361 de 3226.

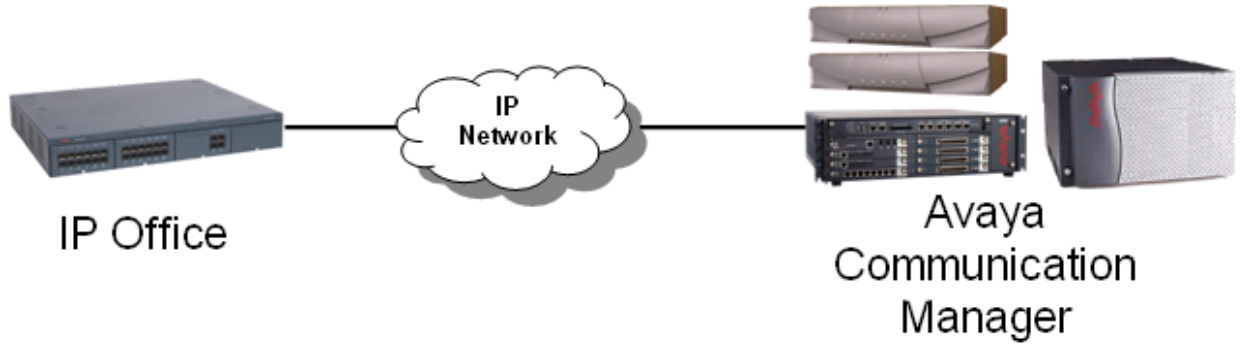


Figure 24: VoIP networking using H.323

Q.SIG provides the following supplementary services which are also available between IP Office and Avaya Aura® Communication Manager equipped with the relevant RFA licenses:

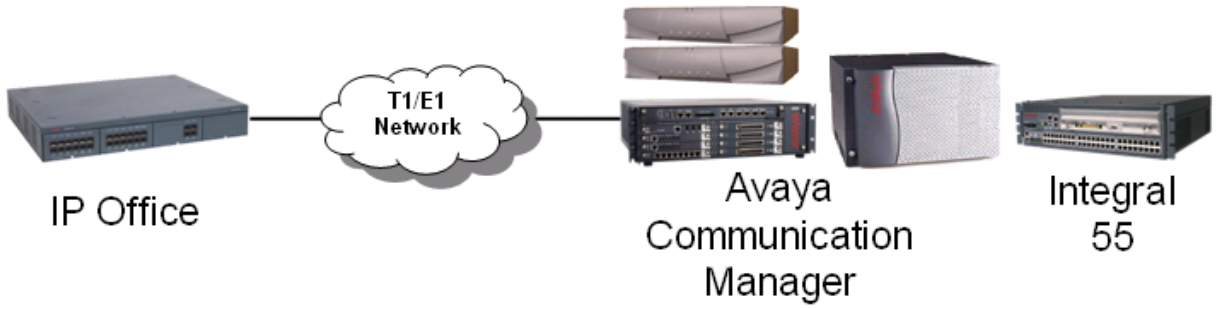


Figure 25: Q.SIG networking using T1/E1 links (TDM)

Related links

Interoperability on page 93

BCM and IP Office interoperability

The SIP interoperability support between IP Office and BCM50/450 allows customers to migrate a network of BCM, step-by-step, to an IP Office SCN or Server Edition network.

Protocol support	IP Office to BCM: SIP BCM to BCM: SIP or SIP/MCDN IP Office to IP Office H.323: SCN or SIP
	Note: It is not possible to connect IP Office and BCM through the MCDN or SCN protocol directly.
IP Office platform requirements	Release 8.1 or higher, Essential, Preferred or Server Editions

Página2362 de 3226.

BCM platform requirements	BCM50 or BCM450 6.0
Centralized voicemail	IP Office with a centralized Voicemail Pro system in the SCN network BCM with a centralized voicemail within the BCM MCDN network. **Note:** Centralized Voicemail across IP Office and BCM systems is not supported.
Phones	All phones supported on the individual call servers and releases including Avaya IP Phone (H.323), Avaya Digital phones, BCM 7000 Series Digital phones, BCM1100/1200 Series IP Phones (SIP), DECT R4 and Analog phones.
Features	Advanced feature set of IP Office SCN available between the IP Office and BCM. MCDN features are also available between the IP Office and BCM. The standard SIP features are supported.

Related links

Interoperability on page 93

Security specification

The Avaya Product Security Support Team (PSST) responds to ongoing security vulnerabilities for all Avaya Products. For more information, see *Avaya Product Security Vulnerability Response Policy* and *Avaya Security Vulnerability Classification* at the Avaya Support website at https://support.avaya.com/security.

Default security

The IP Office software security engine is supplied by Mocana Corporation. For more information, see https://www.mocana.com.

Security features are built-in into the software platform. These features consist of:

- Integrated firewall to prevent Denial of Service (DoS) attacks
- Secure connections to ensure the privacy and integrity of transmitted information including:
  - TSL on administration interfaces
  - HTTPS client
  - HTTPS server
  - IPSec
  - SIP-TLS

Página2363 de 3226.

- SSL/VPN
- VMPro/Exchange MAPI integration (TLS)

For detailed information about SSL/VPN remote access, see *Deploying Avaya IP Office™ Platform SSL VPN Services* and *Avaya IP Office™ Platform Port Matrix* at the Avaya Support website.

Configurable security

Configurable security settings include the following features:

- Encryption and message authentication
- Configuring integrated firewall settings
- Digital certificates
- Prevention of tool fraud by restricting user privileges and using security policy configuration to manage account credentials and access control

See *Avaya IP Office™ Platform Security Guidelines* for more information.

Network security

Network security leverages resources such as VLANs and firewalls available on the enterprise network and includes:

- External firewall configuration
- Separate of network functionality by creating separate VLAN groups and security zones
- Hardening of Layer 2 (data link layer) and Layer 3 (Network layer) by configuring SNMP trap destinations, syslog entries, and an IPSec VPN.
- SSL/VPN remote access

Operational security

Ongoing operational security to maintain a secure system includes:

- Patching
- Logging and monitoring
- Virus protection

Related links

Platform and application security details on page 102

Platform and application security details

For additional information on security, see *Avaya IP Office™ Platform Security Guidelines*

Platform

- The IP Office for Linux operating system is based on Red Hat Enterprise Linux that is further hardened for defaults, packages, and users.
- The operating system of Server Edition Expansion System (L) is developed for IP Office. The operating system is simple, stable, and reliable.

Página2364 de 3226.

- The operating system of Server Edition Expansion System (V2) is developed for IP Office. The operating system is simple, stable, and reliable.
- Components that are secure:
  - Software security engine for all the components.
  - Hardware security engine for Office Server Edition Expansion System (V2).
  - Internal Access Control Engine polices for external service requests and internal applications.

Manager

- Transport Layer Security (TLS) secures the communications between IP Office Manager and IP Office and insecure ciphers are disabled.
- Provides Role based user access control (RBAC).
- Provides comprehensive user account and password controls.
- You can enable a PKI Trust domain.
- The system generates warnings messages if administrative passwords are set to default. The system sends alarms or login failure.
- The system records all the accesses in the audit trail.
- You can disable unused services and ports such as HTTP.

Administration user accounts

The administration user accounts can be controlled for:

- Password complexity
- Previous password history (administrative accounts only)
- Change password on next login
- Idle lockout and login failure lockout
- Time and date the account expires (administrative accounts only)

Single sign-on (SSO)

- Administration credentials to log in to Linux Platform settings are securely transferred to Manager, SSA,Voicemail Pro client.
- All administrative logins on all IP Office components including Voicemail Pro and Avaya one-X® Portal for IP Office use security settings of IP Office.
- Server user management feature in Web Manager synchronizes administrative user credentials with all components of IP Office including Voicemail Pro and Avaya one-X® Portal for IP Office in IP Office Server Edition Solution.

Audit trail

- Each IP Office system maintains an audit trail of access and configuration change.
- Linux Platform settings also maintains an audit trail.
- The IP Office system displays the audit trail in IP Office Server Edition Manager and SSA.
-

Página2365 de 3226.

Public Key Infrastructure (PKI)

- IP Office supports X.509 certificates
- The Server Edition Primary and the Application server support an integrated Certificate Authority (CA)
- The Trusted Certificate Store can be configured and Identity certificate is available.
- The system performs a Certificate Signing Request (CSR) through Simple Certificate Enrollment Protocol (SCEP).
- The system creates a self-signed Identity certificate that can be copied to all HTTPS/TLS interfaces.
- Flexible controls to enforce Trust domain on specific services. Extended trust controls for PKI .
- Web Management Console,Voicemail Pro and Avaya one-X® Portal for IP Office on Linux support X.509 certificates, but not PKI.

LAN

- The servers and expansion systems are thoroughly tested for resistance to Denial of Service and other attacks
- Server Edition Expansion System (V2) supports a configure able Firewall
- Time profiles on Server Edition Expansion System (V2) only
- Static NAT and NAPT in Server Edition Expansion System (V2)
- ICMP Filtering
- L2TP/PPP VPN on Server Edition Expansion System (V2) only
- PAP or CHAP password exchange
- Idle or quota timeout
- IPSec VPN on Server Edition Expansion System (V2) only

Endpoints

- Username and PIN or password or login code are in the IP Office configuration, and you can administer these through IP Office Server Edition Manager
- You can use HTTP or HTTPS for settings and firmware upgrades
- You cannot make calls unless you are logged in

Call barring

- You can configure flexible call barring controls using login name or account code to allow internal, local, national or international calls on the basis of every user and system.
- You cannot use speed dials, transfers, forwarding, and conferences to bypass controls.
- You can enable trunk to trunk calls using IP Office Server Edition Manager. Trunk to trunk calls are disabled by default.
- SIP trunk configuration for incoming calls must match URIs..
- You can use SMDR (CDR) to create a record of all calls.

Voicemail Pro client

- You can enforce user login with Personal Identification Number (PIN) and configure complexity for the PIN.
- You can enforce PIN change when the user logs in for the first time.
- Idle timeout.

Related links

Security specification on page 101

Port assignments

Details of the range of ports used by IP Office and IP Office applications are found at https://support.avaya.com/products/.

DTE port	9 way D-type D-Type female connector: V.24/V.28
Analog trunk ports	RJ45 sockets: Loop Start/Ground Start (regionally dependant)
Power fail ports	RJ45 sockets: 2x sockets for ATM16 and 1x sockets for ATM4
ISDN data rates	BRI: B-channel 64 Kbps or 56 Kbps, D-channel 16 Kbps
Analog phone ports	• RJ45 sockets • REN: 2. (External Bell via POT port: REN = 1) • Off Hook Current: 25 mA. • Ring Voltage: 40 V (nominal) RMS.
LAN	RJ45 sockets. Auto-negotiating 10/100 BaseT Ethernet (10/100 Mbps)
Audio	• 3.5 mm stereo jack socket. Input impedance 10 K/channel. • Maximum AC signal - 200 mV rms.
External output port	• 3.5 mm stereo jack socket. Switching capacity 0.7 A. • Maximum Voltage - 55V DC. On state resistance 0.7. • Short circuit current 1 A. Reverse circuit current capacity 1.4 A.
Embedded voice memory	IP500V2: 512 MB compact flash memory (SD) card for voicemail

Página2367 de 3226.

Typical upgrade paths

Upgrading IP500 V2 platforms

Customers can migrate to the latest release by purchasing an upgrade license or under the terms of their IP Office Support Services support contract, as applicable. Customers migrating to the latest release will be required to have an IP500 V2 control unit or supported servers with Server Edition. IP500 base cards, trunk cards and expansion modules are supported with IP500 V2 control unit and may migrate to the V2 control unit. Licenses will require a dongle swap to move from the IP500 key card to the IP500 V2 SD card.

For systems using the IP500 V2 with any software release prior to 8.1.1.0, a two-stage upgrade process is required to cope with the increased size of the 9.1 binary file. Upgrade to 8.1.1.0 or any 9.0 version before attempting the upgrade to 9.1.

Ensure that the systems do not contain unsupported hardware. Upgrade them if necessary prior to upgrading the software. Install upgrade licenses prior to the upgrade.

Use the Manager Upgrade Wizard to display the software currently present on the SD card and the new versions available for upgrade.

IP400 hardware will no longer be supported, including IP400 series internal cards, expansion modules and trunk cards listed below:

IP400 VCM cards	VCM4
	VCM8
	VCM16
	VCM24
	VCM30
IP400 modules and station cards	Digital Station V1: 16 and 30 port variants
	Phone V1: 8, 16 and 30 port variants
	So8: ETSI BRI SO support
IP400 cards	Analog Trunk Card Uni (ATM4U)
	Analog Trunk Cards (ATM4)
	BRI Trunk Cards
	T1 PRI Trunk Cards
	E1 PRI Trunk Cards
	E1R2 PRI Trunk Cards

The following IP400 trunk and station modules will continue to be supported in the current release.

IP400 expansion modules	Analog trunk 16
	Digital Station V2: 16 and 30 port variants

Página2368 de 3226.

Phone V2: 16 and 30 port variants

Upgrading Server Edition

Upgrade Server Edition primary, secondary and expansion systems using the iso image burned to a DVD or USB. Install upgrade licenses prior to upgrading. There are two options available:

Upgrading to IP Office Select

Existing Server Edition licenses need to be migrated by purchasing a new set of Select PLDS licenses.

Upgrading Application Server

The upgrade process for the Application Server is the same as for IP Office Server Edition.

Upgrading UCM

Upgrade UCM using a USB2 memory Key with new software or the Web Manager ISO upgrade process.

Upgrading Windows server applications

Download the latest windows applications and copy to the server or burn to a DVD.

Upgrading networked systems

In previous releases, networking was achieved using H.323 lines configured with supplementary services set to SCN. From 9.1 and later, these lines will be migrated to IP Office Lines.

Replacing Customer Call Reporter

Advanced Edition and Customer Call Reporter (CCR) are no longer available for sale. Additionally, existing Advanced Edition customers will need to migrate their CCR to IP Office Contact Center via purchase of the IP Office Contact Center solution prior to upgrading. However, CCR will continue to be sold and supported on the previous release consistent with Avaya lifecycle support policy.

Avaya will provide CCR customers with a clear path to move to IP Office Contact Center. Further, as a result of this change, Preferred Edition will now come with the Voicemail Pro database and Visual Basic Scripting (these were previously part of Advanced Edition).

Ordering process

Software applications are orderable by Avaya Partners from their Avaya Authorized Distributor. Avaya Partners must contact their respective distributors directly to purchase all IP Office software applications. Each distributor implements a customized IP Office software purchasing and distribution process for its network of Avaya Partners. These distributor specific internal processes are not covered by this document.

BCM with CS1000 to IP Office migration

This configuration allows migrating a network of BCM and CS1000 to IP Office step-by-step by adding IP Office systems to it.

Protocol support	IP Office to BCM: SIP

Página2369 de 3226.

	IP Office to CS1000: SIP IP Office to IP Office: SIP or H323 - SCN Networking BCM to BCM: SIP or SIP/MCDN BCM to CS1000: SIP or SIP/MCDN **Note:** Only UDP will be supported and not TCP. IP Office to CS1000 using H.323 or PRI trunks is not supported.
IP Office platform requirements	Release 8.1 or higher, Essential, Preferred or Server Editions
BCM platform requirements	BCM50 or BCM450 6.0
CS1000 platform requirements	CS1000 7.5 with NRS
Centralized voicemail	Centralized Voicemail for all IP Office systems in the SCN network. BCM systems may use centralized voicemail of the CS1000. IP Office systems cannot use centralized voicemail of CS1000.
Phones	All phones supported on the individual call servers and releases including Avaya IP Phone (H.323), Avaya Digital phones, BCM 7000 Series digital phones, BCM1100/1200 Series IP phones (SIP), DECT R4 phones, and Analog phones.

IP Office Branch migration

Migration roadmap and limitations

You can upgrade from a B5800 Branch Gateway to the current release of IP Office, or from a previous release of IP Office to the current release of IP Office. The upgrade process for the IP Office Branch solution varies depending on how the architecture is deployed.

If the B5800 Branch Gateway or IP Office release you are upgrading from is connected to the Avaya Aura® infrastructure and uses Avaya Aura® System Manager for centralized management, use Avaya Aura® System Manager to upgrade the firmware and software for the system.

If the architecture is deployed in a stand-alone IP Office branch environment with no centralization or connection to the Avaya Aura® network, you must use IP Office Manager for upgrades. From IP Office Manager, you can perform an upgrade using the upgrade wizard or the System SD card.

Página2370 de 3226.

For procedures on how to perform System Manager or IP Office Manager upgrades for your Branch solution, see *Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*.

Licenses

Many solutions, applications, and features on IP Office systems are licensed and only operate when a valid license is detected. This includes features within IP Office applications connected to the IP Office system.

This section describes the license requirements for IP Office features. For information and procedures on managing licenses, see “Applying Licenses” in the following documents:

- *Administering Avaya IP Office™ Platform with Manager*
- *Administering Avaya IP Office™ Platform with Web Manager*

Ports, channels, and users

Some licenses enable a number of ports, channels, or users. Depending on the particular license, each supported instance can be consumed either when it is configured for use or when it is actually being used. When no further instances of a license are available, further use of the licensed feature is not allowed.

Multiple licenses can be added to give a higher number of supported ports, channels, or users. However, licenses above the capacity supported by the particular IP Office control unit will not work.

PLDS licensing

IP Office uses the Avaya Product Licensing and Delivery System (PLDS) to manage licenses. PLDS is an online, web-based tool for managing license entitlements and electronic delivery of software and related license files. PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads. You can access PLDS from http://plds.avaya.com/.

PLDS license files

Licenses are delivered from PLDS with license files. A PLDS license file is generated for installing on a specific machine. There are two deployment options:

- PLDS Nodal license files are generated for and installed on particular IP Office nodes.
- PLDS WebLM license files are generated for and installed on a WebLM server that can license multiple IP Office nodes.

WebLM centralized licensing is supported in IP Office Server Edition and in IP Office Branch deployments, but not in non-Branch deployments of IP Office Standard mode.

Página2371 de 3226.

PLDS host ID

Each PLDS license file must be created with the PLDS host ID of the system where the license file is to be loaded. PLDS Nodal license files are machine specific and you must specify the host ID in the **PLDS host ID** field in IP Office Manager or Web Manager.

IP500 V2 systems: You can find the PLDS host ID in the **Licensing** tab of IP Office Manager and Web Manager. The PLDS host ID is made of the two digits “11”, followed by the 10 digit feature key serial number printed on the IP Office SD card. If the SD card is changed, the PLDS host ID will also change.

IP Office Linux servers: The PLDS host ID can be found on the server labeling, the server packaging label, and the system ignition Login screen. The PLDS host ID is derived from the system ID. If the system ID changes, the PLDS host ID will also change.

WebLM: The WebLM host ID is the Mac address of the WebLM server. In a virtual environment, the WebLM host ID is a virtual Mac address that starts with the letter “V”. The WebLM host ID must be used when generating a PLDS license file for the WebLM server in order to implement a centralized licensing scheme for multiple IP Office systems. The WebLM host ID can be found on the server labeling, the server packaging label, the system ignition Login screen, and through the WebLM management interface.

Web License Manager (WebLM)

The Web License Manager (WebLM) is a web-based application for managing licenses. If you use the WebLM server running on the IP Office server, then you can use IP Office Web Manager to log in to the WebLM server by selecting **Applications** > **Web License Manager**. WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on (SSO).

Note:

- WebLM license management is supported for Server Edition deployments and for Enterprise Branch deployments using the System Manager WebLM server. It is not supported for Standard Mode systems.
- When upgrading from a previous release, all systems must be running the same software level. IP Office Server Edition does not support mixed versioning.

For more information on WebLM, see *Administering standalone Avaya WebLM*.

Migration of ADI licenses

ADI licenses are no longer supported as of Release 10.0. New licenses must be obtained from PLDS.

Using the One Source Configurator (OSC), all ADI licenses from previous releases are upgraded to PLDS. The **License Migration** option in IP Office Manager can be used to extract license information about the system, and this information can then be uploaded to OSC. After the information is extracted, IP Office Manager signs the file so it cannot be modified.

Página2372 de 3226.

PLDS license creation

The PLDS license must be created with the PLDS host ID of the system where the license will be loaded. If the licenses are loaded locally on the IP Office, then the PLDS host ID is available in IP Office Manager or Web Manager. For IP500 V2, it is also the Feature Key number on the SD card, which starts with “11”. If the PLDS file is loaded on a WebLM server, then the host ID is available on the WebLM interface under **Server Properties**.

For more information about migrating IP Office licenses to PLDS, see *Administering Avaya IP Office™ Platform with Manager* or *Administering Avaya IP Office™ Platform with Web Manager*.

Virtual licenses

As part of the migration process, the following virtual licenses are provided as actual PLDS licenses only through the XML migration process:

- Virtual Essential Edition
- Virtual Preferred Edition for systems with a UCMv1 module
- Virtual Avaya IP endpoints for systems with:
  - VCM32/64 v1 modules that provided 12 Avaya IP endpoints
  - Legacy VCM channel migration licenses
- Additional virtual Voicemail Pro ports for Server Edition

  Te PLDS licensing system adds two Voicemail Pro ports to any Server Edition or Server Edition Select license.

Customers with older systems (IP500 V1 / IP406 V2 / IP412 at release 6.0 or later) can upgrade through A1S Configurator BOM upload and ADI license validation process. Any virtualized licenses on these older systems will not carry forward and must be purchased as new.

Note:

The legacy Windows soft phone is not supported in IP Office Release 11.0 and will not function. The previous virtual licenses provided when upgrading are no longer provided in release 11.0. Avaya Equinox™ for Windows is the replacement. The Teleworker license enables the use of the Avaya Equinox™ for Windows. In earlier releases, this was only available with Office Worker and Power User.

Server Edition Centralized and Nodal licensing

Before release 10, Server Edition deployments used nodal licensing. This type of licensing can still be used in release 10 and higher. However, it is expected that most deployments will prefer to centralize license management using the Avaya Web License Management (WebLM) server. The WebLM server is automatically installed on the Server Edition Primary server. For newly installed systems, centralized licensing is the default configuration.

All systems in the Server Edition solution must use the same **License Source**.

Nodal licensing

With nodal licensing, license files must be installed on each node in the system. For some licensed features, the required license can be installed on the Server Edition Primary server and

Página2373 de 3226.

used by all nodes in the system. However, for other licensed features, the required license must be installed on the node where the feature is used.

Centralized licensing

As of release 10, you can use the WebLM server running on the Server Edition Primary server to fully centralize license management. With centralized license management, all licenses are contained in a single PLDS file uploaded to WebLM. All nodes in the solution obtain their licenses from WebLM.

The IP Office Secondary server and Expansion systems can be configured to request licenses directly from the WebLM server, or to use a proxy option. When configured to use the proxy option, the license requests are sent through the IP Office Primary server, which proxies the requests to the WebLM server. The Primary server does not allocate licenses, but only acts as a proxy.

Systems using nodal licensing can be converted to use centralized licensing. Since PLDS license files are generated using the host ID of the server where they reside, you must regenerate the license file using the host ID of the WebLM server that will host the license file.

Centralized license distribution

When the license source is WebLM, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features. Editable fields can be used to:

- Request additional licenses from the WebLM server.
- Remove licenses from the IP Office node to apply them elsewhere.

Important:

When reallocating licenses, always reduce the number on the IP Office node where they are currently applied before applying them on another node. If you exceed the number of licenses available, you will receive an error message.

Distribution after conversion from Nodal to Centralized licensing

- If the IP Office node needs any of the following licenses, then you must manually configure the respective **Reserved Licenses** editable fields. This will allow the IP Office node to request the licenses from the WebLM server.
  - **VMPro Recordings Administrators**
  - **VMPro TTS Professional**
  - **CTI Link Pro**

Extension Reserved license setting: When the license source is **Local**, the setting **Extension** > **VoIP** > **Reserve License** is set to **None**. Switching the license source to WebLM changes the setting to **Reserve Avaya IP endpoint license**. If required, you must manually change this setting to **Reserve 3rd party endpoint license** or **Both**.

License allocation in WebLM

You can use WebLM to view the licenses used by each node in IP Office Server Edition. In the WebLM navigation pane on the left, click **Licensed Products**. The Acquired licenses table displays information about the licenses acquired for each client ID. In IP Office, the WebLM client ID for each node is displayed on the license Remote Server page.

Página2374 de 3226.

Nodal license distribution

When the **License Source** is **Local**, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features.

Nodal licensing for a Server Edition solution is based on a combination of licensing done through the Server Edition Primary server plus some server-specific licenses. All the user specific and system specific licenses can be managed from the Server Edition Primary server that also acts as a licensing server. Licenses are entered into the configuration of the Server Edition Primary server and are based on the system ID of that server.

Where a license is used to enable features, such as SIP Trunk channels, on other systems, the Server Edition Primary server only allocates those licenses to other systems after it has met its own license needs.

When another system loses connection to the Server Edition Primary server, any license requirements based on those licenses entered in the Server Edition Primary server's configuration are supported for a grace period of 30 days.

Other server specific licenses are entered into the configuration of the server requiring the feature and are based on the System ID of that system.

License	Primary server	Server-specific
Server Edition	Yes	No
Avaya IP endpoints	Yes	No
Third-party IP endpoints	Yes	No
SIP trunk channels	Yes	No
IP500 universal PRI channels	No	Yes
Additional voicemail ports [3]	Yes	No
Web Collaboration	No	Yes
UMS Web Services [1]	No	Yes
Office Worker	Yes	No
Power User	Yes	No
Office Worker to Power User upgrade	Yes	No
Receptionist	No	Yes
CTI Link Pro	No	Yes
Messaging TTS Pro [3]	Yes	No
Voicemail Pro Recording Administrator [2] [3]	Yes	No
WAV User	No	Yes
IPSec tunneling	No	Yes

1. UMS Web Service licenses are for Hunt Groups only.
2. The Voicemail Pro Recording Administrator license refers to Contact Store. Only one license is required for a Server Edition network.

Página2375 de 3226.

3. For deployments with dual Voicemail Pro servers, Messaging TTS Pro, Voicemail Pro Recording Administrator, and Additional voicemail ports licenses must be on the Secondary Server.

WebLM licensing

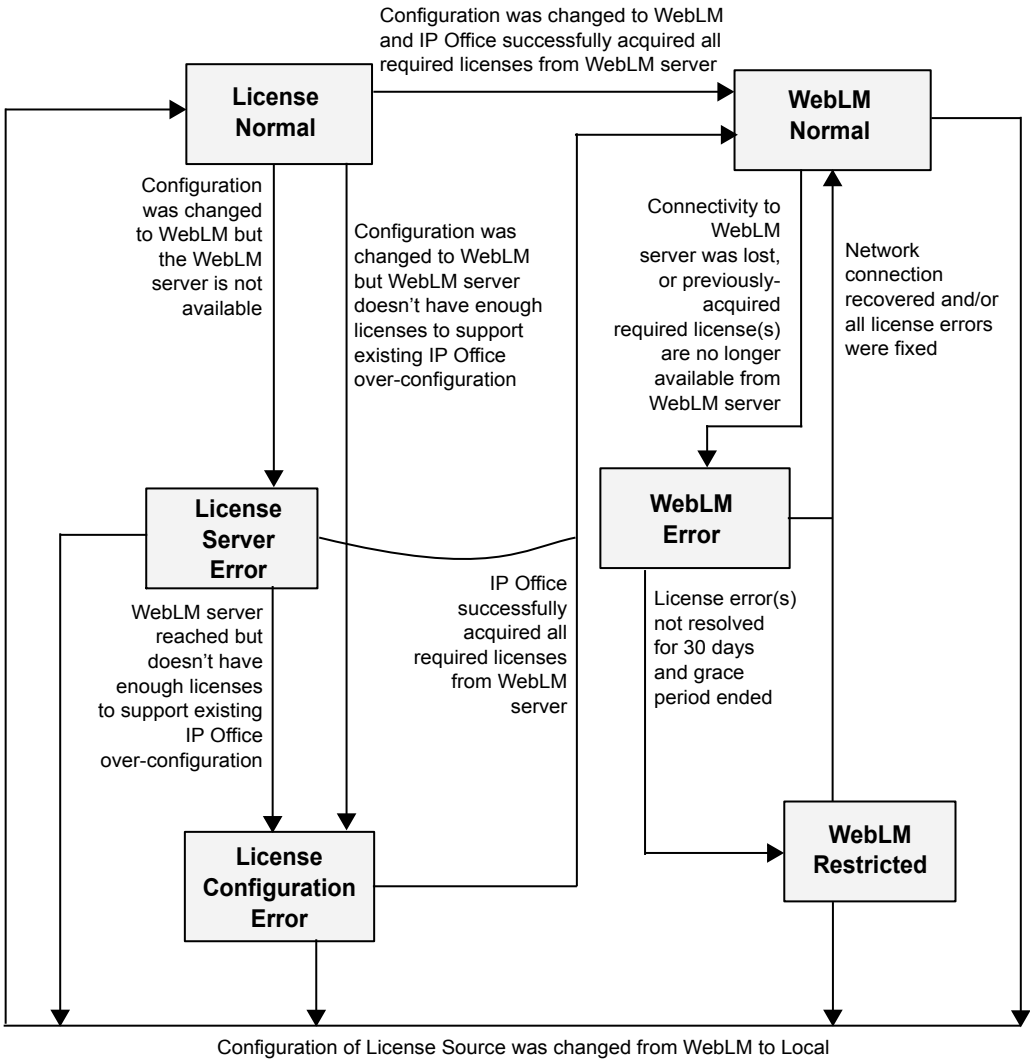
License modes

The following are the IP Office license modes when you are using WebLM licensing. The license mode is displayed in IP Office Manager, Web Manager, and System Status Application (SSA).

Mode	Description
License Normal	WebLM licensing is not configured. Traditional Nodal licensing. No grace period. Over-configuration is allowed.
License Server Error	Configuration was changed to WebLM, but the WebLM server is not available. No grace period. Until the problem is resolved, IP Office is unlicensed and unusable similar to traditional Nodal licensing if no licenses are installed.
License Configuration Error	Configuration was changed to WebLM and the WebLM server is available, but it doesn't have enough licenses to support the existing IP Office configuration. No grace period. Until the problem is resolved, IP Office is unlicensed and unusable similar to traditional Nodal licensing if no licenses are installed. Licenses must be added to the WebLM license file or IP Office configuration must be modified to correct over-configuration.
WebLM Normal	IP Office is configured for WebLM licensing, the WebLM server is available and IP Office successfully acquired all the licenses required to support all of its configured features. New licenses are acquired for newly-configured features, and over-configuration of licensed features is prevented if licenses cannot be acquired. IP Office periodically renews its acquired licenses. Failure to renew will lead to the WebLM Error mode with grace period.
WebLM Error	IP Office is configured for WebLM licensing and was previously in WebLM Normal mode. But IP Office now cannot renew or re-acquire all the licenses required to support all of its configured features. Over configuration of licensed features is prevented if licenses cannot be acquired. IP Office keeps operating for a 30-day grace period based on its existing configuration (lost licenses are replaced with virtual grace licenses).
WebLM Restricted	IP Office was in the WebLM Error mode, but the 30-day grace period has expired and the problems for this error have not been resolved. Unlicensed features will stop working (virtual grace licenses are deleted). Any configuration of IP Office is not allowed, except configuration changes that reduce the licensing errors.

Página2376 de 3226.

License mode state transitions



WebLM licensing configuration

In WebLM licensing, licenses must fully support the IP Office configuration. Over-configuration is not allowed. IP Office, based on its configuration, requests the required licenses from the WebLM server.

For some types of licenses, such as for users, extensions, receptionists, and web collaboration, the type and quantity of required licenses is determined by the configuration of the respective items. For example, the User and Extension records in the IP Office configuration. These quantities are displayed in read-only fields in the 'Reserved Licenses' list in the IP Office Configuration License > Remote Server tab.

For other types of licenses, such as for SIP trunk sessions and Voicemail Pro ports, the quantity of required licenses must be configured explicitly. These quantities have to be configured in editable fields in the Reserved Licenses list in the IP Office Configuration License > Remote Server tab.

Página2377 de 3226.

Licensing configuration warnings and alarms

License Configuration Error mode

- IP Office goes into the License Configuration Error mode when you change the IP Office License Source from “Local” to “WebLM” and it is under-licensed or over-configured.

  In this mode, IP Office is unlicensed and unusable. This mode is a transition error state and not supported as a steady state. Try to avoid entering into this mode and, if it happens, fix the errors immediately.
- Installed systems with traditional licensing may be under-licensed or over-configured. If they are upgraded to version 10.0 and migrated using WebLM licensing without acquiring the additional needed licenses or removing the over-configuration, then the installed systems goes into the License Configuration Error mode after migration.

  To help avoid this problem, warnings are given by the IP Office Manager License Migration Tool. If IP Office has over-configuration relative to its existing old licenses, the License Migration Tool displays a warning and also includes detailed warning information in the License Migration information file.
- If IP Office is in the License Configuration Error mode, Systems Status Application (SSA) alarms page shows alarms indicating the cause of the problem.

  If you encounter this mode, review the SSA alarm errors and resolve them by acquiring the missing required licenses or by modifying the IP Office configuration so as to not require these licenses.

Other warnings

When the administrator sets the License Source to “WebLM”, IP Office Manager and IP Office Web Manager display a warning advising the administrator to check and verify that sufficient licenses are available on the WebLM server.

WebLM user and IP Endpoint licensing

IP endpoint licenses

When IP Office uses WebLM licensing, each configured H.323 or SIP extension requires a license and IP Office requests the required licenses from the WebLM server. Sufficient licenses are required for all the configured H.323 and SIP extensions and not only for the maximum number of concurrently-registered extensions. This is consistent with WebLM licensing for users and receptionists.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of extensions with a small number of licenses to cover only a subset of the extensions registering at the same time. For example, configuring three extensions with one IP endpoint license to cover only one of the three extensions registering at the same time. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing, and set the **Reserve License** field for the extensions to `None`.

For each configured H.323 or SIP extension, IP Office requests from the WebLM server an Avaya or third-party IP endpoint license, as per the **Reserve License** field of the configured extension record. When IP Office uses WebLM licensing, the **Reserve License** field for each configured H.323 and SIP extension is by default set to Avaya IP endpoint license. This field is editable and the

administrator can change it to a third-party IP endpoint license or to both Avaya and third-party IP endpoints.

Note:

For the **Reserve License** field, the value `None` is not available with WebLM licensing because IP Office must request a license from the WebLM server.

User licenses

When IP Office uses WebLM licensing, sufficient User licenses are required as per the IP Office users configuration and not only for the maximum number of concurrently-registered users. This is consistent with WebLM licensing for IP endpoints and receptionists. IP Office requests from the WebLM server the required User licenses (for example, Power User licenses) as per the user profile of all configured users.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of users with a small number of licenses to cover only a subset of the users registering at the same time. For example, configuring three users with one User license to cover only one of the three users registering at the same time. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing.

Receptionist licenses

When IP Office uses WebLM licensing, Receptionist licenses are required for all users that are configured as Receptionist and not only for the maximum number of users that would run their IP Office SoftConsole application concurrently. This is consistent with WebLM licensing for IP endpoints and users. With WebLM, licenses are required according to the configured objects, and over-configuration and under-licensing are not allowed.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of Receptionist users with a small number of licenses to cover only a subset of the users connecting at the same time using IP Office SoftConsole. For example, configuring three Receptionist users with one Receptionist license to cover only one of the three users connecting at the same time using IP Office SoftConsole. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing.

Auto-create support for users and extensions

When IP Office uses WebLM licensing, you cannot auto-create users and extensions as it is not supported. The administrator must manually configure users and extensions. For DECT extensions, the “Preconfigured” method must be used.

However, auto-create for users and extensions is supported if you use local PLDS license file instead of Centralized WebLM licensing.

Basic Edition license for new systems

To upgrade to Release 11.0, the new PLDS R11.0 upgrade runtime license is used in combination with the R11.0 software. Upgrading to IP Office R11.0 from releases prior to R10.0 involves a complete transition to PLDS licenses. To upgrade existing IP Office systems to IP Office R11.0, paid or transactional or entitled Edition R11.0 upgrade or migration licenses are required.

Material code	License	Description
396490	IP OFFICE R11 BASIC EDITION MIG UPGRADE PLDS	R11 Basic Edition starting in PLDS
369472	IP OFFICE R11 BASIC EDITION MIGRATION UPGRADE	ADI or PLDS upgrade to R11 Basic Edition

Customers must also purchase SD cards, which are configured, by default, with Basic Edition.

Customers must obtain this material code, which is merchandisable and does not have to be configured, before ordering IP Office Support Services. This is especially important for customers who already have Basic Edition or for after-market IP Office Support Services purchases, including customers who set up Basic Edition without IP Office Support Services first, but then later choose to get IP Office Support Services. These customers must place a merchandise order for this material code first and then place their after-market purchase of IP Office Support Services and register their equipment for servicing.

Note:

Basic Edition is not a prerequisite for Essential Edition or Preferred Edition, and is not stacked under Essential Edition.

Essential Edition and Preferred Edition licenses

An Essential Edition license is a prerequisite on IP500 V2 systems, and includes mobile twinning for all users and four remote workers.

A Preferred Edition license is a prerequisite for any user profile licenses. In a multisite network, the Preferred Edition license of the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server still requires its own Preferred Edition license for Voicemail Pro operation. For a IP500 V2 system fitted with a Unified Communications Module (UCM V2), the card requires a separate Preferred Edition license.

The Preferred Edition license includes support for 4 messaging ports. The total number of messaging ports supported can be increased by adding additional messaging port licenses, at the time of purchase or later, up to the maximum supported by the particular control unit.

Página2380 de 3226.

Order code	License	Description
396491	IP OFFICE R11 ESSENTIAL EDITION UPGRADE PLDS LIC:DS	Essential Edition (PLDS upgrades)
396474	IP OFFICE R11 ESSENTIAL EDITION MIG UPG LIC:DS	ADI migrations to PLDS and upgrades to R11.0 Essential Edition
396492	IP OFFICE R11 PREFERRED VOICEMAIL PRO UPGRADE PLDS LIC:DS	Preferred Edition (PLDS upgrades)
396476	IP OFFICE R11 PREFERRED VOICEMAIL PRO MIG UPG LIC:DS	ADI migrations to PLDS and upgrades to R11.0 Preferred Edition

Server Edition licenses

A Server Edition license includes:

- Features from Essential Edition
- Features from Preferred Edition
- Centralized Voicemail Pro
- Two ports of Voicemail Pro
- Unlimited multi-site networking channels (IP Office Lines)

A Server Edition license enables:

- Meet-me conferencing
- Advanced messaging
- Automated attendant
- Call recording
- Conditional call routing
- Queue announcements
- Mobile twinning
- Call control
- Call back

One Server Edition license is required for the primary server, the secondary server, and for each Linux or IP500 V2 expansion system. The licenses enable voice networking between systems in the Server Edition network.

Order code	License	Description
PLDS Upgrades (starting PLDS)		
396493	IPO R11 SE/VRTLZD UPG PLDS LIC	Paid Upgrade Code
ADI Migrations to PLDS and upgrade to R11.0		
396480	IP Office R11 SE ADI MIG UPG LIC	Paid Upgrade Code
396478	IPO R11 VRTLZD SE ADI Migration UPG LIC	Paid Upgrade Code
IP Office PLDS upgrades		
396519	IPO-SL 11 SE/VRTLZD UPG PLDS LIC	Paid Upgrade Code

Página2381 de 3226.

Branch licenses

The following table describes key IP Office licenses that are of particular interest to branch deployments.

Display name	Description
Avaya WebLM Model	This license is required by IP Office in branch deployments in order to connect to the WebLM server and use WebLM centralized licensing.
Branch System	This license is required for IP Office in branch deployments. It is used for tracking purpose only.
IP Office Centralized Endpoints license	One license is required for each Centralized user configured on the IP Office with a SIP extension or an analog extension. **Important:** In addition to this IP Office license, each centralized user also requires a license on the central Avaya Aura® system.
SM Trunk Channel	This license is required with sufficient quantity to allow for the maximum number of concurrent SM Line calls to be enabled on the system. The total number of SM Trunk Channel licenses requirements depend on the expected traffic patterns in the particular deployment. **Note:** IP Office also supports SM Line connections to Avaya Aura® Session Manager in other IP Office Server Edition deployments. These connections are not limited to branch deployments.

Small Community Network licenses

In a Small Community Network (SCN), there must be at least one IP Office Preferred Edition. Two are required with resiliency.

The different types of users in an SCN have the same functionality, regardless of where the IP Office Preferred Edition is installed.

In a multisite network, if one or more IP Office Preferred Edition system is installed, then all the IP Office systems in the multisite network will automatically have Preferred licenses as prerequisites for the following user types:

- Power users
- Teleworkers
- Mobile workers
- Office workers

Página2382 de 3226.

Trunk licenses

The tables in this section include all the net new and uplift IP Office PLDS software license material codes. The material codes with indication of R10+ are known as “ANY” codes and can be used for Release 10.0 and later system deployments. The SAP descriptions have been modified to show 10+ for this change, while the material code remains the same. Other codes are R11.0 release specific and contain R11.0 in the description.

SIP trunk sessions

These licenses are used to permit sessions on SIP trunks and SM Lines added to the system. Multiple licenses can be combined for the total number of channels required.

Order code	License	Description
383085	IPO R10+ SIP TRNK 1 LIC	SIP trunk 1 session
307332	IIPO-SL R10+ SIP TRNK 1 LIC	SIP trunk 1 session – Select
383120	IPO R10+ SM LINE SIP TRNK LIC	SM Line session
382917	IPO-SL R10+ SM LINE SIP TRK LIC	IP Office Select SM Line session

IP500 Universal PRI additional channels

The IP500 PRI Universal trunk card (UTC) is available in 1 or 2 port variants, each port supporting a single PRI circuit connection. The ports can be switched between supporting E1, E1R2, or T1 line types as required for the trunk being connected. Each port supports 8 B-channels (“Bearer”) which do not need to be licensed. If additional B-channels are required, they must be licensed through the addition of the licenses below. Multiple licenses can be added to achieve the total number of channels required. D-channels are not subject to licensing. The licenses are consumed by those channels, which are configured as being *in service*, in order of the installed IP500 PRI-U cards.

IP500 Universal PRI additional E1 channels

These licenses are used to enable additional E1 B-channels for IP500 PRI-U cards configured for E1 operation. Each port can support up to 30 B-channels in this mode.

Order code	License	Description
383092	IPO R10+ IP500 E1 ADD 2CH LIC	2 E1 channels
383093	IPO R10+ IP500 E1 ADD 8CH LIC	8 E1 channels
383094	IPO R10+ IP500 E1 ADD 22CH LIC	22 E1 channels
307337	IPO-SL R10+ IP500 E1 ADD 2CH LIC	2 E1 channels – Select
307338	IPO-SL R10+ IP500 E1 ADD 8CH LIC	8 E1 channels – Select
307339	IPO-SL R10+ IP500 E1 22CH LIC	22 E1 channels – Select

IP500 Universal PRI additional E1R2 channels

These licenses are used to enable additional E1R2 B-channels for IP500 PRI-U cards configured for E1R2 operation. Each port can support up to 30 B-channels in this mode.

Página2383 de 3226.

Order code	License	Description
275637	IPO R10 IP500 E1R2 ADD 2CH PLDS LIC	2 E1R2 channels
383096	IPO R10+ IP500 E1R2 ADD 8CH LIC	8 E1R2 channels
383097	IPO R10+ IP500 E1R2 ADD 22CH LIC	22 E1R2 channels
307340	IPO-SL R10+ IP500 E1R2 2CH LIC	2 E1R2 channels – Select
307341	IPO-SL R10+ IP500 E1R2 8CH LIC	8 E1R2 channels – Select
307342	IPO-SL R10+ IP500 E1R2 22CH LIC	22 E1R2 channels – Select

IP500 V2 Universal PRI additional T1 channels

These licenses are used to enable additional T1 B-channels for IP500 PRI-U cards configured for T1 PRI or T1 robbed-bit operation. Each port can support up to 23 B-channels (T1 PRI) or 24 B-channels (T1 robbed bit) in this mode.

Order code	License	Description
383091	IPO R10+ IP500 T1 ADD 2CH LIC	2 T1 channels
307336	IPO-SL R10+ IP500 T1 ADD 2CH LIC	2 T1 channels – Select

IP500 V2 Voice Networking

The use of private voice networking trunks between IP500 V2 control units and other systems requires voice networking channel licenses within the IP500 V2. This applies to H.323 IP trunks configured on the IP500 V2, including IP trunks being used for an IP Office Small Community Network (SCN). A voice networking license is also required for the use of trunks configured for Q.SIG operation. On an H.323 IP trunk, a license instance is consumed for each simultaneous outgoing call. On a Q.SIG trunk, the number of calls is limited by the trunk type rather than available licenses.

Additional licenses can be added to achieve the number of voice networking channels required.

Order code	License	Description
383087	IPO R10+ IP500 VCE NTWK 4 LIC	4 voice networking channels including the Advanced Networking features (distributed groups and hot-desking across Small Community Network)

User licenses

A profile controls whether users can be configured for a number of features. Every user on the system, except users with Basic User profile and non-licensed users, requires one of the user license types.

The table below lists the different user profiles and the features accessible by each profile. Setting a user to a particular profile enables those features by default, but they can be manually disabled if necessary. The number of users that can be configured for each profile is controlled by the user licenses present in the configuration.

Página2384 de 3226.

Except for a Basic User, a Preferred Edition system license is a prerequisite for any user profile licenses. In a multi-site network, the Preferred Edition license for the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server still requires its own Preferred Edition license for Voicemail Pro operation.

Feature		Standard Mode					Server Edition		
	Non-licensed User [1]	Basic User	Office Worker	Teleworker	Mobile Worker	Power User	Basic User	Office Worker	Power User
one-X Portal Services	–	–	Yes	Yes	–	Yes	–	Yes	Yes
Telecommuter options	–	–	–	Yes	–	Yes	–	–	Yes
UMS Web Services	–	–	Yes	Yes	–	Yes	–	Yes	Yes
TTS for Email Reading	–	–	–	–	Yes	Yes	–	–	Yes
Remote Worker [2]	–	–	–	Yes	–	Yes	Yes	Yes	Yes
Avaya Communicator [3]	–	–	Yes	Yes	–	Yes	Yes	Yes	Yes
WebRTC	–	–	Yes	–	–	Yes	–	Yes	Yes
Avaya Equinox™	–	–	Yes	Yes	–	Yes	–	Yes	Yes

User Profile Notes:

1. Non-licensed users can be created on both Standard Mode and Server Edition systems.
2. The system supports users using remote H.323 or SIP extensions. On non-Server Edition systems, up to 4 users are supported as remote extensions without needing to be configured and licensed for a user profile. Additional remote users are supported if licensed and configured for either a **Teleworker** or **Power User** user profile. On Server Edition systems, the remote worker is supported for all user profiles.
3. Supported for advanced Avaya Communicator for IP Office usage if one-X Portal and Voicemail Pro applications are also installed. If otherwise, only basic Avaya Communicator for IP Office usage is supported.
4. Avaya Equinox™ can be used with a Basic User or a Mobile Worker license in conjunction with IP Softphone license but in standard mode only. In such cases, Simultaneous mode, Shared control feature, and Presence support will not be available.

Non-licensed user

A non-licensed user:

- Is allowed dial in access and paging.
- Can be used as a Music on Hold or Analog paging port.
- Can be authenticated to allow remote access for remote administration.
- Can make internal and emergency calls as NoUser.
- Can forward to voice mail box for voice mail box only users.
- Can be used for internal twinning.

Basic users

New users are created as Basic users by default. Basic users can perform hot-desking, make and receive calls, forward calls, and perform mobile twinning.

Basic user licenses are no longer provisioned. For both new systems and upgrades, the **Basic Users** field is greyed out.

Basic user licenses are required only in the Cloud environment.

Office Worker licenses

This option is targeted at users who are working in the office. In conjunction with a wired or wireless Avaya phone, these users are provided with functions to control their communication with a PC. For example, these users can control audio conferences or manage voice mail with an email client (requires a Preferred Edition license).

An Office Worker license enables Avaya Communicator, Avaya Equinox™ for Windows and Mac, and Avaya Communicator for Web. The Office Worker license enables a user to use the Unified Messaging Service (UMS) and Avaya one-X® Portal for IP Office without Telecommuter functionality. The license instances are consumed for each user being configured.

Order code	License	Description
383105	IPO R10+ MOBILE WORKER 5 TRL LIC	5 licenses for Mobile workers
383107	IPO R10+ OFFICE WORKER 5 TRL LIC	5 licenses for Office workers
307347	IPO-SL R10+ OFFICE WORKER 5 TRL LIC	5 users – Select

Teleworker licenses

This option is targeted at users who are working from home or elsewhere with Internet connection to the office. They are provided with the ability to leverage the PLDS or ISDN using Telecommuter mode, without incurring any remote phone charges. Alternatively the new IP Office Video Softphone can be used if the quality of service of the local internet connection is adequate.

Teleworker includes the remote worker capability with the package. An Essential Edition license provides 4 remote worker seats. Customers requiring additional seats will need to purchase the Teleworker solution.

The Teleworker license enables a user to use Avaya Communicator, Avaya Equinox™ for Windows and Mac, and Avaya one-X® Portal for IP Office. UMS functionality for voice mail or email integration is also enabled, providing synchronization with any IMAP email client. The license instances are consumed for each user being configured.

Página2386 de 3226.

Order code	License	Description
383103	IPO R10+ TELEWORKER 5 TRL LIC	5 users

Mobile Worker licenses

This option is targeted at users with mobile devices. For example, field sales and service staff who are often on the road. These users are provided with features, such as one number access and call control as if in the office, enabling them to never miss a call. The Mobile Worker license enables the use of the one-X Mobile Preferred client in callback mode (but not in VoIP mode).

Power User licenses

This option is targeted at key knowledge workers with the need for both Mobile Worker and Teleworker functionality. A Power User license enables Avaya Communicator, Avaya Equinox™ (desktop and mobile), Avaya Communicator for Web, and VoIP mode in one-X Mobile Preferred.

The Power User license enables a user to use Avaya one-X® Portal for IP Office, all mobility features, and UMS. A Power User license is required to enable conference scheduling in Avaya one-X® Portal for IP Office.

The license instances are consumed for each user being configured.

Order code	License	Description
396319	IP Office R11 OFFICE WORKER TO POWER USER 1 UPLIFT LIC	Upgrade from Office Worker to Power User – 1 user
396505	IP OFFICE-SELECT R11 OFFICE WORKER TO POWER USER 1 UPLIFT LIC	Upgrade from Office Worker to Power User – 1 user – Select
396318	IP Office R11 MOBILE TO POWER USER 1 UPLIFT LIC	Upgrade from Mobile Worker to Power User – 1 user
396316	IP Office R11 POWER USER 1 LIC	1 user
396503	IP Office-Select R11 POWER USER 1 LIC	1 user – Select

Receptionist licenses

This option is targeted at operators or receptionists and provides a visual computer interface for call handling and management for multiple sites. Up to 10 Receptionist users are supported on each node. Server Edition supports up to 32 Receptionist users, and Server Edition Select supports up to 50.

The Receptionist license also enables a user to use IP Office SoftConsole, a Windows application intended for receptionists and operators. Up to 4 IP Office SoftConsole clients can run at the same time and be licensed on a single IP Office system. Additional licenses can be added.

Order code	License	Description
307318	IPO-SL R10+ RECEPTS 1 LIC	1 user
382687	IPO R10+ RECEPTIONIST 1 LIC	1 user

Página2387 de 3226.

Centralized User license

In IP Office Branch deployments, where IP Office is deployed as a branch of a central Avaya Aura® system, users with a SIP or analog extension can be configured as Centralized users. Every Centralized user requires a Centralized Endpoint license.

Web Collaboration licenses

Order code	License	Description
383122	IPO R10+ WEB COLLAB USER 1 LIC	1 user
382918	IPO-SL 10+ WEB COLLAB USR 1 LIC	1 user – Select

IP endpoint licenses

All IP endpoints, Avaya and third party, require an endpoint license.

Avaya IP endpoint licenses

All Avaya IP phones, including DECT and Wi-Fi phones, require an Avaya IP Endpoint license and will consume one instance of that license. This does not apply to the Avaya Softphone or Avaya Communicator. Avaya IP phones without a license will still be able to register but will be limited to making emergency calls only. The phone will display `No license available` and `Emergency Calls Only`. If a license becomes available, it will be assigned to any unlicensed DECT handsets first and then to any other unlicensed Avaya IP phone in the order that the phones registered.

Order code	License	Description
307350	IPO-SL R10+ AV IP ENDPT 1 LIC	1 endpoint – Select
383110	IPO R10+ AV IP ENDPT 1 LIC	1 endpoint

Third-party IP endpoint licenses

Non-Avaya IP phones, including SIP or H.323 devices, require a Third Party IP Endpoint license to register to IP Office and will consume one instance of that license.

Order code	License	Description
307323	IPO-SL R10+ 3RD PTY IP END 1 LIC	1 endpoint – Select
383072	IPO R10+ 3RD PTY IP ENDPT 1 LIC	1 endpoint

Trial licenses

Order code	License	Description
396446	IP OFFICE R11 ESSENTIAL EDITION TRIAL LIC	Essential Edition
396448	IP OFFICE R11 PREFERRED VOICEMAIL PRO TRIAL LIC	Preferred Edition

Table continues…

Página2388 de 3226.

Order code	License	Description
383123	IPO R10+ WEB COLLAB 5 TRL LIC	5 Web Collaboration licenses
382919	IPO-SL R10+ WEB COLLAB 5 TRL LIC	5 Web Collaboration licenses — Select
396504	IP OFFICE-SELECT R11 POWER USER 5 TRIAL LIC	5Power User license — Select
396317	IP OFFICE R11 POWER USER 5 TRIAL LIC	5 Power User licenses
383103	IPO R10+ TELEWORKER 5 TRL LIC	5 Teleworker licenses
383105	IPO R10+ MOBILE WORKER 5 TRL LIC	5 Mobile Worker licenses
307347	IPO-SL R10+ OFFICE WORKER 5 TRL LIC	5 Office Worker licenses — Select
383107	IPO R10+ OFFICE WORKER 5 TRL LIC	5 Office Worker licenses
307319	IPO-SL R10+ RECEPTS 5 TRL LIC	5 Receptionist licenses — Select
382688	IPO R10+ RECEPTIONIST 5 TRL LIC	5 Receptionist licenses
307324	IPO-SL 10 3RD PTY IP 5 TRL LIC	Third party IP endpoint trial license — Select
383073	IPO R10 3RDPTY IPENDPT 5 TRL LIC	Third party IP endpoint trial license
382913	IPO-SL R10+ AV IP ENDPT 5 TRL LIC	5 Avaya IP endpoint licenses — Select
383111	IPO R10+ AV IP ENDPT 5 TRL LIC	5 Avaya IP endpoint licenses
383090	IPO R10+ VMPRO UMS 5 TRL LIC	5 Voicemail Pro UMS licenses
307335	IPO-SL R10+ VMPRO UMS 5 TRL LIC	5 Voicemail Pro UMS licenses – Select
383078	IPO R10+ 3RD PTY TTS TRL LIC	Voicemail Pro third party TTS license
383076	IPO R10+ TTS WNDWS TRL LIC	Voicemail Pro Windows TTS license
307327	IPO-SL R10+ TTS PROLINUX TRL LIC	Voicemail Pro Linux TTS license — Select
383080	IPO R10+ TTS PRO LINUX TRL LIC	Voicemail Pro Linux TTS license
307329	IPO-SL R10+ IPSEC VPN TRL LIC	IPSec Tunneling — Select
383082	IPO R10+ IPSEC VPN TRL LIC	IPSec Tunneling
307333	IPO-SL R10+ SIP TRNK 5 TRL LIC	SIP trunk sessions — Select
383086	IPO R10+ SIP TRNK 5 TRL LIC	SIP trunk sessions
383088	IPO R10+ IP500 VCE NTWK 4	IP500 Voice Networking
307321	IPO-SL R10+ CTI TRL LIC	CIT Link Pro — Select
383070	IPO R10+ CTI TRL LIC	CIT Link Pro

Upgrade licenses

To upgrade existing systems to the latest release, upgrade licenses are required. Upgrade licenses are sold separately. Customers can only upgrade to the latest equivalent of their existing Edition.

Página2389 de 3226.

Note:

Upgrading from a previous release of Basic Edition to the latest version of Essential Edition is not a valid upgrade path.

Order code	License	Description
383738	IPO-SL R10+ RECEPTS 1 UPG PLDS LIC	Select Receptionist upgrade
383696	IPO R10+ RECEPTIONIST 1 UPG PLDS LIC	Receptionist upgrade
383739	IPO-SL 10+ CTI UPG PLDS LIC	Select CTI upgrade
383697	IPO R10+ TI UPG PLDS LIC	CTI upgrade
383740	IPO-SL 10+ MPRO 1 UPG PLDS LIC	Select Voicemail Pro upgrade
383698	IPO R10+ VM PRO 1 UPG PLDS LIC	Voicemail Pro upgrade
383741	IPO-SL 10+ 3RDPTY IPEND1 UPG PLDS LIC	Select IP third party endpoint upgrade
383699	IPO R10+ 3RDPTY IPENDPT1 UPG PLDS LIC	IP third party endpoint upgrade
383742	IPO-SL 10+ TAPI WAV 1 UPG PLDS LIC	Select TAPI WAV upgrade
383700	IPO R10+ TAPI WAV 1 UPG PLDS LIC	TAPI WAV upgrade
383702	IPO R10+ 3RD PTY TTS UPG PLDS LIC	Third party TTS upgrade
383744	IPO-SL 10+ IPSEC VPN UPG PLDS LIC	Select IPSec VPN upgrade
383704	IPO R10+ IPSEC VPN UPG PLDS LIC	IPSec VPN upgrade
383747	IPO-SL 10+ VMPRO UMS 1 UPG PLDS LIC	Select Voicemail Pro Unified Messaging Server upgrade
383708	IPO R10+ VM PRO UMS 1 UPG PLDS LIC	Voicemail Pro Unified Messaging Server upgrade
383748	IPO-SL 10+ IP500 T1 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383709	IPO R10+ IP500 T1 CH1 UPG PLDS LIC	IP500 additional channel upgrade
383749	IPO-SL 10+ IP500 E1 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383710	IPO R10+ IP500 E1 CH1 UPG PLDS LIC	IP500 additional channel upgrade
383752	IPO-SL 10+ IP500 E1R2 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383713	IPO R10+ IP500 E1R2 CH1 UPG PLDS LIC	IP500 additional channel upgrade

Table continues…

Página2390 de 3226.

Order code	License	Description
383707	IPO R10+ IP500 VCE NTWK1 UPG PLDS LIC	IP500 voice networking upgrade
383757	IPO-SL 10+ AV IP ENDPT 1 UPG PLDS LIC	Select Avaya IP endpoint upgrade
383722	IPO R10+ SFTPH 1 PLDS UPG LIC	Soft Phone upgrade
383760	IPO-SL 10+ SMLINE SIPTRK UPG PLDS LIC	Select SM Line SIP trunk upgrade
383726	IPO R10+ SM LINE SIPTRNK UPG PLDS LIC	SM Line SIP trunk upgrade
383706	IPO R10+ SIP TRNK 1 UPG PLDS LIC	SIP trunk upgrade
383761	IPO-SL 10+ WEBCOLLB USR1 UPG PLDS LIC	Select Web Collaboration user upgrade
383728	IPO R10+ WEBCOLLAB USER1 UPG PLDS LIC	Web Collaboration user upgrade
383730	IPO R10 ESS ED EVM 1CH UPG PLDS LIC	Essential Edition Embedded Voicemail channel upgrade

Página2391 de 3226.

Chapter 4: Resources

Documentation

See the following related documents on the Avaya Support website at support.avaya.com and the IP Office Knowledge Base at marketingtools.avaya.com/knowledgebase.

Document number	Title	Use this document to:	Audience
Overview			
16–604278	*Avaya IP Office™ Platform Start Here First*	See a list of all the documents related to the solution.	Everyone
Not numbered	*Avaya IP Office™ Platform Feature Description*	Understand the solution features at a high-level.	Everyone
Not numbered	*Avaya IP Office Contact Center Feature Description*	Understand IP Office Contact Center features and capabilities.	Everyone
Planning			
15–604135	*Avaya IP Office™ Platform Server Edition Reference Configuration*	Understand the technical specifications of and plan for IP Office Server Edition deployment.	Sales Engineers Implementation Engineers
15–604253	*Avaya IP Office™ Platform in a Branch Environment Reference Configuration*	Understand the technical specifications of and plan for IP Office in a branch environment deployment.	Sales Engineers Implementation Engineers
Not numbered	*OnAvaya™ and Powered by Avaya Reference Configuration for Business Partners*	Understand the technical specifications of both IP Office Cloud solutions and plan for deployment.	Sales Engineers Implementation Engineers
Not numbered	*Avaya IP Office™ Platform Security Guidelines*	Understand and follow recommended security guidelines.	Sales Engineers Implementation Engineers
Not numbered	*Avaya IP Office Contact Center Reference Configuration*	Understand technical specifications of IP Office Contact Center and plan for deployment.	Sales Engineers Implementation Engineers

Página2392 de 3226.

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Training

Avaya training and credentials are designed to ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website at http://avaya-learning.com/.

The following courses are also available on the Avaya Learning website. After logging in to the website, enter the course code or the course title in the **Search** field.

Course code	Course title
2S00012W	APSS – Small and MidMarket Communications – IP Office™ Platform and Select Overview

Table continues…

Página2393 de 3226.

Course code	Course title
4601W	Avaya IP Office™ Platform — Components
4602W	Avaya IP Office™ Platform — Editions
2S00015O	Small and Midmarket Communications — IP Office — Endpoints
10S00005E	Knowledge Access: Avaya IP Office™ Platform Implementation
5S00004E	Knowledge Access: Avaya IP Office™ Platform Support

Included in all Knowledge Collection Access offers above is a separate area called IP Office Supplemental Knowledge. This floor in the Virtual Campus contains self-directed learning objects, which cover IP Office delta information. This material can be consumed by technicians experienced in IP Office.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Página2394 de 3226.

Additional IP Office resources

You can find information at the following additional resource websites.

Avaya

http://www.avaya.com is the official Avaya website. The front page also provides access to individual Avaya websites for different countries.

Avaya Sales & Partner Portal

http://sales.avaya.com is the official website for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the portal can be customized for specific products and information types that you wish to see and be notified about by email.

Avaya IP Office Knowledge Base

http://marketingtools.avaya.com/knowledgebase provides access to an online, regularly updated version of the IP Office Knowledge Base.

Avaya maintenance, lifecycle and warranty information

Avaya support services complement standard Avaya maintenance, lifecycle and warranty policies that are posted on http://support.avaya.com. For more information, send email to support@avaya.com.

International Avaya User Group

http://www.iaug.org is the official discussion forum for Avaya product users.

Product compatibility

For the latest and most accurate compatibility information go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Related links

Accessing Avaya DevConnect Application Notes on page 134
Interoperability on page 93

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Página2395 de 3226.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya User ID and password.

   The Support page appears.
3. Under **Support by Product**, click **Product-specific support**.
4. Enter the product in **Enter Product Name** text box and press Enter.
5. Select the product from the drop down list and choose the relevant release.
6. Select the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Phones on page 38
Phone interoperability on page 95

Accessing Avaya DevConnect Application Notes

The Avaya DevConnect program conducts testing with service providers to establish compatibility with Avaya products.

Procedure

1. Go to http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp.
2. Sign in or register.
3. Click a timeframe to search within.

   A list of all the application notes for that timeframe appears.

Página2396 de 3226.

4. In the **Search** field, type `IP Office` and press **Enter**.

   A list of relevant Application Notes appear.

Related links

Phones on page 38
Phone interoperability on page 95
Product compatibility on page 133
Hardware and software options on page 84
Interoperability on page 93

Página2397 de 3226.

Glossary list

Automatic Route Selection	A feature of some telephone systems in which the system automatically chooses the most cost-effective way to send a toll call.
Busy Hour Call Completions	A measure of dynamic traffic calls that can be completed in an average busy hour.
Communication Manager	A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.
Computer Supported Telecommunications Application (CSTA)	A standard interface for Computer Telephony Integration (CTI) applications, such as voice mail and auto-attendant, to interact with telephony equipment.
Digital Communications Protocol	A proprietary protocol that is used to transmit both digitized voice and digitized data over the same communications link. A Digital Communications Protocol (DCP) link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels and two telephones or data modules.
Directory Enabled Management	An interface that uses Avaya Directory Server to facilitate administration of Modular Messaging from a centralized location.
Distributed Communications System	A proprietary inter-networking protocol from Avaya with which you can configure two or more Avaya-based private communication networks to operate as one, large network.
Domain Name System (DNS)	An Internet Engineering Task Force (IETF) standard for ASCII strings to represent IP addresses. The DNS is a distributed internal directory service used mostly to translate between domain names and IP addresses. Avaya 9600 Series IP Telephones can use DNS to resolve names into IP addresses. In DHCP, TFTP, and HTTP files, DNS names can be used whenever IP addresses are available as long as a valid DNS server is identified first.

Página2398 de 3226.

Dynamic Data Exchange (DDE)	An interprocess communication (IPC) method.
Dynamic Host Configuration Protocol (DHCP)	An Internet Engineering Task Force (IETF) protocol used to automate IP address allocation and management.
Ethernet Routing Switch (ERS)	The Avaya stackable chassis system that provides high-performance, convergence-ready, secure, and resilient Ethernet switching connectivity.
Expansion Interface	A port circuit pack in a port network (PN) that provides the interface between a time-division multiplex (TDM) bus or a packet bus on the PN and a fiber-optic link. Expansion interface (EI) carries circuit-switched data, packet-switched data, network control, timing control, and digital signal-1 (DS1) control. EI in an expansion port network (EPN) also communicates with the master maintenance circuit pack to provide the environmental status and the alarm status of the EPN to the switch processing element (SPE).
Expansion port network	In Intuity Audix Server configurations, a port network (PN) that is connected to the time-division multiplex (TDM) bus and the packet bus of a processor port network (PPN). Control is achieved by indirect connection of the EPN to the PPN by way of a port network link (PNL).
Extension to Cellular access number	The phone number dialed to connect to the Avaya server that is running Communication Manager. The Extension to Cellular access number initiates the process of enabling or disabling Extension to Cellular or changing the station security code.
Federal Communications Commission (FCC)	A United States federal agency that regulates communications such as wire-line communications and the Internet.
Global Technical Services	An Avaya team that answers customer calls about products in Avaya Integrated Management.
Internet Protocol	A connectionless protocol that operates at Layer 3 of the Open Systems Interconnect (OSI) model. Internet Protocol (IP) is used for Internet addressing and routing packets over multiple networks to a final destination. IP works in conjunction with Transmission Control Protocol (TCP), and is identified as TCP/IP.
Local Survivable Processor	A configuration of the S8300 media server in which the server acts as an alternate server or gatekeeper for IP entities such as IP telephones and G700 media gateways. These IP entities use the Local Survivable Processor (LSP) when the IP entities lose connectivity with the primary server.

Página2399 de 3226.

Media gateway	An application-enabling hardware element that is part of a family of such elements. This family includes intra-switch connectivity, control interfaces, port interfaces, and cabinets. Avaya media gateways support both bearer traffic and signaling traffic that is routed between packet-switched networks and circuit-switched networks to deliver data, voice, fax, and messaging capabilities. Media gateways provide protocol conversion, such as IP to ATM to TDM, conferencing, presence, such as on-hook or off-hook, connectivity to private networks and public networks, such as IP, ATM, TDM, and networking, such as QSIG, DCS, ISDN. Media gateways support optional form factors.
Network Address Port Translation	A network routing technique. Network Address Port Translation (NAPT) is used to access systems on the same subnet as an IP Office.
Network Routing Policy	An application for centrally managing SIP routing for Session Manager instances. A routing policy describes how a call is routed: where it comes from, where it's going, what its dial pattern is, what time of day it is routed, and its cost for a particular route.
Novell® eDirectory™	An X.500-compatible directory service software product initially released in 1993 by Novell® for centrally managing access to resources on multiple servers and computers within a given network. Novell® eDirectory™ was formerly known as Novell® Directory Services. It is sometimes referred to as Netware Directory Services. Novell® eDirectory™ is a hierarchical, object-oriented database used to represent certain assets in an organization in a logical tree, including people, positions, servers, workstations, applications, printers, services, and groups.
OFCOM	The United Kingdom Office of Communication for the regulation of telecommunications.
PARTNER® Contact Closure Adjunct	A device that is connected to the chassis of a media gateway and provides contact closures. Contact Closure Adjunct (CCA) closes a relay in response to a dial-in command from the media gateway to operate a door or perform a similar action.
Product Information Presentation System	The Product Information Presentation System (PIPS) reports provide data from the Product Information Expert (PIE), a data mining tool that extracts Avaya customer switch and adjunct configuration information and stores it in a database.
Product Licensing and Delivery System (PLDS)	The Avaya licensing and download website and management system. Avaya Business Partners and customers use this site to obtain ISO image files and other software downloads.
Public Switched Telephone Network (PSTN)	A telephone network that includes many communication technologies such as microwave transmission, satellites, and undersea cables.

Página2400 de 3226.

Remote Feature Activation	A Web-based Avaya application to remotely activate features and increase capacities on the system of a customer by delivering a new license file.
System Manager	A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity.
System Status Application	An IP Office application that shows the status of things such as outgoing calls.
Telecommuter	The configuration where Communication Manager establishes the voice connection to a circuit-switched telephone. Requires two connections: a TCP/IP connection for signaling control and a circuit-switched connection for voice.
Telephony Application Program Interface (TAPI)	A Microsoft® Windows API that enables computers running Windows to use telephony services. TAPI is used for data, FAX, and voice communications. Applications can use TAPI to control telephony functions, such as dial, answer, and hang up.
Telephony Service Provider Interface (TSPI)	A Microsoft-defined interface to the telephony service provider (TSP). Microsoft® Windows comes with an H.323 TSP, an IP conference TSP, a kernel-mode device driver TSP, and a unimodem TSP.

Página2401 de 3226.

Index

A

a-law PCM 31
application notes 134
application support 87
architecture 71
auto-create support for users and extensions in WebLM ... 117
Avaya Communicator 45
    iPad 46
    Windows 47
Avaya Contact Center Select
    Business Continuity 83
    deployment options 80–83
    DVD 80
    hardware appliance 82
    overview 65
    reference configurations 78
    topology 78, 80–83
    user data synchronization 78
    VMware 81
Avaya Equinox Meeting Online 55
Avaya Spaces overview 55

B

base cards 31
Basic Edition 67
BCM migration 100, 107
browser support 87

C

CA 61
Central Access 61
cloud operations manager 63
cloud overview 75
components 72
Computer Telephony Integration 27
conference calls 51
configuration of WebLM licensing 115
    warnings and alarms 116
contact center 64
control unit 29
CTI 27
customer-provided PC requirements 91

D

data networking 18
deployment options 67
    Avaya Contact Center Select 78, 80–83
    DVD 80, 83
deployment options *(continued)*
    hardware appliance 82
    VMware 81
DevConnect 134
DMM 64
document changes 7

E

Embedded Voicemail 50
endpoints 126
end user applications 40
Equinox for IP Office
    Equinox
        Avaya Equinox 42
Essential Edition 69
external expansion modules 35

F

feature keys 31
features 13
features overview 54

G

gatekeepers 22
gateways 22
guidelines
    WebRTC 38

H

H.323 22
hardware options 84

I

InSite Knowledge Base 134
interfaces 105
interoperability 93, 99
IP500 V2 29
iPad 46
IP endpoint licenses 126
IP endpoint licenses for WebLM 116
IP Office applications
    contact center applications 64
    installation and administration applications 55
    user applications 40
IP Office Contact Center
    deployment options 77
    topology 77

Página2402 de 3226.

ip office editions 10
IP telephony 19

L

License migration
ADI 110
licenses 109
Basic Edition 118
Branch 120
Essential Edition 118
IP endpoints 126
Preferred Edition 118
SCN 120
Server Edition 119
small community network 120
Standard Mode 118
trials 126
trunks 121
upgrades 106, 127
users 122

M

Manager 55
MCUs 22
media manager
overview 58
Meet-Me conferencing 52
Migration
roadmap and limitations 108
Multipoint Connection Units 22

N

new features 11

O

one-X Mobile Preferred 40
one-X Portal for IP Office 41
operating system support 87
options
deployment 73
overview 10, 64, 75
Avaya Contact Center Select 65
Avaya Equinox Meeting Online 55
Avaya Spaces 55
enterprise branch 73
IP Office 73

P

packet-based voice and data networking 18
PCM 31
phones 38
phones *(continued)*
compatibility 95
country availability 98
remote 39
PLDS licensing 109
ports 105
Preferred Edition 70
private circuit switched voice networking 14
product compatibility 133
public voice networking 15
pulse code modulation 31

R

Radvision 53
receptionist licenses for WebLM 117
reference configuration
IP Office Contact Center 77
reference configurations 67, 73
related documents 130
remote phones 39
resource websites 133

S

SCN licenses 120
Scopia 53
SD cards 31
security 101, 102
Server Edition 70
Centralized licensing 111
licenses 119
Nodal licensing 111
Server Edition Manager 56
Session Initiation Protocol 23
SIP 23, 25
SIP endpoint user agents 26
SMA 61
SNMP Management Console 61
SoftConsole 49
SoftConsole administration 61
software options 84
Solution Management Application 61
solution specification 85
specifications
port interfaces 105
SSA 62
Standard Mode 118
support 133
SysMonitor 63

T

telephones 38
topology 14, 71, 74
Avaya Contact Center Select 78, 80–83

Página2403 de 3226.

topology *(continued)*
BP-hosted 76
Business Continuity 83
DVD 80
hardware appliance 82
Partner Powered 76
VMware 81
training 131
trials 126
trunk cards 33
trunks
licenses 121

U

upgrade licenses 127
upgrades 106
user licenses 122
user licenses for WebLM 117

V

VCMs 22
Video Collaboration Solution 53
video conferencing 53
videos 132
virtual environment 93
virtual licenses 111
Voice Compression Modules 22
Voicemail Pro 50
voice networking 14, 15, 18

W

web client
ip office web client
webrtc 44
Web License Manager 110
WebLM 110
WebLM license modes 114
WebLM license mode state transitions 115
WebLM licensing
auto-create support for users and extensions 117
configuration 115
configuration warnings and alarms 116
IP endpoint licenses 116
license modes 114
license mode state transitions 115
receptionist licenses 117
user licenses 117
Web Manager 58
WebRTC 38

Avaya IP Office™ Platform Solution Description

Release 10.1
Issue 1.2
September 2017

© 2017, Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number

indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 7
Purpose 7
Change history 7
Chapter 2: Avaya IP Office™ Platform overview 9
IP Office editions 9
New in this release 10
Features 11
Topology 11
Networking 12
Private circuit switched voice networking 12
Public voice networking 13
Packet-based voice and data networking 16
Internet protocol telephony 17
Computer Telephony Integration 25
Components 27
Hardware components 27
Phones 36
IP Office applications 37
Chapter 3: Solution specifications 61
Reference configurations 61
IP Office editions 61
Other deployment options 67
Hardware and software options 79
Server specifications 80
Operating system and browser support 81
Customer-provided PC requirements 85
Virtual environment requirements 87
Interoperability 88
Phone interoperability 89
IP Office and Avaya Aura® Communication Manager interoperability 93
BCM and IP Office interoperability 94
Security specification 95
Platform and application security details 97
Port assignments 99
Typical upgrade paths 100
BCM with CS1000 to IP Office migration 102
IP Office Branch migration 103
Licenses 103
PLDS licensing 103

Página2409 de 3226.

Migration of ADI licenses 105
Server Edition Centralized and Nodal licensing 105
Basic Edition license for new systems 112
Essential Edition and Preferred Edition licenses 112
Server Edition licenses 113
Branch licenses 114
Small Community Network licenses 114
Trunk licenses 115
User licenses 117
IP endpoint licenses 120
Trial licenses 121
Upgrade licenses 122
Chapter 4: Resources 125
Documentation 125
Finding documents on the Avaya Support website 126
Training 126
Viewing Avaya Mentor videos 127
Additional IP Office resources 128
Product compatibility 128
Support 128
Using the Avaya InSite Knowledge Base 129
Accessing Avaya DevConnect Application Notes 129
Glossary list 131

Página2410 de 3226.

Chapter 1: Introduction

Purpose

This document describes IP Office from a holistic perspective focusing on the strategic, enterprise, and functional views of the architecture. This document also includes a high-level description of solution specifications and available reference configurations.

Change history

The following table describes major changes made in this document for each release.

Issue	Release date	Summary of changes
Release 9.1, Issue 01.18	February 2016	This document was created to replace the *Avaya IP Office Product Description*.
Release 10.0, Issue 1	July 2016	• Updated the “New in this release” section. • Replaced 3740 DECT handset references with 3745 DECT. • Updated Avaya Contact Center Select content. • Made the following major licensing updates: - Added more contextual information. - Updated license names and their associated codes. - Reorganized Server Edition licensing content. - Added Basic Edition licenses. - Clarified basic user license support.
Release 10.1, Issue 1	June 2017	• Updated the “New in this release” section. • Added information about two new applications: IP Office Integrated Contact Reporter and IP Office Media Manager • Added information about additional hypervisor support in the “Virtual environment requirements” section • Added information about two new DECT phones: 3730 and 3735

Table continues…

Página2411 de 3226.

Issue	Release date	Summary of changes
		• Added information about a new Management API/SDK, and two new CTI interfaces: Centralized CTI WebService API and SSI over Web Services • Added information about two new expansion modules: DS16B2 and DS30B2 • Added granular access information in the “Web Manager” section • Added extension information in the “System Status Application (SSA)” section • Updated the “Operating system and browser support” section

Página2412 de 3226.

Chapter 2: Avaya IP Office™ Platform overview

The Avaya IP Office™ Platform is a cost-effective telephony system that supports a mobile, distributed workforce with voice and video on virtually any device. IP Office is an integrated, modular communications solution that scales up to 3000 extensions and 150 sites in a multisite network with resiliency. Match a deployment model to infrastructure needs from simple appliances to virtualized software in a data center with options in between. Improve customer experience and contact center agent efficiency with powerful, affordable multichannel functionality for voice, email and web chat. The solution combines collaboration software plus multichannel contact centers, networking, security and video.

IP Office provides a hybrid PBX with both Time Division Multiplexing (TDM) and IP telephony with trunk support, used in either mode or both concurrently. IP Office has data capabilities built-in, providing IP routing, switching and firewall protection, between LAN and WAN (LAN2).

In addition to basic telephony services and voicemail, IP Office offers both hard phone and soft phone options. Soft phone applications are designed to provide flexibility for remote workers and to allow workers to access telephony services, such as making and receiving calls, voicemail, and call forwarding from their computer or mobile device.

IP Office editions

IP Office also offers advanced features such as audio and video conferencing and voice over IP to meet the evolving needs of small, medium, and large enterprises.

IP Office is available in many deployment models based on the size of the enterprise and the features required using one or all the following elements:

- Virtualized IP Office software running in a virtual machine
- Dedicated server
- IP Office 500 version 2 (IP500 V2) control unit

Página2413 de 3226.

Edition	Platform	Business size (users)	Addresses business needs
Basic Edition	IP500 V2	Less than 25	Simple telephony and messaging capabilities only
Essential Edition	IP500 V2	20–99	Simple telephony and messaging capabilities plus IP telephony with essential mobility
Preferred Edition	IP500 V2	21–250	Essential Edition capabilities plus unified communications with preferred mobility
Server Edition	Linux Server, IP500 V2 and Linux Expansion	100 — 2000	Essential Edition capabilities plus unified communications with preferred mobility
Server Edition Select	Linux Server, IP500 V2 and Linux Expansion	100 — 3000	Essential Edition capabilities plus unified communications with preferred mobility
Server Edition or Server Edition Select with Virtualized Software	Virtualized	100 — 2000 (or) 100 — 3000	Essential Edition capabilities plus unified communications with preferred mobility
Server Edition or Server Edition Select hosted in Cloud	Cloud	100–2000 (or) 100–3000	Essential Edition capabilities plus unified communications with preferred mobility

IP Office Essential and Preferred editions are also referred to as IP Office Standard Mode. Each edition builds upon the next to offer additional functionality.

New in this release

IP Office™ Platform Release 10.1 offers the following new features and capabilities:

Note:

Features are available worldwide unless otherwise specified. Not all features are supported on all platforms and phones. See the descriptions for details.

Applications

Introduces the following applications:

- IP Office Media Manager: A native IP Office application to archive, store, search, playback, and download IP Office call recordings.
- IP Office Integrated Contact Reporter: A fully-integrated, Avaya-developed, reporting solution supporting 5 to 25 contact center agents and up to 5 supervisors.

Página2414 de 3226.

Centralized CTI WebService API

New API that provides a more open platform to allow third-parties to add value and build out solutions. Supports distributed (SE/SCN) environment.

Phone interoperability

Support for two new DECT handsets: 3730 and 3735.

Digital station expansion modules

Support for two updated, new modules: DS16B2 and DS30B2.

System Status Application (SSA) enhancement

Provides information on IP extensions that are registered but are no longer available.

Hypervisors

Support for three additional hypervisors: Microsoft Hyper-V, Amazon Web Services (AWS), and Kernel-based Virtual Machine (KVM).

Open APIs/SDKs

Support for a new Management API/SDK to address the needs of “Easy Button” setups. Provides a REST-based API Interface to the third-party application developers for consuming IP Office configuration objects.

Granular access to Web Manager

Provides organizations the option to allow Service Users access only to the required objects.

Features

See *Avaya IP Office™ Platform Feature Description* for detailed feature descriptions.

Topology

There are many options for IP Office topology. For detailed information about all the deployment scenarios, see the related *Reference Configuration* documents for each deployment scenario.

Página2415 de 3226.

Figure 1: IP Office systems connected to a single IP Office Manager endpoint

Networking

Private circuit switched voice networking

Where leased line circuits are used within a private networking scenario, these E1 or T1 interfaces are typically configured to use Q.SIG signaling between sites.

Q.SIG provides a level of voice feature transparency between PBXs and is the favored signaling standard within multiple vendor and international voice networks. The IP Office E1 or T1 module terminates a QSIG connection with a 120 ohm RJ45 interface.

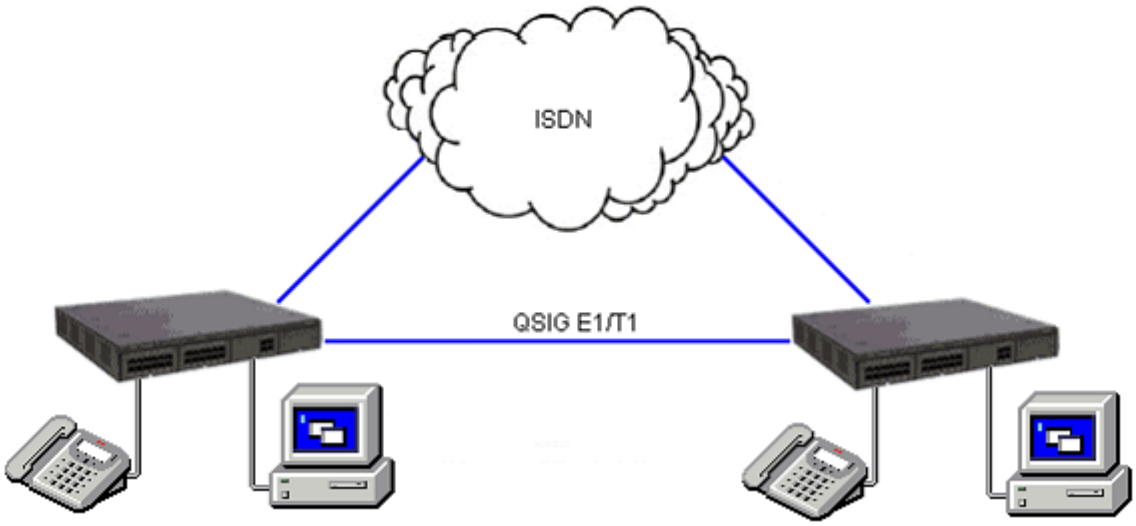


Figure 2: Circuit switched voice networking

IP Office supports the following Q.SIG services across this network:

Simple Telephony Call/Basic Call	ETS300 171/172
Circuit Switched Data Call/Basic Call	ETS300 171/172
Called/Calling Line ID Presentation	ETS300 173
Called/Calling Name Presentation	(SS-CNIP, SS-CONP, SS-CNIR) ETS300 237/238
Message Waiting	(SS-MWI) EN301 260/255
Transfer	(SS-CT) ETS 300 260/261

Public voice networking

IP Office supports a range of trunks and signaling modes for connection to the public switched telephone network (Central Office). Some of these lines are only available in certain territories; please check with your distributor for local availability. Primary rate trunks are available with either a single (24/30 channels) or dual trunk (48/60 channels).

ISDN Primary Rate (ETSI CTR4)

Service is provided by IP500V2 Universal PRI cards. ISDN Primary Rate provides 30 x 64K PCM speech channels over an E1 circuit and one signaling channel. Signaling Conforms to the ETSI Q. 931 standard with Cyclic Redundancy error Checking (CRC).

The following supplementary services are supported:

Página2417 de 3226.

Calling Line Identification Presentation (CLIP)	Provides the telephone number of the incoming call.
Calling Line Identification Restriction (CLIR)	Prevents the telephone number of the IP Office being presented on an outbound call.
Direct Dialing In (DDI)	Where the exchange provides the last x digits of the dialed number on an incoming call. This allows IP Office to route the call to different users or services.
Sub-addressing	Allows the transmission/reception of up to 20 digits, additional to any DDI/DID or CLIP information, for call routing and identification purposes.

IP Office supports the following features on both PRI and BRI trunks.

Note:

Feature availability depends on the ISDN service provider for which there may be charges.

Malicious Call Identification (MCID)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600) Short codes and button programming features are available so that users can trigger this activity at the ISDN exchange when required. This feature is NOT available on standard ISDN DSS1 telephones.
Advice of Charge (AOC)	(T3 digital and IP telephones only; Phone Manager) Advice of charge during a call (AOC-D) and at the end of a call (AOC-E) is supported for outgoing ISDN calls other than Q.SIG. The call cost is displayable on T3 telephones for call accounting purposes. IP Office allows configuration of call cost currency and a call cost mark-up for each user.
Call Completion to Busy Subscriber (CCBS)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, DECT telephones; Phone Manager) CCBS can be used where provided by the ISDN service provider. It allows a callback to be set on external ISDN calls that return busy. It can also be used by incoming ISDN calls to a busy user. This feature is not available on standard ISDN DSS1 telephones.
Partial Rerouting (PR)	(2400, 4600, 5400, 5600, T3, T3 IP, 9500, 9600, DECT telephones; Phone Manager) When forwarding a call on an ISDN channel to an external number using another ISDN channel, partial rerouting informs the ISDN exchange to perform the forward, thus freeing the channels to IP Office. This feature is not available on standard ISDN DSS1 telephones and it is not supported on Q.SIG.

Página2418 de 3226.

Explicit Call Transfer (ECT)	(Typically used by a third-party application) ECT is supported on the S0 interface. A Call to an S0 Endpoint can be transferred to any other device such as an analog, digital or IP endpoint or to any trunk. The normal usage of this feature is by a third party application connected through one or more S0 interfaces to IP Office. One example is the VoiceDirector, an automatic call assistant.

ISDN Basic Rate (ETSI CTR3)

Service is provided by IP500V2 BRI cards. ISDN Basic Rate provides 2 x 64K PCM speech channels and one signaling channel using Q.931 signaling and CRC error checking. Both point to point and point to multipoint operation is supported. Multipoint lines allow multiple devices to share the same line; however point-to-point is the preferred mode.

Basic Rate supports all the services that are supported on the primary rate version with the addition of Multiple Subscriber Number. This service is usually mutually exclusive with the DDI/DID service and provides up to 10 numbers for routing purposes, very similar to DDI/DID.

E1R2 channel associated signaling

Service is provided by IP500V2 Universal PRI cards.

The PRI E1R2 cards are available in two versions supporting either RJ45 or coax network connections. Each card provides channels that can be configured for MFC, Pulse or DTMF dialing dependent on the requirements of the network.

North American T1 Primary Rate

Service is provided by IP500V2 Universal PRI cards. T1 Primary Rate provides up to 24 64K channels over a 1.54M circuit. Each channel of the T1 trunk can be independently configured (channelized) to support the following signaling emulations with handshake types of immediate, delay or wink.

- Loop-Start
- Ground-Start
- E&M Tie Line
- E&M DID
- E&M Switched 56K
- DID - Channels configured for DID/DDI support incoming calls only. The carrier or Central Office will provide the last x digits that were dialed to be used for call routing.
- Wink-Start

IP Office T1 trunks support both DNIS and ANI services, where available from the central office.

Dialed Number Identification String (DNIS)	Provides a string of digits to IP Office depending on the number dialed by the incoming caller. This string can then be used to route callers to individual extensions, groups or services.
Automatic Number Identification (ANI)	Provides IP Office with a number identifying who the caller is. This may then be used for routing or computer telephony applications.

T1 trunk cards incorporate an integral CSU/DSU, eliminating the need for an external unit. The CSU function allows the trunk to be put in loop-back mode for testing purposes. This can be set manually,

Página2419 de 3226.

using the monitor application, or automatically from a Central Office sending a Line Loop Back (LLB) pattern. The DSU function allows the T1 trunk to be shared between data and voice services.

North American Primary Rate Interface (PRI)

Service is provided by the IP500V2 Universal PRI cards. IP Office supports Primary Rate ISDN trunks on 5ESS or DMS100 central office switches provided by AT&T, Sprint, WorldCom and other Local Telcos. Channels can be pre-configured for the supported services or negotiated on a call-by-call basis.

Special services can be configured to route calls to local operators or pre-subscribed carriers for both national and international calls (SSS). Alternate carriers can also be selected through the configuration of IP Office Transit Network Selection (TNS) tables.

IP Office also supports the Calling Name and Number service over Primary Rate Trunks (NI2).

Analog trunks

Loop start	Loop start trunks are available on the IP Office Analog Trunk cards installed within the IP Office control unit, or on the Analog Trunk 16-port expansion modules (ATM16). The first two trunks on the ATM16 are automatically switched to power fail sockets in the event of power being interrupted. Powerfail is also available on the trunk card when fitted to a combination or phone card. They conform to the TIA/EIA-646-B standard. The loop start trunks also support incoming caller line identification (ICLID) conforming to GR-188-CORE and GR-31-CORE standards. IP Office can use this information to route calls or provide it to computer applications to display additional information about the caller.
Ground start	Ground Start trunks are only available on the ATM16, configured through IP Office Manager. The first two trunks on the module are automatically switched to power fail socket in the event of power being interrupted. They conform to ANSI T1.401 and TIA/EIA-646-B standards. Not available in all territories.

Packet-based voice and data networking

IP Office supports data network use for voice communication, called voice over IP (VoIP).

IP Office supports networked voice and data communications with the following services:

- Built-in IP router
- One link for voice and data networking
- Common access to the Internet; share files and send e-mails to other sites
- Support for RIP-2 protocol for dynamic data routing; IPSec VPN, firewall and NAT (Network Address Translation) and for security; Centralized management and proactive fault management via SNMP.

IP Office supports IP packet-based voice networking between sites through VoIP across the campus LAN or VoIP across the public network.

In a factory or campus environment, voice calls can sent over 10/100 Mbps LAN connections on systems equipped with optional Voice Compression Modules (VCM). IP Office supports Diffserve by

Página2420 de 3226.

appropriately marking both RTP packets and signalling packets to facilitate network bandwidth management.

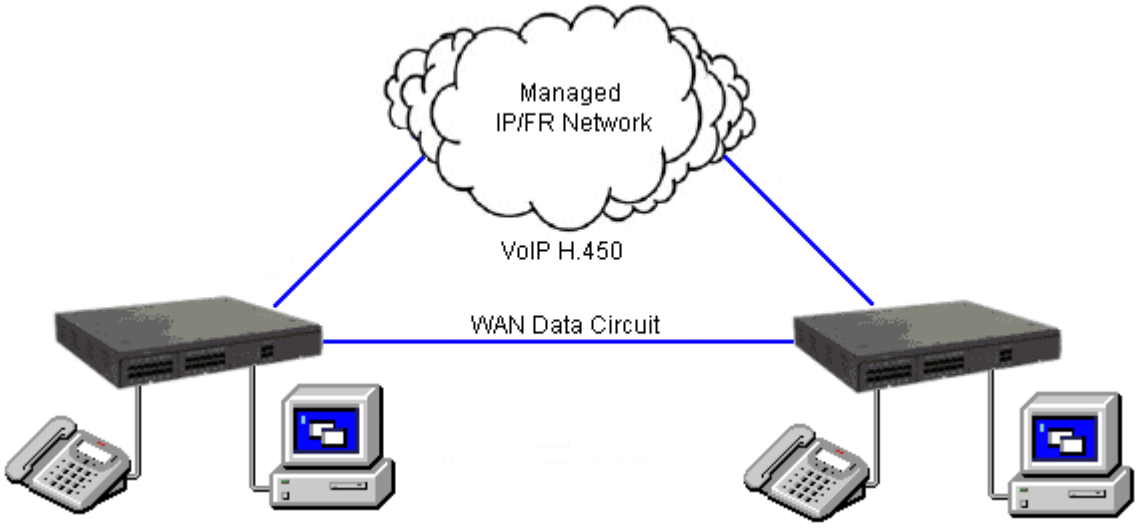


Figure 3: VoIP networking across IP network or WAN

IP Office can realize the benefits of Q.931 and H.450 supplementary service support across a public connection where an appropriate QoS connection can be established.

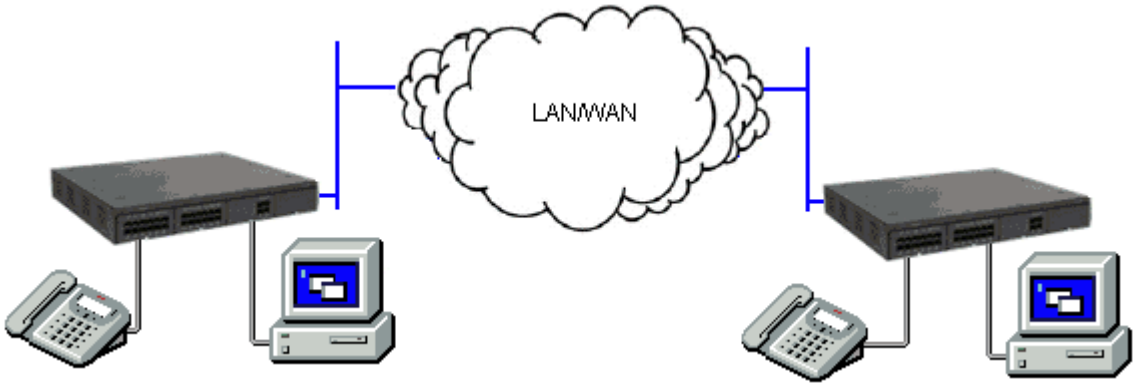


Figure 4: VoIP networking across the LAN

Internet protocol telephony

Internet Protocol (IP) refers to the type of rules that the network uses to send and receive signals. IP telephony converts voice communications into data packets. Conveniently, it runs on Ethernet LAN (local area network) technology. IP telephony unites a company's many locations, including mobile workers, into a single converged communications network.

IP Office is a converged telephony system; it combines aspects of traditional PABX telephony systems and IP data and telephony systems. IP Office supports PSTN, SIP, POTs, digital time division multiplexed telephones and digital IP telephones all on the same system. IP Office allows all the technologies to coexist.

Página2421 de 3226.

IP Office connects to the PSTN and to IP trunks providing a “hybrid” PABX function - where both legacy and future technologies can be used together to minimize operating costs and optimize business communications through both voice and data. The converged functionality works on multiple levels:

- Individual phone users can control the operation of their phone through applications running on their PC.
- Data traffic can be routed from the LAN interface to a telephony trunk interface.
- Voice traffic can be routed across internal and external data links. This option is referred to as voice over IP (VoIP).

Voice over IP (VoIP) and network assessments

Voice over IP (VoIP) means voice transmitted over a packet data network. VoIP is often referred to as IP telephony because it uses the internet protocols to make possible enhanced voice communications wherever IP connections exist.

The VoIP mode of operation can include external SIP trunks, IP trunks between customer systems and/or H.323 or SIP IP telephones for users. In either case the following factors must be considered:

- The IP Office control unit must be fitted with voice compression channels. These are used whenever an IP device (trunk or extension) needs to communicate with a non-IP device (trunk or extension) or to a device that uses a different codec.
- A network assessment is a mandatory requirement for all systems using VoIP. For support issues with VoIP, Avaya may request access to the network assessment results and may refuse support if those are not available or satisfactory.

A network assessment would include a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies, and setting voice quality objectives.
- The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support H.323, DHCP, TFTP and jitter buffers in H.323 applications.

An outline of the expected network assessment targets is:

Test	Minimum assessment target
Latency	Less than 150 ms
Packet loss	Less than 3%
Duration	Monitor statistics once every minute for a full week

Signaling protocols

In order to make use of VoIP, IP Office uses signaling protocols called H.323 and Session Initiation Protocol (SIP), to establish end-to-end connections for the voice path through an IP network. This connection ensures that each end is able to transmit and receive voice and provides the network addressing for end-to-end packet transmission. IP Office also connects the different technologies by translating the signals they use. For example an analog telephone can connect to a VoIP

Página2422 de 3226.

destination. This connection requires both the signaling and voice transmission to be translated. IP Office makes this translation using gateways and gatekeepers.

With IP telephony you connect an IP telephone to an IP PBX through a LAN. There are two basic types of IP telephones:

- A physical telephone, which looks very similar to a standard telephone, referred to as a “hardphone”
- A software application, referred to as a “softphone”, which runs on the user’s PC, allowing them to use a headset and microphone to make and receive calls anywhere they an and IP connection.

Quality of Service considerations

When making use of IP telephony, there are a number of data centric considerations such as which data types have priority on the IP network when there is contention. This is set with IP/TCP quality of service and should not be ignored. In situations where LAN bandwidth is limited, a quality of service capable LAN switch should be used to ensure voice packets are transmitted with the required priority on the network. If not, the conversation carried over IP appears as broken up due to delays or has unacceptable delays introduced in the conversation causing latency and jitter. With IP hardphones there is the need for Power over Ethernet (PoE), or local phone power supplies to be provided to the telephones as the IP telephones are not powered by IP Office.

Voice compression channels

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. IP Office systems use voice compression channels to make the conversion. These channels support the common IP audio codecs G.711, G.723 and G.729a.

The System Status Application can be used to display voice compression channel usage. Within the **Resources** section it displays the number of channel in use. It also displays how often there have been insufficient channels available and the last time such an event occurred.

Table 1: Voice compression channels

Call type	Voice compression channel usage
IP device to non-IP device	Requires a voice compression channel for the duration of the call. If no channel is available, busy indication is returned to the caller.
IP device to IP device	Call progress tones (for example dial tone, secondary dial tone, etc) do not require voice compression channels with the following exceptions: • Short code confirmation, ARS camp on and account code entry tones require a voice compression channel. • Devices using G723 require a voice compression channel for all tones except call waiting. When a call is connected: • If the IP devices use the same audio codec no voice compression channel is used. • If the devices use differing audio codecs, a voice compression channel is required for each.

Table continues…

Página2423 de 3226.

Call type	Voice compression channel usage
Non-IP device to non-IP device	No voice compression channels are required.
Music on hold played to IP device	Provided from the TDM bus and therefore requires a voice compression channel when played to an IP device.
Conference resources and IP devices	Managed by the conference chip which is on the TDM bus. Therefore, a voice compression channel is required for each IP device involved in a conference. This includes services that use conference resources such as call listen, intrusion, call recording and silent monitoring
Page call to IP device	Uses G729a for page calls, therefore only requiring one channel but also only supporting pages to G729a capable devices.
Voicemail services and IP devices	Treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.
Fax calls	These are voice calls but with a slightly wider frequency range than spoken voice calls. IP Office only supports fax across IP between IP Office systems with the Fax transport option selected. It does not currently support T38.
T38 fax calls	IP Office supports T38 fax on SIP trunks and SIP extensions. Each T38 fax call uses a VCM channel. Within a Small Community Network, a T38 fax call can be converted to a call across an H323 SCN lines using the IP Office Fax Transport Support protocol. This conversion uses 2 VCM channels. In order use T38 Fax connection, the Equipment Classification of an analog extension connected to a fax machine can be set Fax Machine. Additionally, a new short code feature Dial Fax is available.

Note:

T3 IP devices must be configured to 20 ms packet size for the above conditions to apply. If left configured for 10 ms packet size, a voice compression channel is needed for all tones and for non-direct media calls.

H.323 signaling protocol

IP Office IP telephony systems use open standards. Digital IP telephones, gateways and gatekeepers support the H.323 standard and it is this that allows devices from different manufacturers to work together. IP Office also supports an optional integral gateway, Voice Compression Modules (VCMs) and gatekeeper functionality.

IP Office uses the H.323 signaling protocol using the following architectural components:

IP telephones — H.323 service endpoint devices that support audio calls. Other types of H.323 devices can support video as part of H.323.

Gateways — Provide media translation to allow calls to be made to non-H.323 devices, for instance an analog telephone or the public network to connect with a H.323 device.

Gatekeepers — Control the call processing and security for H.323 devices.

Página2424 de 3226.

Multipoint Connection Units (MCUs)	Control conferences by adding together media streams.

These elements form an H.323 zone which is analogous to a PABX. Each zone has a single gatekeeper to control call distribution, call control and the resource management. On power-up, IP telephones, gateways and MCUs make registration requests to a gatekeeper which then authenticates (accepts or rejects) the request to become a member of the zone. Once accepted, a telephone wishing to make a call sends a call set-up message to the gatekeeper which then determines how to route the call and will then send an alert to the called telephone, or if the call is to a non-H.323 telephone establish the call via a Gateway within the zone.

Session Initiation Protocol trunking

IP Office uses Session Initiation Protocol (SIP) trunks to allow users to take advantage of telephony services offered by internet service providers (ISPs). In many cases, telephony services offer substantial savings in comparison to traditional exchange lines. To help enable the SIP Service Provider, Avaya offers a SIP Compliance Testing Program (GSSCP) that will validate the operation of IP Office with the ISPs SIP trunk offering. For more information about Avaya's SIP Compliance Testing Program (GSSCP), see https://enterpriseportal.avaya.com/ptlWeb/bp/so/CS201172610238111040.

IP Office allows all users, regardless of their phone type, to make and receive SIP calls. SIP trunks are handled like any other line on IP Office, affording all the call routing and toll control needed to manage inbound and outbound calls.

SIP trunks require provisioning of voice compression channels through the installation of VCM modules within the control unit. A license for the maximum required number of simultaneous SIP calls is also needed. Up to 128 simultaneous calls are supported.

IP Office also supports the T38 protocol which allows Fax over IP.

There are several possible network topologies for SIP trunk systems, as shown in the following diagrams:

Página2425 de 3226.

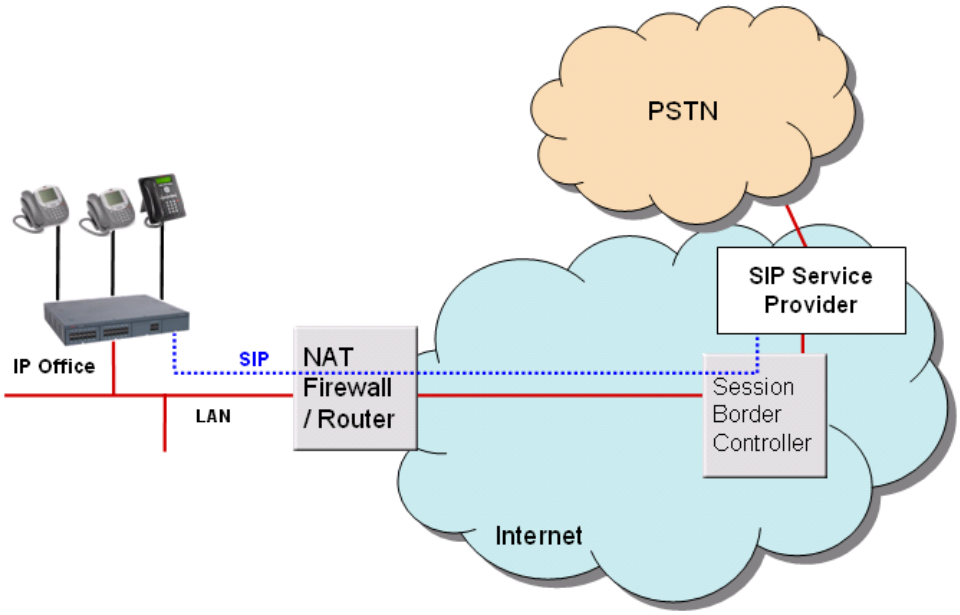


Figure 5: Service provider with Avaya Session Border Controller for Enterprise (recommended)

To make this configuration secure, the IP Office firewall is set to drop all packets except SIP.

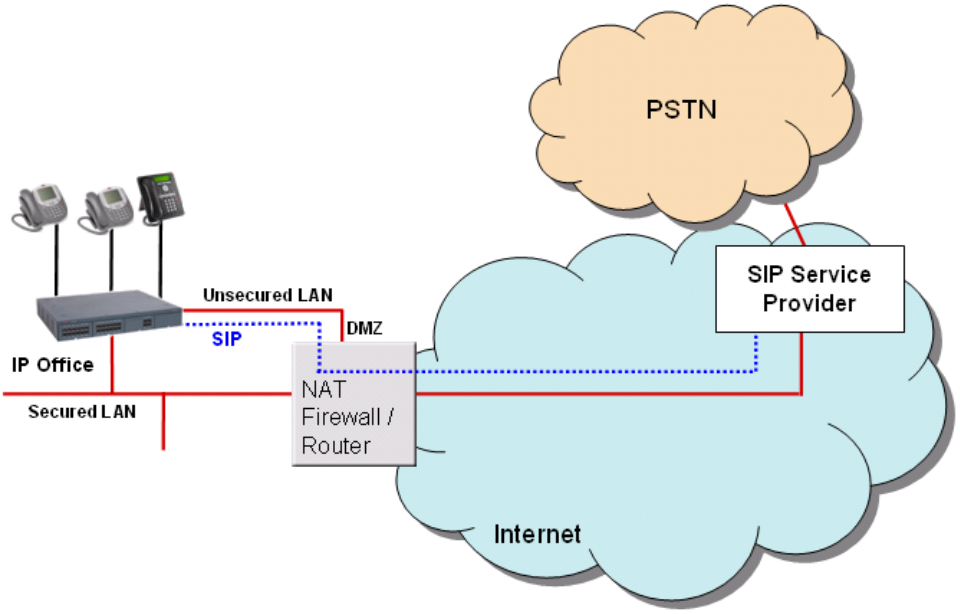


Figure 6: Direct connection from the second Ethernet port to the internet through a DMZ port on the router

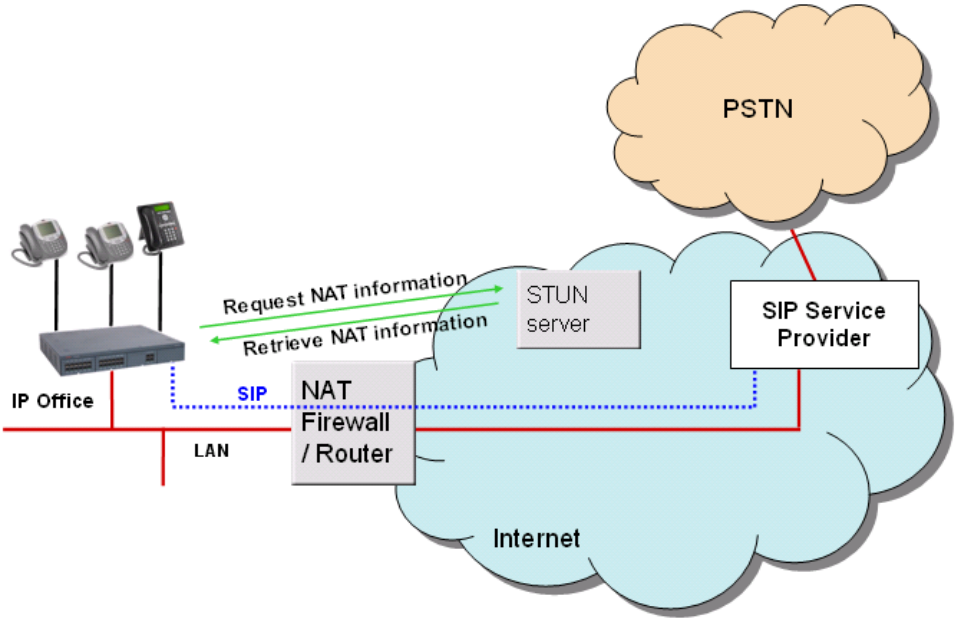


Figure 7: Connection to ITSP over NAT using third-party STUN servers

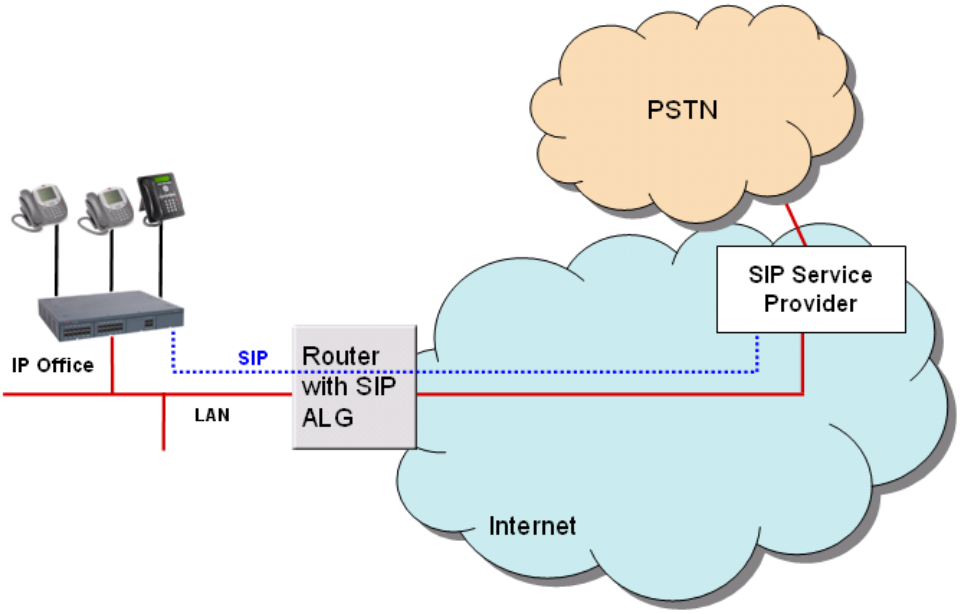


Figure 8: Connection to ITSP through router with ALG to resolves NAT issues

SIP servers

IP Office SIP endpoint implementation is built on two major SIP components: SIP server components SIP endpoint user agent applications.

SIP servers provide SIP endpoint support to allow full interoperability between SIP endpoints, other IP telephones based on H.323, digital and analog telephones as well as IP Office trunks (analog, digital or SIP-based).

Página2427 de 3226.

SIP servers provide centralized information and enablement services in a SIP ecosystem. The core SIP servers and their functions are summarized here. IP Office provides the features of the following two servers for voice and fax communication.

- **Registrar server**

  When SIP IP telephones come online, they need to make sure that others are aware that they're available to take and make calls. The Registrar authenticates and registers the IP phone (often directly related to a specific user) when it comes online, and then stores information on the telephones logical identities.

- **Proxy server**

  A proxy server takes SIP requests, processes them, and passes them downstream while sending responses upstream to other SIP servers or devices. A proxy server may act as both a server and a client, and can modify a SIP request before passing it along. A proxy is involved only in the setup and teardown of a communication session. After user agents establish a session, communications occur directly between the parties.

Functionality of the following two SIP servers are generally available by IP Office using existing IP Office functionality. Therefore, while functionality is provided, for example, allowing hot desking in a small community network, a consistent methodology between SIP and non-SIP endpoints is used to deliver those features

- **Location service**

  As users roam, the network needs to be continually aware of their locations. The location service is a database that keeps track of users and their locations. The location service gets its input from the registrar server and provides key information to the proxy and redirect servers. IP Office provides hot desking support, delivering a similar functionality but working consistently between SIP and non SIP endpoints.

- **Redirect server**

  If users are not in their home domains, sessions bound for them needs to be redirected to them.

  The redirect server maps a SIP request destined for a user to the device closest to the user. In IP Office, call forwarding and Follow me functionality is used to provide again consistent functionality between all type of endpoints.

SIP endpoint user agents

SIP endpoints, such as SIP telephones, cell phones, PDAs, or workstations, use user agent (UA) applications to provide the interface between the users and the SIP network.

SIP endpoint support is fully integrated into IP Office. No other components are needed. SIP endpoints require VCM module capacity like any other IP phone.

SIP extensions function like any other IP Office extension. IP Office provides the following functionality:

- Make and receive calls to any other extension, independent of type of extension.

Página2428 de 3226.

- Deliver end-to-end media. During calls between two SIP extensions or a SIP extension and an Avaya IP telephone, IP Office transmits audio end-to-end for basic telephone calls. Conferencing requires a VCM resource.
- Use short codes and authorization codes.
- Transmit in band call progress tones.
- Register endpoint using authentication with username and password.
- Support Auto-create. Successful endpoint registration uses a third-party license.
- Several extensions can register on one IP address, each using a license. This enables the connection of SIP terminal adapters with more than one analog port, giving a different extension number to each port.

Computer Telephony Integration

Computer Telephony Integration (CTI) bridges the gap between the telephone system and business applications. With IP Office, this is achieved with the IP Office CTI Link, a CTI middleware product and software developers kit (SDK).

On IP Office, CTI is delivered through adherence to open standards. This gives businesses access to a wide range of third-party solutions, addressing vertical markets, and designed to meet their requirements. For developers, migrating their offering from other platforms to IP Office is quick and easy, and the advanced CTI features that IP Office offers makes it easy to demonstrate full integration, and more business benefits.

IP Office provides two levels of CTI interoperability:

CTI Link Lite	Free of charge and provides all the functionality required to support the vast majority of applications, including screen-popping, and many third-party products.
CTI Link Pro	Provides enhanced functionality, including the ability to control multiple telephones and gives access to advanced call center operation.

Because IP networking is integrated into the IP Office system, all CTI is done through the LAN. This introduces additional points of failure, as well as relying on non-standard interfaces and handsets. On IP Office, all devices can be used with CTI.

Supported CTI interfaces

IP Office supports the following interfaces:

TAPILink Lite	Provides first-party CTI support for Microsoft TAPI 2.1 and TAPI 3.0, so each PC can control or monitor one telephone. The software components are supplied with the IP Office system on the User CD, and do not required a license key for use. The specification requires that a certain amount of core functionality is implemented, and additionally defines a series of optional functionality that switch vendors may also implemented.

Página2429 de 3226.

TAPILink Pro	Provides third-party CTI support for TAPI 2.1 and 3.0. These components are identical to their first-party equivalent; the presence of the CTI Link Pro RFA license key (which can be purchased in the usual way for products) enables this additional functionality. TAPILink Pro provides all of the features and functionality of TAPILink Lite, but additionally provides third party CTI operation. This means that a single server can control and monitor any number of telephone devices. In addition, TAPILink Pro provides the ability to monitor and control groups. This allows an application to be notified when a call enters a queue, and can also redirect it to another location.
TAPI-WAV driver	Provides software-based support for voice processing. The TAPI-WAV driver is for use with TAPI 2.1 only; for TAPI 3.0, IP Office supports the Media Service Provider (MSP) interface, defined by Microsoft in TAPI 3.0. This functionality will only work in conjunction with CTI Link Pro and also requires TAPI-WAV licenses. Each license enables 4 ports of voice processing.
DevLink Pro	Provides a real-time event stream in addition to the SMDR interface provided in IP Office SMDR. The real-time event stream takes the form of a call record, which is issued whenever the state of any endpoint of a call changes (typically there are two end points on a call, but for some circumstances, such as conference calls, intruded calls there may be more).
IP Office SMDR	Provides an interface to obtain SMDR events. A comma-separated record is issued for each call, when the call is completed. This interface is designed for call accounting and call billing applications. The IP Office SMDR can be output direct from the IP Office control unit to a designated IP address and port.
IP Office Software Development Kit	This toolkit is delivered on a single CD, containing the developer documentation for TAPILink Lite, TAPILink Pro, DevLink Lite and DevLink pro, as well as pre-compiled programs for exploring TAPI 2.1 and 3.0. In addition, example source code is included, making it easy for developers to become familiar with IP Office CTI interfaces. The Developer Connection Program (DevConnect) is the Avaya developer partner program, and is designed for third-party companies who are creating a product for sale, and who wish to receive technical support. Membership of the program is at the sole discretion of Avaya. DevConnect members pay an annual fee, for which they receive technical support directly from Avaya. In addition, Avaya will perform interoperability testing between IP Office and the member's product, and may also create opportunities for joint marketing, including exhibitions, use of Avaya's logo, and other benefits. More information on the DevConnect program can be found at http://www.devconnectprogram.com.
Centralized CTI WebService API	Provides a more open platform to allow third-parties to add value and build out solutions. Supports distributed (SE/SCN) environment and, therefore, is not limited to nodal like TAPI. It does have a dependency on Avaya one-X® Portal access for the users. When creating a new user in IP Office, it does not require a restart.
SSI over Web Services	Provides system monitoring information of SSI over a read-only REST web service available over https only. Realtime call data and call control are not

Página2430 de 3226.

available via this interface, but they will be made available via the DevConnect program.

This feature already has several areas instrumented but the data is for SSA and delivered over the Proprietary SSI interface, and there is a small set of data available on SNMP.

It does not require a license.

Open APIs/SDKs

With Release 10.1, IP Office supports a new Management API/SDK to address the needs of “Easy Button” setups. Enhancements to cover more areas, specifically what the legacy "XO" Configuration Web Services covers so that the legacy API can be made End Of Life. Management API provides a REST-based API Interface to the third-party application developers for consuming IP Office configuration objects.

- Provides all capabilities of currently supported IP Office configuration services (XO services).
- Request and response are in XML and JSON format.
- Provides Read/Write access to privileged service users only.
- No separate license is required for accessing the APIs.

Components

Hardware components

IP Office control unit

IP Office control unit (IP500 V2) is a stackable unit with an optional 19" rack mounting kit and an optional wall mounting kit for smaller configurations.

The IP500 V2 control unit is compatible with all IP500 base extension and Voice Compression Module (VCM) cards as well as all external IP500 expansion modules.

The IP500 V2 control unit has 4 slots for the insertion of IP500 base cards. The slots are numbered 1 to 4 from left to right. Normally they can be used in any order, however if the capacity for a particular type of card is exceeded, the card in the rightmost slot will be disabled. Each base card includes an integral front panel with ports for cable connections. Typically the first 8 ports on the left are for connection of extension devices. The 4 ports on the left are used for connection of trunks if a trunk daughter card is added to the base card.

The control unit provides the following functionality:

Maximum extensions	Up to 384 extensions.

Página2431 de 3226.

Conference parties	128 as standard but maximum 64 in any individual conference. Silence suppression is applied to conferences with more than 10 parties.
Trunk cards	Up to 4. Any combination of trunk daughter cards.
Voice compression channels	Up to 148 channels using up to VCM and combination cards.
Voicemail channels	Up to 250 voicemail/recording channels supported on the Primary server. For Select deployments, the Secondary server can also support up to 250 voicemail/recording channels.
Locales	Supported in the following countries: Argentina, Australia, Bahrain, Belgium, Brazil, Canada, Chile, China, Colombia, Customize, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Italy, Japan, Korea, Kuwait, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Norway, Oman, Pakistan, Peru, Poland, Portugal, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, United Kingdom, United States, Venezuela.
Power supply	Internal power supply unit.
Mounting	Free-standing, rack mounted or wall mounted (requires mounting kits).
Memory	Maximum configuration file size: 2048 KB.

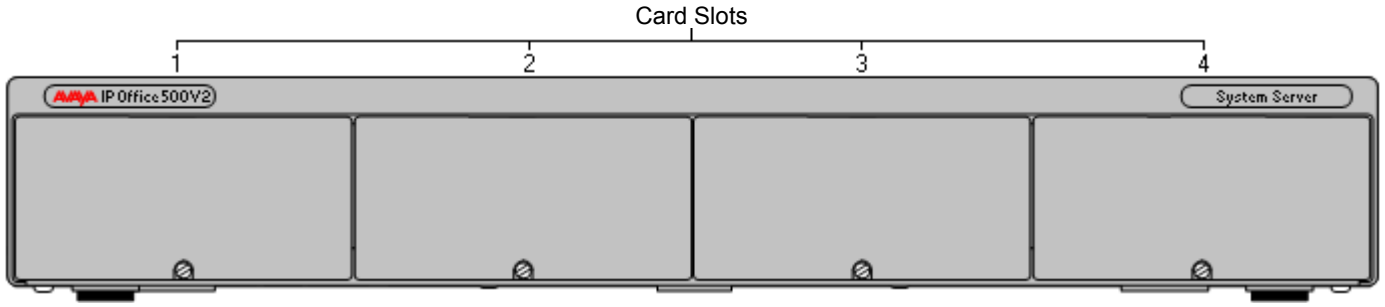


Figure 9: IP500 V2 front view

Página2432 de 3226.

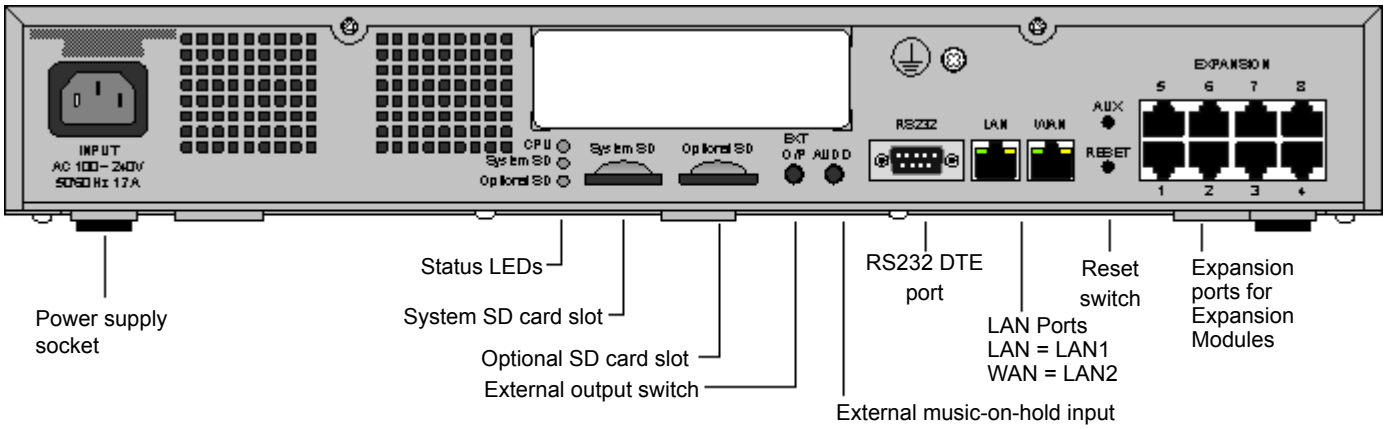


Figure 10: IP500 V2 rear view

Feature keys

The serial number of the feature key SD card fitted to the IP Office control unit is used as the basis for all licenses issued for that IP Office system and is used to regularly validate the licenses. If the feature key SD card is removed, over the next few hours licensed features will stop operating.

Pulse code modulation encoding

Pulse code modulation (PCM) is a method for encoding voice as data. In telephony, two methods PCM encoding are widely used, a-law and µ-law (also called mu-law or u-law). Typically µ-law is used in North America and a few other locations while a-law by the rest of the world. As well as setting the correct PCM encoding for the region, the a-law or µ-law setting of IP Office when it is first started affects a wide range of regional defaults relating to line settings and other values.

Base cards

The following base cards are available:

Table 2: IP500 V2 base cards

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
Digital Station (DS8)	3	Ports 1–8: Digital stations With trunk card: Ports 9–12: Central Office lines	Selected Avaya 2400, 5400 and 9500 series phones T3 phones (EMEA only) 3810 wireless phones (North America only) **Note:** 4400 series phones are not supported on this card. They are supported on external expansion module DS ports. 4100, 7400, M series and T series phones use the TCM8 Digital Station card.

Table continues…

Página2433 de 3226.

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
Analog Phone 2	4	Ports 1–2: Analog stations With trunk card: Ports 9–12: Trunk connections	Analog phones
Analog Phone 8	4	Ports 1–8: Analog stations With trunk card: Ports 9–12: Trunk connections	Analog phones
Digital Station (TCM8)	4	Ports 1–8: BST digital stations With trunk card: Ports 9–12: Central Office lines	Norstar®/BCM phones BST series phones Global M series phones Digital Mobility Controllers (DMCs) 7406e Wireless Telephones Digital Audio Conferencing Unit
Voice Compression Module (VCM V2)	2	Ports 1–8: Not present With trunk card: Ports 9–12: Central Office lines	VoIP calls including IP extensions or IP trunks. Up to 128 voice compression channels depending on the codec used. The IP500V2 control unit supports up to 148 voice compression channels, using the card plus voice compression ports on the Combination card.
ATM Combination (ATM V2)	2	Ports 1–6: Digital stations Ports 7–8: Analog stations Ports 9–12: Central Office lines 10 voice compression channels. Codec support is G.711, G729a and G.723 with 64ms echo cancellation. G.722 is supported by release 8.0 and higher.	Avaya digital phones except 3800 and 4400 series phones Analog phones Preinstalled trunk cards

Table continues…

Página2434 de 3226.

Base card	Maximum per system	RJ45 port assignment description	Telephones supported
BRI Combination	2	Ports 1–6: Digital stations Ports 7–8: Analog stations Ports 9–10: BRI trunk ports (4 BRI channels) 10 voice compression channels. Codec support is G.711, G729a and G.723 with 64ms echo cancellation. G.722 is supported by IP Office Release 8.0 and higher.	Avaya digital phones except 3800 and 4400 series phones (DS type not TCM) Analog phones Preinstalled trunk cards
Unified Communications Module (UCM V2)	1		Requires separate Preferred Edition license. Not supported on Server Edition. More than 200 users when running Voicemail Pro only. Up to 200 users when running Voicemail Pro and Avaya one-X® Portal for IP Office. 50 simultaneous Avaya one-X® Portal for IP Office users. No trunk cards
ETR6	3	Ports 1–6: ETR stations With ATM4: Ports 7–8: Power Failure Transfer Ports 9–12: Central Office lines	Not supported on Server Edition. PARTNER ACS phone ATM4, PRI/T1, or PARTNER mode µ-law SD cards (North America only)

Trunk cards

Trunk cards can be fitted to existing base cards to provide support for trunk ports. The trunk card uses the ports provided on the base card for cable connection. Each trunk card comes with spacer pegs for installation and port identification labels.

Note:

These cards are used for PSTN/FXS gateways with IP Office for Linux.

Página2435 de 3226.

Tip:

In systems with both Analog Phone 8 base cards and analog trunk cards, combining the two types are recommended because it provides analog power failure support for one trunk per extension (not applicable to the Analog Phone 2 base card).

Table 3: IP500 V2 trunk cards

Trunk card	Maximum per system	Works with these base cards	Description
Analog (V2)	4	ETR6 DS8 TCM8 Analog Phone 2/8	4 analog loop start trunks V.32 modem for remote access 1 power failure extension to trunk connection on Phone 8 cards
Universal PRI (PRI-U)	4	ETR6 DS8 TCM8 Analog Phone 2/8 VCM	Up to 2 PRI trunk connections. The card is available in single and dual port variants. The card can be configured for E1 PRI, T1 robbed bit, T1 PRI or E1R2 PRI trunks. Supports primary rate digital trunks. On each card, 8 channels per interface are enabled by default. This means that the single PRI has 8 channels enabled, while the dual PRI has 8 channels enabled on each of the two circuits. Further channels may be enabled by the purchase of additional licenses in 2-channel or 8-channel increments. Available in single and dual version. The single variant can support up to 24 T1 channels or up to 30 E1 channels. The dual variant can support up to 48 T1 channels or 60 E1 channels. Configurable for T1, E1, E1R2 MFC use, depending on territory. Includes an integrated CSU/DSU: • CSU allows trunks to be put into loop-back mode for testing purposes. This can be set manually, using the monitor application, or automatically from a Central Office sending a Line Loop Back (LLB) pattern. • DSU allows the T1 trunk to be shared between data and voice services. Includes diagnostics capabilities: visual indicators to show service state and physical test points to monitor traffic.

Table continues…

Página2436 de 3226.

Trunk card	Maximum per system	Works with these base cards	Description
			Supports mobility features: Mobile Call Control and one-X Mobile clients
BRI (Euro ISDN)	4	DS8 TCM8 Analog Phone 2/8 VCM	Up to 4 BRI trunk connections, each trunk providing 2B+D digital channels. Available in 2 (4 channels) and 4 (8 channels) options. Supports mobility features: Mobile Call Control and one-X Mobile clients.

External expansion modules

External expansion modules can be used with the IP500 V2 control unit.

Analog phone expansion modules

On analog ports, call information is sent while the phone is ringing, and cannot be updated during a call or set on an outbound call (the phone may do a local match but this is not controlled by IP Office). The primary purpose of displays is to give information about incoming calls. Where the caller display standard chosen supports the delivery of text (extension name) as well as the number, both are delivered.

An analog extension port can be set for external paging operation. It does not operate like a normal extension and is connected to external equipment through an isolation device (can also be used as an MoH source). The port will always be busy so it cannot be called directly and can only be accessed by using a paging feature. When not receiving a page, the port will remain silent. When being paged, the page tone is sent before the speech path is opened.

For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.

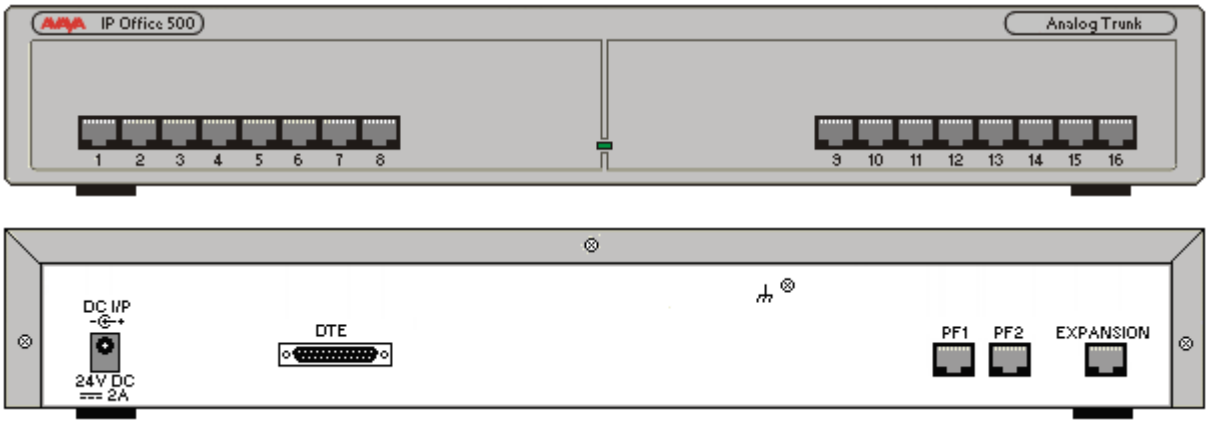
Expansion module	Telephones supported	Interfaces supported
Analog Phone 16	16 analog stations with calling line presentation	DTMF signaling (No rotary or Loop Disconnect) Time Break Recall (No Earth Recall) Message Waiting Indication (MWI): 51V Stepped, 81V, 101V and Line Reversal and Bellcore FSK
Analog Phone 30	30 analog stations with calling line presentation	

Analog trunk modules

This type of module can be used to add 16 additional analog trunks to an IP500 V2 system. The module supports both loop-start and ground-start trunks. The module also provides two powerfail ports for direct connection of analog phones to the first two analog trunks.

Basic Edition systems only support a single ATM16 expansion module. For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.

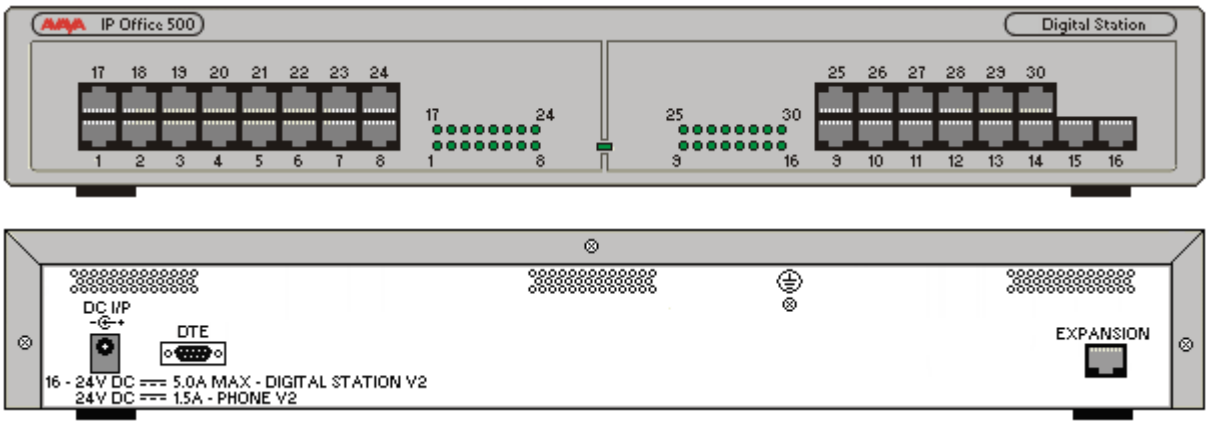
Página2437 de 3226.



Expansion module	Description	Interfaces supported
ATM16	16 analog trunks	Loop-start Ground start

Digital station expansion modules

For installations in a rack, this module requires the IP500 V2 Rack Mounting Kit.



Expansion module	Telephones supported	Description
DS16A	Norstar®/BCM telephones	16 digital station ports
DS30A	BST series telephones Global M series telephones Digital Mobility Controllers (DMCs) 7406e Wireless Telephones Digital Audio Conferencing Unit	30 digital station ports
DS16B, DS16B2[1]	Avaya telephones	16 digital station ports

Table continues…

Página2438 de 3226.

Expansion module	Telephones supported	Description
DS30B, DS30B2[1]	Either DS or TCM mode supporting the telephones connected to either the DS8 or the TCM8 cards.	30 digital station ports

Application server

The IP Office Application Server provides reliability, scalability and processing power for larger scale IP Office deployments. It is an external, rack mounted server that provides scalability for larger installations and multisite deployments not currently supported with the Unified Communications Module (UCM V2).

The IP Office Application Server is a single installation of selected IP Office™ Platform applications running on Linux. The Linux operating system is included as part of the installation. However, installation requires minimal Linux knowledge due to the inclusion of a web based management interface to allow the server to be managed remotely via web browser.

The IP Office Application Server hosts the following applications:

- Management Services
- one-X Portal for IP Office
- Voicemail Pro
- Web License Manager (WebLM)
- Web Manager
- Optional Services
  - Integrated Contact Reporter
  - Media Manager
  - Web Collaboration
  - Contact Recorder for IP Office
  - WebRTC Gateway

WebRTC gateway configuration guidelines

Use the following guidelines when configuring a WebRTC gateway:

- Define WebRTC SIP extensions on the:
  - SIP server that is part of the WebRTC gateway configuration.
  - Primary server if this is part of the deployment topology.
- With IP500 V2 deployments, WebRTC should be enabled on the Application server.

[1] DS16B2 and DS30B2 are supported on 10.1 and 9.1 releases only. For 9.1, support will be added through a Service Pack in August 2017, but partners are advised to visit the Avaya Support website to confirm the availability of support.

Página2439 de 3226.

Gateway limitations

The WebRTC gateway does not support resiliency.

Avaya Session Border Controller for Enterprise

An session border controller acts a router between the enterprise and carrier service, allowing only authorized sessions to pass through the connection point (border). The Avaya Session Border Controller for Enterprise (SBCE) delivers security to a SIP-based Unified Communications network.

For information on the SBCE, see *Avaya Session Border Controller for Enterprise Overview and Specification*.

For information on deploying the SBCE with IP Office, see “Configuring the Avaya Session Border Controller for IP Office Remote Workers” in either

- *Administering Avaya IP Office™ Platform with Web Manager*
- *Administering Avaya IP Office™ Platform with Manager*

Phones

IP Office supports multiple telephone solutions:

- IP telephones
- Digital telephones
- ETR telephones
- Analog telephones
- Wireless telephones
- Third-party SIP endpoints such as, desktop telephones, softphones and conferencing speakerphones

For detailed specifications, see specific telephone information on the Avaya Support site at http://support.avaya.com.

Related links

Remote phone support on page 36
Accessing Avaya DevConnect Application Notes on page 129
Using the Avaya InSite Knowledge Base on page 129
Phone interoperability on page 89

Remote phone support

IP phones using NAT router

IP Office supports remote 9600 Series IP phones with the H.323 FW which resides behind a NAT router to IP Office. The configuration does not require any VPN concentrator equipment. Remote 9600 H.323 IP phones can connect to IP Office even if it is located behind a NAT router. The phones are authenticated in the same way as phones in the private network. IP Office determines that a phone is located outside the private network and relays the VOIP RTP traffic to ensure it transverses the NAT router.

Página2440 de 3226.

Note:

H.323 signaling and the media traffic is not encrypted.

To reach IP Office from the remote private network, remote H.323 IP phones need to be configured to the public IP address of the NAT router hosting the IP Office. Configurable ports need to be forwarded to IP Office. IP Office requires a valid public IP address be configured and the public IP address can be statically configured or dynamically discovered via a STUN server. The Remote Worker feature requires the Essential Edition license which provides 4 remote worker seats. Enable the Remote Worker feature using IP Office Manager. Additional remote worker capability is available with the Teleworker User or Power User licenses and a Preferred Edition license.

VPN phones

VPN phones provide secure communication over public ISP networks to IP Office at the company headquarters. It is a software-only product that runs on 5610/5620/5621 or 4610/21 IP phones. In combination with one of these phones and the most popular VPN gateway products, the software extends enterprise telephony to remote locations. VPN functionality is supported on 9600 IP phones, and does not require a separate software load. VPN phone has been tested with a number of VPN-gateways from major vendors like Cisco or Juniper as well as with smaller VPN-access devices from companies like Adtran, Kentrox, Netgear, and SonicWall. Refer to the Avaya Support website for a list of available application notes on VPN-gateways tested with each line of phones.

IP Office applications

User applications

The following sections provide an overview of the applications intended for end users.

IP Office Media Manager

IP Office Media Manager is a native IP Office application to archive, store, search, playback, and download IP Office call recordings. The Operation, Administration, and Management of (OAM) of the application is integrated within the IP Office solution, for example, IP Office Web Manager.

Media Manager obtains the recordings from the IP Office Voicemail Pro application through a pre-configured hand-off directory in the same way as the current Contact Recorder application. Media Manager moves the recordings from the hand-off directory to an additional hard disk partition on the Server Edition Primary or Application Server and then archives the recordings to a storage location configured by the administrator. The archiving location can be a Network-Attached Storage (NAS), a local DVD drive, or cloud storage. For cloud storage, Media Manager supports only Google Drive in this release.

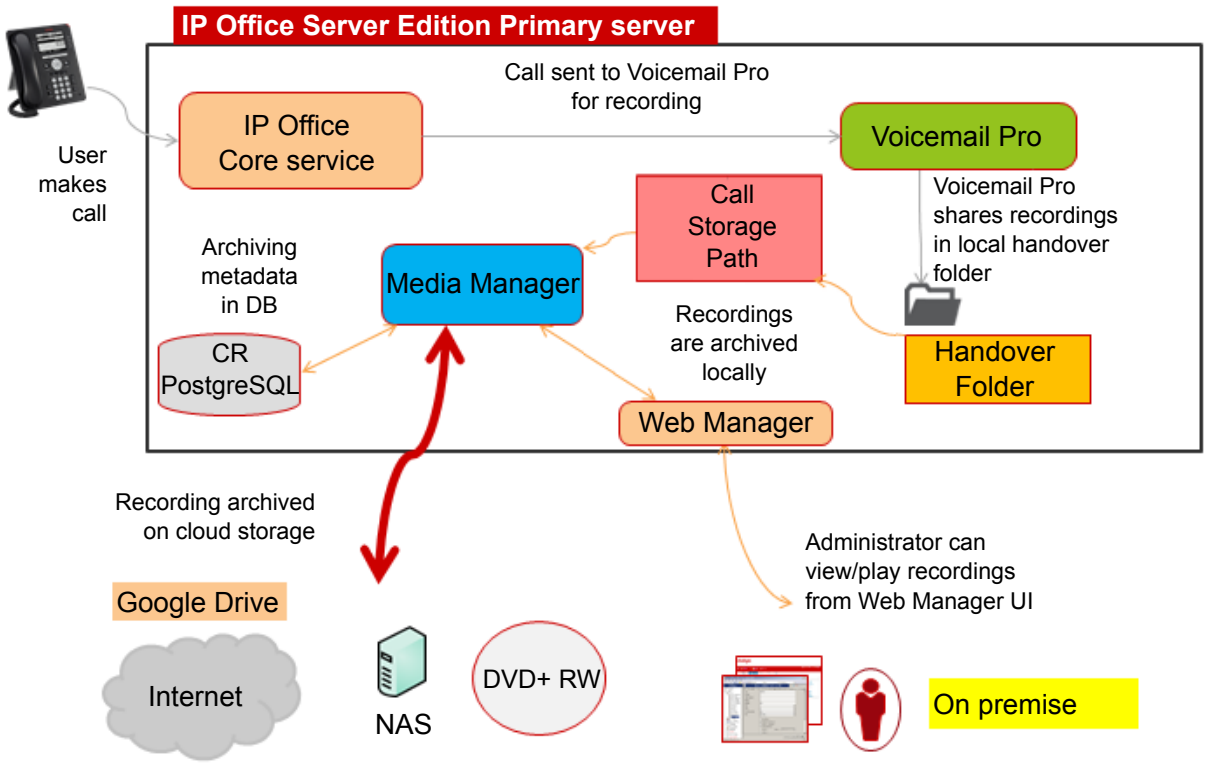
Media Manager is licensed on a system basis. Apart from a new IP Office Release 10.1 Media Manager license, the application also works with an earlier Contact Recorder license, for customers upgrading from an earlier IP Office version. Media Manager allows a 90–day trial period before licensing is enforced.

Media Manager does not support migration of earlier Contact Recorder files in IP Office Release 10.1. It is not supported to run both Media Manager and Contact Recorder at the same time, as this could cause issues with archiving of recording files.

Página2441 de 3226.

Media Manager is available as part of the IP Office Server Edition and Application Server software image. The application runs on the standard Linux distribution supported by IP Office Server Edition and Application Server platforms. The software is installed as a standard Linux RPM only on the Server Edition Primary server or the Application Server in case of IP500 V2 deployments. The application is not supported on UCM or Windows platforms. The management interface is web-based and all popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Internet Explorer are supported.

A standard IP Office Server Edition deployment:



Avaya one-X® Mobile

Avaya one-X® Mobile is an application that mobile users use to connect to IP Office.

Avaya one-X® Mobile works in call-back telephony mode. For example, when a user initiates a call from the client, IP Office initiates a call to the caller's mobile device and then dials the destination. This mode offers cost savings to users in countries where incoming voice calls are free or for users who have a cheaper unlimited voice plan as compared with a data plan.

The one-X Mobile Preferred mobility client also works in Voice over IP (VoIP) mode. In the VoIP mode, the client makes calls over Wi-Fi/3G/4G data networks. The client, using its underlying SIP stack, registers with IP Office over the data network and functions as an office extension.

Users in countries where incoming calls are charged will see a significant cost savings in the VoIP mode especially when on Wi-Fi networks. The availability of both call-back and VoIP modes on the

mobility client will enable users to toggle between the modes based on their network connections. This will empower end-users to make a choice of the appropriate mode based on their voice and data plan as well as the availability and quality of their data connection (WiFi/3G/4G). For example,

- The user can choose the call-back mode when he or she doesn't have Wi-Fi access and the 3G data connection is not providing good quality for voice.
- The user can choose the VoIP mode when he or she has access to a mobile hotspot where a Wi-Fi data connection is available or when the 3G or 4G data connection is good.

One one-X Mobile Preferred mobility client supports VoIP mode on both iOS and Android devices. VoIP mode is available with the Power User profile. Users with Mobile Worker profiles can only use call-back mode. VoIP mode does not require an IP endpoint license. The following features are available:

- Ring-tone selection
- High bandwidth or narrowband codec selection based on the network connection available
- Bluetooth headset audio control on VoIP calls
- Conference screen
- Contact phone number selection
- Voicemail priority indicator
- Swipe support for instant messaging on home screen
- Group action support
- Emoticons
- CLID lookup in contacts for calls
- Send voicemail as WAV in email
- Enable or disable mobile twinning (simultaneous ring)
- Enable or disable DND (send all calls)
- Call log combined with voicemails in the event history
- Call monitoring to see and interact with all calls
- VoIP mode dial plan
- Transfer calls as a third-party call controller (3PCC)

Avaya one-X® Portal for IP Office

Avaya one-X® Portal for IP Office provides users control of their telephone from a networked PC. Use this application with any extension; analog, digital or any IP telephone, wired or wireless, that is available as part of the Office Worker, Power User or Teleworker user licenses.

Avaya one-X® Portal for IP Office is a server-based application that the user accesses via web browser.

Página2443 de 3226.

For Telecommuter mode, One-X applications require answer supervision and disconnect detection for proper functioning. As a result, the one-X applications will not work with trunks that do not support answer supervision and disconnect detection.

Note:

one-X applications function on trunk types such as PRI, BRI, and SIP, however, they will not function on E1R2, T1 RBS and analog loop start trunks.

System administrators can control if Avaya one-X® Portal for IP Office can be accessed over a secure protocol only, recommended for hosted deployments to provide “secure only” access. The other option is to allow users to access the client over a secure and unsecure protocol (HTTP/HTTPS). The client application forces users to change their passwords and voicemail passcodes to meet the complexity settings configured by the administrator.

Through gadgets, Avaya one-X® Portal for IP Office provides the following features:

- Call information
- Call and conference control
- Presence and instant messaging notifications, monitoring and archiving
- Contact import and export
- XMPP groups displayed in the **System Directory** tab
- Dial to user’s own bridge and invite other users to join
- Conference call and other meeting scheduling including port reservations, email support and automatic report creation — available within the Outlook interface
- One-click web conferencing hosting and single sign-on joining web conferences as a participant

Avaya Communicator

Avaya Communicator is a collaboration software client that delivers an innovative interface for real time communications for Windows and on the iPad. It enables users to handle phone calls, instant messages, conferencing, web collaboration, presence, enterprise contacts and e-mail, all from a single interface. Avaya Communicator delivers the intuitive graphic design of spotlights, media menu, notification bar, and contact cards.

Avaya Communicator for IP Office communicates with both IP Office and Avaya one-X® Portal to provide communication and collaboration features. Telephony features such as make/receive calls, hold/unhold, mute/unmute, DTMF, MWI etc. are provided by IP500 V2 and UC features such as IM, presence, and enterprise contacts are provided by the Avaya one-X® Portal server.

If Avaya one-X® Portal server is unavailable, either due to licensing restriction or connectivity issues, the Avaya Communicator client will work in a telephony-only mode providing only telephony features. Interoperability with Avaya Session Border Controller for Enterprise allows the Flare Communicator client to be used by users with the Remote Worker profile and register with IP Office without requiring a VPN connection.

Página2444 de 3226.

Avaya Communicator provides the following features:

- Add participants using dial-pad or drag and drop
- Mute and unmute all or a subset of participants
- Lock and unlock the conference
- Place conference in lecture mode
- Enable and disable entry and exit tones
- Drop all or some participants from the conference
- End the conference
- Enable and disable continuation to allow the conference continue after the moderator drops
- Promote participants to moderator
- Create ad-hoc conferences by merging P2P calls
- Authorization and account codes (Windows only)
- Hold timeout reminder (Windows only)
- Compact user experience
- TSL/SRTP support
- Contact filtering
- Web conferencing integration
- Unsupervised transfer
- Auto-answer
- Simultaneous mode
- Password change
- Account codes
- Auto configuration (iOS only)
- Bluetooth and headset device support and selection (iOS only)
- Interoperability with Scopia (Radvision XT5000)

Note:

Avaya Communicator does not support recording and active speaker indicator.

Avaya Communicator for iPad

Avaya Communicator for iPad integrates voice, video, presence, instant messaging, directories into one unified interface over Wi-Fi or 3G cellular and VPN connections.

Avaya Communicator is a software-only solution that can be easily downloaded from the Apple iTunes Store supporting iPad2, iPad3, iPad4, iPad Mini (with and without retina display), iPad Air both Wi-Fi and 3G models and the following iOS versions: 6.1.x, 7.0.x, 7.1.x, and 8.0.x.

Página2445 de 3226.

Note:

Avaya Communicator is not supported on iOS 6.0.x.

With Avaya Communicator, IP Office users can use iPad devices for:

- Easy access to the real-time communications tools they rely on every day (phone, presence, IM, etc.)
- Blending real-time communications and business processes, such as mobile sales
- Taking advantage of Wi-Fi and 3G connectivity for cost-saving VoIP
- Secure signaling over TLS and secure media exchange over SRTP in cloud environments
- As a web conferencing moderator, the ability to share white board and documents
- Changing passwords
- Auto-answer support
- Unsupervised transfers
- Auto configuration services using a configuration profile hosted on a web server by email address or URL
- Bluetooth and headset device support and selection
- System directory search
- Add/delete members from a team (XMPP Group)
- Search the system directory and add to a team or personal contact
- Radvision XT5000 support for point-to-point video calls

Página2446 de 3226.

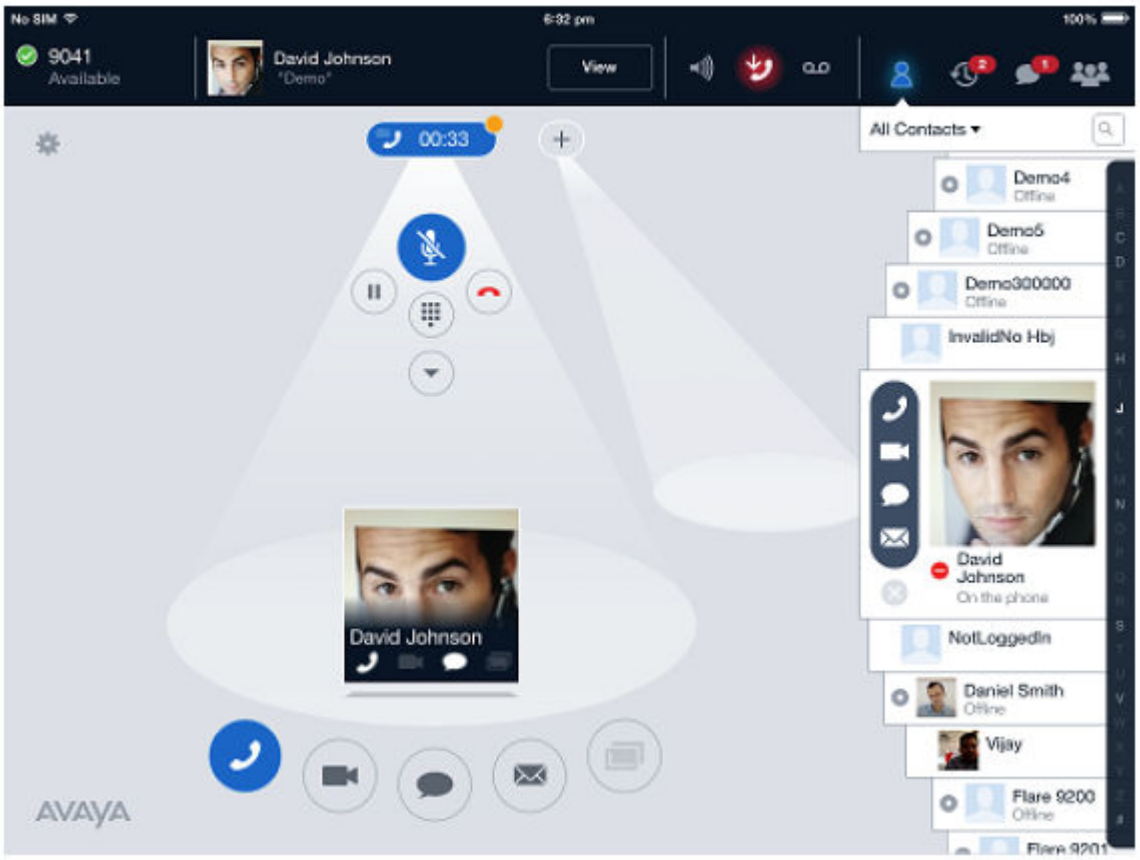


Figure 11: Avaya Communicator for iPad

Avaya Communicator for Windows

Avaya Communicator for Windows integrates voice, presence, instant messaging and directories into one unified offering for Windows laptops and desktops over a LAN connection.

Avaya Communicator provides the following features:

- Compact mode occupying less screen real estate

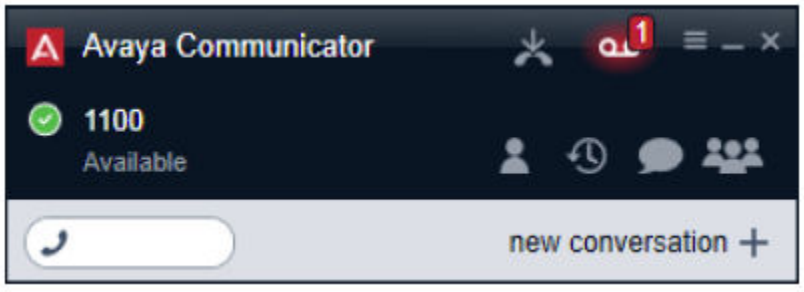


Figure 12: Avaya Communicator for Windows compact view

Página2447 de 3226.

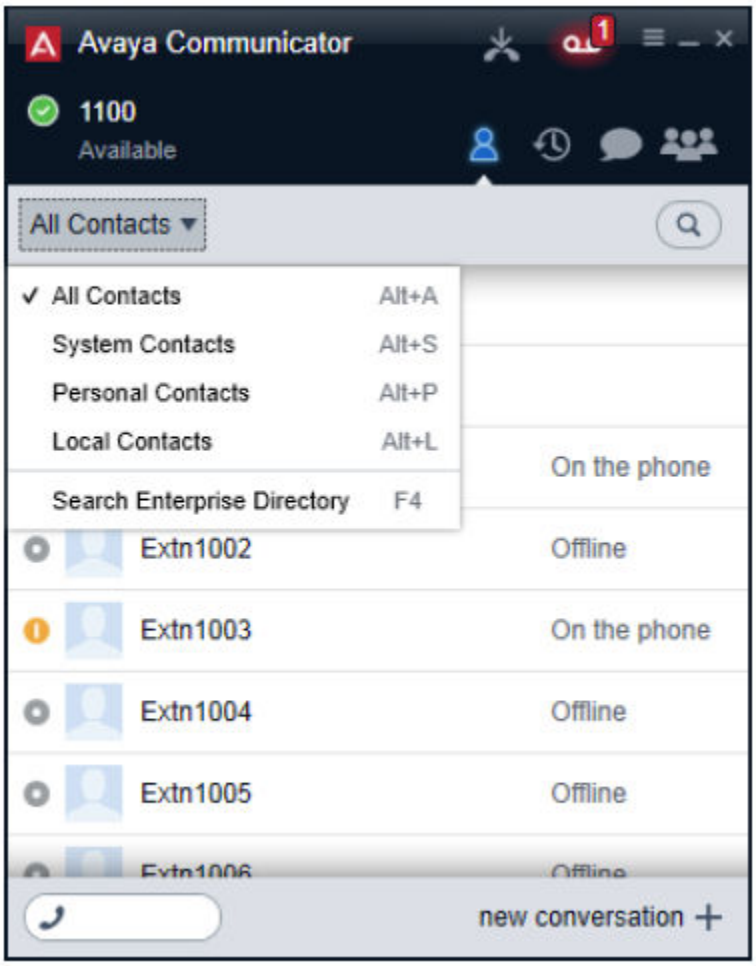


Figure 13: Avaya Communicator for Windows full view

- Secure signaling over TLS and secure media exchange over SRTP for cloud environments
- Contact filtering according to criteria and choosing to view only system, local, or personal contacts
- Web conferencing integration
- Unsupervised transfers
- Auto-answer
- Simultaneous mode for interfaces to one-X Portal, Outlook and Salesforce
- Password changing
- Account codes

IP Office Video Softphone

The IP Office Video Softphone is a full feature telephony client that supports standard telephony features on macOS operating systems.

Página2448 de 3226.

An IP Office Video Softphone macOS license is required and the user must be licensed as a Power User or Teleworker. IP Office Video Softphone works on macOS versions 10.8 and 10.9 only, and in the following languages: English, Spanish, French and Russian.

Note:

IP Office Video Softphone for Windows is no longer supported. Existing users must use Avaya Communicator for Windows.

IP Office Video Softphone includes the following features:

- Single message window to view all messages
- Busy Lamp Field (BLF) busy beep support
- Instant messaging
- Video conference for up to six participants
- Support for the G.722 codec option
- Multiple tabs for calls, contacts and logs
  - On the **Phone** tab, users can type a number or name and then make a phone or video call
  - On the **Contacts** tab, users can type a name in the search field to find matching contacts, then right-click for possible actions (audio call, video call, instant message)
- Two operating modes: client mode and application mode
- Several audio headset options for wireless headsets and full hook-switch support

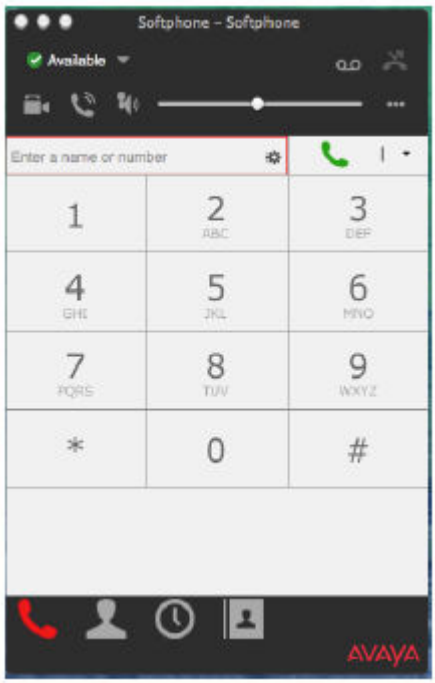


Figure 14: IP Office Video Softphone macOS keypad

Página2449 de 3226.

SoftConsole

SoftConsole is the PC-based Windows receptionist application for IP Office. It can be purchased with the Receptionist user license.

SoftConsole provides enterprise receptionists and operators with call information and call actions to simplify call handling and instant messaging. With SoftConsole, users see the status of other users and adjust basic telephony settings of other users, such as forwarding numbers. Avaya recommends using phones that support Auto Answer. Users can use instant messaging features provided by Avaya one-X® Portal, if available.

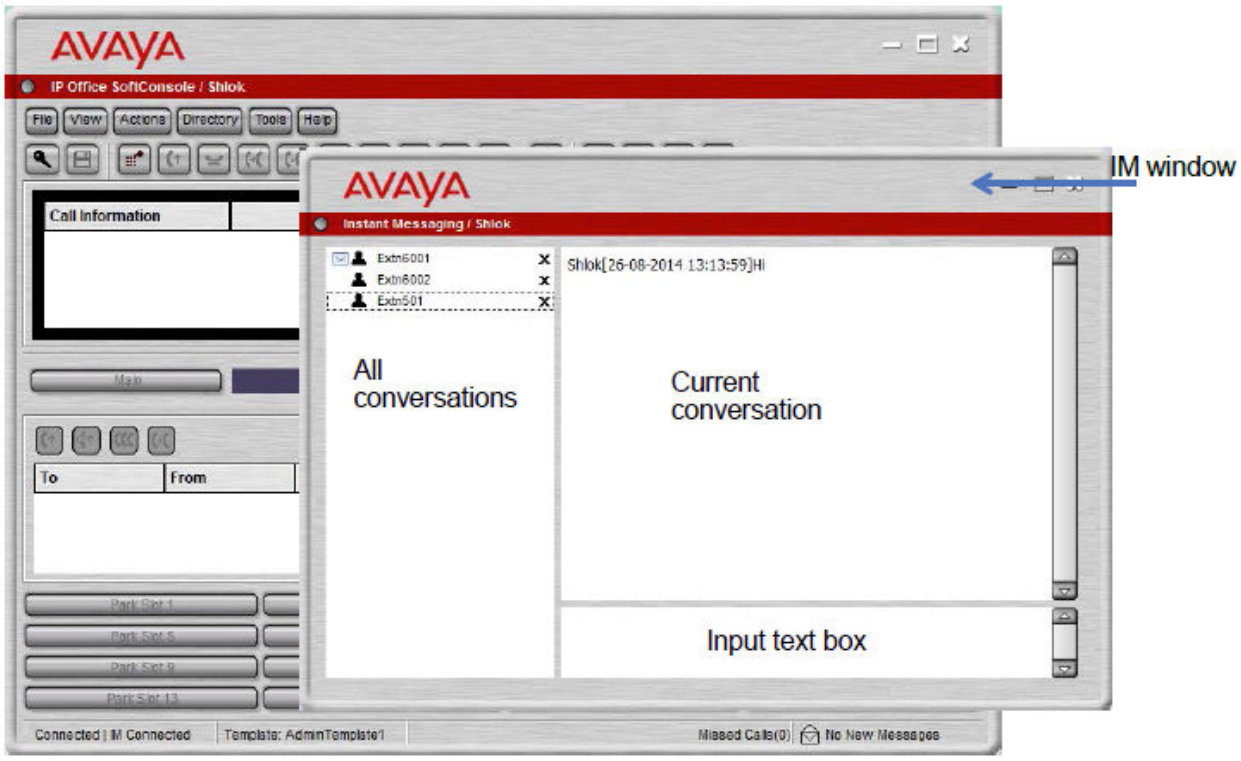


Figure 15: SoftConsole instant messaging window

WebSocket communication allows SoftConsole clients to communicate with IP Office and Avaya one-X® Portal. The WebSocket protocol is bidirectional between the client and the server. As the communication is done over port 80 or 443 (same port used for HTTP), there are no issues with firewall traversal. In a hosted environment, WebSocket communication provides security.

SoftConsole can be minimized in the Windows system tray when not in use, but will pop up on the screen when a call is received. Sound and media files can be associated with calls. If this feature is used, the PC requires a sound card and speakers.

SoftConsole supports the following features:

- Answering calls
- Making outgoing calls
- Supervised and unsupervised transfers

Página2450 de 3226.

- Transfer calls to voicemail
- Hold and park calls
- Monitoring queues and answering queue calls
- Using and viewing conference rooms
- Conferencing held calls
- Adding users to a conference
- Adding text to a call
- Door release
- Intrude
- Sending text messages
- Paging
- Recording calls
- Sending email
- Using dial pad
- Multiple language support, users can select language

Embedded Voicemail

In environments like retail or home office, where space, noise or cost considerations rule out using a PC for voicemail, Embedded Voicemail provides basic voicemail services. Embedded Voicemail is on the IP500 V2 control unit and does not require a separate voicemail server.

Embedded Voicemail is available with IP Office Essential Edition. No additional licenses are required.

Voicemail Pro

Voicemail Pro is provided with IP Office Preferred Edition and is an advanced messaging and call flow application for IP Office systems. Voicemail Pro can handle 40 (up to 250/500 on Server Edition/ Server Edition Select) simultaneous calls depending on license and system settings. Each user has the option of turning their voicemail on or off. When on, the system automatically answers their telephone when they are not available to take a call, plays a personal greeting, and records a message.

When a message has been left, the user will see a message-waiting lamp lit on their telephone and can press a retrieval button to collect their messages.

Voicemail Pro can also ring the user to deliver any new messages. Voicemail messages are time and date stamped and the caller's number recorded. Voicemail Pro can be configured to delete read messages automatically, unless the user chooses to save the message permanently.

Voicemails can be collected remotely by dialing into the Voicemail Pro server. If the number the user is dialing from is recognized (home number or mobile/cell phone for example), the user will listen to their voicemail straight away. If the source number is not recognized, the user will be prompted for a

Página2451 de 3226.

mailbox number and a PIN code for that mailbox, before they can listen to their voicemail. Users have the ability to set and change their own PIN codes.

When a voicemail needs to be forwarded to other users, Voicemail Pro provides many options:

- Voicemails can be forwarded to another mailbox, or group of mailboxes
- Recipients can add their comments to the voicemail before forwarding to another mailbox or mailboxes.
- Voicemails can be forwarded as email WAV attachments.

All options are available in a choice of languages; both spoken voice prompts and graphical programming interfaces and have the choice of IP Office TUI and INTUITY emulation TUI.

Conferencing

Users can place calls on hold and a create a conference using either the telephone or desktop applications. Additional conference members may be added, however a single conference may not have more than 64 members (with IP500 V2 only and more on Server Edition).

For ad-hoc conferencing, the system requires as many digital trunks/VoIP channels as external participants (as well as Preferred Edition for Meet-Me conferences). The system supports 128 conferencing channels on the IP500 V2, allowing multiple conferences of any size from 3 to 64 parties. The system support 42 3-party conferences, 2 64-party conferences or any combination in between. Meet-Me capabilities require Preferred Edition for direct dial into a conference bridge with PIN code security. In an SCN network, only one centralized Preferred Edition license is required to host Meet-Me conferences at any of the sites. Conference IDs are also shared across the SCN sites.

The following conference channel capacities are available:

Table 4: Conferencing channel capacities

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
HP DL120 Dell R210	128	128	414	414
HP DL360	256	256	825	825
Dell R620	256	512	825	825
OVA	256	512	825	825
IP500V2	128	128	128	128

To initiate a conference, users dial the direct number allocated to the conference bridge, type in the PIN (require Preferred Edition and Voicemail Pro) if required. For ad-hoc conferences with a few participants, users can easily set up immediate conferences by calling all parties and bringing them to the conference bridge. With Avaya one-X® Portal for IP Office, the originator of the conference can keep control: the Caller ID number (and the associated name if recognized) of each participant is displayed. If required, they can selectively hang-up a specific participant. The system plays a single beep on entry and a double beep on exit. The owner of the conference may use their extension number as the conference ID. The owner of the conference has control of the conference

Página2452 de 3226.

with the ability to mute and drop calls of participants. All participants will hear the system Music on Hold (MOH) until the owner joins, and will hear MOH when the owner drops. Note that any internal party has the option to view and drop participants (not just the conference originator).

Users can record a personalized greeting for a conference (requires Preferred Edition and Voicemail Pro).

Users can record the conference using Avaya one-X® Portal for IP Office, digital or IP display phone or a short code (requires Preferred Edition and Voicemail Pro). To prevent unauthorized access to the conference bridge, PIN codes, Caller ID number screening as well as time and date profiles can be set-up using Voicemail Pro. One user can manage the conferencing bridge facility from any location.

Conferencing has the following restrictions:

- Only two calls connecting through analog trunks are permitted in any single conference.
- Each external caller requires a digital trunk/VoIP channel (for example 1 T1 allows 23/24 external parties, 1 E1 allows 30 parties and a fully licensed VCM-64 allows 64 parties).
- There are no limits on the mix of internal and external calls in conference, but if all internal participants disconnect from the conference bridge, the external participants can be disconnected automatically by the system for added security (configurable system setting).
- System features such as call intrusion, call recording and silent monitoring all use conference resources, as does automatic recording if enabled. When any of these features are active the number of slots available for conference parties is reduced. For example, a conference call between 3 parties and being recorded will use 4 conference slots.

Meet-Me conferencing

Meet-Me conferencing enables multiple callers to talk in an audio conference. Callers can be on-site personnel as well as external parties whether field-based engineers, sales staff on the road, customers or suppliers. Conference calls can be planned in advance or established ad-hoc as and when required.

Video collaboration

IP Office provides Bring Your Own Device (BYOD) and HD room system support for video collaboration.

IP Office supports video collaboration with data sharing through Avaya Scopia® desktop and mobile applications when using Radvision MCU or Video Collaboration for IP Office. Flare clients can also participate in multiparty video conferences. Avaya Scopia® connects to IP Office as a SIP endpoint using an Avaya IP license.

Avaya Video Collaboration for IP Office provides the following features:

- Direct integration including a common dial plan with IP Office
- “Virtual conference room” for up to eight participants with click-to-join capabilities form any standards-based room system, desktop or mobile device
- Freely distributed desktop and mobile video clients for PCs, Macs and most popular iOS and Android devices, enabling people inside and outside an organization to easily join a video meeting

Página2453 de 3226.

- Low bandwidth HD multiparty video conferencing with data collaboration using native SIP/H.323
- Automatic firewall transversal to engage with participants outside the network

The following diagram shows the topology of IP Office deployed with video endpoints.

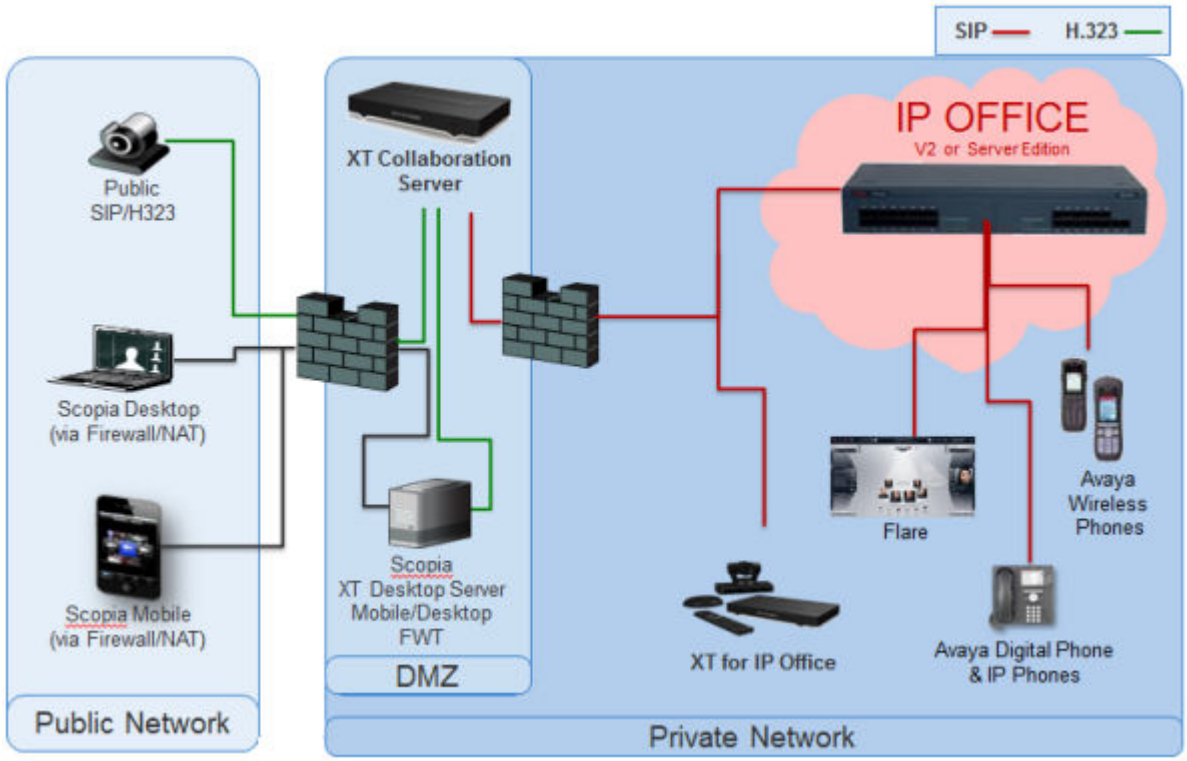


Figure 16: Video endpoints

Collaboration Agent

Collaboration Agent is an application that provides web collaboration and conferencing tools. Users with Avaya Aura® Conferencing accounts and invited guests can use the tools to manage conferences and participate and collaborate in conferences.

Conference participants can join conferences by logging in to Collaboration Agent and dialing in to the audio bridge assigned to the conference. Participants can also use the integrated audio and video feature of Collaboration Agent. Participants can use the Collaboration Agent tools to boost productivity and track action items even after the conference ends. Conference moderators can:

- Record all aspects of conferences.
- Record and edit meeting minutes.
- Create and distribute meeting reports based on the meeting minutes.

Collaboration Agent features

In Collaboration Agent, the participants and moderators can perform multiple tasks such as:

- View a list of other participants.

Página2454 de 3226.

- Virtually raise a hand and seek permission to speak.
- Send messages.
- Annotate shared content.
- Record or edit minutes.
- Set the entry and exit tones.
- Dial out to other users and the users to the conference.
- Disconnect participants.
- Promote participants to the moderator role.
- Invite more participants to join an active conference.

During the conference, participants can view the following information in Collaboration Agent:

- The participants who joined only on the audio bridge
- The participants active on web collaboration
- The participant currently speaking
- The current presenter

Optional features

The following features are optional and must be enabled by the system administrator:

- Starting conferences before moderators join.
- Integrated video
- Promoting all participants to the presenter role so that all participants can share content
- Dialing out from Collaboration Agent to connect users to conferences
- Conference recording

Installation and administration applications

The following sections provide an overview of the installation and administration related applications.

IP Office Manager

Use the Manager to manage IP Office standalone systems or systems in a small community network (SCN). Manager tracks system configuration changes, manages upgrades, and configuration imports and exports.

IP Office has a built-in audit trail that tracks changes to the system configuration, and who has made them. Manager can display the audit trail to assist with problem resolution. The audit trail records the last 15 changes in the configuration and records the following elements:

- Configuration Changed - For configuration changes, the log will report at a high level on all configuration categories (users, hunt group...) that have been changed.
- Configuration Erased
- Configuration merged

Página2455 de 3226.

- Reboot - user instigated reboot
- Upgrade
- Cold Start
- Warm Start
- Write at HH:MM - This is when the administrator saved the configuration via the schedule option
- Write with Immediate Reboot
- Write with Reboot When Free

IP Office Manager is also used for maintenance functions such as:

- Upgrade to the IP Office system software
- Ability to send software over an IP network link to a system and have it validated before committing to the upgrade
- Backwards compatibility with systems from Release 2.1 onwards to allow a single management application
- Importing and Exporting IP Office configuration information in ACSII-CSV files.

Server Edition Manager

Server Edition Manager supports complete centralized administration for Server Edition Primary, Server Edition Secondary, and Server Edition Expansion Systems. Manager also provides IP Office telephony and Unified Communications features.

Manager enables management of all the components within the solution for activities such as:

- Single point of configuration for IP Office and voicemail
- Simple initial installation wizard
- Overview of the system with inventory and status
- Common settings consolidated to the Server Edition Primary
- Integrated Voicemail Proclient, System Status Application, and Linux Platform settings access
- Supports online, offline administration, and configuring a complete solution
- Template operations
- Centralized configuration and template storage
- Administrator account management utility
- Retains existing IP Office expertise
- Context sensitive help

Even though Manager is a Windows application, Manager can be installed directly from the Web administration portal of Server Edition Primary server. This enables you to use any Windows personal computer that has any IP Office Manager that is pre-installed immediately.

Página2456 de 3226.

Using Manager, the administrator can create templates for many management items such as users, extensions, Hunt Groups, and Lines. The administrator can then create any new item using the default settings or the template. You can create multiple users and extensions using one template.

Call Routing Support:

- Full IP Office ARS and dial plan support
- Default routing simplifies configuration
- Solution wide auto line group numbering
- Common incoming call routes provide resilience
- Resilient Hunt Groups

Offline Operation:

- Complete solution can be created and/or managed offline if required
- Can still manage when some deices offline
- On/offline configuration sync options to harmonize as required

Solution Management:

- Complete solution view with status and inventory
- Users and Hunt Groups are solution wide
- Centralized User Rights, feature short codes, Time Profiles, Incoming Call Routes, and Account Codes
- Permits advanced per-device configuration if desired
- All configurations stored on primary server
- Solution wide system directory
- Easy management of central and per-device licenses

Resilience management:

- You can manage every device locally for ‘rainy day’ events
- You can manage the solution through a secondary server when the primary server fails or in a split WAN setup
- On/Offline configuration sync options to harmonize as required

Add or Remove Devices:

- Single process for addition or removal of device
- Built-in Initial Configuration Utility (ICU) to simplify adding a new device
- Common configuration items from primary server is auto populated
- Can configure before you install a new device

Validation :

- Configuration validation on read and any change.
- Solution wide validations

Página2457 de 3226.

Template:

- Create a local and centralized template from an existing Line, Extension, User, Hunt Group, Time Profile, Firewall Profile, IP Route and Service entries
- Recreate multiple Extension and Users from one template

Remote access:

- Supports access from service through SSL VPN

Security:

- Single Sign On to all except one-X Portal administration

Web Manager

Web Manager is a browser-based management tool designed to simplify the installation and maintenance process and provides access to most, but not all, IP Office configuration settings. Web Manager eliminates the need to have windows operating system because it can run on any device that supports standard browsers.

Granular access:

Web manager provides service users with access to entire configuration objects if the service user has the configuration access. However, large customers who have multiple service users roles or customers having deployments in the cloud environment need to have granular configuration access for different service users. Hosting partners will be able to build an account for customer or re-seller with limited permissions. These permissions shall restrict the customer or re-seller from performing activities that affects service of the system.

Solution Management Application

IP Office Manager and Web Manager use the Solution Management Application (SMA) to access the system configuration.

SMA resides on the primary or secondary server. Settings are available for remote access and Server Edition Central Access. Central Access communicates with the primary or secondary server rather than to each node individually. Avaya requires Central Access for a hosted environment and recommends it for non-hosted environments with more than 32 nodes.

SoftConsole Administrator mode

System administrators can start SoftConsole in administrator mode. When run in this mode, there is no access to the telephony functions.

SoftConsole administrator mode enables users to configure the following functions:

- Create and edit user profiles
- Amend the length of call notes
- Create and edit templates
- Remove or display the interface panels

SNMP Management Console

Simple Network Management Protocol (SNMP) is an industry standard designed to allow the management of data equipment from different vendors using a single Network Manager application.

Página2458 de 3226.

The Network Manager periodically polls equipment to solicit a response, if no response is received an alarm is raised. In addition to responding to polls, IP Office monitors the state of its Extensions, Trunk cards, Expansion Modules and Media cards so that if an error is detected IP Office will notify the Network Manager.

As the IP Office platform comprises many applications, the core software notifies SNMP events from both Voicemail Pro and Embedded Voicemail to warn of approaching storage capacity limits.

IP Office sends email notifications directly to the email server; no additional PC client is needed.

On customer sites where SNMP management is not available, IP Office can email events using up to 3 email addresses each containing a different set of alarms.

The following system event categories can be chosen for email notification, if installed on the system:

- Generic
- Trunk lines
- Embedded Voicemail Card
- VCM
- Expansion modules
- Applications
- License
- Phone change
- CSU Loop-Back

IP Office has been tested against CastleRock's SNMPc-EE™ and HP's Network Node Manager (part of the OpenView application suite).

System Status Application (SSA)

The System Status Application (SSA) is a diagnostic tool for system managers and administrators to monitor and check the status of IP Office systems locally or remotely. SSA shows both the current state of an IP Office system and details of any problems that have occurred. The information reported is a combination of real-time events, historical events, status and configuration data to assist fault finding and diagnosis. SSA provides real-time status, historic utilization and alarm information for ports, modules and expansion cards on the system. SSA connects to all variants of IP Office using an IP connection that can be remote or local. Modem connections at 14.4kbps or above are supported for remote diagnostics.

SSA provides information on the following:

Alarms SSA displays all alarms which are recorded within IP Office for each device in error. The number, date and time of the occurrence is recorded. The last 50 alarms are stored within IP Office to avoid need for local PC.

Página2459 de 3226.

Call Details	Information on incoming and outgoing calls, including call length, call ID and routing information.
Extensions	SSA details all extensions (including device type and port location) on the IP Office system. Information on the current status of a device is also displayed. SSA shows IP Extensions that were registered but no longer available and IP extensions that are configured but have not been registered after last re-boot. This helps to spot phones that are Idle, disconnected, or are misconfigured. SSA also shows quarantined phones and blacklisted extensions and IP addresses.
Trunks	IP Office trunks and connections (VoIP, analog and digital) and their current status are displayed. For VoIP trunks, QoS information is also displayed (e.g. round trip delay, jitter and packet loss).
System Resources	IP Office includes central resources that are utilized to perform various functions. Diagnosing these resources is often critical to the successful operation of the system. This includes details on resources for VCM, Voicemail and conferencing.
QoS Monitoring	QoS Parameters from connected calls, such as jitter and roundtrip delay, are monitored.

SSA can be launched independently or from IP Office Manager and there can be up to two (2) SSA clients connected to an IP Office unit at one time.

Note: SSA is not a configuration tool for IP Office systems.

SysMonitor

Use SysMonitor to troubleshoot IP Office from both local (LAN) and remote locations (WAN).

Select the protocols and interfaces to monitor and diagnose through a graphical interface. Capture traces directly to the screen or as a log file for later analysis. Color code different traces to improve the clarity in large files. The utility also captures system alarms and displays the activity log of the last 20 alarms that have occurred.

Data Migration Manager (DMM)

The Data Migration Manager (DMM) facilitates migration from BCM and Norstar systems to IP Office. There are three steps in the migration process: extract, convert and apply.

DMM migrates:

- Announcements and greetings
- Voicemail messages
- Extract Call Pilot configuration

Contact center applications

The following sections provide an overview of the contact center applications.

Página2460 de 3226.

For general information about:

- IP Office Integrated Contact Reporter, see *Using Avaya IP Office™ Platform Integrated Contact Reporter*.
- IP Office Contact Center, see *Avaya IP Office Contact Center Feature Description*.
- Avaya Contact Center Select, see *Avaya Contact Center Select Solution Description*.

IP Office Integrated Contact Reporter overview

IP Office Integrated Contact Reporter provides a fully-integrated, Avaya-developed, reporting solution that supports 5 to 25 Contact Center agents and up to 5 supervisors. Integrated Contact Reporter is installed with every IP Office hosted or server image, making it immediately available to IP Office customers on R10.1 with no additional hosting, server, or installation costs.

Integrated Contact Reporter is easy to deploy and easy to sell with minimal extra training. Operations, Administration, and Maintenance (OAM) are integrated with the IP Office solution. Integrated Contact Reporter leverages the IP Office Contact Center Chrome client for agent and supervisor reporting, call control, and existing hunt group capabilities on IP Office to "tag" specific hunt groups for reporting and analytics. The solution uses Voicemail Pro for queue announcements.

Note:

In Release 10.1, only incoming external calls are reported in real-time and historical reporting. There is no reporting on internal and outgoing calls.

IP Office Integrated Contact Reporter provides the following features:

- Real-time and historical reporting for IP Office hunt groups.
- Agent desktop – call control of associated telephony device and real-time reporting.
- Supervisor desktop – call control of associated telephony device, real-time and historical reporting.
- Agent and supervisor user interface is a web-based client that is supported on Google Chrome, Mozilla Firefox, and Safari browsers.
- Pre-configured summary and detailed historical reports:

  Note:

  In Release 10.1, reports cannot be scheduled, customized, or exported. You can view and download reports in PDF and print them.

  - Agent Summary Report
  - Call Detail Report by Agents
  - Call Detail Report by CLI
  - Call Detail Report by Hunt Group
  - Call Summary Report by Agents
  - Call Summary Report by CLI

Página2461 de 3226.

  - Call Summary Report by Hunt Group
  - Call Summary Report by Time Bucket
- Deployment options: IP Office Integrated Contact Reporter is dependent on Avaya one-X® Portal for IP Office as both are co-resident.
  - Application Server in case of IP500 V2:
    - Standalone IP500 V2 with Application Server.
    - For SCN – all agents, supervisors, hunt groups, and trunks, must be configured on the IP500 V2 that is monitored by Integrated Contact Reporter.
  - Server Edition Primary on IP Office Server Edition:
    - All agents, supervisors, hunt groups, trunks, and Voicemail Pro on the Server Edition Primary server.
    - All agents, supervisors, hunt groups, and Voicemail Pro on the Server Edition Primary; only trunks can be on the Server Edition Expansion System.
  - Preferred Edition, Select, and Cloud deployments.

The Integrated Contact Reporter Agent and Integrated Contact Reporter Supervisor licenses are $0 licenses with IP Office Release 10.1. The licenses are based on the number of logged-in Integrated Contact Reporter users. The Integrated Contact Reporter Supervisor license is a “superset” of the Integrated Contact Reporter Agent capabilities; the Integrated Contact Reporter Supervisor can also operate as an Integrated Contact Reporter Agent if required.

A number of Power User licenses equal to the number of active Integrated Contact Reporter users (agents and supervisors) is required. Customers are required to order a number of Integrated Contact Reporter Agent and Integrated Contact Reporter Supervisor licenses ($0) to enable Integrated Contact Reporter with IP Office Release 10.1.

IP Office Contact Center overview

Avaya is the market leader in call center technology, and IP Office Contact Center can take your business to a new level. IP Office Contact Center provides integrated contact center capabilities specifically designed for businesses supporting between 5 and 250 contact center agents and supervisors.

IP Office Contact Center provides the following features and characteristics:

- All-in-one customer service solution that delivers consistent service to customers across multiple media channels and locations. IP Office Contact Center includes a user interface (UI) on Microsoft Windows, a Chrome UI for Chrome OS devices, and a web interface supported on multiple browsers with Windows and Mac.

  The IP Office Contact Center User Interface for Chrome Devices and IP Office Contact Center Web User Interface provide similar functionality.
- Fast implementation with minimum disruption to the business. IP Office Contact Center also includes an automatic synchronization feature for configuration. This feature can be enabled and disabled as needed during implementation.

Página2462 de 3226.

- Access to Agent UI functionality, including call control, from a SalesForce (SFDC) plug-in or SAP CRM connector.
- Access to call control options with a Plantronics headset if you are using IP Office Contact Center User Interface for Chrome Devices.
- Email and chat capabilities on all UIs.
- Inbound and outbound voice calls with telephony and dialer capabilities.
- Skills-based routing.
- Address book access so agents can quickly find the contact information they need to make calls and send emails.
- Real time and historical reporting for all media channels.
- Interactive Voice Response (IVR) and Task Flow Editor scripts.
- User profile and agent group privilege configuration to determine which features are available to users of the interface. Administrators must assign privileges and create agent groups.
- Access to a web-based administration portal. You can use the administration portal to perform configuration, maintenance, monitoring, and management tasks. You can also upload certificates, collect logs, and download email archives and the IP Office Contact Center User Interface for Windows. Advanced administration tasks must be performed in the IP Office Contact Center User Interface for Windows. You cannot perform administration tasks with the IP Office Contact Center User Interface for Chrome Devices and IP Office Contact Center Web User Interface.
- Access to a wallboard that displays IP Office Contact Center statistics. For more information about Wallboard, see *Using Avaya IP Office Contact Center Wallboard*.
- Option to easily integrate chat functionality into a web page. For more information, see *Avaya IP Office Contact Center Email and Chat Services Task Based Guide*.
- Optional integration with Avaya Contact Recorder. Calls are recorded with Voicemail Pro and the details of the complete recording are stored in the Avaya Contact Recorder database. You can search for and manage recordings using a web browser.
- Optional interoperability with Avaya Workforce Optimization Select, which is a stand-alone product that does not currently integrate with IP Office Contact Center UIs or applications.

Avaya Contact Center Select overview

Avaya Contact Center Select is a context-sensitive, collaborative, voice and multimedia contact center solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform.

Avaya Contact Center Select uses industry-standard SIP and CTI interfaces to integrate with IP Office. This integration gives Avaya Contact Center Select access to and control of a wide range of IP Office phones and features. Customers integrating Avaya Contact Center Select with IP Office gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility.

Avaya Agent Desktop is a single-interface client application used by Avaya Contact Center Select agents to assist customers. Avaya Contact Center Select agents use Agent Desktop software to

Página2463 de 3226.

respond to customer voice and multimedia contacts. Agent Desktop supports a range of IP Office phones and a wide variety of multimedia contact types.

By default, Avaya Contact Center Select connections and Web Services use secure TLS communication. The Avaya Contact Center Select Certificate Management tool makes it easier to manage security certificates.

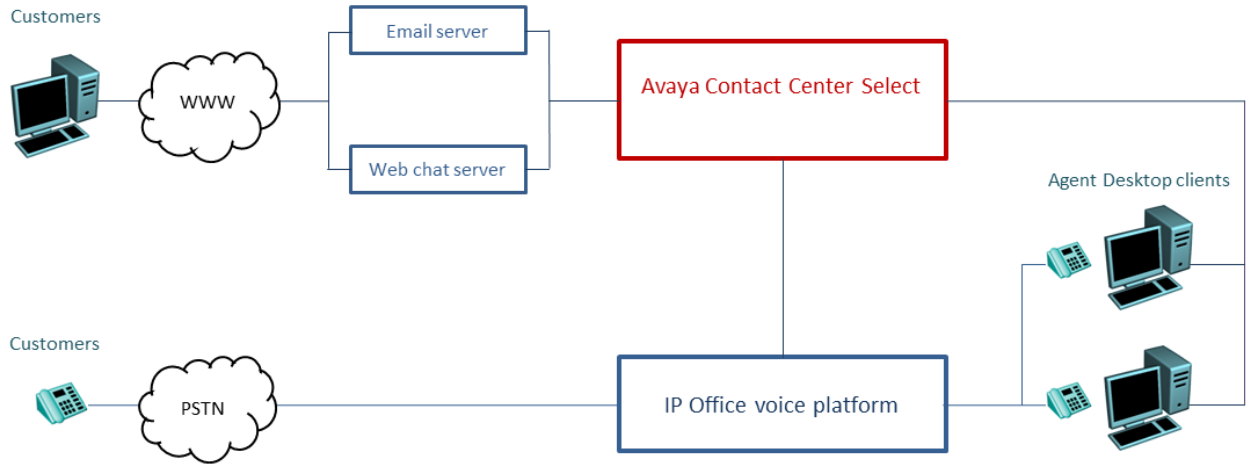


Figure 17: Typical contact center solution using voice and multimedia Avaya Contact Center Select and the Avaya IP Office voice phone system

Avaya Contact Center Select provides a feature-rich voice and multimedia solution with integrated routing and reporting for small to midsize enterprises. Avaya Contact Center Select provides unified contact center and IP Office phone user account management for agents and supervisors. Voice-enabled agents and supervisors created in Avaya Contact Center Select are automatically added to IP Office. Avaya Contact Center Select synchronizes user (agent and supervisor) information between Avaya Contact Center Select and IP Office.

Chapter 3: Solution specifications

Reference configurations

IP Office is sold in different editions, reference configurations, and deployment scenarios to meet different customer requirements. The editions build on one another to offer advanced functionality, including presence, instant messaging, web collaboration, and Microsoft software integration.

The following sections summarize IP Office editions and other configuration options. These sections do not provide complete reference configuration details for every IP Office option. Separate Reference Configuration documents are available for IP Office Server Edition, IP Office Branch, the OnAvaya™ and Powered Cloud solutions, and IP Office Contact Center.

IP Office editions

IP Office Basic Edition

IP Office Basic Edition is intended for small and growing enterprises that need higher productivity with a professional touch. Businesses can increase capacity as needed.

IP Office Basic Edition provides basic telephony features such as:

- 64 trunk capacity: analog, PRI/T1, and SIP
- Key system operation
- 64 party conferencing capacity
- Automated Attendant
- Multiple language support
- Call forwarding
- Caller ID
- Dial by name
- Breakout to reception
- Integrated voicemail:
  - Maximum of 6 concurrent calls to voicemail with approximately 25 hours of storage
  - Message control including Save, Delete, Forward, Repeat, Rewind, Fast Forward, and Skip Message

Página2465 de 3226.

- Visual voicemail
- Message time and date stamping

Modes of operation

IP500V2 control units are supplied with no installed firmware or configuration. When first powered up, the control unit loads and installs the necessary firmware from the system SD card installed in it. It creates a default configuration matching the card installed in the control unit and external expansion modules attached to it. IP500V2 control units can operate in a number of modes. The initial mode is determined by the type of system SD card.

Mode	SD card
IP Office Basic Edition Quick mode	• a-law telephony PBX system operation. • µ-law telephony key system operation.
IP Office Basic Edition - PARTNER Mode	Defaults to a-law telephony PARTNER mode operation.
IP Office Basic Edition - NORSTAR Mode	Defaults to µ-law telephony NORSTAR mode operation.

Basic Edition runs on the IP500V2 control unit. An SD is required and is installed in the rear of the control unit, providing operating software, feature keys, and licenses. An optional SD card can be installed in the optional SD card slot, providing redundant backup and system upgrade capabilities.

Table 5: Supported base cards

Basic Edition supports following base cards:

Base card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
Combination analog	4	4
Combination BRI		2
ETR6	3	
DS8	3	3
TCM8	4	4
Phone 2	4	4
Phone 8	4	4

Table 6: Supported trunk cards

Basic Edition supports the following trunk cards:

Trunk card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
ATM4	4	4
PRI/T1	1	
PRI/E1		1

Table continues…

Trunk card	PARTNER mode Maximum per system	NORSTAR mode Maximum per system
BRI4		4
BRI8		1

Expansion modules

Basic Edition supports the following expansion modules:

Note:

DS16B2 and DS30B2 are supported on 10.1 and 9.1 releases only. For 9.1, support will be added via a Service Pack in August 2017, but partners are advised to visit the Avaya Support website to confirm the availability of support.

- DS16A
- DS16B
- DS16B2
- ATM16
- Phone 16
- Phone 30
- DS30A
- DS30B
- DS30B2

IP Office Essential Edition

IP Office Essential Edition provides the same features as Basic Edition as well as the following:

- Mobile call control with one number access and simultaneous ringing on mobile devices
- Up to 4 remote workers through an internet connection and an Avaya 9600 series IP phone
- 24 hour access with customized voicemail greetings for each staff member
- Voicemail:
  - Maximum of 6 concurrent calls to voicemail
  - Send voicemails to email
  - Up to 25 hours of voicemail storage (with 6 ports)
  - Up to 40 automated attendants with a maximum of 6 concurrent calls
- Multiple language support
- Up to 128 party audio conference bridge with 64 in any one conference

Note:

Basic Edition is not a prerequisite for Essential Edition or Preferred Edition, and is not stacked under Essential Edition.

Página2467 de 3226.

IP Office Preferred Edition

IP Office Preferred Edition provides intelligent call routing, messaging, call handling and application integration.

In addition to the features provided with Essential Edition, IP Office Preferred Edition provides the following:

- Scalable voicemail:
  - Up to 40 simultaneous calls
  - Send a voicemail to all employees, a department, or a team
  - Address messages by extension or by name
  - Voicemail messages can “find” users to alert them a message is waiting
- Secure conferencing for up to 128 parties with 64 per conference
- Automated call routing with an unlimited number of automatic attendants that can be customized for time of day, day of week or other variables as well as to recognize callers and deliver personalized messages
- Call recording for incoming and outgoing calls that can be sent to voicemail or email inboxes as WAV files

Components

- IP500 V2 control unit
- Ethernet attached PC running the supported version of Windows Server
- Ethernet attached PC configured with Application Server software
- IMAP mail client (Outlook) for voicemail synchronization in email and browser-based access to voicemail
- Digital trunks and channels to support users
- IP Office supported telephones

IP Office Server Edition

IP Office Server Edition provides IP Office telephony capabilities, unified communications, mobility, and collaboration. It also provides high availability, ease of use, and low total cost of ownership (TCO). Targeted at the midsize enterprise, IP Office Server Edition supports up to 150 sites, 3000 users, and comprehensive resilience.

IP Office Server Edition Solution provides the following:

- A single Server Edition Primary server provides IP Office, Voicemail Pro, and Avaya one-X® Portal for IP Office.
- A Server Edition Secondary server increases the capacity and provide resilience.
- Expansion systems, which provide additional capacity, support analog or digital interfaces, and remote locations.
- A Select IP Office Server Edition Solution provides additional capacity.
- Support for an existing IP500 V2 control unit optimized for a hybrid of analog/TDM and IP deployments, or a Linux server optimized for IP only deployments.

- Users and extensions can be configured on the IP Office Server Edition server or the Server Edition Expansion System.
- Software distribution includes the various user and administration applications such as IP Office Manager, SSA, Voicemail Pro, and IP Office SoftConsole.
- Components can be in the same location or in different locations.
- Optionally configure a separate application server dedicated to Avaya one-X® Portal to provide more user capacity than the Server Edition Primary supports.
- Add additional servers and expansion systems any time.

.

Topology

IP Office Server Edition is based on a double star network topology that provides comprehensive features and their management, enables ease of use, installation, and administration. The overall solution provides a flexible and modular architecture starting with a single server and you can scale up the number of users and locations by networking multiple servers. The components automatically act as a single logical unit and you can administer the components from a single console through an integrated management system.

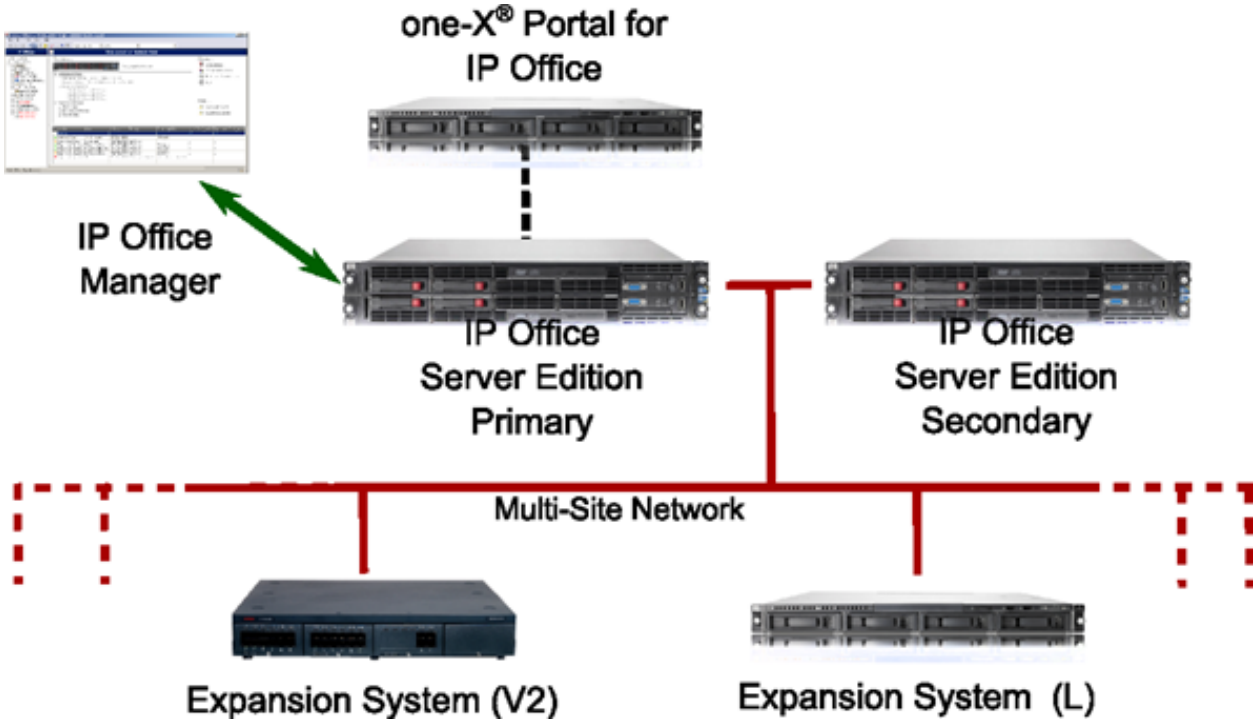


Figure 18: IP Office Server Edition topology

Deployment models

Centralized IP only	One primary server located at the customer headquarters

Página2469 de 3226.

Centralized IP analog and digital	One primary server and one expansion server located at the customer headquarters
Distributed IP only	One primary server located at the customer headquarters and one secondary server located at a remote location
Distributed IP analog and digital	One primary server and one expansion system located at the customer headquarters and one expansion system located at each remote site
Virtualized environment	Customer-provided software and hardware VMware vSphere platform with IP Office Server Edition and application server OVA ignited as a primary, secondary, expansion or application server.

Components

Component	Server options	Description
Server Edition Primary server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Software distribution includes: • IP Office Server Edition • Voicemail Pro • Avaya one-X® Portal for IP Office • IP Office Manager • System Status Application (SSA) • SoftConsole
Server Edition Secondary server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component to support resilience either centrally or at a remote site.
Server Edition Expansion System	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component to support remote locations. Up to 148 expansion systems provide additional capacity, support analog or digital interfaces, and local trunks at remote sites. Can be set up either centrally or at a remote site. **Note:** In a cloud environment, the IP500 V2 expansion system provides support for analog and digital endpoints.
Server Edition Expansion System	IP500 V2	Optional component to support remote locations and as a gateway.

Table continues…

Página2470 de 3226.

Component	Server options	Description
		Can be an existing IP500 V2 or IP Office Server Edition server. Can be set up either centrally or at a remote site.
Avaya one-X® Portal for IP Office application server	Dell R630 Dell R620 HP DL360G7 Dell R220 Dell R210 HP DL120G7	Optional component. You can optionally configure a separate application server dedicated to Avaya one-X® Portal to provide more Power User capacity above the maximum that Server Edition Primary supports.

Virtualized environment components

Avaya provides a virtualized equivalent to the IP Office Server Edition and applications server packaged as a single OVA ready for installation on vSphere supported host hardware from a PC. The OVA is available as a download from Avaya or on an orderable DVD. Once deployed, it can be ignited as a primary, secondary, expansion or applications server.

Other deployment options

You can also deploy IP Office in:

- An enterprise branch environment.

  You can deploy an IP Office system as a standalone branch or connect it to the Avaya Aura® network. A CS 1000 branch environment is also supported.

- A Cloud environment with the OnAvaya™ or Powered offers.

Contact center options are also available.

IP Office as an enterprise branch overview

You can deploy IP Office as an enterprise branch to provide a communications solution that is adaptable to meet the growing needs of an enterprise branch network while providing investment protection of the installed hardware platform and phones. You can implement an IP Office enterprise branch on an IP Office Standard Mode, Essential, or Preferred system. The IP Office system can be installed as an independent, standalone branch, or be connected to the Avaya Aura® network and migrated to a Distributed, Centralized, or Mixed enterprise branch to provide specific features and applications to meet the needs of individual employees in each branch location.

In addition to centralized SIP endpoints or centralized analog devices configured as ATA, IP Office can concurrently support other IP and TDM endpoints for a community of Centralized users and IP Office users in the same branch. Ideal for enterprises wanting applications deployed in customer data centers or in the branch, an IP Office Branch can effectively deliver a range of communication tools without complex infrastructure and administration.

IP Office is also supported in an Avaya Communication Server 1000 (CS 1000) branch environment. Only the Distributed enterprise branch option is supported. IP Office can be deployed as a new

Página2471 de 3226.

branch in an existing CS 1000 configuration with the addition of Avaya Aura® Session Manager to which IP Office connects through the SM Line for branch connectivity. Providing phone investment protection, IP Office can also be deployed as a replacement for Business Communications Manager (BCM) or Norstar in a branch office and connect to CS 1000 through Avaya Aura® Session Manager. IP Office cannot operate as a survivable gateway to CS 1000 endpoints as similar to Survivable Remote Gateway (SRG).

Topology

The IP Office Branch solution provides the flexibility to support independent, stand-alone IP Office branches as well as IP Office branches connected to an Avaya Aura® system. The Branch solution also supports CS 1000 integration. The following deployment options are available for the solution architecture:

- **Stand-alone IP Office branch option**: Independent IP Office systems are deployed within the network. These IP Office systems are not connected to each other or to anything else in the network. With this option, IP Office Branches are not connected to an Avaya Aura® system and users cannot access any Avaya Aura® services.
- **Distributed enterprise branch deployment option**: All users in this deployment option are IP Office users. These IP Office users obtain telephony services from the local IP Office and not from Avaya Aura®. The IP Office systems in this deployment option can be connected to Avaya Aura® Session Manager and administrators can obtain Centralized management services through Avaya Aura® System Manager. The enterprise can choose to connect IP Office users in this deployment option to an IP Office voice mail system, Embedded Voicemail or Voicemail Pro, or a Centralized voice mail system, such as Avaya Aura® Messaging or Avaya Modular Messaging. IP Office users in this deployment also have access to some Centralized Avaya Aura® applications and services.

  With the Distributed branch deployment option, you can also connect CS 1000 to IP Office in the branch through Avaya Aura® Session Manager. Users still obtain telephony services from the local IP Office, but can use Avaya CallPilot® as their voice mail system. When connected to CS 1000, IP Office and CS 1000 interoperate as peers through Avaya Aura® Session Manager.
- **Centralized enterprise branch deployment option**: All users in the enterprise are Centralized users.

  Centralized users register to Avaya Aura® Session Manager and obtain telephony services from the Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. If WAN connectivity to Avaya Aura® Session Manager is lost, the user automatically gets basic telephony services from the local IP Office. The telephony features provided by IP Office in survivability mode is limited compared to the features that are normally provided to the Centralized phone.

  Centralized users must be configured on the Avaya Aura® Session Manager, Communication Manager, and IP Office. A Centralized user must be configured on the Avaya Aura® Session Manager and Avaya Aura® Communication Manager as a SIP user. On IP Office, the Centralized user must have either a SIP extension, an analog extension, or an analog fax device.
- **Mixed enterprise branch deployment option**: An enterprise branch with both Centralized users and IP Office users. Centralized users and IP Office users obtain the same telephony

Página2472 de 3226.

services described above. All users in this deployment option must use a Centralized voice mail system: Avaya Aura® Messaging or Avaya Modular Messaging.

The deployment options in the Branch solution allow you to start off with stand-alone IP Office systems and then slowly evolve the solution architecture into a Centralized environment as your enterprise grows.

The following image shows the topology of the solution architecture with the deployment options described above. This image does not show CS 1000 in the Distributed branch deployment.

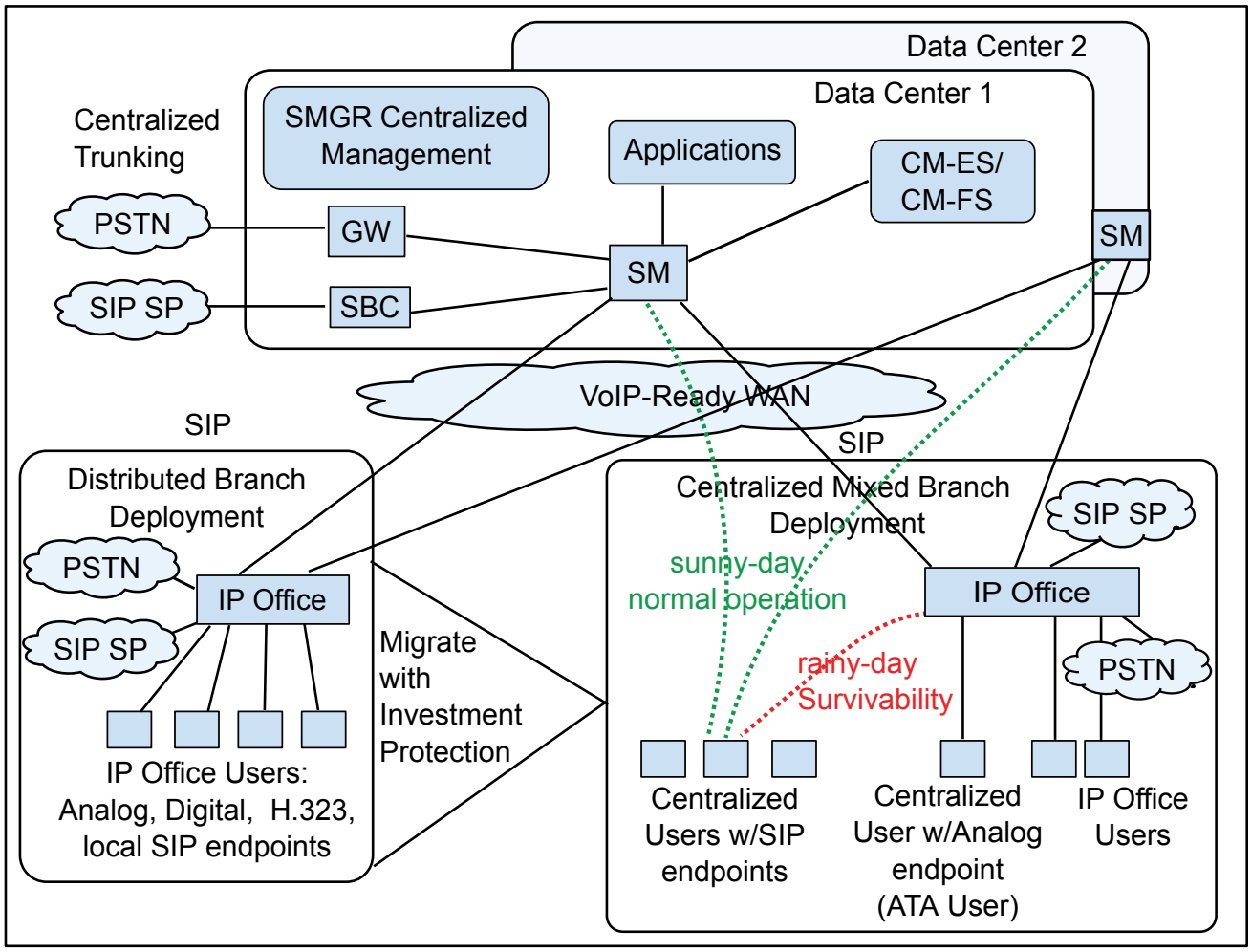


Figure 19: Topology of solution architecture

OnAvaya™ and Powered Cloud overview

Avaya offers the following Cloud solutions that enable BPs to sell core IP Office and IP Office Contact Center Telephony and Unified Communications (UC) features to users in small and medium enterprises:

- Powered, where you, as the Business Partner (BP), install and host the product instances in a Cloud data center at your site. IP Office Contact Center is optional with Powered.

Página2473 de 3226.

- OnAvaya™, where Avaya hosts the product instances in the Cloud data center. Two OnAvaya™ offers are available:
  - Customer Engagement offer, which includes both IP Office and IP Office Contact Center.
  - Team Engagement offer, in which IP Office Contact Center is optional.

Key benefits of the Cloud solution include the following:

- Reduction in operational costs for the enterprise by reducing the IT complexity of equipment maintenance.
- Reduction in service delivery costs for the BP through virtualization and shared infrastructure.
- Ability to upgrade software as new versions are released.
- Programmatic interface to support license installations, configure centralized licensing, or delete a license file.
- Automated billing with Avaya One Source Cloud Services.
- Flexibility to change your Avaya One Source Cloud Services order any time. You can add or remove users anytime. With Powered and the Team Engagement OnAvaya™ offer where IP Office Contact Center is optional, you can update your order to add or remove IP Office Contact Center as needed.
- Support for IP500 V2 expansion systems at the enterprise site with Hybrid Cloud.
- Support for resiliency with High Availability (HA).

OnAvaya™ topology

OnAvaya™ supports the Public Network deployment model. This deployment model uses a public over-the-internet connection between the Cloud data center and the enterprise premises. All users connecting over the Public Network are considered Remote Workers. The solution supports a one-to-one NAT, which translates IP addresses, but not TCP or UDP ports. The solution supports any kind of NAT at the enterprise site.

As a Partner, you need the SIP Broker Trunk Service to access SIP trunks. You can optionally integrate IP Office Contact Center with third-party CRM systems, such as Salesforce.

Important:

OnAvaya™ does not currently support Private Network deployments.

Página2474 de 3226.

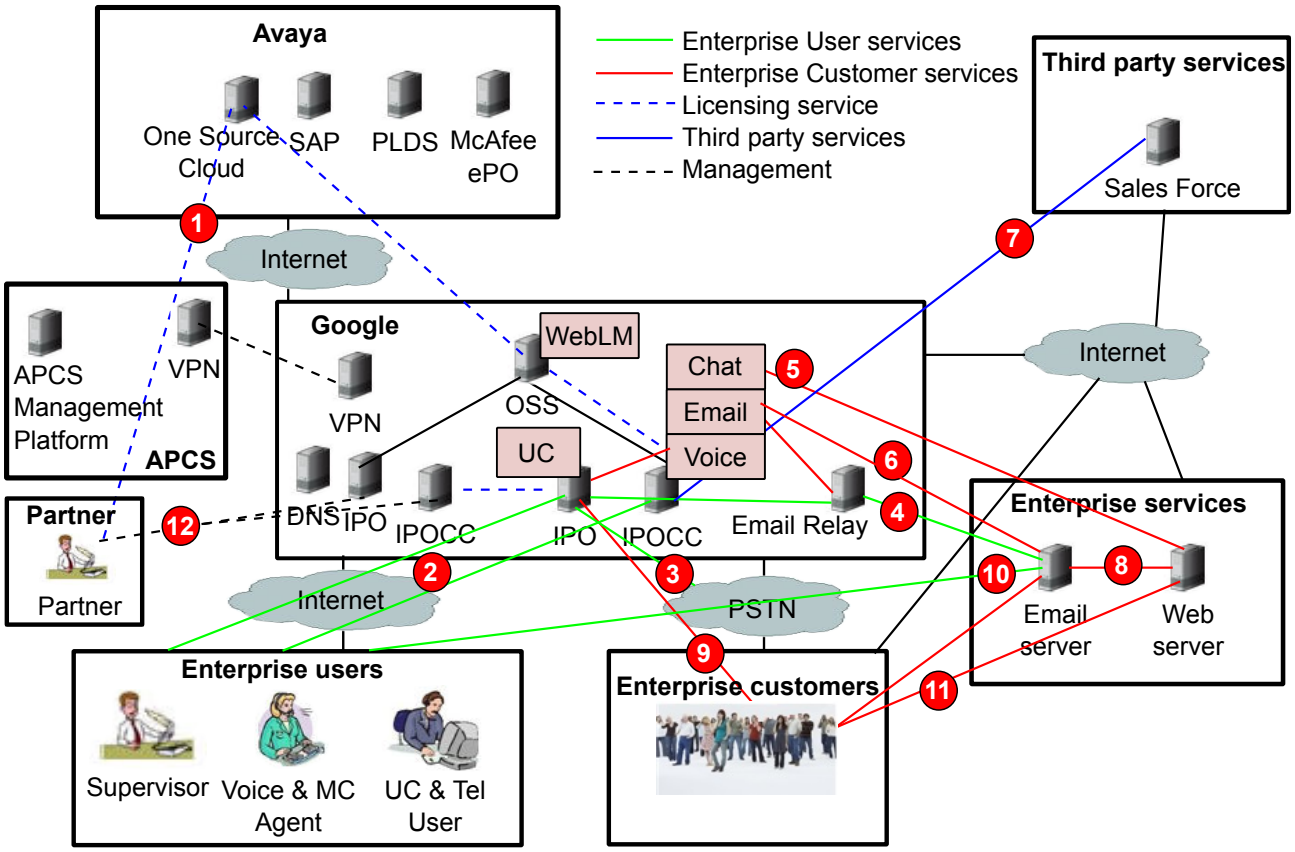


Figure 20: OnAvaya™

Powered topology

Powered supports the following deployment models:

- Public Network: This deployment model uses a public over-the-internet connection between the Cloud data center and the enterprise premises. All users connecting over the Public Network are considered Remote Workers.
- Private Network: This deployment model requires an MPLS or site-to-site VPN connection between the Cloud data center and the enterprise premises.

Página2475 de 3226.

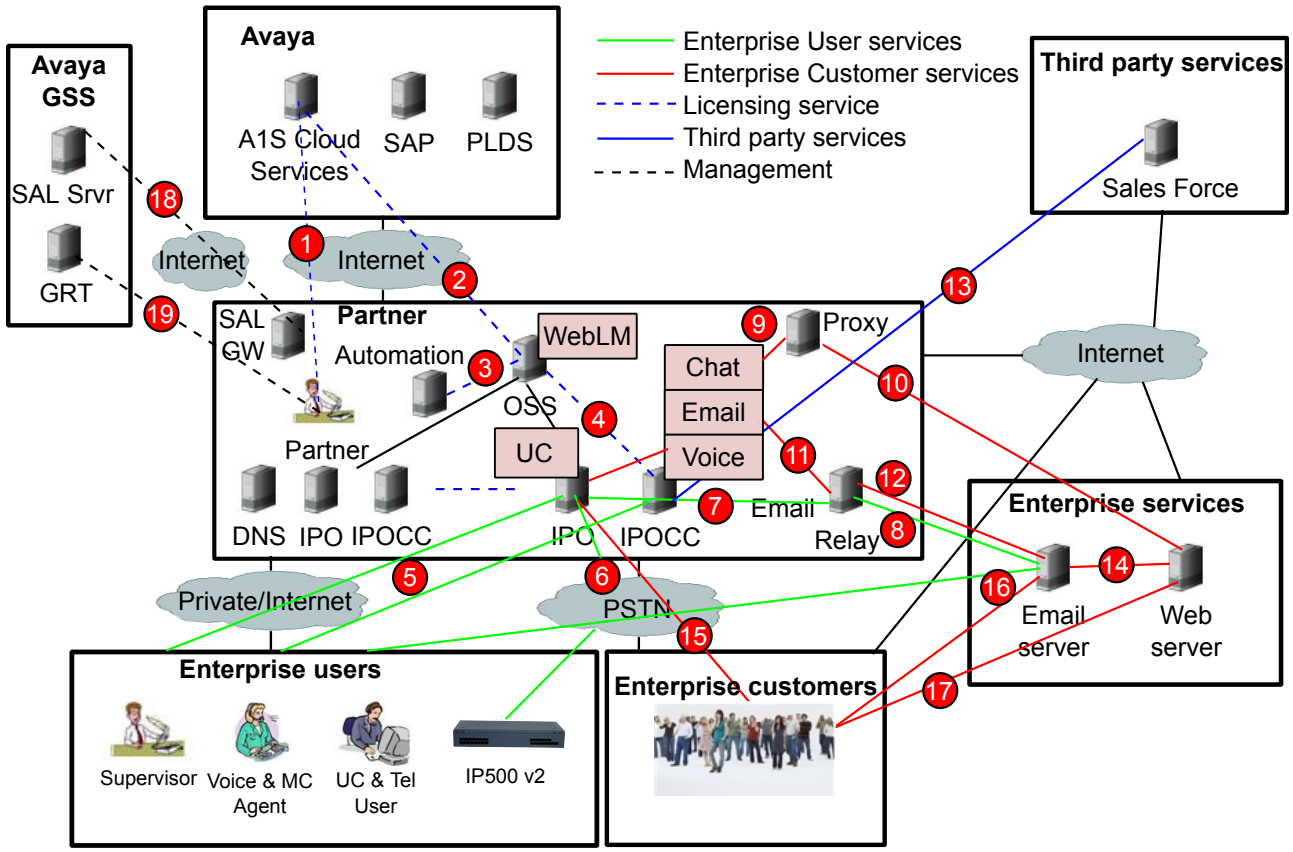


Figure 21: Powered topology

Contact center reference configurations

IP Office Contact Center deployment options

IP Office Contact Center can be deployed using the following deployment configurations and options:

Configuration	Deployment options	Agents and trunks
IP Office Contact Center with IP500V2	IP500V2, IP Office Contact Center server, and an application server	Up to 30 agents on SIP and digital trunks.
IP Office Contact Center with IP Office Server Edition	IP Office Server Edition server and IP Office Contact Center server *and/or* a Linux expansion server (optional) *or* Hosted as a service in a cloud environment	Up to 250 agents on SIP trunks. Only 125 agents can be deployed on each Linux expansion node.

Table continues…

Página2476 de 3226.

Configuration	Deployment options	Agents and trunks
IP Office Contact Center with IP Office Server Edition and IP500V2 expansion	IP Office Server Edition server, IP500V2 expansion server, and IP Office Contact Center server	Up to 250 agents on SIP and digital trunks. Only 30 agents can be deployed on each IP500V2 node.
IP Office Contact Center with IP Office Server Edition in a distributed environment	IP Office Server Edition server, IP500V2 expansion server, IP Office Contact Center server, and a Linux expansion in a distributed environment	Up to 250 agents on SIP and digital trunks. Up to 30 agents can be deployed on each IP500V2 node, and up to 125 agents can be deployed on each Linux expansion node. Agents and trunks are distributed on any expansion server.

Detailed IP Office Contact Center topologies are shown in the following documents:

- *Avaya IP Office Contact Center Feature Description*
- *Avaya IP Office Contact Center Reference Configuration*

Avaya Contact Center Select reference configurations

Avaya Contact Center Select is a feature-rich contact center solution that provides skill-based routing for customer voice and multimedia contacts. Avaya Contact Center Select provides extensive tools for agent management, real-time and historical reporting, and graphical tools to create contact flows and treatment rules. It provides license management, networking, and Open Interfaces Web Services. Customers integrating Avaya Contact Center Select with the IP Office platform gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility.

At deployment time, Avaya Contact Center Select automatically launches a simple configuration wizard to rapidly deploy a functional contact center solution. It is preloaded with sample users, skillsets, and contact center parameters. Use this sample data to rapidly commission the solution and make the first routed customer call and email contact.

Avaya Contact Center Select supports the following routed contact types:

- Voice
- Email
- Outbound
- Web communications (Web chat)
- SMS text messages
- Fax messages
- Scanned documents
- Voice mail messages
- Social Networking

Página2477 de 3226.

Avaya Contact Center Select also supports peer-to-peer Instant Messaging. To support the email-based contact types, you must add an email server to your solution. To support the Web communications contact type, you must add a Web communications server to your solution.

Avaya Contact Center Select provides a simplified voice prompt management utility. The contact center supervisor can perform prompt management work without requiring administrator access to the Avaya Contact Center Select server. Avaya Contact Center Select provides a number of status monitoring utilities to monitor the integration points with IP Office.

Contact Center Manager Administration is a browser-based configuration and reporting interface for Avaya Contact Center Select. Avaya Contact Center Select supervisors use Contact Center Manager Administration to configure contact center resources, agents, skillsets, contact flows, components, and activities. Contact Center Manager Administration provides historical and real-time reporting about the contact center.

User data synchronization

Avaya Contact Center Select provides unified administration for contact center agents and IP Office users. The users (agents and agent-supervisors) that you configure in Avaya Contact Center Select are automatically mirrored to the connected IP Office.

When you create an agent in Avaya Contact Center Select, a matching user account is created in IP Office. When you modify agent details in Avaya Contact Center Select, the corresponding IP Office user details are automatically updated. However, if you delete an agent in Avaya Contact Center Select, the corresponding IP Office user is not deleted. Synchronization works in one direction — from Avaya Contact Center Select to IP Office. The IP Office administrator can manually force data synchronization from Avaya Contact Center Select.

Topology

In a contact center solution using Avaya Contact Center Select and an IP Office telephone system, the following network and connectivity topology considerations apply:

- The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain.
- Each Avaya Contact Center Select connects to a single IP Office Server Edition Primary server. Alternatively, each Avaya Contact Center Select can connect to a single IP Office 500V2 Standard Mode with an Advanced Edition license.
- A Small Community Network (SCN) is a system of networked IP Office systems that can, among other features, share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select. Avaya Contact Center Select connects to the IP Office Server Edition Primary server of the SCN. To support an IP Office SCN, Avaya Contact Center Select must connect to an IP Office Server Edition Primary server in that SCN network.
- The Avaya Contact Center Select server and the connected IP Office telephone system must be located in the same campus location.
- Each supervisor client computer communicates with the Avaya Contact Center Select server. The supervisor uses the Contact Center Manager Administration Web interface to configure agents and run reports. The agent supervisor uses the Avaya Agent Desktop software to handle customer calls, to accept emergency or supervisor calls from agents and to observe calls or Web communication contacts. Each voice-enabled supervisor with Agent Desktop requires an associated IP Office telephone.

Página2478 de 3226.

- Each agent client computer communicates with the Avaya Contact Center Select server. The agent uses Agent Desktop to handle customer voice and multimedia contacts. Each voice-enabled agent requires an associated IP Office telephone.

Avaya Contact Center Select supports the following deployment options:

- Avaya Contact Center Select DVD
- Avaya Contact Center Select VMware
- Avaya Contact Center Select hardware appliance
- Avaya Contact Center Select Business Continuity

For more information about Avaya Contact Center Select deployment options, refer to *Avaya Contact Center Select Solution Description*.

Related links

Reference configurations on page 61
Avaya Contact Center Select DVD on page 75
Avaya Contact Center Select and VMware on page 76
Avaya Contact Center Select hardware appliance on page 77
Avaya Contact Center Select Business Continuity on page 78

Avaya Contact Center Select DVD

The Avaya Contact Center Select DVD contains the contact center application software. The DVD deployment option supports Platform Vendor Independence (PVI). PVI gives the customer the flexibility to purchase a server that meets the Avaya Contact Center Select server requirements and conforms to the customer's own corporate standards.

Avaya Contact Center Select supports a range of PVI server specifications, each specification supporting a specified maximum agent capacity and call rate. This range of PVI specifications gives the customer the flexibility to use the minimum hardware to meet their solutions requirements while allowing for future expansions.

The Avaya Contact Center Select DVD deployment option does not require VMware resources or infrastructure, which keeps Total Cost of Ownership (TCO) and solution complexity to the minimum.

Página2479 de 3226.

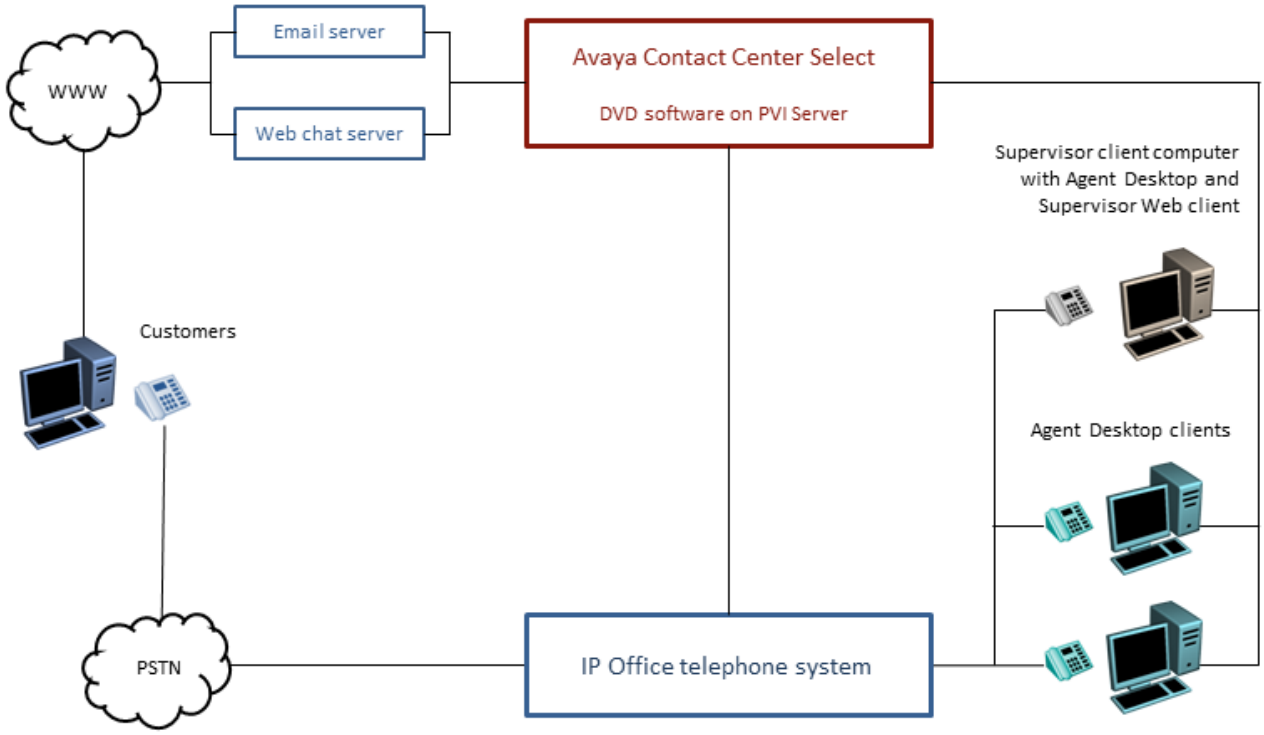


Figure 22: Typical Avaya Contact Center Select DVD deployment

To use the Avaya Contact Center Select DVD deployment option, the customer must provide the following:

- Server hardware that meets one of the Avaya Contact Center Select PVI specifications: Entry-level, Mid-range, or High-end.
- Microsoft Windows 2012 R2 Standard or Datacenter Edition operating system and license.

For more information about the Avaya Contact Center Select DVD option, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select and VMware

Avaya Contact Center Select supports VMware virtualization for increased productivity, flexibility and efficiency. All Avaya Contact Center Select deployment options support the virtualized IP Office Server Edition OVA on VMware.

Avaya Contact Center Select offers a software appliance package that consists of the following components:

- Avaya Contact Center Select virtual machine
- Avaya Aura® Media Server OVA
- Avaya WebLM OVA

Deploy these virtual machines and IP Office to build a virtualized and scalable contact center solution.

Página2480 de 3226.

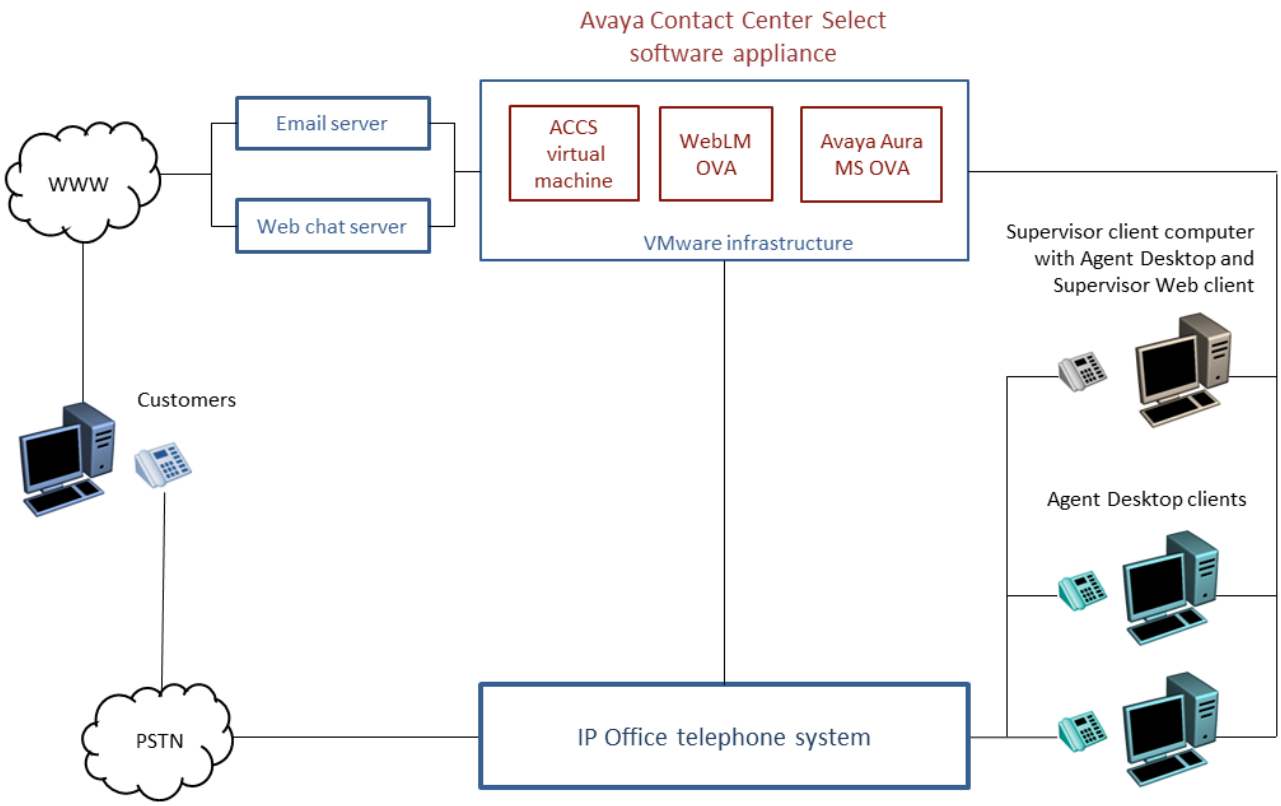


Figure 23: Typical Avaya Contact Center Select and VMware solution

Avaya Contact Center Select is a collection of applications providing real-time call control, multimedia handling, and statistical reporting. Deploy Avaya Contact Center Select on an enterprise-grade VMware virtual environment. Avaya recommends that you apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a virtualization infrastructure.

Avaya Contact Center Select supports VMware ESXi. VMware vCenter software is not required; however it is supported and it is useful for Avaya Contact Center Select in multi-host contact center environments.

For more information about Avaya Contact Center Select and VMware, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select hardware appliance

The Avaya Contact Center Select hardware appliance is a physical rack-mount server with the Avaya Contact Center Select application software already loaded and partially preconfigured. Avaya supplies the server hardware and a license for the Microsoft Windows 2012 R2 Standard Edition operating system.

The Avaya Contact Center Select hardware appliance server delivers speedy and simplified contact center deployment.

Página2481 de 3226.

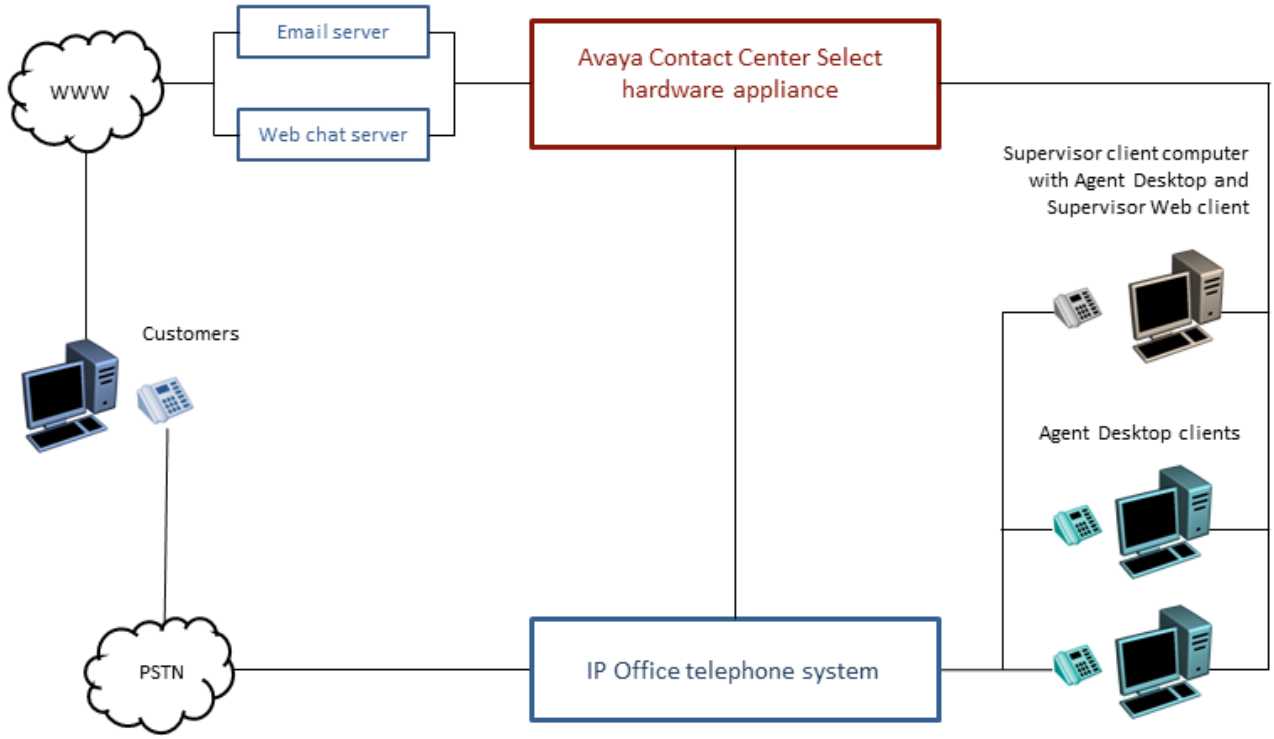


Figure 24: Typical Avaya Contact Center Select hardware appliance solution

After the basic telephony and email features are working, you can then configure more multimedia contacts, multiplicity, custom prompts, and other enhanced features and functions to improve your customer's experience.

The hardware appliance server supplied by Avaya is optimized to provide all of the real-time computational and logging resources required by Avaya Contact Center Select. The hardware appliance supports the Avaya Contact Center Select maximum agent and call rate capacity.

Avaya provides the Microsoft Windows operating system product key for the hardware appliance. The product key is displayed on a sticker attached to the top of the Avaya Contact Center Select hardware appliance server.

For more information about the Avaya Contact Center Select hardware appliance, refer to *Avaya Contact Center Select Solution Description*.

Avaya Contact Center Select Business Continuity

Business Continuity is an Avaya Contact Center Select licensed feature. Avaya Contact Center Select solutions that support Business Continuity have two Avaya Contact Center Select servers. One server, called the active server, processes customer contacts. The other server, called standby or Remote Geographic Node, shadows the active server. If the active server fails, the other Avaya Contact Center Select server can take over contact processing. This feature provides Avaya Contact Center Select redundancy, data resiliency, and disaster recovery.

To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and

Página2482 de 3226.

standby servers. Avaya Contact Center Select agents are also supported in domains with a two-way trust relationship with the Avaya Contact Center Select server domain.

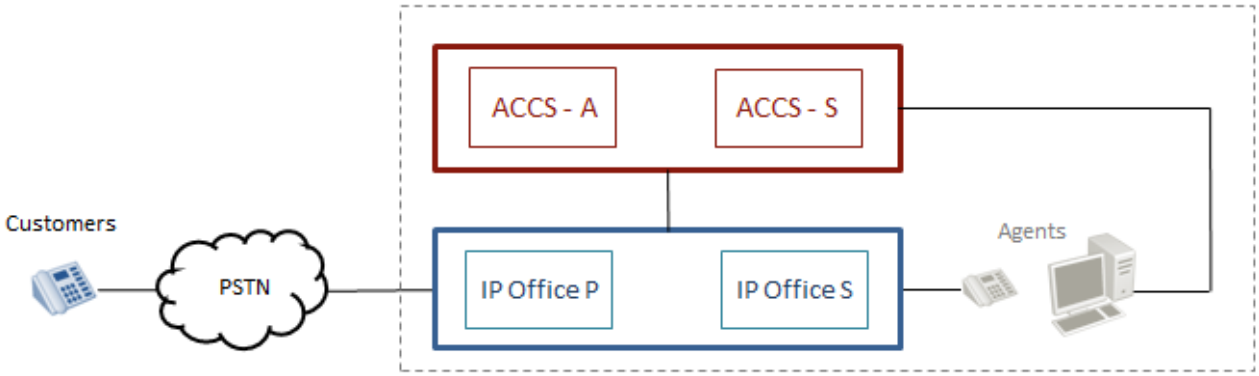


Figure 25: Avaya Contact Center Select Business Continuity with IP Office resilience

IP Office Server Edition solutions support voice platform resilience when an IP Office Secondary Server is added to the solution. Avaya Contact Center Select supports this IP Office resilience feature.

All Avaya Contact Center Select deployment options, DVD, VMware, and Hardware Appliance, support Contact Center Business Continuity and IP Office resilience. Avaya Contact Center Select Business Continuity adds additional resource requirements, topology, network connectivity, and domain layout considerations to the solution.

For more information, refer to *Avaya Contact Center Select Business Continuity*.

Hardware and software options

Hardware options

Server, base card, trunk card, and expansion module hardware options are available depending on the edition required:

- Dell PowerEdge™ R210 or R620
- Hewlett Packard ProLiant DL120 G7 or DL360 G7
- Avaya IP500 V2

Software options

IP Office acts as a server for a variety of applications, including:

- Avaya Communicator for IP Office supported on Windows and iPad devices
- Avaya one-X® Mobile for IP Office
- Avaya one-X® Portal for IP Office

Página2483 de 3226.

- Lync Integration for IP Office
- IP Office SoftConsole
- Contact Recorder for IP Office

IP Office can also be deployed with other components. You can deploy IP Office with Radvision or other video endpoints. You can also use IP Office Branch solution offer to connect IP Office branches to the Avaya Aura® infrastructure, allowing users to leverage core Avaya Aura® applications and services including centralized dial plans, voice mail, management, and licensing.

Related links

Accessing Avaya DevConnect Application Notes on page 129
Interoperability on page 88

Server specifications

The following tables list the minimum server specifications for the IP Office Server Edition Solution:

Server option	Large server #1	Large server #2	Large server #3
Chassis	Dell R630 1U	Dell R620 1U	HP DL360G7 1U
Processor	2 x E5-2620v3, 2.4 GHz	2 x E5-2630, 2.3 GHz	2 x E5620, 2.4 GHz
Memory (RAM)	32 GB	32 GB	12 GB
Hard disk drive	2 x 600 GB	2 x 600 GB	2x 300 GB, 10K
RAID	RAID 1 Hot swap	RAID 1 Hot swap	RAID 1 Hot swap
RAID Controller	H730	H710	P410i
Power Supplies	2x 750W AC Hot swap	2x 495W AC Hot swap	2x 460W AC Hot swap
NICS	6x GB full duplex	4x GB full duplex	4 Port, Motherboard
Optical Drive	1x DVD +/- RW	1x DVD +/- RW	1x DVD+/-RW, SATA, INTERNAL
PCI Type	2 x8 Gen2 Slots (PCIe)	2 x8 Gen2 Slots (PCIe)	1-LP X8 PCIe & 1-FL/FH X16 PCIe Riser

Server option	Small server #1	Small server #2	Small server #3
Chassis	HP DL120G7 1U	Dell R210 1U	Dell R220 1U
Processor	1 x E3-1220, 3.1 GHz	1 x E3-1220, 3.1 GHz	1 x E3-1220, 3.1 GHz
Memory (RAM)	12 GB	12 GB	16 GB
Hard disk drive	1x 250 GB, 7.5K	1x 250 GB, 7.5K	1x 500 GB, 7.2K
RAID	RAID 0 (none)	RAID 0 (none)	RAID 0 (none)
RAID Controller	P212, 256 MB	On board	On board
Power Supplies	1 x 400 W AC	1 x 502 W AC	1 x 250 W AC
NICS	2 Port, Motherboard	2 Port, Motherboard	2 Port, Motherboard

Table continues…

Página2484 de 3226.

Server option	Small server #1	Small server #2	Small server #3
Optical Drive	1x DVD+/-RW, SATA, INTERNAL	1x DVD+/-RW, SATA, INTERNAL	1x DVD+/-RW, SATA, INTERNAL
PCI Type	1-HL/LP X8 PCIe & 1-FL/FH X16 PCIe Riser	1 x16 Gen2 Slots (PCIe)	1 x16 Gen2 Slots (PCIe)

Note:

In some geographies, where 12 GB of RAM is not a standard Dell option use 16 GB RAM.

Server Combinations and Usage

- The Server Edition Primary and Server Edition Secondary must be on the same platform. This constraint applies equally to virtual servers. It is possible to mix native and virtual central servers, but the resources allocated to the virtual environment should match the native server.
- Virtualised and native servers can be mixed in the same Server Edition solution in any role, provided the Server Edition Primary and Server Edition Secondary are the same as indicated above.
- It is possible to use the Unified Communication / Application Server R210 / DL120 is / R220 servers as this is the same hardware and software as the Server Edition R210 / DL120 / R220 servers. If the server is installed with theServer Edition software, it will be supported by Avaya.
- You cannot set up a Server Edition Expansion System(L) in the Standard IP Office mode of operation in the IP Office Server Edition Solution.
- You cannot re-provision a Server Edition server without a complete reinstall. For example, you cannot convert a primary server to a secondary or expansion system.
- You cannot set up a Server Edition Expansion System (L) in the Standard IP Office mode of operation in the IP Office Server Edition Solution. You cannot convert a Server Edition Expansion System (V2) to a Server Edition Primary or Server Edition Secondary server.
- The use of any external Voicemail Pro server (either Linux or Windows) is not supported.
- The use of an external Avaya one-X® Portal server not running Server Edition software, and not running on a supported server, is not supported.

  Note:

  Salesforce (SFDC) has been removed from Avaya one-X® Portal.

Operating system and browser support

Windows Operating System

Table 7: Windows Editions and Service Packs

Operating System*	Service Pack	Edition
Windows 7	SP1	Professional, Enterprise, Ultimate
Windows 8.1	N/A	Professional, Enterprise

Table continues…

Página2485 de 3226.

Operating System*	Service Pack	Edition
Windows 10	N/A	Professional (SMB), Enterprise
Windows Server 2012	N/A	Standard
Windows Server 2012 R2	N/A	Standard
Windows Server 2016	N/A	Standard, Essentials

* Windows Server 2008 R2 (64-bit) is not supported from Release 10.1.

Table 8: Windows Support – Server Components

Server	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
Preferred Edition server (Voicemail Pro) Standalone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Preferred Edition server with UMS	No	No	No	No	No	No	Yes	Yes
Preferred Edition server with Campaigns	No	No	No	No	No	No	Yes	Yes
Preferred Edition server with IMS	No	No	No	No	No	No	No	No
Preferred Edition server with MAPI service for Voicemail Pro on Linux	Yes	Yes	No	No	No	No	Yes	Yes
Avaya one-X® Portal for IP Office server	No	No	No	No	No	No	Yes	Yes
TAPI first-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI third-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI WAV[2]	Yes	No	Yes	No	Yes	No	No	No

* Windows 8.1 is the replacement/Service Pack for Windows 8.0. Therefore, we no longer support Windows 8.0.

[2] TAPI WAV is not recommended for new designs and is not supported on a 64-bit OS.

Página2486 de 3226.

Table 9: Windows Support – Thick Client Apps

Application	Windows 7		Windows 8.1*		Windows 10		Windows Server 2012, 2012 R2	Windows Server 2016
	32-bit	64-bit	32-bit	64-bit	32-bit	64-bit	64-bit	64-bit
Preferred Edition client	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Office SoftConsole	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
IP Office Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SysMonitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System Status Application	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI first-party	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TAPI WAV[3]	Yes	No	Yes	No	Yes	No	No	No
Video Softphone [4]	Yes	Yes	No	No	No	No	No	No
Avaya Communicator for Windows	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Avaya one-X® Portal plug-in for Microsoft Outlook	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Call Assistant	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Plug-in for Microsoft Lync 2013/Skype for Business[5]	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Web Conferencing [6]	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Avaya Equinox™ Select for IP Office	Yes	Yes	Yes	Yes	Yes	Yes	No	No

* Windows 8.1 is the replacement/service pack for Windows 8.0. Therefore, we no longer support Windows 8.0.

[3] TAPI WAV is not recommended for new designs and is not supported on a 64-bit OS.
[4] Legacy support only.
[5] Plug-in for Microsoft Lync 2010 is not supported from Release 10.1.
[6] Includes Adobe Flash and Java Applet for sharing.

Página2487 de 3226.

macOS Operating System

Table 10: macOS Support – Thick Client Apps

Application	macOS 10.8 (Mountain Lion)	macOS 10.9 (Mavericks)	macOS 10.10 (Yosemite)	macOS 10.11 (El Capitan)	macOS 10.12 (Sierra)
Video Softphone version 4.0	Yes	Yes	No	No	No
Web Conferencing[7]	Yes	Yes	Yes	Yes	Yes

Browsers

Table 11: Supported Browsers

Application	Internet Explorer 10*	Internet Explorer 11	Edge	Firefox	Chrome	Safari 8, 9, 10
Voicemail Pro Campaigns	Yes	Yes	Yes	No	No	No
Voicemail Pro UMS WebMail	Yes	Yes	Yes	No	No	No
Avaya Contact Recorder client	Yes	Yes	No	No	No	No
Avaya one-X® Portal for IP Office client	Yes	Yes	Yes	Yes	Yes	Yes
Web Conferencing[8]	Yes	Yes	Yes	Yes	Yes	Yes
Web Manager and Web Control Page	Yes	Yes	Yes	Yes	Yes	Yes
D100 DECT Admin	Yes	Yes	Yes	Yes	Yes	Yes
IP DECT R4 Admin	Yes	Yes	Yes	Yes	Yes	Yes
Avaya Communicator for Web	No	Yes	No	No	Yes	No
Avaya Communicator for Windows	No	No	No	No	Yes	No
IP Office Integrated Contact Reporter	Yes	Yes	Yes	Yes	Yes	Yes
IP Office Media Manager	Yes	Yes	Yes	Yes	Yes	No

* Only on Windows Server 2012; however, Server 2012 R2 supports Internet Explorer 11.

[7] Includes Adobe Flash and Java Applet for sharing.
[8] Includes Adobe Flash and Java Applet for sharing.

Página2488 de 3226.

Other Apps

Table 12: Microsoft Exchange

Application	Exchange 2010	Exchange 2013	Exchange 2016
Voicemail Pro UMS	Yes	Yes	Yes
Avaya one-X® Portal for IM and Presence	Yes	Yes	Yes

Table 13: Microsoft Outlook

Application	Outlook 2010	Outlook 2013	Outlook 2016
Voicemail Pro IMS	No	No	No
TAPI (for dialing)	Yes	Yes	Yes
Voicemail Pro UMS with IMAP	Yes	Yes	Yes
Avaya one-X® Portal Outlook Plug-in[9]	Yes	Yes	Yes

Virtualization

Table 14: Virtualization support

Hypervisor	IP Office Server Edition	IP Office Partner-Hosted
VMware ESXi 5.1	Yes	Yes
VMware ESXi 5.5 U2+	Yes	Yes
VMware ESXi 6.0	Yes	Yes
VMware ESXi 6.5	Yes	Yes
Microsoft HyperV on Server 2012 R2	Yes	Yes
Microsoft HyperV on Server 2016	Yes	Yes
KVM	No	Yes
Amazon AWS	No	Yes

Customer-provided PC requirements

The following customer-provided PC requirements for applications are the minimum required.

IP Office Manager

IP Office Manager is used to access all parts of the configuration. Different levels of access can be defined to control which parts of the configuration the IP Office Manager user can view and alter. IP Office Manager is also used to upgrade the software files on the system. IP Office Manager acts as a TFTP server from which some Avaya telephones can request new software.

[9] For Outlook 2013 and later, the contact screen popping feature is not supported.

Página2489 de 3226.

RAM	Standard Edition: 4 GB Server Edition: 6 GB Select Server Edition: 8 GB
Hard disk free space	1 GB
Processor	Standard Edition: Core i3 Server Edition: Core i5 Select Server Edition: Core i5
Operating system	Operating system and browser support on page 83
Additional software	.NET Framework 4.0: Installed with the software if not already installed.

IP Office SysMonitor

RAM	128 MB
Hard disk free space	10 GB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 83

IP Office System Status Application

RAM	256 MB
Hard disk free space	1.4 GB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 83
Additional software	Sun Java Virtual Machine Web Browser: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

TAPI

RAM	64 MB

Página2490 de 3226.

Hard disk free space	50 MB
Processor	Pentium: PIII 800 MHz Celeron: Celeron 3 800 MHz AMD: Athlon B 650 MHz
Operating system	Operating system and browser support on page 83
Additional software	Web Browser: Microsoft Internet Explorer 7+, Mozilla Firefox 3.0

Virtual environment requirements

Ensure you have the following:

- VMware vSphere client software for management (vSphere ESXi software and virtualized instances running on a single host server)

  Note:

  vCenter software is not required, however might be useful for multi-host server environments.

- Host hardware supporting VMware vSphere and IP Office Server Edition resource requirements and specifications to meet configuration needs.

VMWare ESXi support:

- IP Office Server Edition and IP Office Contact Center support VMWare ESXi 5.1 and 5.5 U2.
- IP Office Contact Center supports VMWare ESXi 6.0. IP Office Server Edition supports VMWare ESXi 6.0 for only versions 10.0 and later.

  For more information about IP Office Contact Center support and specifications, see *Avaya IP Office Contact Center Reference Configuration*.

Note:

ESXi 4.x is no longer supported.

Additional hypervisor support:

Hypervisor support is now extended to:

- Microsoft Hyper-V
- AWS (for Amazon Web Services): An AMI (Amazon Machine Image) is provided that can perform Auto Ignition and ICU based on User Data set in AWS. The AMI will behave similar to the existing Google Compute Image. Consult the instance types that Amazon EC2 supports on the Amazon AWS website.

  In Amazon Dashboard, you need to select Launch Instance under Create Instance. Select Community AMIs and search for Avaya IP Office.

- KVM (for Kernel-based Virtual Machine)

Página2491 de 3226.

Interoperability

Interoperability means that two systems can communicate with an interface in each system to handle the communication. Compatibility means that two components in the same environment are compatible with each other if they run or reside in the environment without adversely affecting the behavior of the other.

For detailed information about IP Office interoperability and supported releases, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=IP+Office+Platform.

Avaya product interfaces

IP Office includes an interface to the following Avaya products:

- Avaya Aura®
- Avaya Contact Center Select
- Avaya Aura® Messaging
- Avaya CallPilot®
- Avaya Cloud Video Phase
- Avaya Communicator for Windows
- Avaya Communicator for iOS
- Avaya one-X® Communicator
- Avaya Session Border Controller for Enterprise
- Avaya Business Communications Manager
- Avaya Communication Server 1000
- Avaya Modular Messaging
- Avaya Scopia®
- Secure Access Link
- Avaya Aura® Experience Portal

ISDN interfaces

EU interfaces:

- BRI: RJ45 sockets. ETSI T-Bus and S-Bus interfaces to CTR3 for Pan European connection
- PRI E1: RJ45 socket. ETSI T-Bus interface to CTR4 for Pan European connection
- PRI T1/J1: RJ45 socket: FCC Part 68/JATE connection

USA interfaces:

- PRI T1 service: Ground Start (GS) - Default, E&M, 56 K data for 5ESS, 56/64/64 restricted for 4ESS
- PRI ISDN switch support: 4ESS, 5ESS, DMS-100, DMS-250 (includes conformance to ANSI T1.607 and Bellcore Special Report SR4287, 1992)
- PRI ISDN Services: AT&T Megacom 800, AT&T WATS (4ESS), AT&T SDS Accunet 56 Kbps and 64 Kbps (4ESS), AT&T Multiquest (4ESS)

Página2492 de 3226.

Related links

Phone interoperability on page 89
IP Office and Avaya Aura Communication Manager interoperability on page 93
BCM and IP Office interoperability on page 94
Accessing Avaya DevConnect Application Notes on page 129
Product compatibility on page 128
Hardware and software options on page 79

Phone interoperability

The following table summarizes the phone interoperability comparison by IP Office edition.

Table 15: Generally available phones

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
Analog deskphones:			
POTS	Yes	Yes	No
1000 Series Video phones:			
1010, 1020, 1030, 1040 (Lifesize)	No	Yes	No
1400 Series : DS Digital phones – IP Office and Communication Manager			
1403, 1408, 1416	Yes	Yes	No
DBM32	Yes	Yes	No
1600 Series : IP (H.323) phones – IP Office and Communication Manager			
1603, 1603SW, 1603SW–i, 1608, 1608–i, 1616, 1616–I	No	Yes	Yes
2400 Series: DS Digital phones – IP Office and Communication Manager			
2402D, 2410D, 2420	Yes	Yes	No
EU24	Yes	Yes	No
3600 Series: WiFi H.323 – IP Office and Communication Manager			
3641, 3645	No	Yes	Yes
3700 Series: DECT – IP Office and Communication Manager			
3720, 3525, 3730, 3735, 3745, 3749	No	Yes	Yes
3900 Series: ETR DECT Cordless			
3920	Yes	No	No
9500 Series: DS digital – IP Office only			

Table continues…

Página2493 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
9504, 9508	Yes	Yes	No
BM12	Yes	Yes	No
9600 Series: IP H.323 – IP Office and Communication Manager			
9620L, 9620C, 9630, 9640G, 9650, 9650C	No	Yes	Yes
SBM24 with 96x0	No	Yes	Yes
9608, 9611, 9621, 9641	No	Yes	Yes
BM12	No	Yes	Yes
B100 Series Conference Phones:			
B149, B159	Yes	Yes	No
B179 SIP	No	Yes	Yes
D100/D160 DECT Phones:			
D160	Yes	Yes	Yes
E100 Series IP Phones:			
E129	No	Yes	Yes
E159	No	Yes	Yes
E169	No	Yes	Yes
H100 Series Video Collaboration Stations:			
H175	No	Yes	Yes
Softphone:			
IP Office Video Softphone Mac (SIP)	No	Yes	Yes
Avaya Communicator Windows	No	Yes	Yes
Avaya Communicator iPad	No	Yes	Yes

Table 16: Generally available NORSTAR/BCM phones

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
1100 Series SIP phones: BCM Unistim migration			
1120E, 1140E	No	Yes	Yes
BM LED and paper labels	No	Yes	Yes
BM LCD	No	Yes	Yes

Table continues…

Página2494 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
1200 Series SIP phones: BCM Unistim migration			
1220, 1230	No	Yes	Yes
BCM paper	No	Yes	Yes
BCM LCD	No	Yes	Yes
NORSTAR/BCM Digital phones:			
T7000, T7100, T7208, T7316, T7316E	Yes	Yes	No
T24 Key Module	Yes	Yes	No
M7100(N), M7208(N), M7310(N), M7310BLF, M7324(N)[10]	Yes	Yes	No
CAP Key Module	Yes	Yes	No
NORSTAR/BCM Digital Conference Phone	Yes	Yes	No
Nortel Digital Mobility phones:			
T7406, T7406E	Yes	Yes	No
7420, 7430, 7434, 7439, 7440, 7449	Yes	Yes	No
4135, 4136, 4145, 4146, 4145EX, 4146EX	Yes	Yes	No

Avaya has tested the following phones for interoperability with IP Office. These phones may not support all features. If the phone is past its Avaya Manufacturer Support Period, issue resolution is limited to those already fixed.

Table 17: Supported Avaya phones no longer for sale

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
3700 Series DECT phones: IP Office and Communication Manager			
3701, 3711	No	Yes	Yes
3800 Series Digital Cordless phones:			
3810	No	Yes	No
3900 Series ETR DECT Cordless phones:			
3910	Yes	No	No

Table continues…

[10] Only the global version of the M7000 Series phones are supported. The non-global versions are not supported and can be identified by the contrast levels; the global version has 9 contrast levels and the non-global version has only 4 contrast levels.

Página2495 de 3226.

Phone	Basic Edition	Essential and Preferred Editions	Server Edition Select Server Edition Virtualized
4400 Series phones: Digital, Magix and IP Office			
4408D, 4412D, 4424D	No	Yes	No
4450 DSS unit	No	Yes	No
4600 Series IP H.323 phones: IP Office and Communication Manager			
4601, 4602IP, 4602SW, 4610IP, 4610SW, 4620, 4621, 4625	No	Yes	Yes
5400 Series DS Digital phones: IP Office only			
5402, 5410, 5420	No	Yes	No
EU24	No	Yes	No
5600 Series IP H.323 phones: IP Office only			
5601, 5602IP, 5602SW, 5610IP, 5610SW, 5620, 5621	No	Yes	Yes
EU24	No	Yes	Yes
ETR phones: Analog Feature Phone, PARTNER and IP Office			
“Refreshed” 34, 18 and 6 button display	Yes	No	No
“Euro” 34 and 18 button display	Yes	No	No
“Euro” 18 and 6 button display	Yes	No	No
T3 and T3 IP Series phones:			
T3 Compact, Classic, Comfort, DSS	No	Yes	No
T3 IP Compact, Classic, Comfort	Yes	No	Yes

Related links

Interoperability on page 88
Phone availability on page 92
Accessing Avaya DevConnect Application Notes on page 129
Using the Avaya InSite Knowledge Base on page 129
Phones on page 36

Phone availability

Phones available worldwide

The Avaya phones listed below are the recommended phones for use with IP Office. These phones are sold worldwide in every country where IP Office is available.

For detailed specifications, see specific phone information on the Avaya Support site at http://support.avaya.com.

Página2496 de 3226.

Digital phone models	IP phone models
1403	1603
1408	1608
1416	1616
9504	9608
9508	9611
	9621
	9641

Phones only available in certain countries

In addition to the phones listed above, the following Avaya phones are available in certain countries and regions.

Digital/Analog phone models	IP phones
2402	9620L/9620C
2410	9630G/9640/9640G
2420	9650/9650C
3810 Wireless	3720 DECT R4 Wireless Handset
EU24/EU24BL DSS Unit	3725 DECT R4 Wireless Handset
	3730 DECT R4 Wireless Handset
	3735 DECT R4 Wireless Handset
	3745 DECT R4 Wireless Handset
	3749 DECT R4 Wireless Handset
	3641 Wireless (WiFi) phone
	3645 Ruggedized Wireless (WiFi) phone
	D100

Related links

Phone interoperability on page 89

IP Office and Avaya Aura® Communication Manager interoperability

IP Office uses H.323 protocol for trunks between the nodes and the Avaya Aura® Communication Manager. Centralized voicemail for all IP Office systems in the SCN network and all phones are supported on the individual call servers. Advanced call handling features are available between the IP Office nodes. This interface works on Essential and Preferred Editions.

Supported phones include:

- Avaya IP phones (H.323)

Página2497 de 3226.

- Avaya digital phones
- BCM 7000 series digital phones
- BCM 1100/1200 series IP phones (SIP)
- DECT R4 phones
- Analog phones

These features allow for simple networking needs between IP Office remote branches to an Avaya Aura® Communication Manager at the main site.

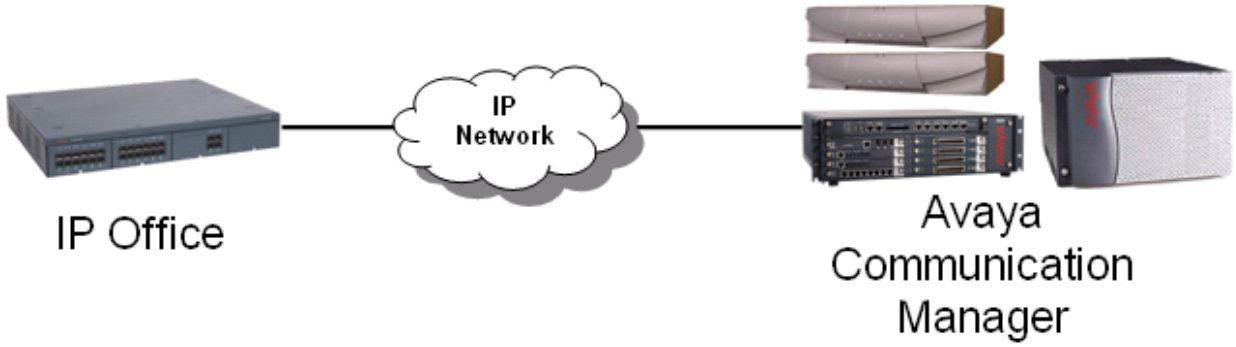


Figure 26: VoIP networking using H.323

Q.SIG provides the following supplementary services which are also available between IP Office and Avaya Aura® Communication Manager equipped with the relevant RFA licenses:

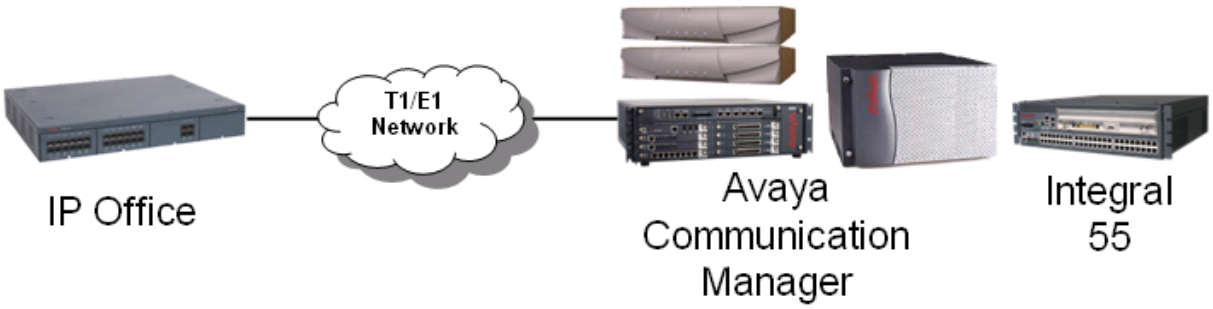


Figure 27: Q.SIG networking using T1/E1 links (TDM)

Related links

Interoperability on page 88

BCM and IP Office interoperability

The SIP interoperability support between IP Office and BCM50/450 allows customers to migrate a network of BCM, step-by-step, to an IP Office SCN or Server Edition network.

Protocol support	IP Office to BCM: SIP
	BCM to BCM: SIP or SIP/MCDN

Página2498 de 3226.

	IP Office to IP Office H.323: SCN or SIP **Note:** It is not possible to connect IP Office and BCM through the MCDN or SCN protocol directly.
IP Office platform requirements	Release 8.1 or higher, Essential, Preferred or Server Editions
BCM platform requirements	BCM50 or BCM450 6.0
Centralized voicemail	IP Office with a centralized Voicemail Pro system in the SCN network BCM with a centralized voicemail within the BCM MCDN network. **Note:** Centralized Voicemail across IP Office and BCM systems is not supported.
Phones	All phones supported on the individual call servers and releases including Avaya IP Phone (H.323), Avaya Digital phones, BCM 7000 Series Digital phones, BCM1100/1200 Series IP Phones (SIP), DECT R4 and Analog phones.
Features	Advanced feature set of IP Office SCN available between the IP Office and BCM. MCDN features are also available between the IP Office and BCM. The standard SIP features are supported.

Related links

Interoperability on page 88

Security specification

The Avaya Product Security Support Team (PSST) responds to ongoing security vulnerabilities for all Avaya Products. For more information, see *Avaya Product Security Vulnerability Response Policy* and *Avaya Security Vulnerability Classification* at the Avaya Support website at https://support.avaya.com/security.

Default security

The IP Office software security engine is supplied by Mocana Corporation. For more information, see https://www.mocana.com.

Security features are built-in into the software platform. These features consist of:

- Integrated firewall to prevent Denial of Service (DoS) attacks

Página2499 de 3226.

- Secure connections to ensure the privacy and integrity of transmitted information including:
  - TSL on administration interfaces
  - HTTPS client
  - HTTPS server
  - IPSec
  - SIP-TLS
  - SSL/VPN
  - VMPro/Exchange MAPI integration (TLS)

For detailed information about SSL/VPN remote access, see *Deploying Avaya IP Office™ Platform SSL VPN Services* and *Avaya IP Office™ Platform Port Matrix* at the Avaya Support website.

Configurable security

Configurable security settings include the following features:

- Encryption and message authentication
- Configuring integrated firewall settings
- Digital certificates
- Prevention of tool fraud by restricting user privileges and using security policy configuration to manage account credentials and access control

See *Avaya IP Office™ Platform Security Guidelines* for more information.

Network security

Network security leverages resources such as VLANs and firewalls available on the enterprise network and includes:

- External firewall configuration
- Separate of network functionality by creating separate VLAN groups and security zones
- Hardening of Layer 2 (data link layer) and Layer 3 (Network layer) by configuring SNMP trap destinations, syslog entries, and an IPSec VPN.
- SSL/VPN remote access

Operational security

Ongoing operational security to maintain a secure system includes:

- Patching
- Logging and monitoring
- Virus protection

Related links

Platform and application security details on page 97

Página2500 de 3226.

Platform and application security details

For additional information on security, see *Avaya IP Office™ Platform Security Guidelines*

Platform

- The IP Office for Linux operating system is based on Red Hat Enterprise Linux that is further hardened for defaults, packages, and users.
- The operating system of Server Edition Expansion System (L) is developed for IP Office. The operating system is simple, stable, and reliable.
- The operating system of Server Edition Expansion System (V2) is developed for IP Office. The operating system is simple, stable, and reliable.
- Components that are secure:
  - Software security engine for all the components.
  - Hardware security engine for Office Server Edition Expansion System (V2).
  - Internal Access Control Engine polices for external service requests and internal applications.

Manager

- Transport Layer Security (TLS) secures the communications between IP Office Manager and IP Office and insecure ciphers are disabled.
- Provides Role based user access control (RBAC).
- Provides comprehensive user account and password controls.
- You can enable a PKI Trust domain.
- The system generates warnings messages if administrative passwords are set to default. The system sends alarms or login failure.
- The system records all the accesses in the audit trail.
- You can disable unused services and ports such as HTTP.

Administration user accounts

The administration user accounts can be controlled for:

- Password complexity
- Previous password history (administrative accounts only)
- Change password on next login
- Idle lockout and login failure lockout
- Time and date the account expires (administrative accounts only)

Single sign-on (SSO)

- Administration credentials to log in to Linux Platform settings are securely transferred to Manager, SSA,Voicemail Pro client.
- All administrative logins on all IP Office components including Voicemail Pro and Avaya one-X® Portal for IP Office use security settings of IP Office.

Página2501 de 3226.

- Server user management feature in Web Manager synchronizes administrative user credentials with all components of IP Office including Voicemail Pro and Avaya one-X® Portal for IP Office in IP Office Server Edition Solution.

Audit trail

- Each IP Office system maintains an audit trail of access and configuration change.
- Linux Platform settings also maintains an audit trail.
- The IP Office system displays the audit trail in IP Office Server Edition Manager and SSA.
-

Public Key Infrastructure (PKI)

- IP Office supports X.509 certificates
- The Server Edition Primary and the Application server support an integrated Certificate Authority (CA)
- The Trusted Certificate Store can be configured and Identity certificate is available.
- The system performs a Certificate Signing Request (CSR) through Simple Certificate Enrollment Protocol (SCEP).
- The system creates a self-signed Identity certificate that can be copied to all HTTPS/TLS interfaces.
- Flexible controls to enforce Trust domain on specific services. Extended trust controls for PKI .
- Web Management Console,Voicemail Pro and Avaya one-X® Portal for IP Office on Linux support X.509 certificates, but not PKI.

LAN

- The servers and expansion systems are thoroughly tested for resistance to Denial of Service and other attacks
- Server Edition Expansion System (V2) supports a configure able Firewall
- Time profiles on Server Edition Expansion System (V2) only
- Static NAT and NAPT in Server Edition Expansion System (V2)
- ICMP Filtering
- L2TP/PPP VPN on Server Edition Expansion System (V2) only
- PAP or CHAP password exchange
- Idle or quota timeout
- IPSec VPN on Server Edition Expansion System (V2) only

Endpoints

- Username and PIN or password or login code are in the IP Office configuration, and you can administer these through IP Office Server Edition Manager
- You can use HTTP or HTTPS for settings and firmware upgrades
- You cannot make calls unless you are logged in

Página2502 de 3226.

Call barring

- You can configure flexible call barring controls using login name or account code to allow internal, local, national or international calls on the basis of every user and system.
- You cannot use speed dials, transfers, forwarding, and conferences to bypass controls.
- You can enable trunk to trunk calls using IP Office Server Edition Manager. Trunk to trunk calls are disabled by default.
- SIP trunk configuration for incoming calls must match URIs..
- You can use SMDR (CDR) to create a record of all calls.

Voicemail Pro client

- You can enforce user login with Personal Identification Number (PIN) and configure complexity for the PIN.
- You can enforce PIN change when the user logs in for the first time.
- Idle timeout.

Related links

Security specification on page 95

Port assignments

Details of the range of ports used by IP Office and IP Office applications are found at https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003.

Most PC firewalls requests the user to allow various exceptions when a newly installed application first runs. However this is not always the case, especially if the firewall is located elsewhere than the user's PC. The file `avayafw.bat` can be used to open up the necessary firewall exceptions for IP Office applications. The file can be downloaded from http://marketingtools.avaya.com/knowledgebase/tools/firewall.

DTE port	9 way D-type D-Type female connector: V.24/V.28
Analog trunk ports	RJ45 sockets: Loop Start/Ground Start (regionally dependant)
Power fail ports	RJ45 sockets: 2x sockets for ATM16 and 1x sockets for ATM4
ISDN data rates	BRI: B-channel 64 Kbps or 56 Kbps, D-channel 16 Kbps
Analog phone ports	• RJ45 sockets • REN: 2. (External Bell via POT port: REN = 1) • Off Hook Current: 25 mA. • Ring Voltage: 40 V (nominal) RMS.
LAN	RJ45 sockets. Auto-negotiating 10/100 BaseT Ethernet (10/100 Mbps)

Página2503 de 3226.

Audio	• 3.5 mm stereo jack socket. Input impedance 10 K/channel. • Maximum AC signal - 200 mV rms.
External output port	• 3.5 mm stereo jack socket. Switching capacity 0.7 A. • Maximum Voltage - 55V DC. On state resistance 0.7. • Short circuit current 1 A. Reverse circuit current capacity 1.4 A.
Embedded voice memory	IP500V2: 512 MB compact flash memory (SD) card for voicemail

Typical upgrade paths

Upgrading IP500 V2 platforms

Customers can migrate to the latest release by purchasing an upgrade license or under the terms of their IP Office Support Services support contract, as applicable. Customers migrating to the latest release will be required to have an IP500 V2 control unit or supported servers with Server Edition. IP500 base cards, trunk cards and expansion modules are supported with IP500 V2 control unit and may migrate to the V2 control unit. Licenses will require a dongle swap to move from the IP500 key card to the IP500 V2 SD card.

For systems using the IP500 V2 with any software release prior to 8.1.1.0, a two-stage upgrade process is required to cope with the increased size of the 9.1 binary file. Upgrade to 8.1.1.0 or any 9.0 version before attempting the upgrade to 9.1.

Ensure that the systems do not contain unsupported hardware. Upgrade them if necessary prior to upgrading the software. Install upgrade licenses prior to the upgrade.

Use the Manager Upgrade Wizard to display the software currently present on the SD card and the new versions available for upgrade.

IP400 hardware will no longer be supported, including IP400 series internal cards, expansion modules and trunk cards listed below:

IP400 VCM cards	VCM4 VCM8 VCM16 VCM24 VCM30
IP400 modules and station cards	Digital Station V1: 16 and 30 port variants Phone V1: 8, 16 and 30 port variants So8: ETSI BRI SO support

Página2504 de 3226.

IP400 cards	Analog Trunk Card Uni (ATM4U)
	Analog Trunk Cards (ATM4)
	BRI Trunk Cards
	T1 PRI Trunk Cards
	E1 PRI Trunk Cards
	E1R2 PRI Trunk Cards

The following IP400 trunk and station modules will continue to be supported in the current release.

IP400 expansion modules	Analog trunk 16
	Digital Station V2: 16 and 30 port variants
	Phone V2: 16 and 30 port variants

Upgrading Server Edition

Upgrade Server Edition primary, secondary and expansion systems using the iso image burned to a DVD or USB. Install upgrade licenses prior to upgrading. There are two options available:

Upgrading to IP Office Select

Existing Server Edition licenses need to be migrated by purchasing a new set of Select PLDS licenses.

Upgrading Application Server

The upgrade process for the Application Server is the same as for Server Edition.

Upgrading UCM

Upgrade UCM using a USB2 memory Key with new software or the Web Manager ISO upgrade process.

Upgrading Windows server applications

Download the latest 9.1 windows applications and copy to the server or burn to a DVD.

Upgrading networked systems

In previous releases, networking was achieved using H.323 lines configured with supplementary services set to SCN. After upgrading to 9.1, these lines will be migrated to IP Office Lines.

Replacing Customer Call Reporter

Advanced Edition and Customer Call Reporter (CCR) will no longer be available for new system sales. Additionally, existing Advanced Edition customers will need to migrate their CCR to IP Office Contact Center via purchase of the IP Office Contact Center solution prior to upgrading. However, CCR will continue to be sold and supported on the previous release consistent with Avaya lifecycle support policy.

Avaya will provide CCR customers with a clear path to move to IP Office Contact Center. Further, as a result of this change, Preferred Edition will now come with the Voicemail Pro database and Visual Basic Scripting (these were previously part of Advanced Edition).

TTS and Contact Store will only be available to be ordered separately. Someone upgrading who had Advanced Edition licensed on their system will continue to have the 8 ports of TTS and Contact Recorder enabled on their upgraded systems. These features were previously part of Advanced Edition. CCR will not function upon the upgrade.

Ordering process

Software applications are orderable by Avaya Partners from their Avaya Authorized Distributor. Avaya Partners must contact their respective distributors directly to purchase all IP Office software applications. Each distributor implements a customized IP Office software purchasing and distribution process for its network of Avaya Partners. These distributor specific internal processes are not covered by this document.

BCM with CS1000 to IP Office migration

This configuration allows migrating a network of BCM and CS1000 to IP Office step-by-step by adding IP Office systems to it.

Protocol support	IP Office to BCM: SIP IP Office to CS1000: SIP IP Office to IP Office: SIP or H323 - SCN Networking BCM to BCM: SIP or SIP/MCDN BCM to CS1000: SIP or SIP/MCDN **Note:** Only UDP will be supported and not TCP. IP Office to CS1000 using H.323 or PRI trunks is not supported.
IP Office platform requirements	Release 8.1 or higher, Essential, Preferred or Server Editions
BCM platform requirements	BCM50 or BCM450 6.0
CS1000 platform requirements	CS1000 7.5 with NRS
Centralized voicemail	Centralized Voicemail for all IP Office systems in the SCN network. BCM systems may use centralized voicemail of the CS1000. IP Office systems cannot use centralized voicemail of CS1000.
Phones	All phones supported on the individual call servers and releases including Avaya IP Phone (H.323), Avaya Digital phones, BCM 7000 Series digital phones, BCM1100/1200 Series IP phones (SIP), DECT R4 phones, and Analog phones.

Página2506 de 3226.

IP Office Branch migration

Migration roadmap and limitations

You can upgrade from a B5800 Branch Gateway to the current release of IP Office, or from a previous release of IP Office to the current release of IP Office. The upgrade process for the IP Office Branch solution varies depending on how the architecture is deployed.

If the B5800 Branch Gateway or IP Office release you are upgrading from is connected to the Avaya Aura® infrastructure and uses Avaya Aura® System Manager for centralized management, use Avaya Aura® System Manager to upgrade the firmware and software for the system.

If the architecture is deployed in a stand-alone IP Office branch environment with no centralization or connection to the Avaya Aura® network, you must use IP Office Manager for upgrades. From IP Office Manager, you can perform an upgrade using the upgrade wizard or the System SD card.

For procedures on how to perform System Manager or IP Office Manager upgrades for your Branch solution, see *Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*.

Licenses

Many solutions, applications, and features on IP Office systems are licensed and only operate when a valid license is detected. This includes features within IP Office applications connected to the IP Office system.

This section describes the license requirements for IP Office features. For information and procedures on managing licenses, see “Applying Licenses” in the following documents:

- *Administering Avaya IP Office™ Platform with Manager*
- *Administering Avaya IP Office™ Platform with Web Manager*

Ports, channels, and users

Some licenses enable a number of ports, channels, or users. Depending on the particular license, each supported instance can be consumed either when it is configured for use or when it is actually being used. When no further instances of a license are available, further use of the licensed feature is not allowed.

Multiple licenses can be added to give a higher number of supported ports, channels, or users. However, licenses above the capacity supported by the particular IP Office control unit will not work.

PLDS licensing

IP Office uses the Avaya Product Licensing and Delivery System (PLDS) to manage licenses. PLDS is an online, web-based tool for managing license entitlements and electronic delivery of software and related license files. PLDS provides customers, Avaya Partners, distributors, and Avaya

Página2507 de 3226.

Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads. You can access PLDS from http://plds.avaya.com/.

PLDS license files

Licenses are delivered from PLDS with license files. A PLDS license file is generated for installing on a specific machine. There are two deployment options:

- PLDS Nodal license files are generated for and installed on particular IP Office nodes.
- PLDS WebLM license files are generated for and installed on a WebLM server that can license multiple IP Office nodes.

WebLM centralized licensing is supported in IP Office Server Edition and in IP Office Branch deployments, but not in non-Branch deployments of IP Office Standard mode.

PLDS host ID

Each PLDS license file must be created with the PLDS host ID of the system where the license file is to be loaded. PLDS Nodal license files are machine specific and you must specify the host ID in the **PLDS host ID** field in IP Office Manager or Web Manager.

IP500 V2 systems: You can find the PLDS host ID in the **Licensing** tab of IP Office Manager and Web Manager. The PLDS host ID is made of the two digits “11”, followed by the 10 digit feature key serial number printed on the IP Office SD card. If the SD card is changed, the PLDS host ID will also change.

IP Office Linux servers: The PLDS host ID can be found on the server labeling, the server packaging label, and the system ignition Login screen. The PLDS host ID is derived from the system ID. If the system ID changes, the PLDS host ID will also change.

WebLM: The WebLM host ID is the Mac address of the WebLM server. In a virtual environment, the WebLM host ID is a virtual Mac address that starts with the letter “V”. The WebLM host ID must be used when generating a PLDS license file for the WebLM server in order to implement a centralized licensing scheme for multiple IP Office systems. The WebLM host ID can be found on the server labeling, the server packaging label, the system ignition Login screen, and through the WebLM management interface.

Web License Manager (WebLM)

The Web License Manager (WebLM) is a web-based application for managing licenses. If you use the WebLM server running on the IP Office server, then you can use IP Office Web Manager to log in to the WebLM server by selecting **Applications** > **Web License Manager**. WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on (SSO).

Note:

- WebLM license management is supported for Server Edition deployments and for Enterprise Branch deployments using the System Manager WebLM server. It is not supported for Standard Mode systems.
- When upgrading from a previous release, all systems must be running the same software level. IP Office Server Edition does not support mixed versioning.

For more information on WebLM, see *Administering standalone Avaya WebLM*.

Página2508 de 3226.

Migration of ADI licenses

ADI licenses are no longer supported as of Release 10.0. New licenses must be obtained from PLDS.

Using the One Source Configurator (OSC), all ADI licenses from previous releases are upgraded to PLDS. The **License Migration** option in IP Office Manager can be used to extract license information about the system, and this information can then be uploaded to OSC. After the information is extracted, IP Office Manager signs the file so it cannot be modified.

PLDS license creation

The PLDS license must be created with the PLDS host ID of the system where the license will be loaded. If the licenses are loaded locally on the IP Office, then the PLDS host ID is available in IP Office Manager or Web Manager. For IP500 V2, it is also the Feature Key number on the SD card, which starts with “11”. If the PLDS file is loaded on a WebLM server, then the host ID is available on the WebLM interface under **Server Properties**.

For more information about migrating IP Office licenses to PLDS, see *Administering Avaya IP Office™ Platform with Manager* or *Administering Avaya IP Office™ Platform with Web Manager*.

Virtual licenses

As part of the migration process, the following virtual licenses are no longer created as of release 10.0. They are provided as actual PLDS licenses.

- Virtual Essential Edition
- Virtual Preferred Edition for systems with a UCMv1 module
- Virtual Avaya IP endpoints for systems with:
  - VCM32/64 v1 modules that provided 12 Avaya IP endpoints
  - Legacy VCM channel migration licenses
- Additional virtual Voicemail Pro ports for Server Edition

  In earlier releases, two virtual Voicemail Pro ports were provided per instance. As of release 10.0, the PLDS licensing system will add two Voicemail Pro ports to any Server Edition or Server Edition Select license.

Note:

The legacy Windows soft phone is not supported in IP Office release 10.0 and will not function. The previous virtual licenses provided when upgrading are no longer provided in release 10.0. Avaya Communicator for Windows is the replacement. The Teleworker license enables the use of the Avaya Communicator for Windows. In earlier releases, this was only available with Office Worker and Power User.

Server Edition Centralized and Nodal licensing

Before release 10, Server Edition deployments used nodal licensing. This type of licensing can still be used in release 10 and higher. However, it is expected that most deployments will prefer to

Página2509 de 3226.

centralize license management using the Avaya Web License Management (WebLM) server. The WebLM server is automatically installed on the Server Edition Primary server. For newly installed systems, centralized licensing is the default configuration.

All systems in the Server Edition solution must use the same **License Source**.

Nodal licensing

With nodal licensing, license files must be installed on each node in the system. For some licensed features, the required license can be installed on the Server Edition Primary server and used by all nodes in the system. However, for other licensed features, the required license must be installed on the node where the feature is used.

Centralized licensing

As of release 10, you can use the WebLM server running on the Server Edition Primary server to fully centralize license management. With centralized license management, all licenses are contained in a single PLDS file uploaded to WebLM. All nodes in the solution obtain their licenses from WebLM.

The IP Office Secondary server and Expansion systems can be configured to request licenses directly from the WebLM server, or to use a proxy option. When configured to use the proxy option, the license requests are sent through the IP Office Primary server, which proxies the requests to the WebLM server. The Primary server does not allocate licenses, but only acts as a proxy.

Systems using nodal licensing can be converted to use centralized licensing. Since PLDS license files are generated using the host ID of the server where they reside, you must regenerate the license file using the host ID of the WebLM server that will host the license file.

Centralized license distribution

When the license source is WebLM, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features. Editable fields can be used to:

- Request additional licenses from the WebLM server.
- Remove licenses from the IP Office node to apply them elsewhere.

Important:

When reallocating licenses, always reduce the number on the IP Office node where they are currently applied before applying them on another node. If you exceed the number of licenses available, you will receive an error message.

Distribution after conversion from Nodal to Centralized licensing

- If the IP Office node needs any of the following licenses, then you must manually configure the respective **Reserved Licenses** editable fields. This will allow the IP Office node to request the licenses from the WebLM server.
  - **VMPro Recordings Administrators**
  - **VMPro TTS Professional**
  - **CTI Link Pro**

Extension Reserved license setting: When the license source is **Local**, the setting **Extension** > **VoIP** > **Reserve License** is set to **None**. Switching the license source to WebLM changes the setting to **Reserve Avaya IP endpoint license**. If required, you must manually change this setting to **Reserve 3rd party endpoint license** or **Both**.

Página2510 de 3226.

License allocation in WebLM

You can use WebLM to view the licenses used by each node in IP Office Server Edition. In the WebLM navigation pane on the left, click **Licensed Products**. The Acquired licenses table displays information about the licenses acquired for each client ID. In IP Office, the WebLM client ID for each node is displayed on the license Remote Server page.

Nodal license distribution

When the **License Source** is **Local**, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features.

Nodal licensing for a Server Edition solution is based on a combination of licensing done through the Server Edition Primary server plus some server-specific licenses. All the user specific and system specific licenses can be managed from the Server Edition Primary server that also acts as a licensing server. Licenses are entered into the configuration of the Server Edition Primary server and are based on the system ID of that server.

Where a license is used to enable features, such as SIP Trunk channels, on other systems, the Server Edition Primary server only allocates those licenses to other systems after it has met its own license needs.

When another system loses connection to the Server Edition Primary server, any license requirements based on those licenses entered in the Server Edition Primary server's configuration are supported for a grace period of 30 days.

Other server specific licenses are entered into the configuration of the server requiring the feature and are based on the System ID of that system.

License	Primary server	Server-specific
Server Edition	Yes	No
Avaya IP endpoints	Yes	No
Third-party IP endpoints	Yes	No
SIP trunk channels	Yes	No
IP500 universal PRI channels	No	Yes
Additional voicemail ports [3]	Yes	No
Web Collaboration	No	Yes
UMS Web Services [1]	No	Yes
Office Worker	Yes	No
Power User	Yes	No
Office Worker to Power User upgrade	Yes	No
Receptionist	No	Yes
CTI Link Pro	No	Yes
Messaging TTS Pro [3]	Yes	No
Voicemail Pro Recording Administrator [2] [3]	Yes	No

Table continues…

License	Primary server	Server-specific
WAV User	No	Yes
IPSec tunneling	No	Yes
Video SoftPhone for Mac	No	Yes

1. UMS Web Service licenses are for Hunt Groups only.
2. The Voicemail Pro Recording Administrator license refers to Contact Store. Only one license is required for a Server Edition network.
3. For deployments with dual Voicemail Pro servers, Messaging TTS Pro, Voicemail Pro Recording Administrator, and Additional voicemail ports licenses must be on the Secondary Server.

WebLM licensing

License modes

The following are the IP Office license modes when you are using WebLM licensing. The license mode is displayed in IP Office Manager, Web Manager, and System Status Application (SSA).

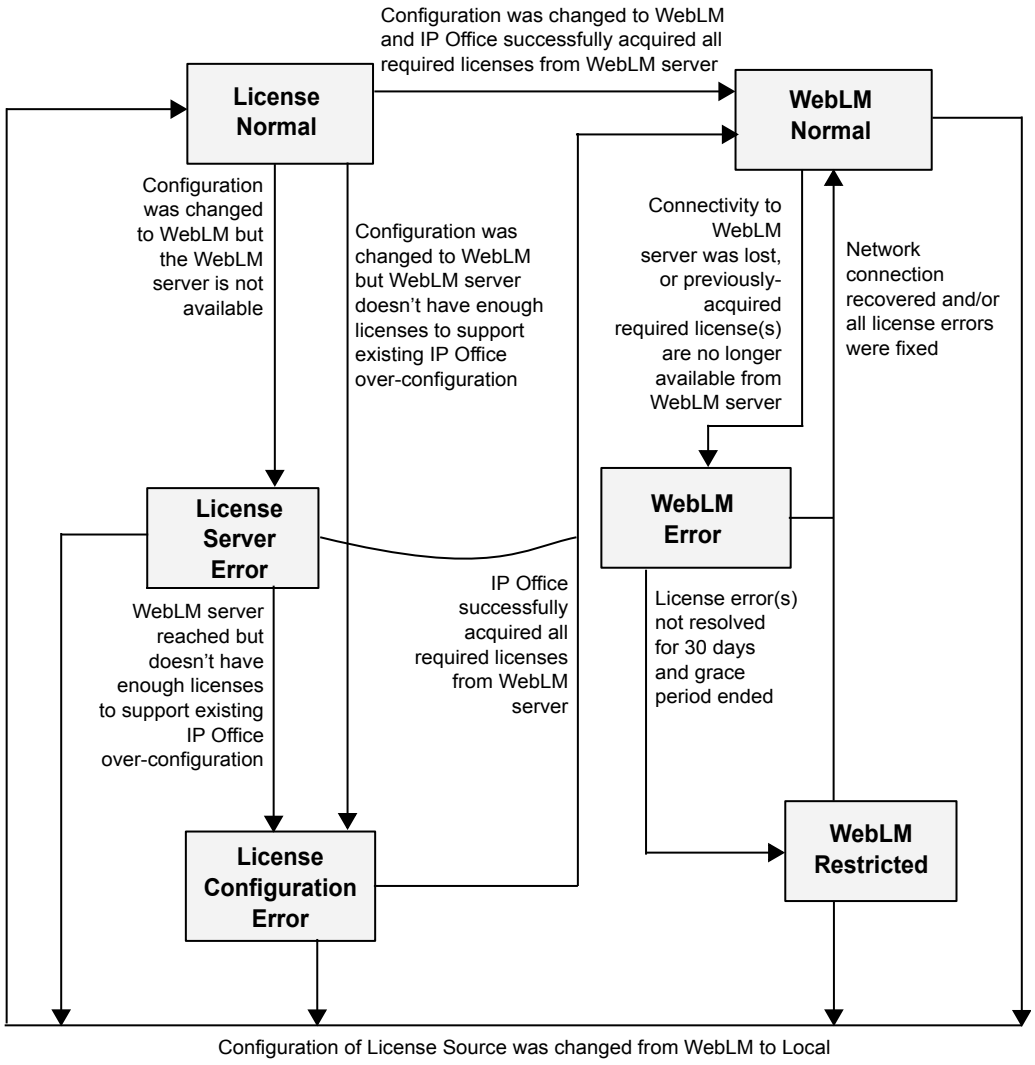
Mode	Description
License Normal	WebLM licensing is not configured. Traditional Nodal licensing. No grace period. Over-configuration is allowed.
License Server Error	Configuration was changed to WebLM, but the WebLM server is not available. No grace period. Until the problem is resolved, IP Office is unlicensed and unusable similar to traditional Nodal licensing if no licenses are installed.
License Configuration Error	Configuration was changed to WebLM and the WebLM server is available, but it doesn't have enough licenses to support the existing IP Office configuration. No grace period. Until the problem is resolved, IP Office is unlicensed and unusable similar to traditional Nodal licensing if no licenses are installed. Licenses must be added to the WebLM license file or IP Office configuration must be modified to correct over-configuration.
WebLM Normal	IP Office is configured for WebLM licensing, the WebLM server is available and IP Office successfully acquired all the licenses required to support all of its configured features. New licenses are acquired for newly-configured features, and over-configuration of licensed features is prevented if licenses cannot be acquired. IP Office periodically renews its acquired licenses. Failure to renew will lead to the WebLM Error mode with grace period.
WebLM Error	IP Office is configured for WebLM licensing and was previously in WebLM Normal mode. But IP Office now cannot renew or re-acquire all the licenses required to support all of its configured features. Over configuration of licensed features is prevented if licenses cannot be acquired. IP Office keeps operating for a 30-day grace period based on its existing configuration (lost licenses are replaced with virtual grace licenses).

Table continues…

Página2512 de 3226.

Mode	Description
WebLM Restricted	IP Office was in the WebLM Error mode, but the 30-day grace period has expired and the problems for this error have not been resolved. Unlicensed features will stop working (virtual grace licenses are deleted). Any configuration of IP Office is not allowed, except configuration changes that reduce the licensing errors.

License mode state transitions



WebLM licensing configuration

In WebLM licensing, licenses must fully support the IP Office configuration. Over-configuration is not allowed. IP Office, based on its configuration, requests the required licenses from the WebLM server.

For some types of licenses, such as for users, extensions, receptionists, and web collaboration, the type and quantity of required licenses is determined by the configuration of the respective items. For

Página2513 de 3226.

example, the User and Extension records in the IP Office configuration. These quantities are displayed in read-only fields in the ‘Reserved Licenses’ list in the IP Office Configuration License > Remote Server tab.

For other types of licenses, such as for SIP trunk sessions and Voicemail Pro ports, the quantity of required licenses must be configured explicitly. These quantities have to be configured in editable fields in the Reserved Licenses list in the IP Office Configuration License > Remote Server tab.

Licensing configuration warnings and alarms

License Configuration Error mode

- IP Office goes into the License Configuration Error mode when you change the IP Office License Source from “Local” to “WebLM” and it is under-licensed or over-configured.

  In this mode, IP Office is unlicensed and unusable. This mode is a transition error state and not supported as a steady state. Try to avoid entering into this mode and, if it happens, fix the errors immediately.

- Installed systems with traditional licensing may be under-licensed or over-configured. If they are upgraded to version 10.0 and migrated using WebLM licensing without acquiring the additional needed licenses or removing the over-configuration, then the installed systems goes into the License Configuration Error mode after migration.

  To help avoid this problem, warnings are given by the IP Office Manager License Migration Tool. If IP Office has over-configuration relative to its existing old licenses, the License Migration Tool displays a warning and also includes detailed warning information in the License Migration information file.

- If IP Office is in the License Configuration Error mode, Systems Status Application (SSA) alarms page shows alarms indicating the cause of the problem.

  If you encounter this mode, review the SSA alarm errors and resolve them by acquiring the missing required licenses or by modifying the IP Office configuration so as to not require these licenses.

Other warnings

When the administrator sets the License Source to “WebLM”, IP Office Manager and IP Office Web Manager display a warning advising the administrator to check and verify that sufficient licenses are available on the WebLM server.

WebLM user and IP Endpoint licensing

IP endpoint licenses

When IP Office uses WebLM licensing, each configured H.323 or SIP extension requires a license and IP Office requests the required licenses from the WebLM server. Sufficient licenses are required for all the configured H.323 and SIP extensions and not only for the maximum number of concurrently-registered extensions. This is consistent with WebLM licensing for users and receptionists.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of extensions with a small number of licenses to cover only a subset of the extensions registering at the same

Página2514 de 3226.

time. For example, configuring three extensions with one IP endpoint license to cover only one of the three extensions registering at the same time. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing, and set the **Reserve License** field for the extensions to `None`.

For each configured H.323 or SIP extension, IP Office requests from the WebLM server an Avaya or third-party IP endpoint license, as per the **Reserve License** field of the configured extension record. When IP Office uses WebLM licensing, the **Reserve License** field for each configured H.323 and SIP extension is by default set to Avaya IP endpoint license. This field is editable and the administrator can change it to a third-party IP endpoint license or to both Avaya and third-party IP endpoints.

Note:

For the **Reserve License** field, the value `None` is not available with WebLM licensing because IP Office must request a license from the WebLM server.

User licenses

When IP Office uses WebLM licensing, sufficient User licenses are required as per the IP Office users configuration and not only for the maximum number of concurrently-registered users. This is consistent with WebLM licensing for IP endpoints and receptionists. IP Office requests from the WebLM server the required User licenses (for example, Power User licenses) as per the user profile of all configured users.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of users with a small number of licenses to cover only a subset of the users registering at the same time. For example, configuring three users with one User license to cover only one of the three users registering at the same time. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing.

Receptionist licenses

When IP Office uses WebLM licensing, Receptionist licenses are required for all users that are configured as Receptionist and not only for the maximum number of users that would run their IP Office SoftConsole application concurrently. This is consistent with WebLM licensing for IP endpoints and users. With WebLM, licenses are required according to the configured objects, and over-configuration and under-licensing are not allowed.

Note:

With WebLM licensing, IP Office does not support configuring of a large number of Receptionist users with a small number of licenses to cover only a subset of the users connecting at the same time using IP Office SoftConsole. For example, configuring three Receptionist users with one Receptionist license to cover only one of the three users connecting at the same time using IP Office SoftConsole. However, if you want support of this behavior, you can use a local PLDS license file instead of Centralized WebLM licensing.

Página2515 de 3226.

Auto-create support for users and extensions

When IP Office uses WebLM licensing, you cannot auto-create users and extensions as it is not supported. The administrator must manually configure users and extensions. For DECT extensions, the “Preconfigured” method must be used.

However, auto-create for users and extensions is supported if you use local PLDS license file instead of Centralized WebLM licensing.

Basic Edition license for new systems

As of Release 10.0, customers purchasing only Basic Edition will receive the following license:

Material code	License	Description
383714	IPO R10 BASIC ED PLDS LIC	Basic Edition

Customers must also purchase SD cards, which are configured, by default, with Basic Edition.

Customers must obtain this material code, which is merchandisable and does not have to be configured, before ordering IP Office Support Services. This is especially important for customers who already have Basic Edition or for after-market IP Office Support Services purchases, including customers who set up Basic Edition without IP Office Support Services first, but then later choose to get IP Office Support Services. These customers must place a merchandise order for this material code first and then place their after-market purchase of IP Office Support Services and register their equipment for servicing.

Note:

Basic Edition is not a prerequisite for Essential Edition or Preferred Edition, and is not stacked under Essential Edition.

Essential Edition and Preferred Edition licenses

An Essential Edition license is a prerequisite on IP500 V2 systems, and includes mobile twinning for all users and four remote workers.

A Preferred Edition license is a prerequisite for any user profile licenses. In a multisite network, the Preferred Edition license of the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server still requires its own Preferred Edition license for Voicemail Pro operation. For a IP500 V2 system fitted with a Unified Communications Module (UCM V2), the card requires a separate Preferred Edition license.

The Preferred Edition license includes support for 4 messaging ports. The total number of messaging ports supported can be increased by adding additional messaging port licenses, at the time of purchase or later, up to the maximum supported by the particular control unit.

Página2516 de 3226.

Order code	License	Description
383125	IPO R10 ESSNTL ED PLDS LIC	Essential Edition
383128	IPO R10 PREFRD VM PRO PLDS LIC	Preferred Edition

Additional Messaging licenses

The following licenses enable specific messaging features. These additional licenses all require the Preferred Edition Voicemail Pro license as a prerequisite.

Order code	License	Description
383089	IPO R10 VM PRO UMS 1 PLDS LIC	1 user
307334	IPO-SL 10 VMPRO UMS 1 PLDS LIC	1 user
383075	IPO R10 TTS WNDWS PLDS LIC	Messaging TTS for Windows (ScanSoft)
383077	IPO R10 3RD PTY TTS PLDS LIC	Generic TTS license

Server Edition licenses

A Server Edition license includes:

- Features from Essential Edition
- Features from Preferred Edition
- Centralized Voicemail Pro
- Two ports of Voicemail Pro
- Unlimited multi-site networking channels (IP Office Lines)

A Server Edition license enables:

- Meet-me conferencing
- Advanced messaging
- Automated attendant
- Call recording
- Conditional call routing
- Queue announcements
- Mobile twinning
- Call control
- Call back

One Server Edition license is required for the primary server, the secondary server, and for each Linux or IP500 V@ expansion system. The licenses enable voice networking between systems in the Server Edition network.

Order code	License	Description
383130	IPO R10 SE PLDS LIC	Server Edition license
382920	IPO-SL 10 SE PLDS LIC	Server Edition Select license

Table continues…

Página2517 de 3226.

Order code	License	Description
383132	IPO R10 Media Encr Disable PLDS LIC	Server Edition license for media encryption
382922	IPO-SL R10 Media Encr Disable PLDS LIC	Server Edition Select license for media encryption
383131	IPO R10 VRTLZD SE PLDS LIC	Virtualized Server Edition license
382921	IPO-SL 10 VRTLZD SE PLDS LIC	Virtualized Server Edition Select license
383134	IPO R10 ACCS ENABLEMENT PLDS LIC	Avaya Contact Center Select enablement
382924	IPO-SL 10 ACCS ENABLEMENT PLDS LIC	Avaya Contact Center Select enablement

Branch licenses

The following table describes key IP Office licenses that are of particular interest to branch deployments.

Display name	Description
Avaya WebLM Model	This license is required by IP Office in branch deployments in order to connect to the WebLM server and use WebLM centralized licensing.
Branch System	This license is required for IP Office in branch deployments. It is used for tracking purpose only.
IP Office Centralized Endpoints license	One license is required for each Centralized user configured on the IP Office with a SIP extension or an analog extension. **Important:** In addition to this IP Office license, each centralized user also requires a license on the central Avaya Aura® system.
SM Trunk Channel	This license is required with sufficient quantity to allow for the maximum number of concurrent SM Line calls to be enabled on the system. The total number of SM Trunk Channel licenses requirements depend on the expected traffic patterns in the particular deployment. **Note:** IP Office also supports SM Line connections to Avaya Aura® Session Manager in other IP Office Server Edition deployments. These connections are not limited to branch deployments.

Small Community Network licenses

In a Small Community Network (SCN), there must be at least one IP Office Preferred Edition. Two are required with resiliency.

Página2518 de 3226.

The different types of users in an SCN have the same functionality, regardless of where the IP Office Preferred Edition is installed.

In a multisite network, if one or more IP Office Preferred Edition system is installed, then all the IP Office systems in the multisite network will automatically have Preferred licenses as prerequisites for the following user types:

- Power users
- Teleworkers
- Mobile workers
- Office workers

Trunk licenses

SIP trunk sessions

These licenses are used to permit sessions on SIP trunks and SM Lines added to the system. Multiple licenses can be combined for the total number of channels required.

Order code	License	Description
383085	IPO R10 SIP TRNK 1 PLDS LIC	SIP trunk 1 session
307332	IPO-SL 10 SIP TRNK 1 PLDS LIC	SIP trunk 1 session – Select
383120	IPO R10 SM LINE SIP TRNK PLDS LIC	SM Line session
382917	IPO-SL 10 SM LINE SIP TRK PLDS LIC	IP Office Select SM Line session

IP500 Universal PRI additional channels

The IP500 PRI Universal trunk card (UTC) is available in 1 or 2 port variants, each port supporting a single PRI circuit connection. The ports can be switched between supporting E1, E1R2, or T1 line types as required for the trunk being connected. Each port supports 8 B-channels (“Bearer”) which do not need to be licensed. If additional B-channels are required, they must be licensed through the addition of the licenses below. Multiple licenses can be added to achieve the total number of channels required. D-channels are not subject to licensing. The licenses are consumed by those channels, which are configured as being *in service*, in order of the installed IP500 PRI-U cards.

IP500 Universal PRI additional E1 channels

These licenses are used to enable additional E1 B-channels for IP500 PRI-U cards configured for E1 operation. Each port can support up to 30 B-channels in this mode.

Order code	License	Description
383092	IPO R10 IP500 E1 ADD 2CH PLDS LIC	2 E1 channels
383093	IPO R10 IP500 E1 ADD 8CH PLDS LIC	8 E1 channels
383094	IPO R10 IP500 E1 ADD 22CH PLDS LIC	22 E1 channels
307337	IPO-SL 10 IP500 E1 ADD 2CH PLDS LIC	2 E1 channels – Select

Table continues…

Página2519 de 3226.

Order code	License	Description
307338	IPO-SL 10 IP500 E1 ADD 8CH PLDS LIC	8 E1 channels – Select
307339	IPO-SL 10 IP500 E1 22CH PLDS LIC	22 E1 channels – Select

IP500 Universal PRI additional E1R2 channels

These licenses are used to enable additional E1R2 B-channels for IP500 PRI-U cards configured for E1R2 operation. Each port can support up to 30 B-channels in this mode.

Order code	License	Description
275637	IPO R10 IP500 E1R2 ADD 2CH PLDS LIC	2 E1R2 channels
383096	IPO R10 IP500 E1R2 ADD 8CH PLDS LIC	8 E1R2 channels
383097	IPO R10 IP500 E1R2 ADD 22CH PLDS LIC	22 E1R2 channels
307340	IPO-SL 10 IP500 E1R2 2CH PLDS LIC	2 E1R2 channels – Select
307341	IPO-SL 10 IP500 E1R2 8CH PLDS LIC	8 E1R2 channels – Select
307342	IPO-SL 10 IP500 E1R2 22CH PLDS LIC	22 E1R2 channels – Select

IP500 Universal PRI additional T1 channels

These licenses are used to enable additional T1 B-channels for IP500 PRI-U cards configured for T1 PRI or T1 robbed-bit operation. Each port can support up to 23 B-channels (T1 PRI) or 24 B-channels (T1 robbed bit) in this mode.

Order code	License	Description
383091	IPO R10 IP500 T1 ADD 2CH PLDS LIC	2 T1 channels
307336	IPO-SL 10 IP500 T1 ADD 2CH PLDS LIC	2 T1 channels – Select

IP500 Voice Networking

The use of private voice networking trunks between IP500 control units and other systems requires voice networking channel licenses within the IP500. This applies to H.323 IP trunks configured on the IP500, including IP trunks being used for an IP Office Small Community Network (SCN). A voice networking license is also required for the use of trunks configured for Q.SIG operation. On an H.323 IP trunk, a license instance is consumed for each simultaneous outgoing call. On a Q.SIG trunk, the number of calls is limited by the trunk type rather than available licenses.

Additional licenses can be added to achieve the number of voice networking channels required.

Order code	License	Description
383087	IPO R10 IP500 VCE NTWK 4 PLDS LIC	4 voice networking channels including the Advanced Networking features (distributed groups and hot-desking across Small Community Network)

Página2520 de 3226.

User licenses

A profile controls whether users can be configured for a number of features. Every user on the system, except users with Basic User profile and non-licensed users, requires one of the user license types.

The table below lists the different user profiles and the features accessible by each profile. Setting a user to a particular profile enables those features by default, but they can be manually disabled if necessary. The number of users that can be configured for each profile is controlled by the user licenses present in the configuration.

Except for a Basic User, a Preferred Edition system license is a prerequisite for any user profile licenses. In a multi-site network, the Preferred Edition license for the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server still requires its own Preferred Edition license for Voicemail Pro operation.

Feature		Standard Mode					Server Edition		
	Non-licensed User [1]	Basic User	Office Worker	Tele-worker	Mobile Worker	Power User	Basic User	Office Worker	Power User
one-X Portal Services	–	–	Yes	Yes	–	Yes	–	Yes	Yes
Telecommuter options	–	–	–	Yes	–	Yes	–	–	Yes
UMS Web Services	–	–	Yes	Yes	–	Yes	–	Yes	Yes
TTS for Email Reading	–	–	–	–	Yes	Yes	–	–	Yes
Remote Worker [2]	–	–	–	Yes	–	Yes	Yes	Yes	Yes
Avaya Communicator [3]	–	–	Yes	Yes	–	Yes	Yes	Yes	Yes
WebRTC	–	–	Yes	–	–	Yes	–	Yes	Yes

User Profile Notes:

1. Non-licensed users can be created on both Standard Mode and Server Edition systems.

Página2521 de 3226.

2. The system supports users using remote H.323 or SIP extensions. On non-Server Edition systems, up to 4 users are supported as remote extensions without needing to be configured and licensed for a user profile. Additional remote users are supported if licensed and configured for either a **Teleworker** or **Power User** user profile. On Server Edition systems, the remote worker is supported for all user profiles.
3. Supported for advanced Avaya Communicator for IP Office usage if one-X Portal and Voicemail Pro applications are also installed. If otherwise, only basic Avaya Communicator for IP Office usage is supported.

Non-licensed user

A non-licensed user:

- Is allowed dial in access and paging.
- Can be used as a Music on Hold or Analog paging port.
- Can be authenticated to allow remote access for remote administration.
- Can make internal and emergency calls as NoUser.
- Can forward to voice mail box for voice mail box only users.
- Can be used for internal twinning.

Basic users

New users are created as Basic users by default. Basic users can perform hot-desking, make and receive calls, forward calls, and perform mobile twinning.

Basic user licenses are no longer provisioned. For both new systems and upgrades, the **Basic Users** field is greyed out.

Basic user licenses are required only in the Cloud environment.

Office Worker licenses

This option is targeted at users who are working in the office. In conjunction with a wired or wireless Avaya phone, these users are provided with functions to control their communication with a PC. For example, these users can control audio conferences or manage voice mail with an email client (requires a Preferred Edition license).

An Office Worker license enables Avaya Communicator for Windows and Avaya Communicator for Web. The Office Worker license enables a user to use the Unified Messaging Service (UMS) and Avaya one-X® Portal for IP Office without Telecommuter functionality. The license instances are consumed for each user being configured.

Order code	License	Description
383106	IPO R10 OFF WORKER 1 PLDS LIC	PLDS license for Office workers
307346	IPO-SL 10 OFF WRK 1 PLDS LIC	1 user – Select
307347	IPO-SL 10 OFF WRK 5 TRL PLDS LIC	5 users – Select

Teleworker licenses

This option is targeted at users who are working from home or elsewhere with Internet connection to the office. They are provided with the ability to leverage the PLDS or ISDN using Telecommuter

Página2522 de 3226.

mode, without incurring any remote phone charges. Alternatively the new IP Office Video Softphone can be used if the quality of service of the local internet connection is adequate.

Teleworker includes the remote worker capability with the package. An Essential Edition license provides 4 remote worker seats. Customers requiring additional seats will need to purchase the Teleworker solution.

The Teleworker license enables a user to use Avaya Communicator for Windows and Avaya one-X® Portal for IP Office. UMS functionality for voice mail or email integration is also enabled, providing synchronization with any IMAP email client. The license instances are consumed for each user being configured.

Order code	License	Description
383102	IPO R10 TELEWORKER 1 PLDS LIC	1 user

Mobile Worker licenses

This option is targeted at users with mobile devices. For example, field sales and service staff who are often on the road. These users are provided with features, such as one number access and call control as if in the office, enabling them to never miss a call. The Mobile Worker license enables the use of the one-X Mobile Preferred client in callback mode (but not in VoIP mode).

Power User licenses

This option is targeted at key knowledge workers with the need for both Mobile Worker and Teleworker functionality. A Power User license enables Avaya Communicator for Windows, Avaya Communicator for Web, and VoIP mode in one-X Mobile Preferred.

The Power User license enables a user to use Avaya one-X® Portal for IP Office, all mobility features, and UMS. A Power User license is required to enable conference scheduling in Avaya one-X® Portal for IP Office.

The license instances are consumed for each user being configured.

Order code	License	Description
383101	IPO R10 OFF WK-PW USR1 UPLT PLDS LIC	Upgrade from Office Worker to Power User – 1 user
307345	IPO-SL 10 OFF WKR TO PWR 1 PLDS LIC	Upgrade from Office Worker to Power User – 1 user – Select
383100	IPO R10 MBL-PWR USR 1 UPLT PLDS LIC	Upgrade from Mobile Worker to Power User – 1 user
383098	IPO R10 PWR USER 1 PLDS LIC	1 user
307343	IPO-SL 10 PWR USR 1 PLDS LIC	1 user – Select

Receptionist licenses

This option is targeted at operators or receptionists and provides a visual computer interface for call handling and management for multiple sites. Up to 10 Receptionist users are supported on each node. Server Edition supports up to 32 Receptionist users, and Server Edition Select supports up to 50.

Página2523 de 3226.

The Receptionist license also enables a user to use IP Office SoftConsole, a Windows application intended for receptionists and operators. Up to 4 IP Office SoftConsole clients can run at the same time and be licensed on a single IP Office system. Additional licenses can be added.

Order code	License	Description
307318	IPO-SL 10 RECEPTS 1 PLDS LIC	1 user
382687	IPO R10 RECEPTIONIST 1 PLDS LIC	1 user

Centralized User license

In IP Office Branch deployments, where IP Office is deployed as a branch of a central Avaya Aura® system, users with a SIP or analog extension can be configured as Centralized users. Every Centralized user requires a Centralized Endpoint license.

Web Collaboration licenses

Order code	License	Description
383122	IPO R10 WEB COLLAB USER 1 PLDS LIC	1 user
382918	IPO-SL 10 WEB COLLAB USR 1 PLDS LIC	1 user – Select

IP endpoint licenses

All IP endpoints, Avaya and third party, require an endpoint license.

Avaya IP endpoint licenses

All Avaya IP phones, including DECT and Wi-Fi phones, require an Avaya IP Endpoint license and will consume one instance of that license. This does not apply to the Avaya Softphone or Avaya Communicator. Avaya IP phones without a license will still be able to register but will be limited to making emergency calls only. The phone will display `No license available` and `Emergency Calls Only`. If a license becomes available, it will be assigned to any unlicensed DECT handsets first and then to any other unlicensed Avaya IP phone in the order that the phones registered.

Order code	License	Description
307350	IPO-SL 10 AV IP ENDPT 1 PLDS LIC	1 endpoint – Select
383110	IPO R10 AV IP ENDPT 1 PLDS LIC	1 endpoint

Third-party IP endpoint licenses

Non-Avaya IP phones, including SIP or H.323 devices, require a Third Party IP Endpoint license to register to IP Office and will consume one instance of that license.

Order code	License	Description
307323	IPO-SL 10 3RD PTY IP END 1 PLDS LIC	1 endpoint – Select
383072	IPO R10 3RD PTY IP ENDPT 1 PLDS LIC	1 endpoint

Página2524 de 3226.

Video Softphone for Mac licenses

Order code	License	Description
383115	IPO R10 VIDEO SOFTPH MAC 1 PLDS LIC	Video Softphone Mac license
382915	IPO-SL 10 VIDEO SOFTPH MAC 1PLDS LIC	Video Softphone Mac license – Select

Trial licenses

Order code	License	Description
383126	IPO R10 ESSNTL ED TRL PLDS LIC	Essential Edition
383129	IPO R10 PREFRD VM PRO TRL PLDS LIC	Preferred Edition
383123	IPO R10 WEB COLLAB 5 PLDS TRL LIC	5 Web Collaboration licenses
382919	IPO-SL 10 WEB COLLAB 5 TRL PLDS LIC	5 Web Collaboration licenses — Select
307344	IPO-SL 10 PWR USR 1 TRL PLDS LIC	1 Power User license — Select
383099	IPO R10 PWR USER 5 TRL PLDS LIC	5 Power User licenses
383103	IPO R10 TELEWORKER 5 TRL PLDS LIC	5 Teleworker licenses
383105	IPO R10 MOBILE WORKER 5 TRL PLDS LIC	5 Mobile Worker licenses
307347	IPO-SL 10 OFF WRK 5 TRL PLDS LIC	5 Office Worker licenses — Select
383107	IPO R10 OFF WORKER 5 TRL PLDS LIC	5 Office Worker licenses
307319	IPO-SL 10 RECEPTS 5 TRL PLDS LIC	5 Receptionist licenses — Select
382688	IPO R10 RECEPTIONIST 5 TRL PLDS LIC	5 Receptionist licenses
307324	IPO-SL 10 3RD PTY IP 5 TRL PLDS LIC	Third party IP endpoint trial license — Select
383073	IPO R10 3RDPTY IPENDPT 5 TRLPLDS LIC	Third party IP endpoint trial license
382913	IPO R10 AV IP ENDPT 5 TRIAL PLDS LIC	5 Avaya IP endpoint licenses — Select
383111	IPO R10 AV IP ENDPT 5 TRL PLDS LIC	5 Avaya IP endpoint licenses
383090	IPO R10 VMPRO UMS 5 TRL PLDS LIC	5 Voicemail Pro UMS licenses
307335	IPO-SL 10 VMPRO UMS 5 TRL PLDS LIC	5 Voicemail Pro UMS licenses – Select
383078	IPO R10 3RD PTY TTS TRIAL PLDS LIC	Voicemail Pro third party TTS license
383076	IPO R10 TTS WNDWS TRL PLDS LIC	Voicemail Pro Windows TTS license
307327	IPO-SL 10 TTS PROLINUX TRL PLDS LIC	Voicemail Pro Linux TTS license — Select
383080	IPO R10 TTS PRO LINUX TRL PLDS LIC	Voicemail Pro Linux TTS license
307329	IPO-SL 10 IPSEC VPN TRL PLDS LIC	IPSec Tunneling — Select
383082	IPO R10 IPSEC VPN TRL PLDS LIC	IPSec Tunneling
307333	IPO-SL 10 SIP TRNK 5 TRL PLDS LIC	SIP trunk sessions — Select
383086	IPO R10 SIP TRNK 5 TRL PLDS LIC	SIP trunk sessions

Table continues…

Página2525 de 3226.

Order code	License	Description
383088	IPO R10 IP500 VCE NTWK 4 TRLPLDS LIC	IP500 Voice Networking
307321	IPO-SL 10 CTI TRL PLDS LIC	CIT Link Pro — Select
383070	IPO R10 CTI TRL PLDS LIC	CIT Link Pro

Upgrade licenses

To upgrade existing systems to the latest release, upgrade licenses are required. Upgrade licenses are sold separately. Customers can only upgrade to the latest equivalent of their existing Edition.

Note:

Upgrading from a previous release of Basic Edition to the latest version of Essential Edition is not a valid upgrade path.

Order code	License	Description
383738	IPO-SL 10 RECEPTS 1 UPG PLDS LIC	Select Receptionist upgrade
383696	IPO R10 RECEPTIONIST 1 UPG PLDS LIC	Receptionist upgrade
383739	IPO-SL 10 CTI UPG PLDS LIC	Select CTI upgrade
383697	IPO R10 CTI UPG PLDS LIC	CTI upgrade
383740	IPO-SL 10 VMPRO 1 UPG PLDS LIC	Select Voicemail Pro upgrade
383698	IPO R10 VM PRO 1 UPG PLDS LIC	Voicemail Pro upgrade
383741	IPO-SL 10 3RDPTY IPEND1 UPG PLDS LIC	Select IP third party endpoint upgrade
383699	IPO R10 3RDPTY IPENDPT1 UPG PLDS LIC	IP third party endpoint upgrade
383742	IPO-SL 10 TAPI WAV 1 UPG PLDS LIC	Select TAPI WAV upgrade
383700	IPO R10 TAPI WAV 1 UPG PLDS LIC	TAPI WAV upgrade
383743	IPO-SL 10 TTS PROLINUX UPG PLDS LIC	Select TTS Pro Linux upgrade
383703	IPO R10 TTS PRO LINUX UPG PLDS LIC	TTS Pro Linux upgrade
383701	IPO R10 TTS WNDWS UPG PLDS LIC	TTS Windows upgrade
383702	IPO R10 3RD PTY TTS UPG PLDS LIC	Third party TTS upgrade
383744	IPO-SL 10 IPSEC VPN UPG PLDS LIC	Select IPSec VPN upgrade
383704	IPO R10 IPSEC VPN UPG PLDS LIC	IPSec VPN upgrade
383745	IPO-SL 10 CONTACT RCRDR UPG PLDS LIC	Select Avaya Contact Recorder upgrade
383705	IPO R10 CONTACT RCDR UPG PLDS LIC	Avaya Contact Recorder upgrade

Table continues…

Página2526 de 3226.

Order code	License	Description
383746	IPO-SL 10 SIP TRNK 1 UPG PLDS LIC	Select SIP trunk upgrade
383747	IPO-SL 10 VMPRO UMS 1 UPG PLDS LIC	Select Voicemail Pro Unified Messaging Server upgrade
383708	IPO R10 VM PRO UMS 1 UPG PLDS LIC	Voicemail Pro Unified Messaging Server upgrade
383748	IPO-SL 10 IP500 T1 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383709	IPO R10 IP500 T1 CH1 UPG PLDS LIC	IP500 additional channel upgrade
383749	IPO-SL 10 IP500 E1 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383710	IPO R10 IP500 E1 CH1 UPG PLDS LIC	IP500 additional channel upgrade
383752	IPO-SL 10 IP500 E1R2 CH1 UPG PLDS LIC	Select IP500 additional channel upgrade
383713	IPO R10 IP500 E1R2 CH1 UPG PLDS LIC	IP500 additional channel upgrade
383707	IPO R10 IP500 VCE NTWK1 UPG PLDS LIC	IP500 voice networking upgrade
383755	IPO-SL 10 PWR USR 1 UPG PLDS LIC	Select Power user upgrade
383716	IPO R10 PWR USER 1 UPG PLDS LIC	Power user upgrade
383756	IPO-SL 10 OFF WKR 1 UPG PLDS LIC	Select Office worker upgrade
383719	IPO R10 OFFICE WORKER 1 UPG PLDS LIC	Office worker upgrade
383717	IPO R10 TELEWORKER 1 UPG PLDS LIC	Teleworker upgrade
383718	IPO R10 MOBILE WORKER 1 UPG PLDS LIC	Mobile worker upgrade
383757	IPO-SL 10 AV IP ENDPT 1 UPG PLDS LIC	Select Avaya IP endpoint upgrade
383721	IPO R10 BT RACE PLDS UPG LIC	BT Race system upgrade
383722	IPO R10 SFTPH 1 PLDS UPG LIC	Soft Phone upgrade
383759	IPO-SL 10 VSFTPHN MAC 1 UPG PLDS LIC	Select Video Soft Phone for Mac upgrade
383723	IPO R10 VSFTPHN MAC 1 UPG PLDS LIC	Video Soft Phone for Mac upgrade
383760	IPO-SL 10 SMLINE SIPTRK UPG PLDS LIC	Select SM Line SIP trunk upgrade
383726	IPO R10 SM LINE SIPTRNK UPG PLDS LIC	SM Line SIP trunk upgrade
383706	IPO R10 SIP TRNK 1 UPG PLDS LIC	SIP trunk upgrade

Table continues…

Página2527 de 3226.

Order code	License	Description
383761	IPO-SL 10 WEBCOLLB USR1 UPG PLDS LIC	Select Web Collaboration user upgrade
383728	IPO R10 WEBCOLLAB USER1 UPG PLDS LIC	Web Collaboration user upgrade
383715	IPO R10 BASIC EDITION MIGRATION UPGRADE	Basic Edition migration upgrade
383736	IPO R10 BASIC EDITION MIGRATION UPG ENTL	Entitled Basic Edition migration upgrade
383729	IPO R10 ESSNTL ED UPG PLDS LIC	Essential Edition upgrade
383737	IP OFFICE R10 ESS/PREF EDITION ENTL UPGRADE PLDS LIC:DS	Essential Edition/Preferred Edition entitlement upgrade
383730	IPO R10 ESS ED EVM 1CH UPG PLDS LIC	Essential Edition Embedded Voicemail channel upgrade
383731	IPO R10 PREFRD VM PRO UPG PLDS LIC	Preferred Edition Voicemail Pro upgrade
383762	IPO-SL 10 SE/VRTLZD UPG PLDS LIC	Select Server Edition Virtualized upgrade
383732	IPO R10 SE/VRTLZD PAID UPG PLDS LIC	Server Edition Virtualized upgrade
385845	IPO-SL 10 SE/VRTLZD ENTL UPG PLDS LIC	Select Server Edition Virtualized entitlement upgrade
	IPO R10 SE/VRTLZD ENTL UPG PLDS LIC	Server Edition Virtualized entitlement upgrade
383766	IPO-SL 10 ACCS ENBLMNT UPG PLDS LIC	Avaya Contact Center Select upgrade for Select editions
383735	IPO R10 ACCS ENABLEMENT UPG PLDS LIC	Avaya Contact Center Select upgrade

Página2528 de 3226.

Chapter 4: Resources

Documentation

See the following related documents on the Avaya Support website at support.avaya.com and the IP Office Knowledge Base at marketingtools.avaya.com/knowledgebase.

Document number	Title	Use this document to:	Audience
Overview			
16–604278	*Avaya IP Office™ Platform Start Here First*	See a list of all the documents related to the solution.	Everyone
Not numbered	*Avaya IP Office™ Platform Feature Description*	Understand the solution features at a high-level.	Everyone
Not numbered	*Avaya IP Office Contact Center Feature Description*	Understand IP Office Contact Center features and capabilities.	Everyone
Planning			
15–604135	*Avaya IP Office™ Platform Server Edition Reference Configuration*	Understand the technical specifications of and plan for IP Office Server Edition deployment.	Sales Engineers Implementation Engineers
15–604253	*Avaya IP Office™ Platform in a Branch Environment Reference Configuration*	Understand the technical specifications of and plan for IP Office in a branch environment deployment.	Sales Engineers Implementation Engineers
Not numbered	*OnAvaya™ and Powered Reference Configuration for Business Partners*	Understand the technical specifications of both IP Office Cloud solutions and plan for deployment.	Sales Engineers Implementation Engineers
Not numbered	*Avaya IP Office™ Platform Security Guidelines*	Understand and follow recommended security guidelines.	Sales Engineers Implementation Engineers
Not numbered	*Avaya IP Office Contact Center Reference Configuration*	Understand technical specifications of IP Office Contact Center and plan for deployment.	Sales Engineers Implementation Engineers

Página2529 de 3226.

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Training

Avaya training and credentials are designed to ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website at http://avaya-learning.com/.

The following courses are also available on the Avaya Learning website. After logging in to the website, enter the course code or the course title in the **Search** field.

Course code	Course title
2S00012W	APSS – Small and MidMarket Communications – IP Office™ Platform and Select Overview

Table continues…

Página2530 de 3226.

Course code	Course title
4601W	Avaya IP Office™ Platform — Components
4602W	Avaya IP Office™ Platform — Editions
2S00015O	Small and Midmarket Communications — IP Office — Endpoints
10S00005E	Knowledge Access: Avaya IP Office™ Platform Implementation
5S00004E	Knowledge Access: Avaya IP Office™ Platform Support

Included in all Knowledge Collection Access offers above is a separate area called IP Office Supplemental Knowledge. This floor in the Virtual Campus contains self-directed learning objects, which cover IP Office delta information. This material can be consumed by technicians experienced in IP Office.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Página2531 de 3226.

Additional IP Office resources

You can find information at the following additional resource websites.

Avaya

http://www.avaya.com is the official Avaya website. The front page also provides access to individual Avaya websites for different countries.

Avaya Sales & Partner Portal

http://sales.avaya.com is the official website for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the portal can be customized for specific products and information types that you wish to see and be notified about by email.

Avaya IP Office Knowledge Base

http://marketingtools.avaya.com/knowledgebase provides access to an online, regularly updated version of the IP Office Knowledge Base.

Avaya maintenance, lifecycle and warranty information

Avaya support services complement standard Avaya maintenance, lifecycle and warranty policies that are posted on http://support.avaya.com. For more information, send email to support@avaya.com.

International Avaya User Group

http://www.iaug.org is the official discussion forum for Avaya product users.

Product compatibility

For the latest and most accurate compatibility information go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Related links

Accessing Avaya DevConnect Application Notes on page 129
Interoperability on page 88

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Página2532 de 3226.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya User ID and password.

   The Support page appears.
3. Under **Support by Product**, click **Product-specific support**.
4. Enter the product in **Enter Product Name** text box and press Enter.
5. Select the product from the drop down list and choose the relevant release.
6. Select the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Phones on page 36
Phone interoperability on page 89

Accessing Avaya DevConnect Application Notes

The Avaya DevConnect program conducts testing with service providers to establish compatibility with Avaya products.

Procedure

1. Go to http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp.
2. Sign in or register.
3. Click a timeframe to search within.

   A list of all the application notes for that timeframe appears.

Página2533 de 3226.

4. In the **Search** field, type `IP Office` and press **Enter**.

   A list of relevant Application Notes appear.

Related links

Phones on page 36
Phone interoperability on page 89
Product compatibility on page 128
Hardware and software options on page 79
Interoperability on page 88

Página2534 de 3226.

Glossary list

Automatic Route Selection	A feature of some telephone systems in which the system automatically chooses the most cost-effective way to send a toll call.
Busy Hour Call Completions	A measure of dynamic traffic calls that can be completed in an average busy hour.
Communication Manager	A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.
Computer Supported Telecommunications Application (CSTA)	A standard interface for Computer Telephony Integration (CTI) applications, such as voice mail and auto-attendant, to interact with telephony equipment.
Digital Communications Protocol	A proprietary protocol that is used to transmit both digitized voice and digitized data over the same communications link. A Digital Communications Protocol (DCP) link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels and two telephones or data modules.
Directory Enabled Management	An interface that uses Avaya Directory Server to facilitate administration of Modular Messaging from a centralized location.
Distributed Communications System	A proprietary inter-networking protocol from Avaya with which you can configure two or more Avaya-based private communication networks to operate as one, large network.
Domain Name System (DNS)	An Internet Engineering Task Force (IETF) standard for ASCII strings to represent IP addresses. The DNS is a distributed internal directory service used mostly to translate between domain names and IP addresses. Avaya 9600 Series IP Telephones can use DNS to resolve names into IP addresses. In DHCP, TFTP, and HTTP files, DNS names can be used whenever IP addresses are available as long as a valid DNS server is identified first.

Página2535 de 3226.

Dynamic Data Exchange (DDE)	An interprocess communication (IPC) method.
Dynamic Host Configuration Protocol (DHCP)	An Internet Engineering Task Force (IETF) protocol used to automate IP address allocation and management.
Ethernet Routing Switch (ERS)	The Avaya stackable chassis system that provides high-performance, convergence-ready, secure, and resilient Ethernet switching connectivity.
Expansion Interface	A port circuit pack in a port network (PN) that provides the interface between a time-division multiplex (TDM) bus or a packet bus on the PN and a fiber-optic link. Expansion interface (EI) carries circuit-switched data, packet-switched data, network control, timing control, and digital signal-1 (DS1) control. EI in an expansion port network (EPN) also communicates with the master maintenance circuit pack to provide the environmental status and the alarm status of the EPN to the switch processing element (SPE).
Expansion port network	In Intuity Audix Server configurations, a port network (PN) that is connected to the time-division multiplex (TDM) bus and the packet bus of a processor port network (PPN). Control is achieved by indirect connection of the EPN to the PPN by way of a port network link (PNL).
Extension to Cellular access number	The phone number dialed to connect to the Avaya server that is running Communication Manager. The Extension to Cellular access number initiates the process of enabling or disabling Extension to Cellular or changing the station security code.
Federal Communications Commission (FCC)	A United States federal agency that regulates communications such as wire-line communications and the Internet.
Global Technical Services	An Avaya team that answers customer calls about products in Avaya Integrated Management.
Internet Protocol	A connectionless protocol that operates at Layer 3 of the Open Systems Interconnect (OSI) model. Internet Protocol (IP) is used for Internet addressing and routing packets over multiple networks to a final destination. IP works in conjunction with Transmission Control Protocol (TCP), and is identified as TCP/IP.
Local Survivable Processor	A configuration of the S8300 media server in which the server acts as an alternate server or gatekeeper for IP entities such as IP telephones and G700 media gateways. These IP entities use the Local Survivable Processor (LSP) when the IP entities lose connectivity with the primary server.

Página2536 de 3226.

Media gateway	An application-enabling hardware element that is part of a family of such elements. This family includes intra-switch connectivity, control interfaces, port interfaces, and cabinets. Avaya media gateways support both bearer traffic and signaling traffic that is routed between packet-switched networks and circuit-switched networks to deliver data, voice, fax, and messaging capabilities. Media gateways provide protocol conversion, such as IP to ATM to TDM, conferencing, presence, such as on-hook or off-hook, connectivity to private networks and public networks, such as IP, ATM, TDM, and networking, such as QSIG, DCS, ISDN. Media gateways support optional form factors.
Network Address Port Translation	A network routing technique. Network Address Port Translation (NAPT) is used to access systems on the same subnet as an IP Office.
Network Routing Policy	An application for centrally managing SIP routing for Session Manager instances. A routing policy describes how a call is routed: where it comes from, where it's going, what its dial pattern is, what time of day it is routed, and its cost for a particular route.
Novell® eDirectory™	An X.500-compatible directory service software product initially released in 1993 by Novell® for centrally managing access to resources on multiple servers and computers within a given network. Novell® eDirectory™ was formerly known as Novell® Directory Services. It is sometimes referred to as Netware Directory Services. Novell® eDirectory™ is a hierarchical, object-oriented database used to represent certain assets in an organization in a logical tree, including people, positions, servers, workstations, applications, printers, services, and groups.
OFCOM	The United Kingdom Office of Communication for the regulation of telecommunications.
PARTNER® Contact Closure Adjunct	A device that is connected to the chassis of a media gateway and provides contact closures. Contact Closure Adjunct (CCA) closes a relay in response to a dial-in command from the media gateway to operate a door or perform a similar action.
Product Information Presentation System	The Product Information Presentation System (PIPS) reports provide data from the Product Information Expert (PIE), a data mining tool that extracts Avaya customer switch and adjunct configuration information and stores it in a database.
Product Licensing and Delivery System (PLDS)	The Avaya licensing and download website and management system. Avaya Business Partners and customers use this site to obtain ISO image files and other software downloads.
Public Switched Telephone Network (PSTN)	A telephone network that includes many communication technologies such as microwave transmission, satellites, and undersea cables.

Página2537 de 3226.

Remote Feature Activation	A Web-based Avaya application to remotely activate features and increase capacities on the system of a customer by delivering a new license file.
System Manager	A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity.
System Status Application	An IP Office application that shows the status of things such as outgoing calls.
Telecommuter	The configuration where Communication Manager establishes the voice connection to a circuit-switched telephone. Requires two connections: a TCP/IP connection for signaling control and a circuit-switched connection for voice.
Telephony Application Program Interface (TAPI)	A Microsoft® Windows API that enables computers running Windows to use telephony services. TAPI is used for data, FAX, and voice communications. Applications can use TAPI to control telephony functions, such as dial, answer, and hang up.
Telephony Service Provider Interface (TSPI)	A Microsoft-defined interface to the telephony service provider (TSP). Microsoft® Windows comes with an H.323 TSP, an IP conference TSP, a kernel-mode device driver TSP, and a unimodem TSP.

Página2538 de 3226.

Index

A

a-law PCM 29
application notes 129
application support 81
architecture 65
auto-create support for users and extensions in WebLM ... 112
Avaya Communicator 40
  iPad 41
  Windows 43
Avaya Contact Center Select
  Business Continuity 78
  deployment options 75–78
  DVD 75
  hardware appliance 77
  overview 59
  reference configurations 73
  topology 73, 75–78
  user data synchronization 73
  VMware 76

B

base cards 29
Basic Edition 61
BCM migration 94, 102
browser support 81

C

CA 54
Central Access 54
cloud overview 69
components 66
Computer Telephony Integration 25
conference calls 48
configuration of WebLM licensing 109
  warnings and alarms 110
contact center 56
control unit 27
CTI 25
customer-provided PC requirements 85

D

data networking 16
deployment options 61
  Avaya Contact Center Select 73, 75–78
  DVD 75, 78
  hardware appliance 77
  VMware 76
DevConnect 129
DMM 56
document changes 7

E

Embedded Voicemail 47
endpoints 120
end user applications 37
Essential Edition 63
external expansion modules 33

F

feature keys 29
features 11
features overview 50

G

gatekeepers 20
gateways 20
guidelines
  WebRTC 35

H

H.323 20
hardware options 79

I

InSite Knowledge Base 129
integrated contact reporter
  overview 57
interfaces 99
interoperability 88, 93
IP500 V2 27
iPad 41
IP endpoint licenses 120
IP endpoint licenses for WebLM 110
IP Office applications
  contact center applications 56
  installation and administration applications 51
  user applications 37
IP Office Contact Center
  deployment options 72
  topology 72
IP Office editions 9
IP Office Video Softphone 44
IP telephony 17

Página2539 de 3226.

L

License migration
ADI 105
licenses 103
Basic Edition 112
Branch 114
Essential Edition 112
IP endpoints 120
Preferred Edition 112
SCN 114
Server Edition 113
small community network 114
Standard Mode 112
trials 121
trunks 115
upgrades 100, 122
users 117

M

Manager 51
MCUs 20
media manager
overview 37
Meet-Me conferencing 49
Migration
roadmap and limitations 103
Multipoint Connection Units 20

N

new features 10

O

one-X Mobile Preferred 38
one-X Portal for IP Office 39
operating system support 81
options
deployment 67
overview 9, 58, 69
Avaya Contact Center Select 59
enterprise branch 67
IP Office 67

P

packet-based voice and data networking 16
PCM 29
phones 36
compatibility 89
country availability 92
remote 36
PLDS licensing 103
ports 99
Preferred Edition 64
private circuit switched voice networking 12
product compatibility 128
public voice networking 13
pulse code modulation 29

R

Radvision 49
receptionist licenses for WebLM 111
reference configuration
IP Office Contact Center 72
reference configurations 61, 67
related documents 125
remote phones 36
resource websites 128

S

SCN licenses 114
Scopia 49
SD cards 29
security 95, 97
Server Edition 64
Centralized licensing 105
licenses 113
Nodal licensing 105
Server Edition Manager 52
Session Initiation Protocol 21
SIP 21, 23
SIP endpoint user agents 24
SMA 54
SNMP Management Console 54
SoftConsole 46
SoftConsole administration 54
software options 79
Solution Management Application 54
solution specification 80
specifications
port interfaces 99
SSA 55
Standard Mode 112
support 128
SysMonitor 56

T

telephones 36
topology 11, 65, 68
Avaya Contact Center Select 73, 75–78
Avaya-hosted 70
BP-hosted 71
Business Continuity 78
Customer Engagement Powered by Google Cloud 70
DVD 75
hardware appliance 77

Página2540 de 3226.

topology *(continued)*
Partner Powered 71
VMware 76
training 126
trials 121
trunk cards 31
trunks
licenses 115

U

upgrade licenses 122
upgrades 100
user licenses 117
user licenses for WebLM 111

V

VCMs 20
Video Collaboration Solution 49
video conferencing 49
videos 127
virtual environment 87
virtual licenses 105
Voice Compression Modules 20
Voicemail Pro 47
voice networking 12, 13, 16

W

Web License Manager 104
WebLM 104
WebLM license modes 108
WebLM license mode state transitions 109
WebLM licensing
auto-create support for users and extensions 112
configuration 109
configuration warnings and alarms 110
IP endpoint licenses 110
license modes 108
license mode state transitions 109
receptionist licenses 111
user licenses 111
Web Manager 54
WebRTC 35

Página2541 de 3226.

Avaya Session Border Controller for Enterprise Overview and Specification

Release 7.2.2.2
Issue 8
April 2019

© 2017-2019, Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the

software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed on this site, the Documentation, Hosted Service(s), and product(s) provided

by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 8
Purpose 8
Change history 8
Warranty 9
Chapter 2: Avaya Session Border Controller for Enterprise overview 10
Standard services 10
Advanced Services 11
Functional entities 12
Signaling element 12
Media element 13
Element and management provisioning 13
Avaya SBCE deployment 14
Deployment models 14
Deployment modes 14
Supported deployment platforms for SBCE 16
Additional network security deployment 19
Password policies 20
New features for Release 7.2.1 21
New features for Release 7.2.2 21
New features for Release 7.2.2.2 22
Feature description 22
Media anchoring 22
Media unanchoring 22
Remote worker configuration 22
Remote management services 23
Signaling manipulation 23
SIP trunking 24
UCID 25
Support for video SRTP 26
REFER Handling 27
Multi Device Access 29
Reinvite handling 30
RTCP Monitoring 30
RTCP monitoring report generation 35
Reverse proxy 36
Far End Camera Control 37
Binary Floor Control Protocol 38
Forward Error Correction 42
User registration 43
Real Time SIP Server Status 43

Página2546 de 3226.

Licensing requirements ... 43
Single Sign-On and Identity Engine ... 44
Multiple Avaya SBCE deployment ... 44
WebRTC-enabled call handling ... 45
Virtualization architecture overview ... 46
SRTP overview ... 47
Multiple subnet and multiple interfaces ... 48
traceSBC tool ... 54
Avaya SBCE support for Serviceability Agent ... 55
Multi-tenancy ... 56
Support for IP Office trunk from a dynamic IP address ... 59
Reuse of connection established by IP Office for delivering calls ... 59
Secure Client Enablement Services proxy ... 60
Support for integrated Dell Remote Access Card and integrated Lights-Out ... 60
SIPREC-based recording solution ... 61
End-to-end secure indication ... 64
Media encryption by using AES-256 ... 65
Transcoding ... 65
Support for IPv6 addresses ... 66
Edge Server for Converged Conference solution ... 67
ENUM support ... 70
Call preservation ... 71
Support for TILEncore-Gx36 Intelligent Application Adapter ... 72
Chapter 3: Interoperability ... 76
Product compatibility ... 76
Avaya SBCE supported servers ... 76
Avaya products ... 77
Third-party product requirements ... 77
Operating system compatibility ... 77
Chapter 4: Performance specifications ... 78
Supported capacity ... 78
Redundancy and high availability ... 79
Avaya SBCE high availability ... 80
EMS replication ... 81
Chapter 5: Environmental requirements ... 82
Altitude requirements ... 82
Hardware dimensions ... 82
Temperature and humidity requirements ... 83
Power requirements ... 83
Physical system protection requirements ... 84
Regulatory standards ... 84
Chapter 6: Security ... 86
Security specification ... 86

Página2547 de 3226.

Unified communications intrusion protection..... 86
Attack protection..... 87
Avaya SBCE hardening..... 88
Protection against layer 3 and layer 4 floods and port scans..... 88
DoS security features..... 89
Protocol scrubber..... 90
Topology hiding..... 90
Firewall rules..... 90
Port utilization specification..... 94
Management interface port restrictions..... 94
TCP packets..... 95
SSH port..... 95
Additional port assignments..... 95
Chapter 7: Licensing requirements..... 97
Avaya SBCE license features..... 97
WebLM server details..... 98
Chapter 8: Resources..... 100
Documentation..... 100
Finding documents on the Avaya Support website..... 101
Training..... 101
Viewing Avaya Mentor videos..... 101
Support..... 102
Glossary..... 103

Página2548 de 3226.

Chapter 1: Introduction

Purpose

This document describes tested Avaya Session Border Controller for Enterprise (Avaya SBCE) characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements.

This document is intended for people who want to gain a high-level understanding of the Avaya SBCE features, functions, capacities, and limitations.

Change history

Issue	Date	Summary of changes
1	June 2017	Release 7.2 document.
2	June 2017	Updated the Capacity and Scalability specification table.
3	September 2017	Added the support of Dell 330 in Redundancy and High Availability topic.
4	November 2017	Updated the document for following Release 7.2.1 changes: • Added the support of SHA2 in media tunneling • Added the support of ESXi 6.5 for VMware • Added Nutanix support for KVM deployment • Added new feature of RTCP monitoring report generation • Added symmetric NAT and multiple IP address support for WebRTC-enabled browser • Updated the Capacity and Scalability specification table for Nutanix.
5	December 2017	Updated the support for Vmware ESXi topic for all ESXi software versions.

Table continues…

Página2549 de 3226.

Issue	Date	Summary of changes
6	April 2018	Added introduction of following new features for Release 7.2.2: • Centralized licensing • Charging rules • WebRTC enhancement Added a new topic of supported deployment platforms for Avaya SBCE.
7	June 2018	• Added a note in the Training topic. • Added a new topic of Password policies. • Updated the Capacity and scalability specification table.
8	April 2019	• Added a new topic New features for Release 7.2.2.2. • Updated the topic of Features for session recording for Release 7.2.2.2. • Updated the Avaya SBCE supported servers topic for Release 7.2.2.2. • Updated the Supported Capacity topic for Release 7.2.2.2.

Warranty

Avaya provides a one-year limited warranty on Avaya SBCE hardware and 90 days on Avaya SBCE software. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the support details for Avaya SBCE in the warranty period is available on the Avaya Support website http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Página2550 de 3226.

Chapter 2: Avaya Session Border Controller for Enterprise overview

Avaya SBCE provides security to SIP-based Unified Communications (UC) networks. Avaya SBCE is available in two versions: Advanced Services and Standard Services. Either version can reside on supported servers. For information about supported servers, see the Avaya SBCE supported servers section.

Avaya SBCE has two main components: the Session Border Controller (Avaya SBCE) and a management system called the Element Management System (EMS). Depending on the network size and service requirement, you can deploy Avaya SBCE in one of the following configurations:

- Standalone configuration

  In the standalone configuration, the Avaya SBCE and EMS coreside in the same physical server.

- Multiple server configuration

  In the multiple server configuration, EMS and Avaya SBCE are deployed on separate physical servers.

- High availability (HA) configuration

  In the High Availability or HA configuration, Avaya SBCE servers are deployed in pairs. Each pair has one Avaya SBCE server acting as primary while the other is secondary. Both servers are controlled by a single Avaya Element Management System (EMS) device or a replicated EMS pair.

Related links

Avaya SBCE supported servers on page 76

Standard services

Avaya SBCE Standard Services provides a subset of the functionality of the Advanced Services offer. Standard services has the functionality required for an enterprise to terminate SIP trunks without the complexity and higher price associated with a typical Session Border Controller (SBC).

Página2551 de 3226.

Avaya SBCE Standard Services is a true enterprise SBC, not a repackaged carrier SBC. This product provides a lower-cost alternative to the more expensive Carrier SBCs. Standard Services also provide an Enterprise SBC that is affordable, highly scalable, and easy to install and manage. Standard Services is a Plug and Play solution for Enterprises and Small to Medium Businesses.

With this product, customers can benefit from Avaya's extensive experience in SIP trunk deployments and supporting large numbers of enterprise users. Avaya SBCE Standard Services features the unique Signaling Manipulation module (SigMa module), which dramatically simplifies the deployment of SIP trunks. The SigMa module streamlines integration of SIP trunks into thousands of variations of enterprise SIP telephony environments, greatly reducing implementation time. As a result, SIP trunk deployment in many standard configurations can occur in 2 hours or less.

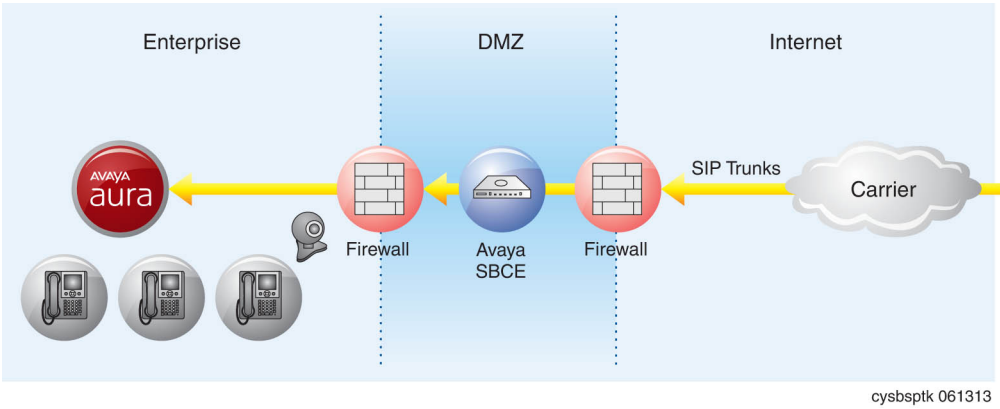


Figure 1: SIP trunking

Advanced Services

Advanced Services is a specialized Unified Communications (UC) security product. Advanced Services protects all IP-based real-time multimedia applications, endpoints, and network infrastructure from potentially catastrophic attacks and misuse. This product provides the real-time flexibility to harmonize and normalize enterprise communications traffic to maintain the highest levels of network efficiency and security.

Advanced Services provides the security functions required by the ever changing and expanding UC market. Advanced Services protects any wire-line or wireless enterprise or service provider that has deployed UC, from malicious attacks. These attacks can originate from anywhere in the world anytime. Advanced Services is the only UC-specific security solution that effectively and seamlessly incorporates all approaches into a single, comprehensive system.

Avaya SBCE Advanced Services incorporates the best practices of all phases of data security to ensure that new UC threats are immediately recognized, detected, and eliminated. Advanced Services incorporates security techniques that include UC protocol anomaly detection and filtering,

Página2552 de 3226.

and behavior learning-based anomaly detection. Together, these techniques monitor, detect, and protect any UC network from known security vulnerabilities by:

- Validating and supporting remote users for extension of Avaya Aura® UC services.
- Using encryption services such as SRTP.

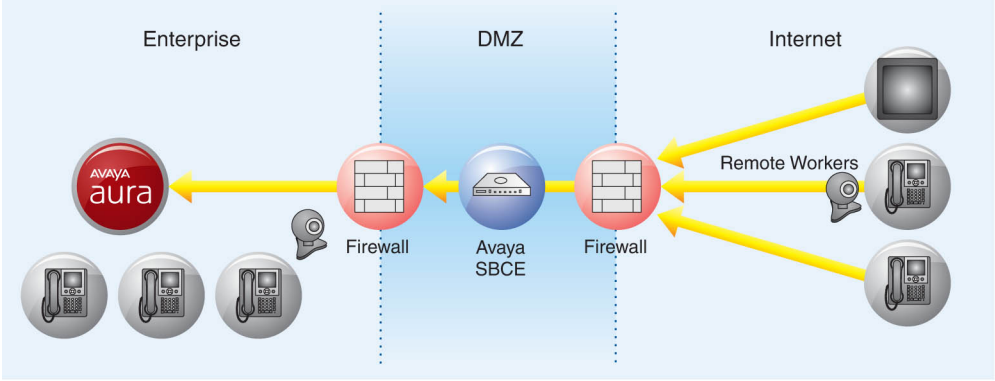


Figure 2: Advanced Services Solution

Functional entities

Avaya SBCE security products perform security functions using three interrelated and complementary functional entities: signaling, media, and intelligence.

Signaling element

The Signaling element is the primary call signaling protection subsystem. The Signaling element is typically deployed at the edge of the network, in the DMZ. Functioning as a proxy, the Signaling element accounts for less than 2 ms of the end-to-end latency budget.

The Signaling element provides the following features:

- Inline signaling decryption and secure key management through TCP and TLS support
- Enhanced SIP validation through source limiting, policy enforcement, and DDoS detection
  - NAT/FW traversal
  - SIP network protection
  - SIP trunk and encrypted voice extranet protection
  - Protocol anomaly detection and prevention
  - SIP source limiting
  - DoS and DDoS attack detection and prevention

Página2553 de 3226.

  - Message sequence anomaly detection and prevention
  - Continuous user behavior learning
  - Bypass for all non-SIP traffic including ARP, DNS, ICMP, STUN, and TURN
  - Domain-based policy filtering based upon user-definable call source and destination criteria
  - Behavior anomaly detection
- Spoofing and machine-generated call detection (MCD)
- Alarm generation and incident reporting to the Avaya SBCE intelligence functional element

This entity also provides the configuration information to the remote endpoints. The Signaling element uses http or https to send the Personal Profile Manager (PPM) information to the phone.

Media element

The Media element is the primary RTP media protection subsystem. A Media element is deployed in the network with the Signaling element.

The Media element provides the following features:

- Media policy enforcement
- RTP anomaly detection
- Timing and bandwidth validation
- FAX and modem tone detection intelligence

Element and management provisioning

Element and management provisioning is the primary UC security information management subsystem of the Avaya SBCE solution. Element and management provisioning receives the variously formatted event and alarm reports from the different security components in the network. This system then stores, normalizes, aggregates and correlates the information into a comprehensive format that allows distributed attacks to be effectively detected and mitigated.

Element and management provisioning provides the following features:

- Collects event logs
- Propagates instructions to the Signaling entity for preventive actions
- Propagates alarms to network management systems
- Maintains caller Trust Scores, White Lists, and Black Lists
- Provides a master storage repository for callers and domains
- Maintains per-user, per-caller, and per-network element behavior models on a ToD and DoW basis

Página2554 de 3226.

Avaya SBCE deployment

Deployment models

Depending on the network size and service requirement, you can deploy Avaya SBCE in one of the following configurations:

- **Standalone configuration**: In the standalone configuration, the Avaya SBCE and EMS coreside in the same physical server. In this deployment, the phones maintain two separate socket connections to Avaya SBCE, at two different IP addresses hosted by Avaya SBCE.
- **Multi-server configuration**: A multi-server configuration requires EMS and Avaya SBCE to be deployed on different servers.
- **High availability (HA) configuration**: A High availability (HA) configuration requires a separate EMS server. Avaya SBCE HA pairs can be deployed in an enterprise in a parallel mode configuration. In the parallel configuration, the signaling packets are routed only to the active or primary Avaya SBCE, which performs all data processing. The interface ports on the standby Avaya SBCE do not process any traffic. The Management interfaces on the Avaya SBCE appliances have different IP addresses, but the signaling or media interfaces have the same IP address. Upon failover, the standby Avaya SBCE advertises its new MAC as the L2 address for the common IP address. The Avaya SBCE devices are synchronized via the heartbeat on the dedicated interfaces, and both Avaya SBCE devices are in continuous communication with the Avaya EMS.

These configurations are also available with deployment in the virtualized environment.

Avaya SBCE is packaged as a vAppliance (OVA) ready for deployment on VMware certified hardware to run in VMware environment. From Release 6.3, Avaya SBCE is also delivered in vAppliance (OVA) format for VMware based deployments. From Release 7.0, Avaya SBCE has a single OVA file for EMS, SBCE+EMS, and Avaya SBCE only deployment. The .ova file is available in PLDS. This configuration supports VMware features, such as vMotion, HA across datacenters, and mixed hardware configuration.

For more information about virtualization, see *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*.

Deployment modes

Avaya SBCE devices can be deployed with or without Transport Layer Security (TLS) or Secure Real-Time Transport Protocol (SRTP) encryption.

Regardless of the deployment scenario, Avaya SBCE offers complete flexibility and intuitive configuration. These products do not require any management on the endpoints in addition to what is necessary to enable TLS, SRTP, and digest authentication.

Página2555 de 3226.

Two-wire deployment

The two-wire topology, also referred to as inline, is the simplest and most basic deployment. Avaya SBCE is positioned at the edge of the network in the DMZ. Avaya SBCE is directly inline with the call servers, and protects the enterprise network against all inadvertent and malicious intrusions and attacks.

In this configuration, the Avaya SBCE performs border access control functionality such as internal and external Firewall or Network Address Translation (FW/NAT) traversal, access management and control. These functions are based on domain policies that the user can configure, and intrusion functionality to protect against DoS, spoofing, stealth attacks, and voice SPAM.

The two-wire Avaya SBCE deployment enables TLS encryption of the signaling traffic and SRTP encryption of the media traffic.

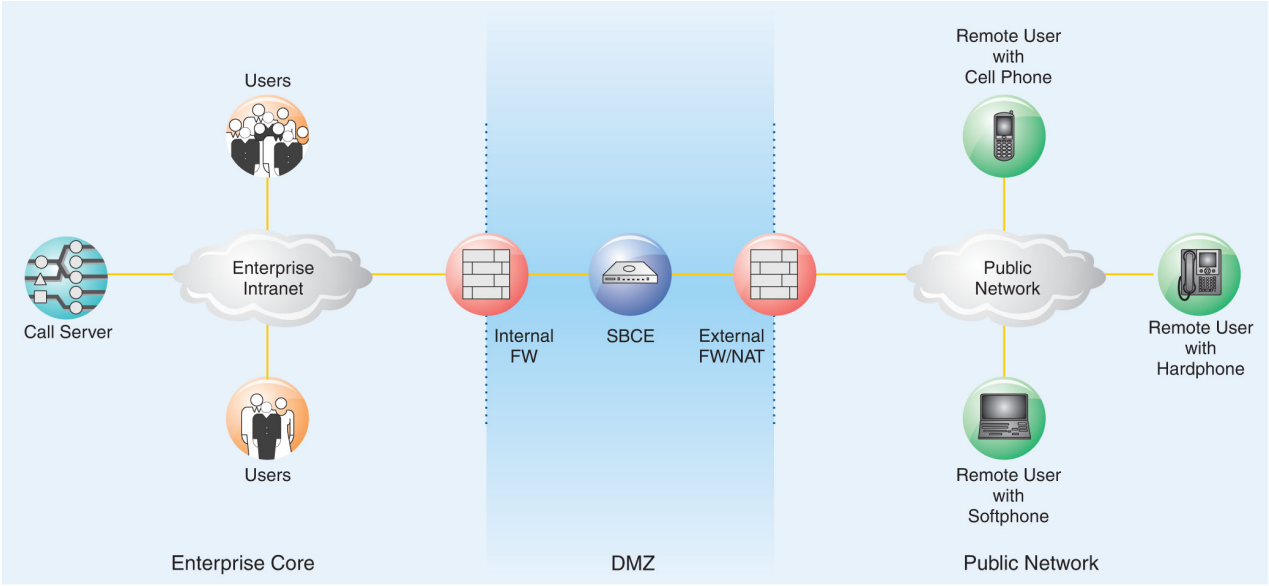


Figure 3: Avaya SBCE Deployment – Two-Wire

One-wire deployment

With the one-wire deployment, also referred to as the screened subnet, the Avaya SBCE is deployed in the enterprise DMZ, but not directly inline with the enterprise call servers. The Avaya SBCE is in the direct signaling path, uses a single Ethernet interface, and is the next hop for SIP traffic.

The Avaya SBCE in a one-wire deployment provides a high level of security functionality characteristic of inline deployment. This deployment does not add any latency to time-critical, multimedia applications such as video conferencing or music-on-demand as compared to a two-wire deployment.

Página2556 de 3226.

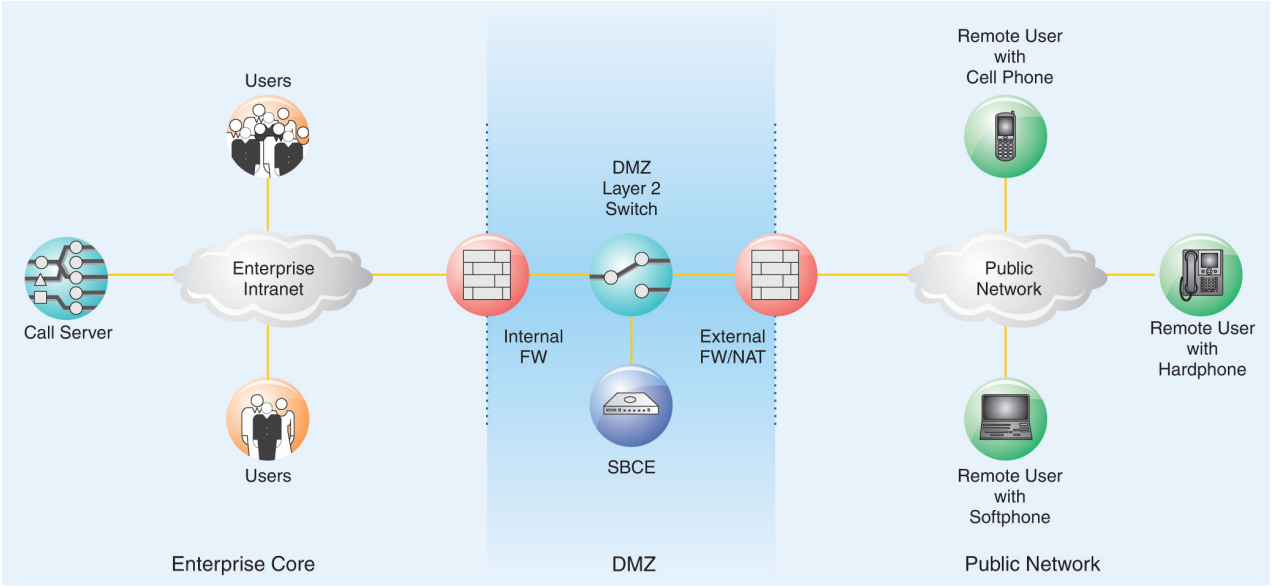


Figure 4: Avaya SBCE Deployment – One-Wire

Supported deployment platforms for SBCE

Virtualization architecture overview

For deployment on VMware-certified hardware, Avaya SBCE is packaged as vAppliance ready (OVA) to run in the virtualized environment. Therefore, from Release 6.3, Avaya SBCE is also available for VMware-based deployments.

From Release 7.0, a single OVA file is available to deploy EMS and Avaya SBCE.

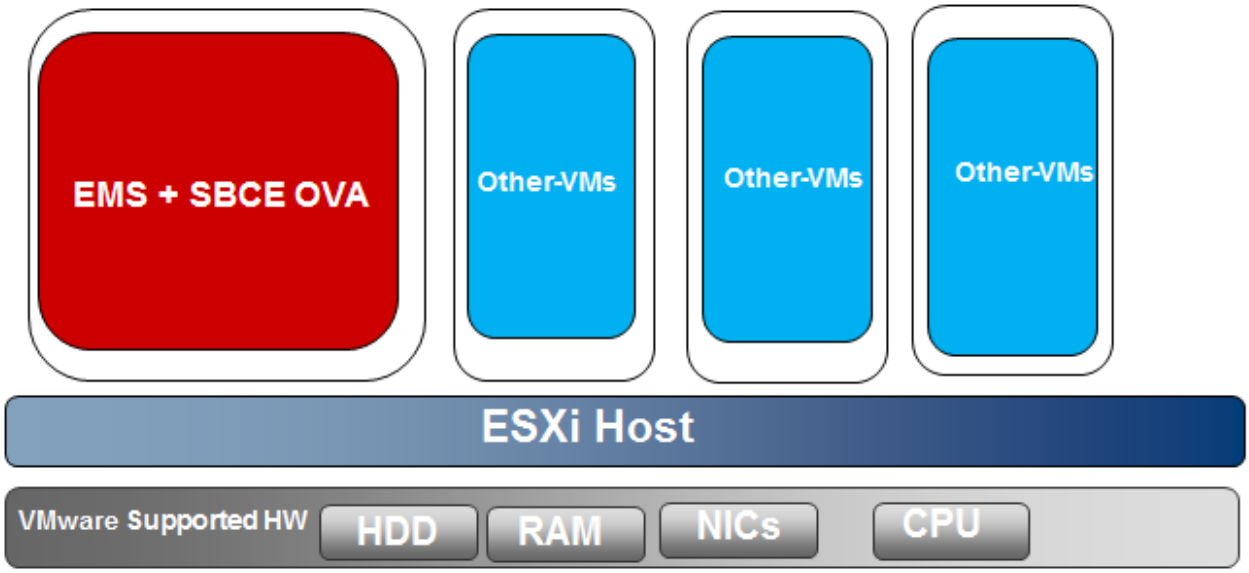
Avaya SBCE supports VMware features, such as vMotion, HA across data centers, and mixed hardware configurations.

The Avaya SBCE OVA files are offered as vAppliance for EMS and Avaya SBCE configurations. The .ova file is available in Product Licensing and Delivery System (PLDS).

Avaya SBCE standalone mode

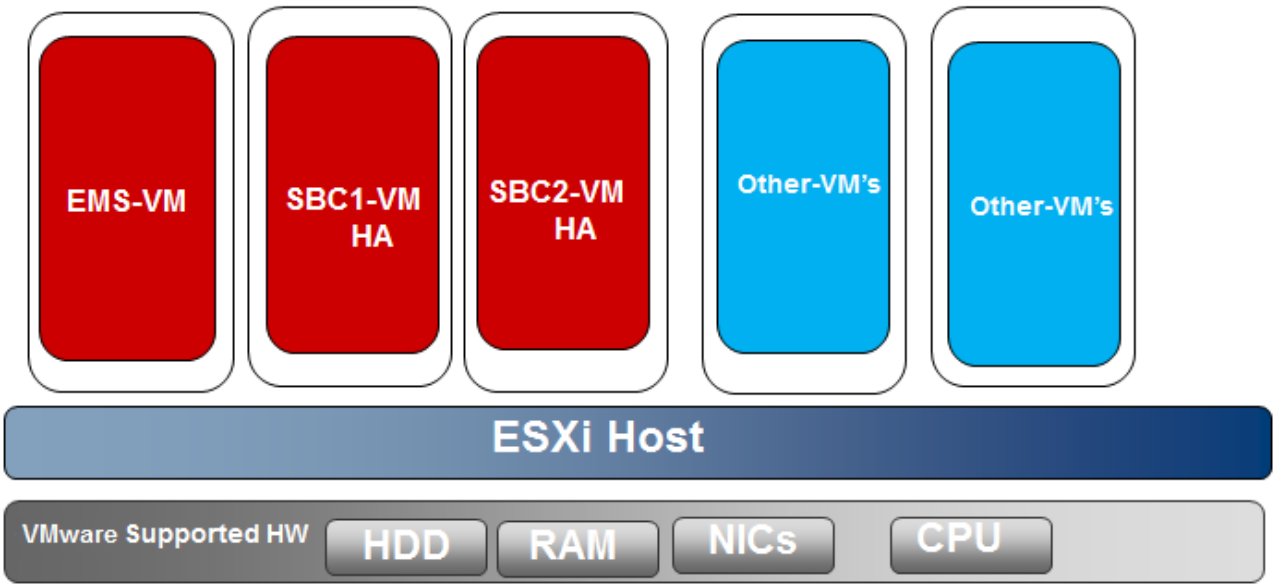
If you select a standalone deployment, the OVA file installs configurations for both Avaya SBCE and EMS.

Página2557 de 3226.



EMS and SBC in High Availability (HA) mode

For HA mode, deploy the OVA file separately for EMS and Avaya SBCE. From release 7.0, a single OVA file is available to deploy EMS and Avaya SBCE. Therefore, you can use the same OVA file, but choose different configurations to deploy EMS and Avaya SBCE.



For more information, see *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*.

Avaya Aura® on Amazon Web Services overview

Amazon Web Services (AWS) is a cloud services platform that enables enterprises to securely run applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

Supporting the Avaya applications on the AWS Infrastructure as a service (IaaS) platform provides the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to operational expense (OPEX).
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.

You can deploy the following Avaya Aura® applications on Amazon Web Services:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Utility Services
- Avaya WebLM
- Presence Services using Avaya Breeze™
- Avaya Session Border Controller for Enterprise
- Avaya Aura® Device Services
- Avaya Aura® Application Enablement Services (Software only)
- Avaya Aura® Media Server (Software only)
- Avaya Diagnostic Server (Software only)

The supported Avaya Aura® AWS applications can also be deployed on-premises.

You can connect the following applications to the Avaya Aura® AWS instances from the customer premises:

- Avaya Aura® Conferencing Release 8.0 and later
- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway, G450 Branch Gateway, and G650 Media Gateway

For more information, see *Deploying Avaya Session Border Controller for Enterprise on Amazon Web Services*

Página2559 de 3226.

Kernel-based Virtual Machine overview

Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

KVM virtualization solution is:

- Cost effective for the customers.
- Secure as it uses the advanced security features of SELinux.
- Performance reliable and highly scalable.
- Open source software that can be customized as per the changing business requirements of the customers.

You can deploy KVM using Nutanix as well.

For more information, .see *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*.

Additional network security deployment

This deployment provides protection to the core UC infrastructure while allowing access to services delivered through the core Aura® applications infrastructure. The following diagram shows this deployment.

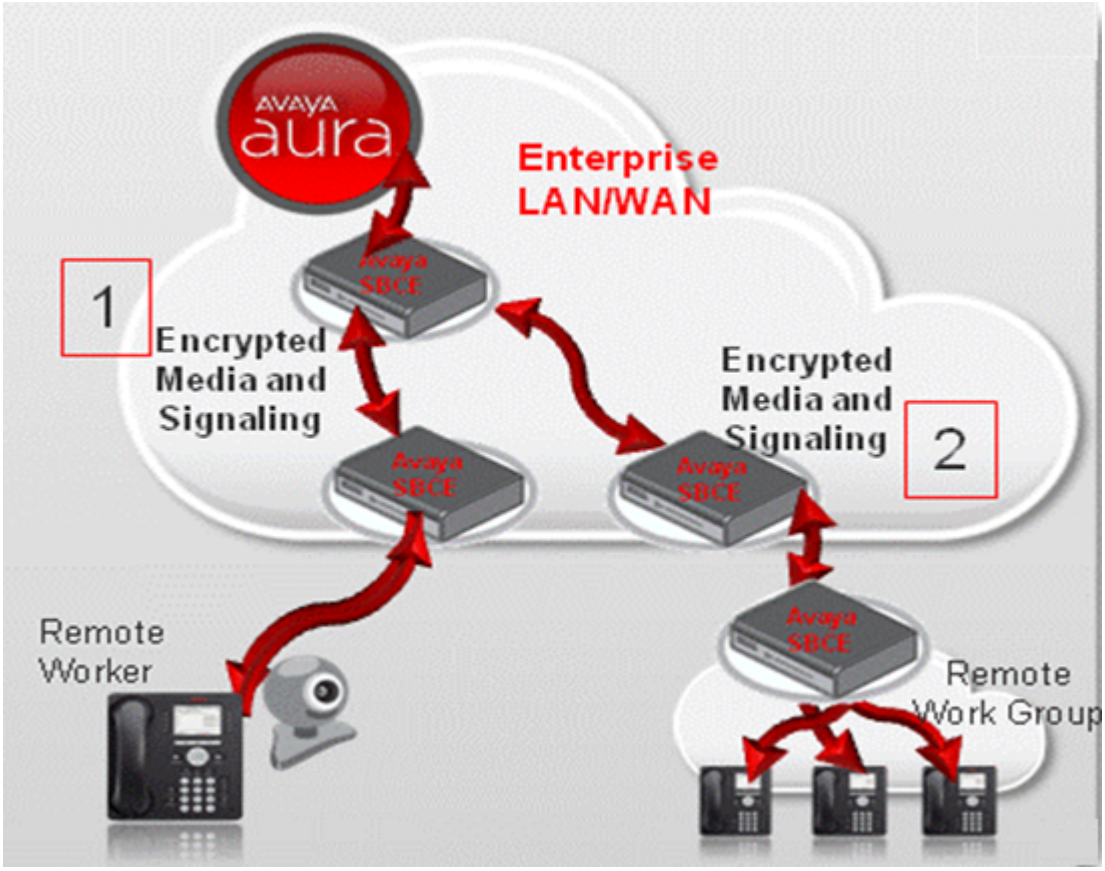


Figure 5: Additional network security deployment

In the diagram, two use cases are depicted. The first configuration shows a back-to-back scenario in which the Aura core is protected by Avaya SBCE internally, and Remote Workers connect to the core via a different Avaya SBCE. Avaya SBCE maintains security and NAT bindings and end-to-end encryption in this back-to-back (B2B) scenario. The second scenario depicts a Remote work group using a Avaya SBCE at the local edge of the group, creating a back-to-back-to-back (B2B2B) scenario. This configuration allows for treatment of the work group as Remote from both the main network and the Aura core and supports encryption of signaling and media from the clients to Avaya SBCE and then to the core if desired. This configuration is supported with Avaya 96x1 SIP clients.

Password policies

The root and ipcs passwords are determined and set during product installation. The EMS GUI has a separate password. When you log in for the first time after installation, the system prompts you to create a new password for accessing the EMS GUI. The default user ID and password is ucsec.

Página2561 de 3226.

Password restrictions are enforced on the `ucsec` and ipcs accounts. The new password must meet the password criteria of minimum 8 characters, including:

- One uppercase letter, one lowercase letter, and one number.
- One special character from the hyphen (-), underscore(_), at sign(@), asterisk (*), and exclamation point (!).You must not use the number sign (#), dollar sign ($), and ampersand (&).

Note:

The Avaya SBCE CLI root and ipcs passwords are determined by the customer network administrator during the installation procedure. Two installation steps prompt the installer to enter a chosen password.

New features for Release 7.2.1

Avaya Session Border Controller for Enterprise Release 7.2.1 supports the following new features and enhancements:

- Support for VMWare ESXi 6.0 and ESXi 6.5
- Support for KVM deployment using Nutanix
- RTCP Monitoring Report Generation
- Log Collection
- SHA2 support for Media Tunneling
- Symmetric NAT and multiple IP addresses support for WebRTC enabled browsers

New features for Release 7.2.2

Avaya Session Border Controller for Enterprise Release 7.2.2 supports the following new features and enhancements:

- Centralized licensing.
- DNS-SRV feature by adding Registration support for configuring SIP server profile
- Charging rules.
- Support for configuring secondary EMS to the factory default state.
- Support for TURN using SEND and DATA indication and TURN signalling on TCP, TLS and UDP.
- Support for configuring TURN relay service for WebRTC calls
- Added the support of Monitoring interval in absence of RTCP report for RTCP monitoring report generation

Página2562 de 3226.

New features for Release 7.2.2.2

Avaya Session Border Controller for Enterprise Release 7.2.2 2 supports the following new features and enhancements:

- Added the support of KDDI option in the Extension field of Interworking profile
- RTT calculation with the help of RTCP streams by Avaya SBCE
- Identification of the trunk or the user agent with the help of media stream
- Added the support of Avaya Converged Platform 100 series server with profile 3
- Added the support of Avaya Converged Platform 100 series server with profile 5

Feature description

Media anchoring

The Avaya SBCE anchors the media streams of all media that passes through the Avaya SBCE. With media anchoring, Avaya SBCE can perform SRTP termination, where Avaya SBCE decrypts or encrypts RTP traffic based on security policies and NAT traversal. All supported configurations require Media Anchoring.

Media unanchoring

To enhance bandwidth usage for endpoints within the same subnetwork and to allow direct media to flow between these endpoints, unanchor media for sessions. Use this feature to enhance bandwidth usage when you connect to a managed MPLS network or a cloud network.

From Release 7.1, Avaya SBCE supports media unanchoring for all non-hairpin calls, including trunk to enterprise, enterprise to trunk, remote to enterprise, and enterprise to remote. Avaya SBCE supports media unanchoring for audio, video, and multimedia calls.

Remote worker configuration

The Remote worker configuration gives remotely located SIP users access to the internal enterprise Unified Communication (UC) network by implementing comprehensive UC security features. These features include sophisticated firewall/NAT traversal, encryption, user authentication, and session and endpoint call policy enforcement.

Remote worker configuration is available for SIP deployments. This configuration uses authentication to verify the legitimacy of the remote user and decrypts TLS-encrypted signaling

Página2563 de 3226.

SIP traffic in real-time. When decryption is completed, the Avaya SBCE analyzes traffic for anomalous behavior, attacks, and intrusions, and applies the user-defined UC policies.

The call can originate from a remotely located Remote worker configuration, outside the enterprise network, to an internal user inside the core enterprise network. Then, the Avaya SBCE in the enterprise DMZ decrypts the SRTP media coming in to the enterprise from the external IP network or the Internet. The Avaya SBCE performs any required Network Address Translation (NAT), analyzes traffic for anomalous behavior, and applies the relevant UC media policies. The Avaya SBCE in the DMZ passes the RTP stream to the intended recipient.

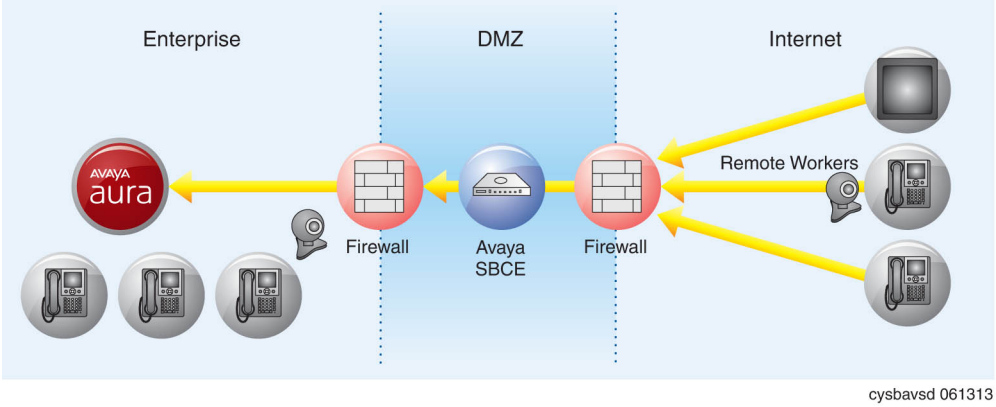


Figure 6: Remote worker

Remote management services

An IP Office Secure Sockets Layer (SSL) virtual private network (VPN) service provides secure tunneling between an Avaya services or support site and an Avaya SBCE that is installed at a customer site. With the secure tunnel, Avaya service providers can offer remote management services such as fault management, monitoring, and administration to IP Office customers.

Avaya SBCE also supports remote access through the SAL gateway.

Remote Management Services gives Avaya customer support agents easy access to the Session Border Controller GUI or SSH.

Signaling manipulation

With Avaya SIP signaling header manipulation, users can add, change, and delete the headers and other information in a SIP message. Signaling manipulation can be configured at each flow level using a proprietary scripting language.

SIP trunking

SIP Trunking allows SIP trunk-enabled enterprises to completely secure SIP connectivity over the Internet through SIP Trunking services obtained from an Internet Telephony Service Provider (ITSP).

SIP trunking ensures the privacy of all calls traversing the enterprise network, while maintaining a well-defined demarcation point between the core and access network. In addition, the SIP trunking feature allows an enterprise to maintain granular control through well-defined domain policies securing SIP implementations or servers of customers from known SIP and Media vulnerabilities.

Because the Avaya SBCE is deployed in the enterprise DMZ as a trusted host, all SIP signaling traffic destined for the enterprise is received by the external firewall and sent to the Avaya SBCE for processing.

If the signaling traffic is encrypted, the Avaya SBCE decrypts all TLS encrypted traffic and looks for anomalous behavior before forwarding the packets through the internal firewall to the appropriate IP PBX in the enterprise core to establish the requested call session.

When a valid call session has been set up, Real-Time Transport Protocol (RTP) or Secure Real-Time Transport Protocol (SRTP) media packets are allowed to flow through the external firewall to the Avaya SBCE in the DMZ. The SBC then looks for anomalous behavior in the media before passing the RTP/SRTP stream on to the intended endpoint.

Página2565 de 3226.

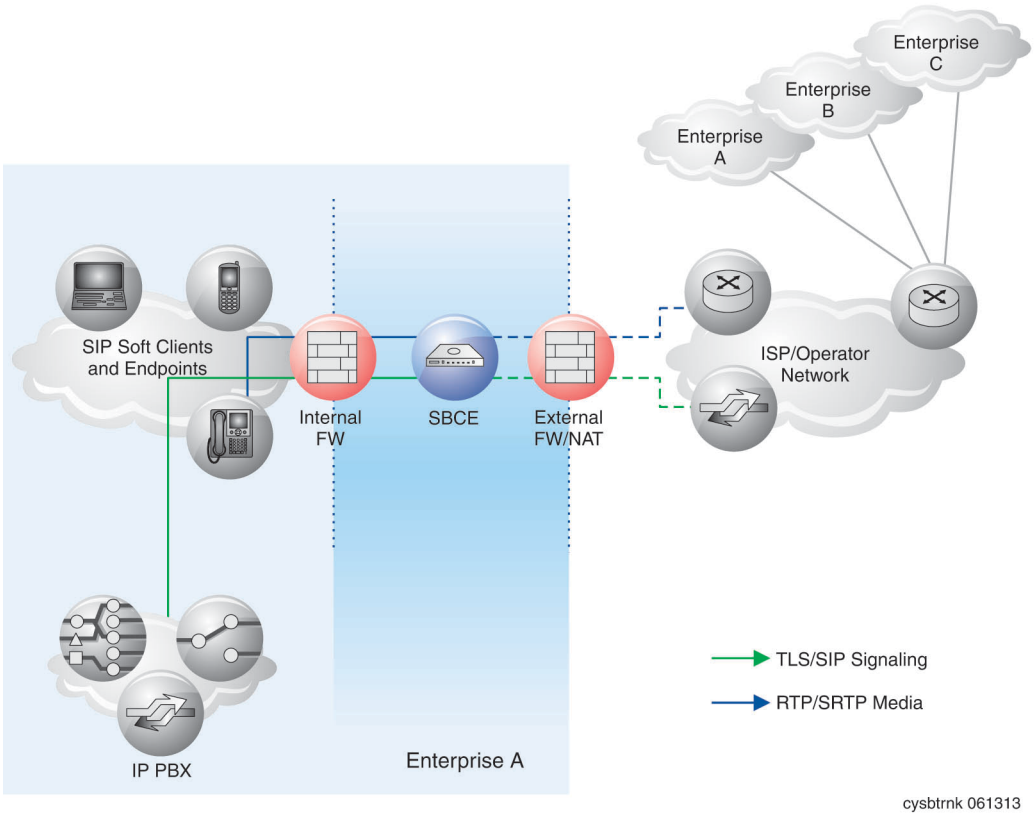


Figure 7: SIP Trunking

UCID

The Universal Call ID (UCID) is an Avaya proprietary call identifier used in Contact Center applications. UCID is used for monitoring, control and recording of calls at non SIP interfaces of CTI. It can also be used to track call history.

AACC

The generation of UCID by Avaya SBCE is required in Avaya Aura® Contact Center 7.0 environment. A UCID is assigned to any incoming call at the border Avaya SBCE so that AACC has a unique handle for each call. For instance, AACC then monitors or controls any application including call recorder using the CTI interface and the UCID for the call.

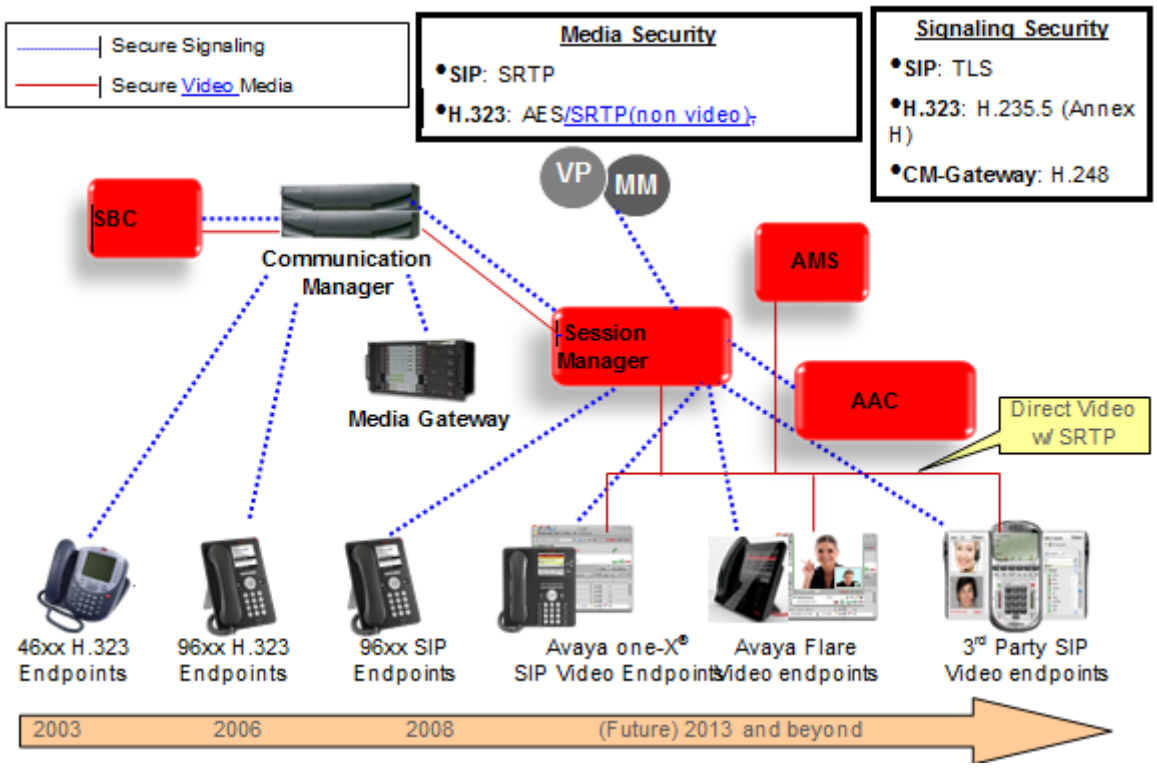
CC Elite

The generation of UCID by Avaya SBCE does not impact Avaya Aura® Call Center Elite. In this scenario, contact center application receives a unique identifier of the call from Avaya Aura® Communication Manager. Avaya SBCE generates a UCID for all incoming SIP calls and ACM reuses the same UCID. No conflict of UCID occurs among ACM, Avaya SBCE, and Contact Center Applications. In features such as call holding, an association is maintained between the new UCID and parent UCID by ACM.

Página2566 de 3226.

Support for video SRTP

Communication Manager supports SRTP for video when appropriate settings are enabled in the system parameter features table. The enabling of SRTP for video in a SIP-to-SIP call is based on the policy set in the ip-codec-set table. The cryptosuite filtering based on ip-codec-set rules do not apply to video media stream. The ip-codec-set rules enable the SRTP policy for video media stream.



Supported user cases

- Desktop Users – Avaya SIP Video Endpoint, such as 1XC to 1XC SRTP encrypted SIP video call : Enabling video calls between two video-enabled IntereXchange carrier SIP endpoints. All standard telephony and video features such as mute, transfer, and hold can be used.
- Mixed – SIP SRTP video call between 1XC and third party (SIP) video endpoint: Third-party devices can be registered to the URE as with 1XC. However, PPM configuration, user or station profile, is unavailable to those devices. Third-party SIP endpoints might include video conference hardware. These endpoints also include SRTP-capable video endpoints calling non-SRTP video endpoint and vice versa.
- Third Party: SIP video call between third party (SIP) video endpoints.

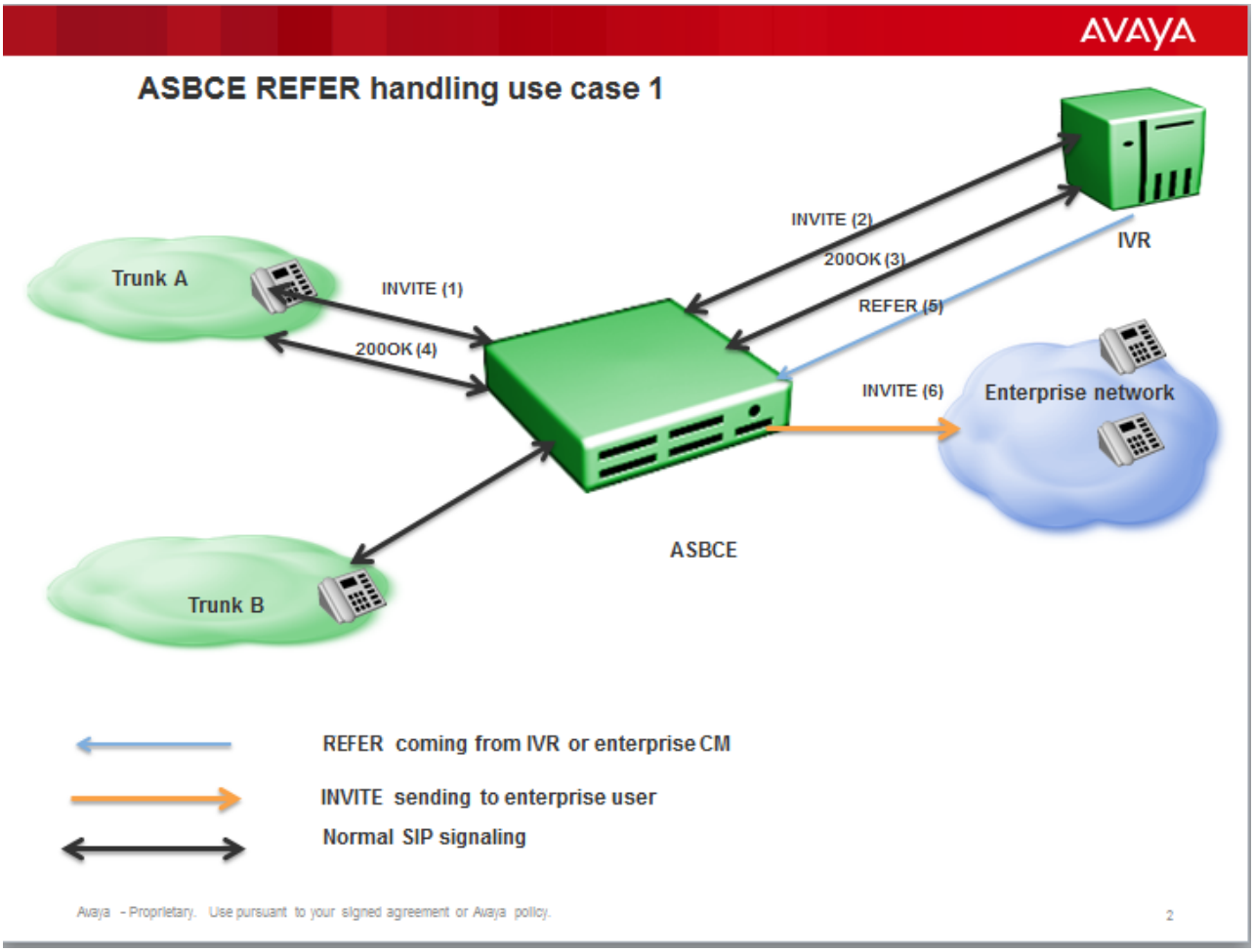
Página2567 de 3226.

REFER Handling

When REFER handling is enabled, Avaya SBCE translates the incoming SIP REFER request to a SIP INVITE request. REFER message comes from enterprise, such as Communication Manager, or IVR and Avaya SBCE handles that REFER going towards trunk server based on the trunk server interworking profile configuration. Following are three use cases for REFER handling.

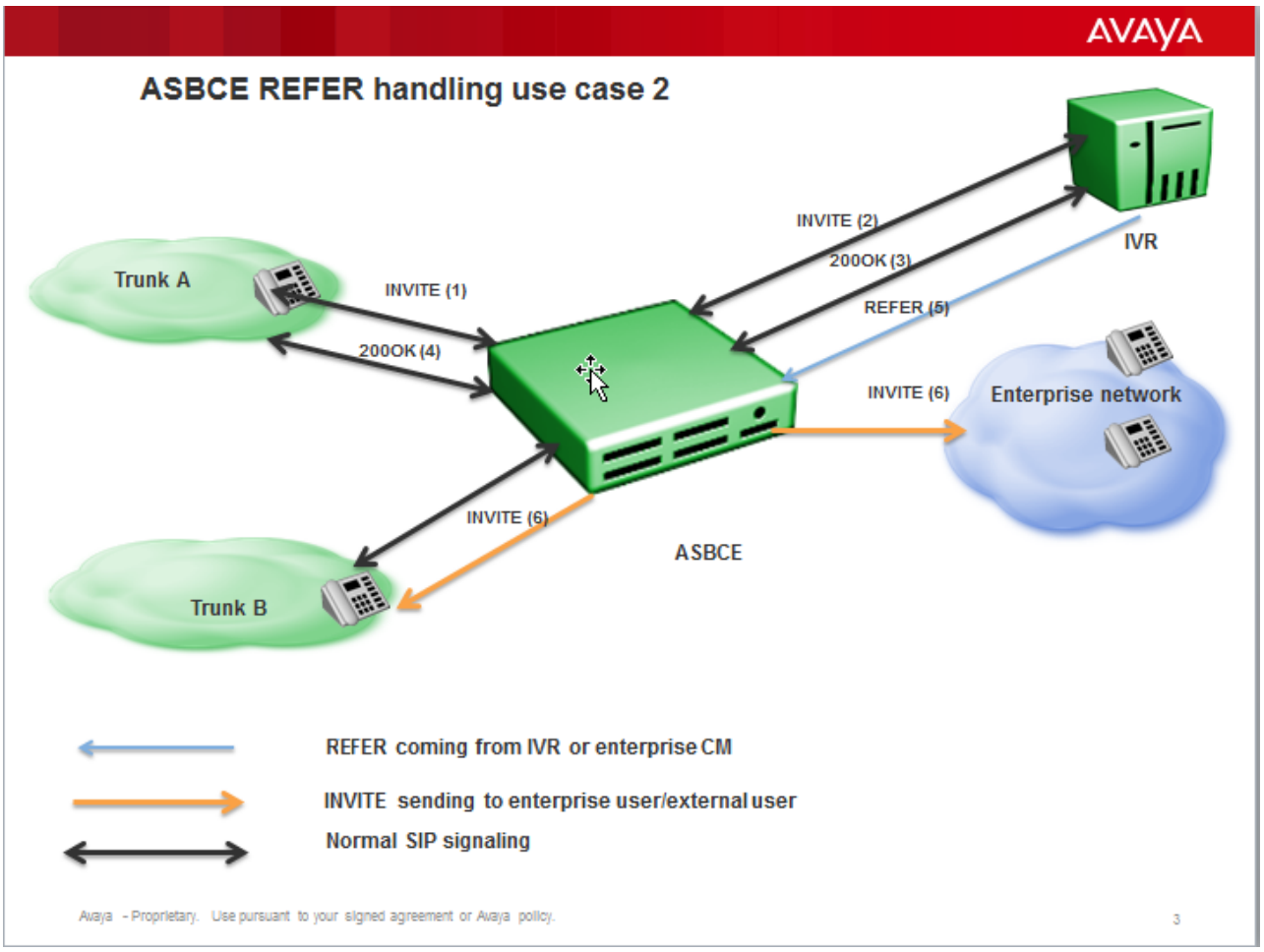
Use case 1

Avaya SBCE uses REFER message and sends a routing INVITE towards enterprise user.



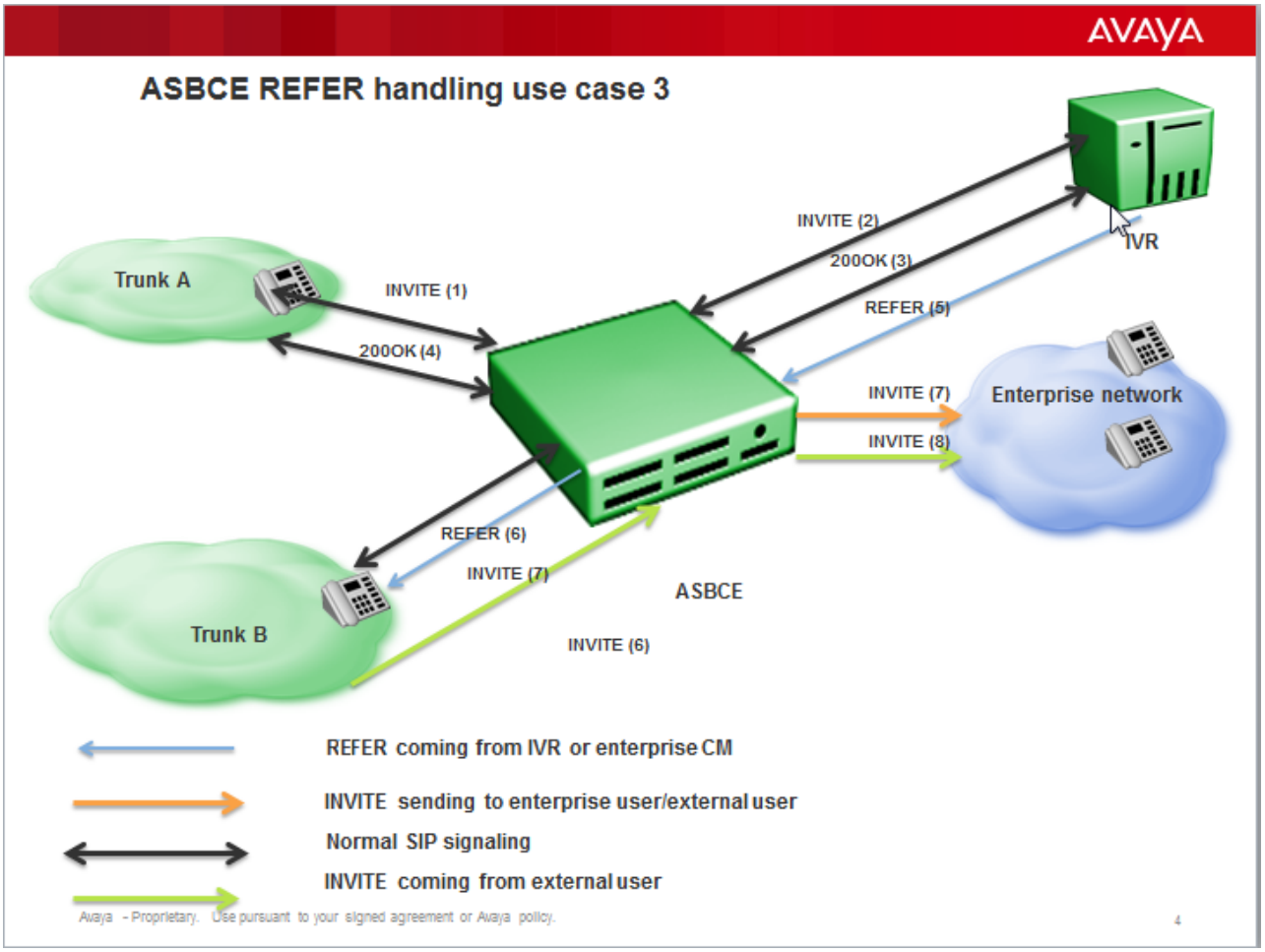
Use case 2

Avaya SBCE uses the REFER message to send an INVITE towards trunk user or enterprise user based on routing profiles created to route the new INVITE. INVITE created from REFER is routed using URI based routing. Routing entries must be created in the trunk server routing profile to route the request to external trunk. By default, the request is routed back to enterprise server. In Aura AST2 transfer mode, Avaya SBCE should always route the new INVITE towards the enterprise server as Avaya SBCE cannot find the dialog to replace.



Use case 3

Based on URI group configuration under refer handling configuration, Avaya SBCE uses some REFER messages. Depending on URI group configuration, REFER messages are relayed to the external trunk. External trunks generate new INVITE message for the target users.



Multi Device Access

With the Multi Device Access (MDA) feature, a user can access calls on multiple devices of various capabilities, but using the same number. All devices of the user will ring for an incoming call, and the user can answer with the chosen device or a paired mobile device. After the call is answered, the remaining devices stop ringing. If the user wants to use a device with better capability, the user can join the existing call using that device. Hence, a conference is created on ACM and the user can manually disconnect the previous device. This procedure is known as a handoff. In case of an AAC-hosted conference, the last MDA device to join the call remains active and all earlier devices are dropped.

The Multi Device Access feature consists of the same user and extension using the same AOR to register multiple devices to Session Manager. All registered devices ring simultaneously and the device on which the user takes the call becomes a device with the active call. Other paired MDA devices receive notification of the active call and dialog information. The paired MDA devices can join the call using this dialog information. The display shows a two-party call, and not a conference. Only one active MDA call is maintained for a call involving AAC.

Página2570 de 3226.

Reinvite handling

Some customers and service providers do not want reinvite messages to be passed on to the SIP trunk. Avaya SBCE blocks reinvite messages coming without change in Session Description Protocol, known as Session Refresh Invites. The same rule applies for Hold or Resume invites without change in SDP, except port, IP, and SDP attributes. The SDP attributes include send recv, send only, and recv only.

RTCP Monitoring

The RTCP monitoring feature in Avaya SBCE updates RTCP packet with appropriate endpoint IP address and hop information. Endpoints are configured to send RTCPMON messages to the Avaya SBCE to which the endpoint is registered. A single Avaya SBCE is designated core Avaya SBCE which is sent to Prognosis. Avaya SBCE maintains the RTCP port mapping and updates this mapping on a per call basis as part of the SIP signaling. Avaya SBCE implements a new feature in the application that has the capability to traceroute multiple destinations simultaneously.

- APIs are provided for the SIP Application to fetch the traceroute information for later reuse when modifying the RTCPMON messages.
- Avaya SBCE tracerouting feature implementation reuses the linux based tracerouting APIs.
- The ICMP/UDP/TCP Avaya SBCE configuration modes can use tracerouting and can be administered from GUI.

On receiving RTCPMON message for Prognosis, Avaya SBCE does a lookup in RTCP port-mapping. Avaya SBCE then modifies the remote IP address and RTCP Port in rtcp message Avaya Subtype 4, based on the mapping. Avaya SBCE then appends the trace hop information of the next network node where the RTP packets are forwarded in Avaya Subtype 5. If this Avaya SBCE is the designated core Avaya SBCE, then perform additional steps before forwarding the packets to Prognosis. Determine the SSRC field from RTCP monitoring packets from endpoint, for example SSRC1. Avaya SBCE also determines the SSRC of the incoming RTP stream from media gateway or caller, for example SSRC2. Avaya SBCE creates a mapping key using SSRC1 and SSRC2, if the mapping does not exist.The mapping key contains the following information:

- Media origination IP address or port for SSRC1 – populated from the RTCPMON Subtype 4 message.
- Media origination IP address or port for SSRC2 – populated from the RTCPMON Subtype 4 message.
- Traceroute information for all the hops from the endpoint [Caller] upto the Core Avaya SBCE – Populated from the RTCPMON Subtype 5 Message.
- Traceroute information for all the hops from the endpoint [Callee] upto the Core Avaya SBCE – Populated from the RTCPMON Subtype 5 Message.

Página2571 de 3226.

If mapping exists in the Avaya SBCE for SSRC1 and SSRC2, then Avaya SBCE uses the mapping information to rewrite the following in the RTCPMON packets to be sent to Prognosis:

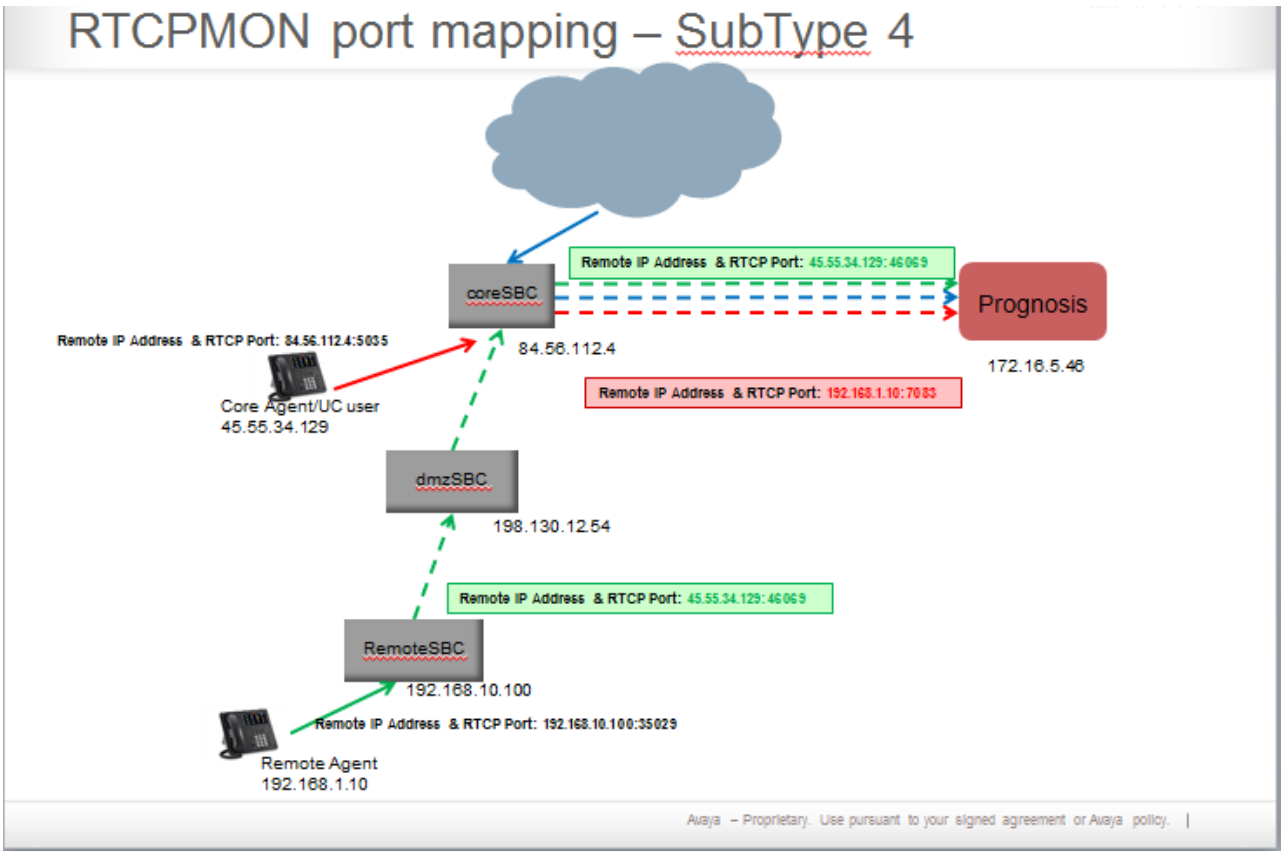
- Subtype 4 RTCPMON.
- Remote IP Address/port of SSRC1 will be set to media origination IP address/port of SSRC2 from the mapping.
- Remote IP Address/Port of SSRC2 will be set to media origination IP address/port of SSRC1 from the mapping.
- Subtype 5
- Trace hop info for SSRC1 will include the current trace hop information received in RTCPMON packet plus trace hop information saved for SSRC2.
- Trace Hop Info for SSRC2 will include the current trace hop information received in RTCPMON packet plus trace hop information saved for SSRC1.

Processed RTCPMON packets will now be sent to Prognosis based on the information filled in by Avaya SBCE.

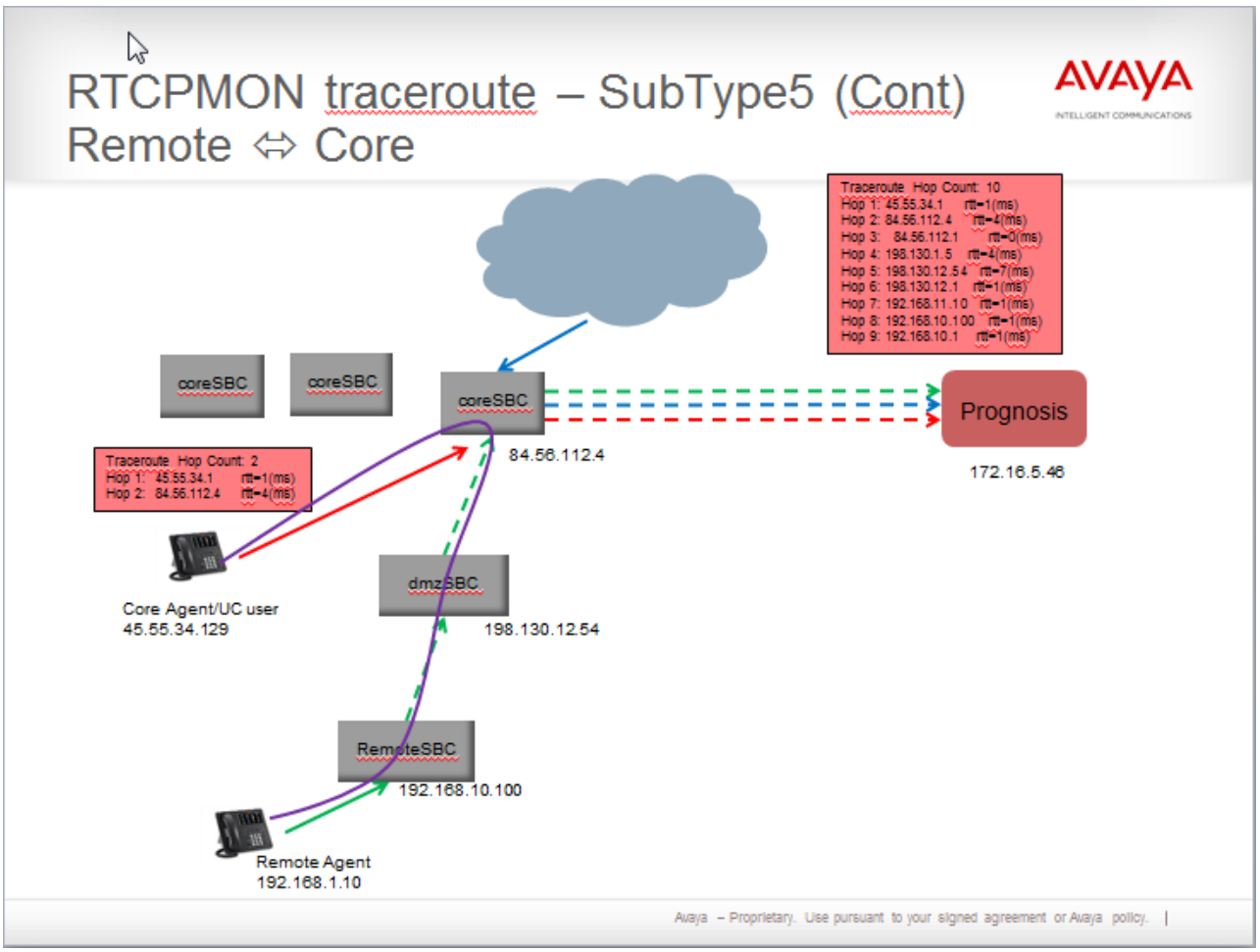
Modes of configuration

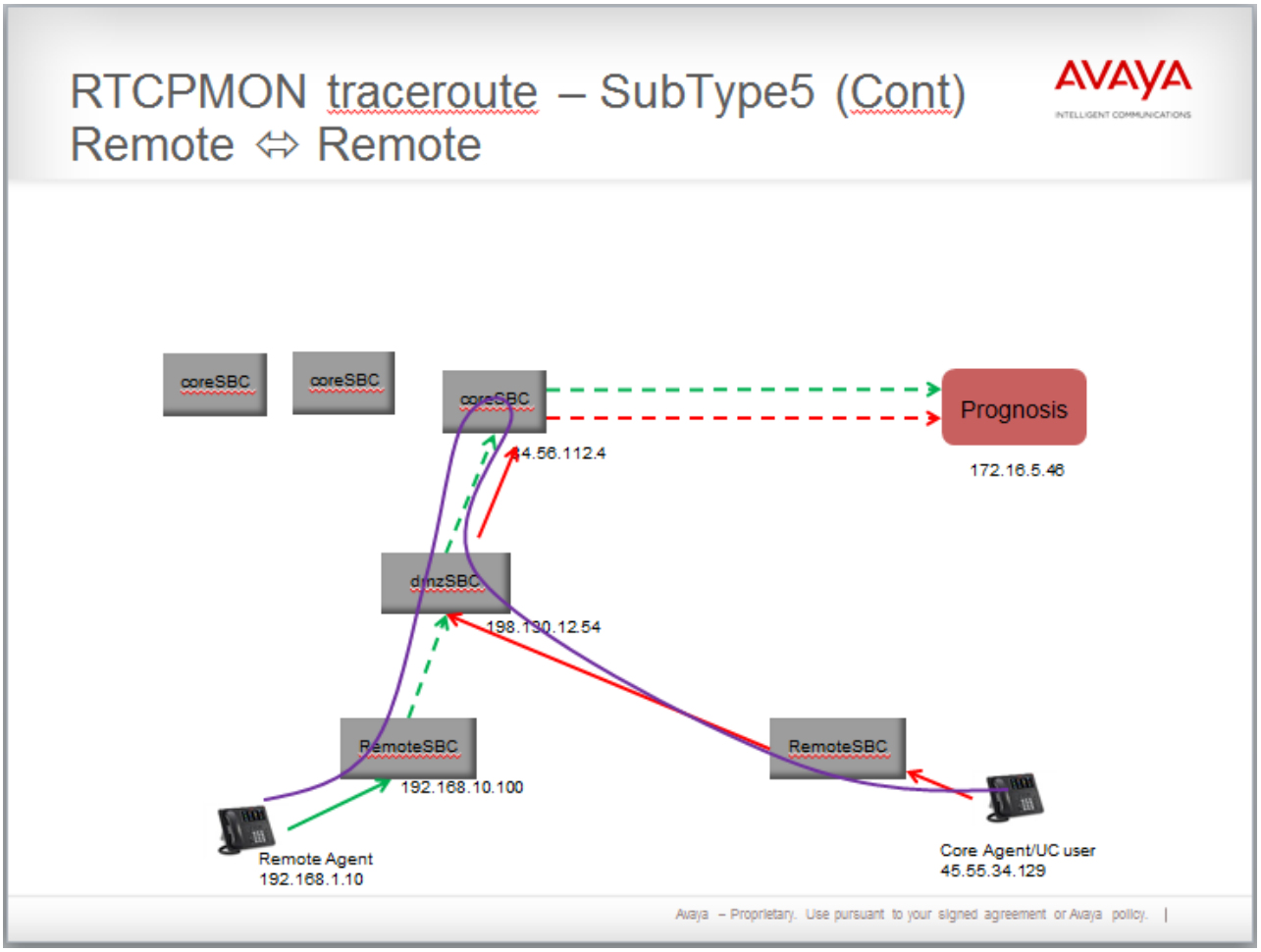
- **END-end Rewrite:** Avaya SBCE updates the RTCP subtype-4 packet from the media terminating endpoint. In Subtype-4, Avaya SBCE rewrites the Remote IP Address field with the Remote endpoint address who is the recipient of the RTCP packets. End-end rewrite must be configured in all Avaya SBCE devices which have media terminating endpoints connected to it directly. No other Avaya SBCE devices exist between that particular Avaya SBCE device and the media terminating endpoints.

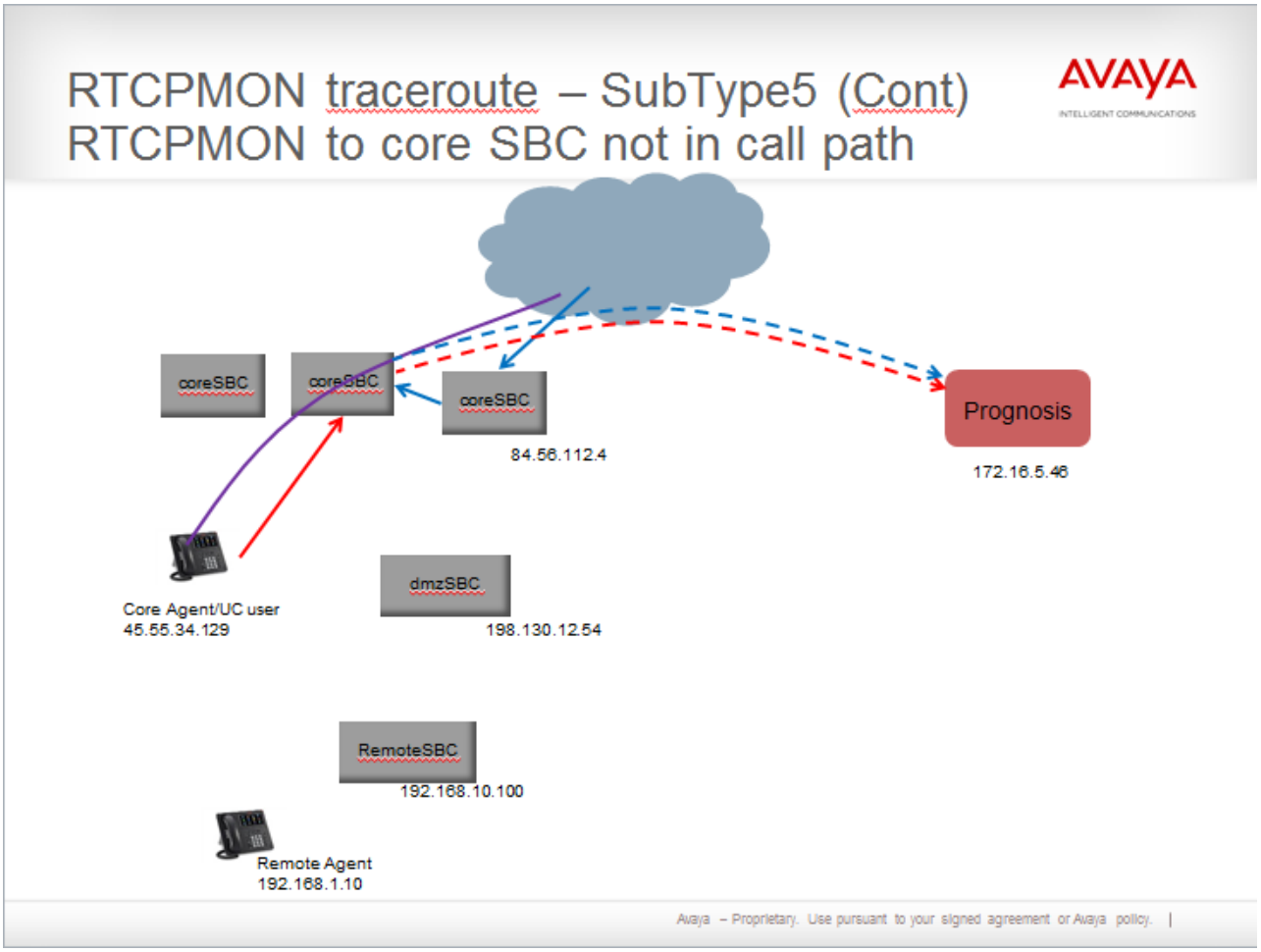
Página2572 de 3226.



- **Hop-by-Hop trace route:** Avaya SBCE updates the RTCP subtype-5 packet with the trace route information. In subtype-5 packet, Avaya SBCE appends the trace route towards the entity to which Avaya SBCE forwards the RTP packet. Avaya SBCE sends the trace route towards the entity from which the Avaya SBCE received the RTP packet. You must configure hop-by-hop trace route for all Avaya SBCE devices.


RTCPMON traceroute – SubType5 (Cont)
Remote ⇔ Core
AVAYA
INTELLIGENT COMMUNICATIONS
Traceroute Hop Count: 10
Hop 1: 45.55.34.1 rtt=1(ms)
Hop 2: 84.56.112.4 rtt=4(ms)
Hop 3: 84.56.112.1 rtt=0(ms)
Hop 4: 198.130.1.5 rtt=4(ms)
Hop 5: 198.130.12.54 rtt=7(ms)
Hop 6: 198.130.12.1 rtt=1(ms)
Hop 7: 192.168.11.10 rtt=1(ms)
Hop 8: 192.168.10.100 rtt=1(ms)
Hop 9: 192.168.10.1 rtt=1(ms)
coreSBC
coreSBC
coreSBC
84.56.112.4
Prognosis
172.16.5.46
Traceroute Hop Count: 2
Hop 1: 45.55.34.1 rtt=1(ms)
Hop 2: 84.56.112.4 rtt=4(ms)
Core Agent/UC user
45.55.34.129
dmzSBC
198.130.12.54
RemoteSBC
192.168.10.100
Remote Agent
192.168.1.10
Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy.


RTCPMON traceroute – SubType5 (Cont)
Remote ⇔ Remote
AVAYA
INTELLIGENT COMMUNICATIONS
coreSBC
coreSBC
coreSBC
Prognosis
172.16.5.48
4.56.112.4
dmzSBC
198.190.12.54
RemoteSBC
192.168.10.100
RemoteSBC
Remote Agent
192.168.1.10
Core Agent/UC user
45.55.34.129
Avaya – Proprietary. Use pursuant to your signed agreement or Avaya policy.



- **Bridging:** Avaya SBCE strips the reverse trace routes added by the Hop-by-Hop trace route and appends this data to the RTCP subtype-5 packet coming from the opposite side. Bridging must be configured only in CORE Avaya SBCE devices.

Note:

If a solution includes only one Avaya SBCE, all these configurations are required.

RTCP monitoring report generation

From Release 7.2.1 and later Avaya SBCE supports RTCP monitoring report generation feature.

Avaya SBCE receives RTCP streams from a trunk that does not have any Avaya specific control information as present in Avaya endpoints

Avaya SBCE generates an RTCP monitoring report that uses this feature. You must configure Avaya SBCE with the IP address of the RTCP monitoring server to send the generated data

This feature is applicable only for SIP trunks.

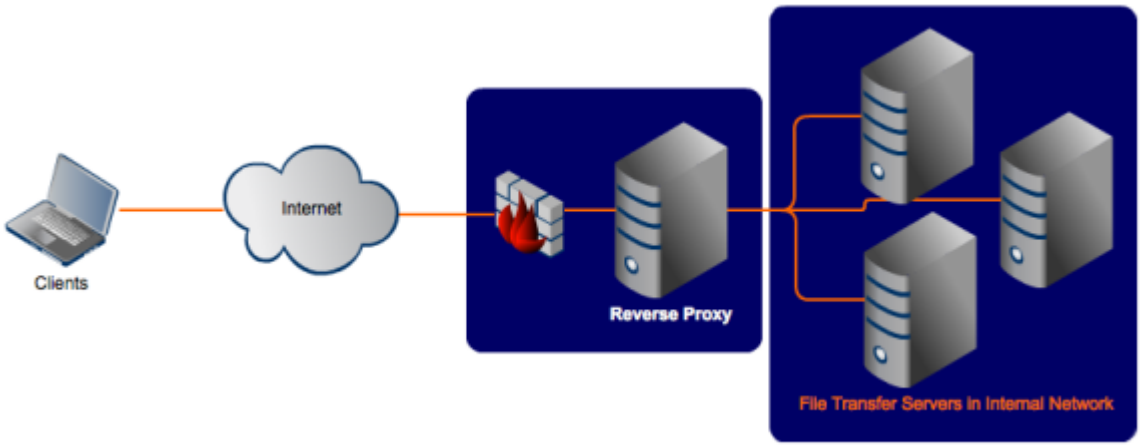
Reverse proxy

A reverse proxy is a web server that terminates connections with clients and makes new connections to backend servers on their behalf.

A backend server is defined as a server to which the reverse proxy makes a connection to fulfill the request from the client. These backend servers can take various forms, and reverse proxy can be configured differently to handle each of them.

A reverse proxy is also known as an inbound proxy, because the server receives requests from the Internet and forwards or proxies them to a small set of servers. The servers are usually located on an internal network and not directly accessible from outside. This proxy is reverse, because a traditional or outbound proxy receives requests from a small set of clients on an internal network and forwards them to the Internet.

The following diagram illustrates the typical configuration of reverse proxy for file transfer servers.



Advantages of Reverse Proxies

- Security:

  A reverse proxy can hide the topology and characteristics of backend servers by removing the need for direct internet access to them. You can place your reverse proxy in an internet facing DMZ, but hide your web servers inside a non-public subnet.

- Caching:

  The reverse proxy can also act as a cache. You can either have a dumb cache that expires after a set period, or better still a cache that respects Cache-Control and Expires headers. This can considerably reduce the load on the backend servers.

- Compression:

  To reduce the bandwidth needed for individual requests, the reverse proxy can decompress incoming requests and compress outgoing ones. This reduces the load on the backend servers that would otherwise have to compress outgoing requests. The reverse proxy makes debugging requests to, and responses from, the backend servers easier.

Página2577 de 3226.

- Simplifies access control tasks:

  Clients only have a single point of access, you can concentrate access control on that single point.

- Aggregating Multiple Websites Into the Same URL Space:

  In a distributed architecture, different pieces of functionality can be served by isolated components. A reverse proxy can route different branches of a single URL address space to different internal web servers.

- Rewriting request URL:

  Sometimes the URL scheme that a legacy application presents is not ideal for discovery or search engine optimization. A reverse proxy can rewrite URLs before passing them on to your backend servers.

- Authentication:

  Reverse proxy can use client certificates to verify the identity of the client.

- Whitelisting of users:

  Whitelisting can be used to block or allow a specific set of user IP addresses to use the reverse proxy service. For example, if you add a whitelisted user IP address, all IPs other than the whitelisted IP are denied access to use the reverse proxy service.

- SSL Termination:

  The reverse proxy handles incoming HTTPS connections, decrypts the requests, and passes unencrypted requests on to the web servers. This has several benefits:

  - Removes the need to install certificates on many backend web servers.
  - Provides a single point of configuration and management for SSL/TLS.
  - Takes the processing load of encrypting or decrypting HTTPS traffic away from web servers.
  - Makes testing and intercepting HTTP requests to individual web servers easier.

Far End Camera Control

Avaya SBCE supports FECC Offer and Answer in SDP. Avaya SBCE checks if the media application line uses the H.224 codec. Any other media application line without an H.224 codec type is ignored.

Avaya SBCE does not negotiate Offer and Answer SDP for the Far End Camera Control (FECC) media application line. Offer and Answer exchange and negotiation is done end-to-end between the sender and receiver. Avaya SBCE does not support mixed encryption because FECC is tied to Media Rules. Therefore, FECC is encrypted if main video is encrypted. Similarly, FECC is on RTP if the main video is on RTP. If FECC is not negotiated in Offer and Answer end-to-end, the principal video channel works without FECC.

Avaya SBCE applies encryption according to SDP Capability Negotiation and SDES by Avaya SBCE policy.

Página2578 de 3226.

Binary Floor Control Protocol

To provide continuous presence during video conferencing, applications use the switched video or the mixed and switched video technique.

Avaya Aura® Conferencing uses the switched video technique to provide continuous presence. Video streams are relayed to all participants so that each participant receives the corresponding multiple video streams from the far ends. Avaya Scopia® uses the mixed video technique where a single video media stream is mixed for all participating users.

Through the video channel, one of the continuous presence streams provides information about the presentation apart from the main video. The presentation channel is through the web and not through a video channel. Switched video streams use only one presentation video channel for multiple main video media streams for each participant. Mixed video devices use one video media stream for presentation. The main video media stream displays participants in one frame. The floor control of this presentation video channel is by Binary Floor Control Protocol (BFCP) messages.

BFCP messages control how multiple video streams access and use the shared video channel.

Detailed description of Binary Floor Control Protocol

In a conference, some applications control access to a shared set of resources. With BFCP, these applications provide users coordinated access to the resources.

Terminologies

To understand how BFCP works, you must be familiar with the following terms:

- **Floor**: A temporary permission to access a specific shared resource or set of resources.
- **Floor chair**: A logical entity that manages a floor.
- **Floor control**: A mechanism that enables applications or users to gain shared or exclusive access to the resource.
- **Floor control server**: A logical entity that maintains the state of the floor, including details such as which floors exist and who holds a floor.
- **Floor participant**: A logical entity that requests floors and related information from a floor control server. In floor-controlled conferences, a floor participant might be co-located with a media participant.

Página2579 de 3226.

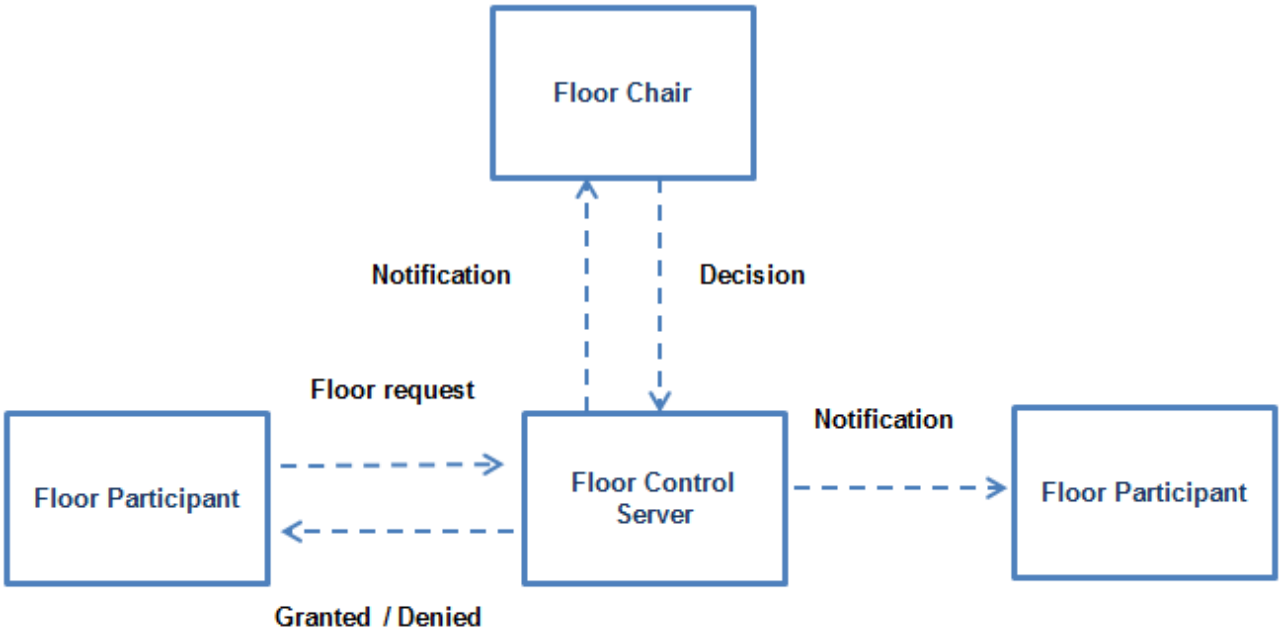


Figure 8: BFCP components

Functioning of BFCP

With BFCP, floor participants can send floor requests to floor control servers and floor control servers can grant or deny access to the requested resource. Also, floor control servers can keep floor participants and floor chairs informed about the status of a given floor or a given floor request.

Avaya SBCE relays BFCP control messages to control the presentation channel. Avaya SBCE supports BFCP for only two video channels, one of which is a video presentation channel.

In this release, Avaya SBCE supports TCP and UDP for the BFCP application.

Avaya SBCE negotiates with Avaya Scopia® MCU or Avaya Scopia® XT clients and obtains the value of the setup attribute as passive. The far-end then starts the TCP connection for the BFCP application. If Avaya SBCE fails to negotiate the setup attribute, the TCP connection is started by Avaya SBCE. However, if the connection is not established due to firewall restrictions, the far-end establishes the TCP connection. All the known attributes, such as floor-control, conf-id, user-id, and floor-id are also relayed in SDP.

SDP Offer and Answer exchange rules

Participants and the floor control server use the SDP offer and Answer exchange rules to establish and authenticate the BFCP connection. Avaya SBCE does not play any role in connection establishment or reestablishment and authentication.

Avaya SBCE negotiates offer and Answer SDP for BFCP based on the following rules:

- Avaya SBCE receives an offer on the incoming leg with the setup attribute as actpass or active. Avaya SBCE answers with the setup attribute as passive with a valid port parameter in the BFCP application line.

Página2580 de 3226.

- Avaya SBCE sends an offer with the setup attribute as passive on the outgoing leg. The far-end entity answers with the setup attribute as active with the discarded port parameter in the BFCP application line.
- Avaya SBCE receives an offer on the incoming leg with the setup attribute as passive.Avaya SBCE answers with the setup attribute as active with a valid port parameter in the BFCP application line. Avaya SBCE tries to start the TCP connection as indicated by the setup attribute as active. The far-end entity starts the TCP connection on the same connection after time out.
- Avaya SBCE receives an offer with the connection attribute as new. Avaya SBCE answers with a connection attribute as new.
- Avaya SBCE receives an offer with the connection attribute as existing. Avaya SBCE answers with a connection attribute as existing.
- Avaya SBCE starts an offer on the outgoing leg with the connection attribute as new for all cases.

Avaya SBCE relays other BFCP application attributes such as floor-ctrl, label, floorid, confid, and userid. Avaya SBCE negotiates these attribute parameters for the end-to-end connection.

Architecture of Binary Floor Control Protocol

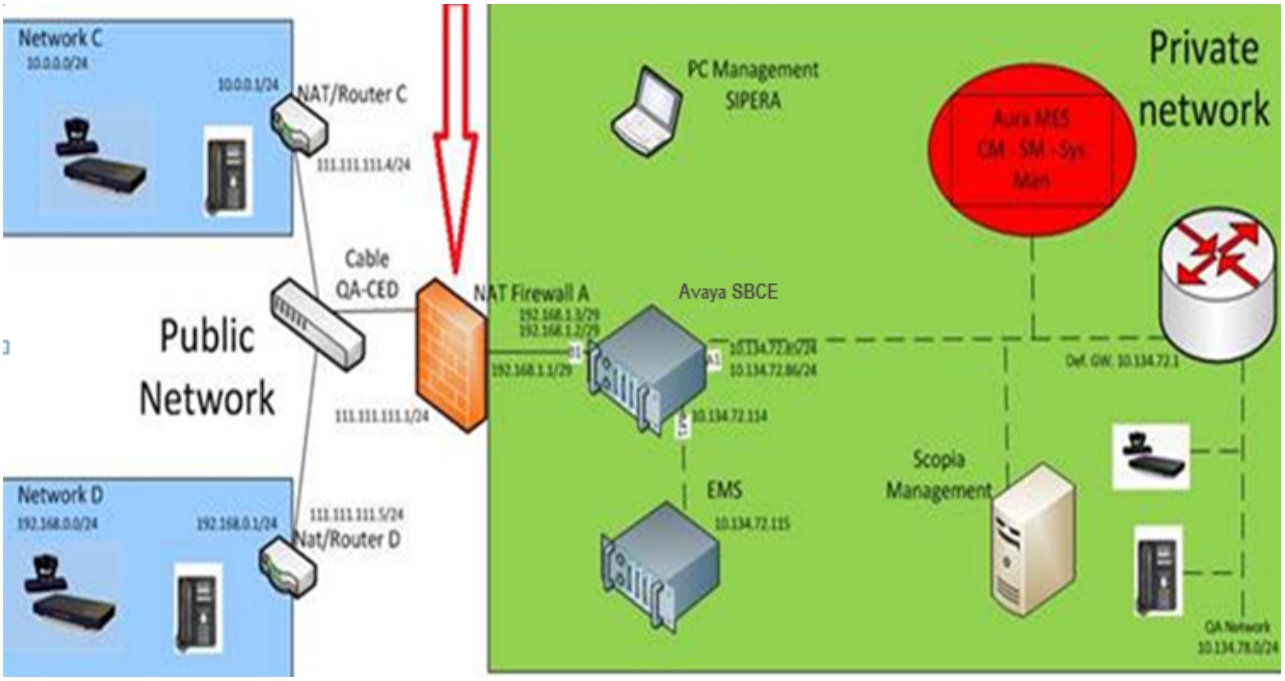


Figure 9: BFCP architecture

An internal firewall exists in most installations on the A1 interface, which is the private interface towards the enterprise. The diagram shows an external firewall on the B1 interface.

Binary Floor Control Protocol scenarios

Examples of scenarios in which BFCP is used and the offer and answer messages for each scenario.

Página2581 de 3226.

Remote Worker XT-client calls XT-MCU

Sr No	Sender	Floor-ctrl	Setup attribute	Connection	BFCP application line
1	Remote Worker XT-client	c-only	actpass	new	Valid connection and port
2	Avaya SBCE	c-only	passive	new	Valid connection and port
3	XT-MCU	s-only	active	new	Discarded port. For example, 9
4	Avaya SBCE (responds to Remote Worker XT-client)	s-only	passive	new	Valid connection and port

The same parameters are exchanged when a Remote Worker XT-client calls Elite-MCU.

Remote Worker XT-MCU calls internal XT-client

Sr No	Sender	floor-ctrl	setup attribute	connection	BFCP application line
1	Remote Worker XT-MCU	c-s	actpass	new	Valid connection and port
2	Avaya SBCE	c-s	passive	new	Valid connection and port
3	XT-client	c-only	active	new	Discarded port
4	Avaya SBCE	c-only	passive	new	Valid connection and port

XT-MCU internal to enterprise dials out and calls XT-client, which is a remote worker

Sr. no	Sender	floor-ctrl	setup attribute	connection	BFCP application line
1	XT-MCU	c-s	actpass	new	Valid connection and port
2	Avaya SBCE	c-only	passive	new	Valid connection and port
3	Remote worker XT-client	c-only	active	new	Discarded port

Table continues…

Sr. no	Sender	floor-ctrl	setup attribute	connection	BFCP application line
4	Avaya SBCE responds to XT-MCU	c-only	passive	new	Valid connection and port

Elite-MCU Release 8.3 internal to enterprise dials out and calls XT-Client which is remote worker

Sr No.	Sender	floor-ctrl	setup attribute	connection	BFCP application line
1	Elite-MCU	s-only	passive	new	Valid connection and port
2	Avaya SBCE	s-only	passive	new	Valid connection and port
3	Remote worker XT-client	c-only	active	new	Discarded port
4	Avaya SBCE responds to Elite MCU	c-only	active	new	Valid connection and port

After Avaya SBCE responds to Elite MCU, Avaya SBCE does not start any TCP connection towards Elite MCU 8.3. Elite MCU 8.3 times out and tries to establish a TCP connection.

Failover or network outage

In a failover or network outage, an entity tries to reestablish a TCP connection on the existing connection. If the entity fails, Avaya Scopia® does not set up the connection again.

Forward Error Correction

Video over IP requires high bandwidth. Transmission of video data over unreliable communication channels might result in packet loss and error. Forward Error Correction (FEC) is a mechanism to control packet loss and errors in data transmission over the IP network. The sender encodes the messages in a redundant way by using the error-correcting code. The redundancy feature enables the receiver to detect errors and correct the errors without retransmission. This mechanism is useful when communication is one way and has multiple receivers.

The FEC mechanism uses the FEC schemes defined in RFC 5445, the FEC building block defined in RFC 5052, and the SDP signaling defined in RFC 5109. Avaya Scopia® uses the proprietary SDP signaling and FEC building blocks and schemes, which are not compatible with the IETF standard.

Página2583 de 3226.

FEC detects errors and protects the principal video but does not protect the data for audio channels. FEC is also applicable for H264/SVC video codecs.

User registration

From Avaya SBCE Release 6.3, you can view the list of users that are registered through Avaya SBCE in the **Registrations State** column on the User Registrations page. You can also enter custom search criteria for the fields that are displayed on the system.

Real Time SIP Server Status

Avaya SBCE Release 6.3 onwards, you can view the current status of the configured SIP servers. The system displays the connectivity status for trunk servers and enterprise call servers. You can use the **Server Status** option of the **Status** toolbar to view the status of the connection. The Server Status screen displays the list of servers based on the settings on the Server Configuration screen.

For the servers to show up in the Status window, you must configure server heartbeat in Server Configuration.

Licensing requirements

Avaya SBCE uses WebLM for licensing requirements. You can install the Avaya SBCE license file on Element Management System (EMS) using the System Management page. Ensure that the license file of the WebLM server displays the product code Session Border Controller E AE. Before you configure the license file, you can view the **License State**, **Grace Period State**, and **Grace Period Expiration Date** fields on the Dashboard page. To install a license file on a newly installed or upgraded EMS, you have a 30-day grace period from the day of installation or upgrade.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

  The primary host ID of WebLM is used for creating the license file.
- Licensed features
- Licensed capacity

All hardware Avaya SBCE devices can use a local WebLM server for licenses. However, for mixed deployment environments with EMS on VMware and Avaya SBCE on hardware, use a WebLM server installed on VMware or System Manager WebLM.

Página2584 de 3226.

Avaya SBCE supports pooled licensing. As opposed to static license allocation, Avaya SBCE dynamically reserves and unreserves pooled licenses when needed. For example, customers with multiple Avaya SBCE devices can use a pool of licenses dynamically across the devices as required.

Single Sign-On and Identity Engine

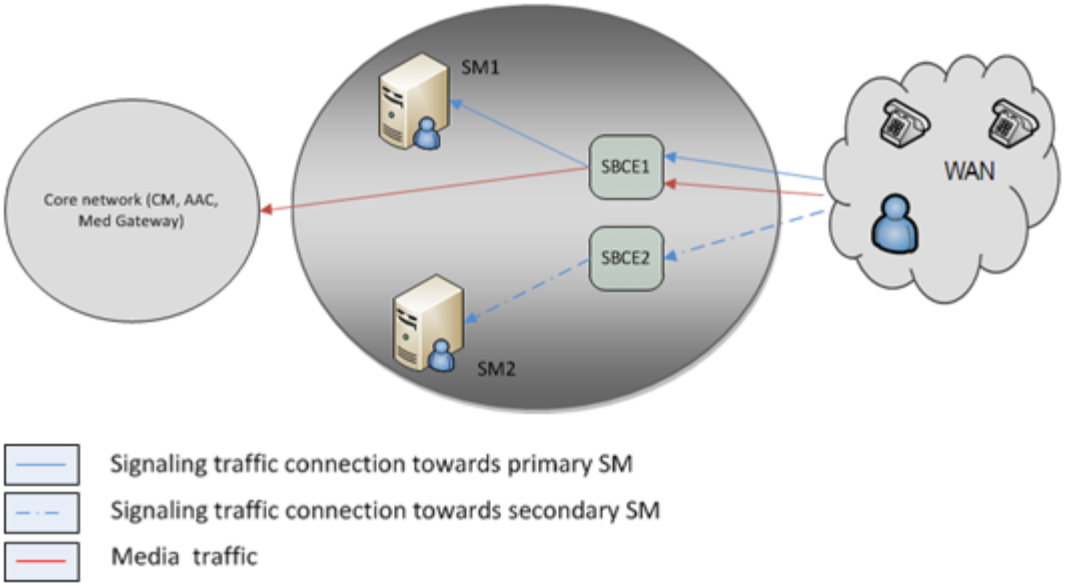
Avaya SBCE uses split DNS for the Single Sign-On and Identity Engine feature. In a split DNS infrastructure, internal hosts are directed to an internal domain name server for name resolution. Internal hosts resolve the IDE domain to an IDE server address. External hosts are directed to an external domain name server for name resolution. External hosts resolve the IDE domain to an Avaya SBCE external address.

Multiple Avaya SBCE deployment

In a Geo-redundant deployment, you can deploy two different Avaya SBCE devices in two different data centers. You can deploy the devices as individual Avaya SBCE devices or devices managed by their own EMS. You can deploy these Avaya SBCE devices in a High Availability mode or a non-High Availability mode.

Multiple Avaya SBCE deployment in the non-HA mode

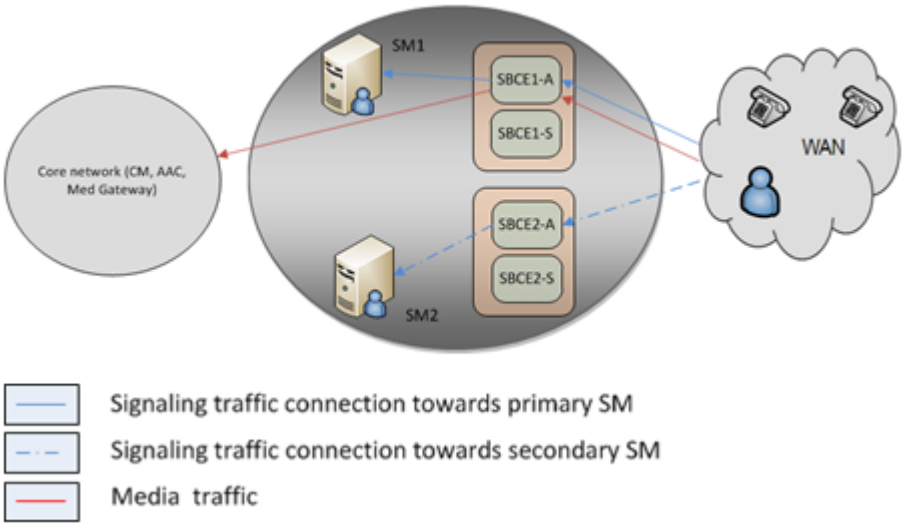
In the following diagram, SBCE1 and SBCE2 are two different physical devices deployed in different data centers. The endpoints have one connection with SBCE1 corresponding to the primary Session Manager, SM1. The second connection with SBCE2 corresponds to the secondary Session Manager, SM2.



Multiple Avaya SBCE deployment in the HA mode

In the following diagram, SBCE1 and SBCE2 are two different physical devices that are deployed in an HA mode in different data centers. The endpoints have one connection with SBCE1-A, that is Active SBCE corresponding to the primary Session Manager, SM1. The second connection is with SBCE2-A, Active SBCE corresponding to the secondary Session Manager, SM2.

During an SBCE1-A fail over, SBCE1-S, which is the standby Avaya SBCE, handles the media of the active calls. During an SBCE2-A fail over, SBCE2-S, which is the standby Avaya SBCE, handles the media of the active calls.



WebRTC-enabled call handling

Avaya SBCE supports incoming calls from WebRTC-enabled web browsers to an internal Avaya Aura® network with SIP at the core. For example, a consumer can call an Avaya Aura® network by using a WebRTC-enabled browser from an external network. This WebRTC call is possible if the organization discloses the organization website to real-time multimedia calls and enables the browser with APIs for real-time multimedia communication. The signaling and media traverse the border edge of the enterprise network that contains the firewall and Avaya SBCE in DMZ. In this scenario, Avaya SBCE, Avaya Breeze™, and Avaya Aura® Media Server together function as the WebRTC-SIP gateway. The signaling and media must traverse the border edge of the enterprise network. Avaya SBCE relays HTTP signaling by using the Reverse Proxy feature and the media relay by using TURN Server relay functionality. Additionally, for a WebRTC call, STUN binding, STUN reflexive address discovery, and ICE connectivity checks are required. All these aspects are implemented within the TURN/STUN server functionality built into Avaya SBCE.

From Release 7.2.1 and later, a WebRTC-enabled browser supports symmetric NAT and multiple IP addresses.

From Release 7.2.2 and later, Avaya SBCE supports TURN using SEND or DATA indication and TURN signalling on TCP, TLS and UDP.

For information about WebRTC performance and capacity, see *Avaya WebRTC Snap-in Reference*.

Virtualization architecture overview

For deployment on VMware-certified hardware, Avaya SBCE is packaged as vAppliance ready (OVA) to run in the virtualized environment. Therefore, from Release 6.3, Avaya SBCE is also available for VMware-based deployments.

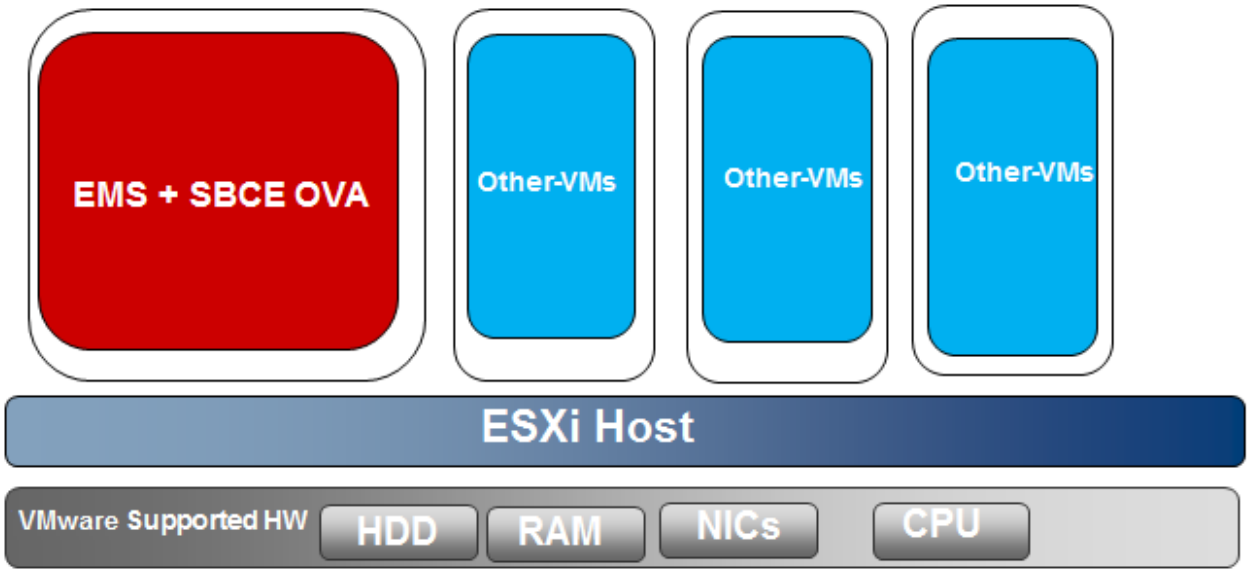
From Release 7.0, a single OVA file is available to deploy EMS and Avaya SBCE.

Avaya SBCE supports VMware features, such as vMotion, HA across data centers, and mixed hardware configurations.

The Avaya SBCE OVA files are offered as vAppliance for EMS and Avaya SBCE configurations. The .ova file is available in Product Licensing and Delivery System (PLDS).

Avaya SBCE standalone mode

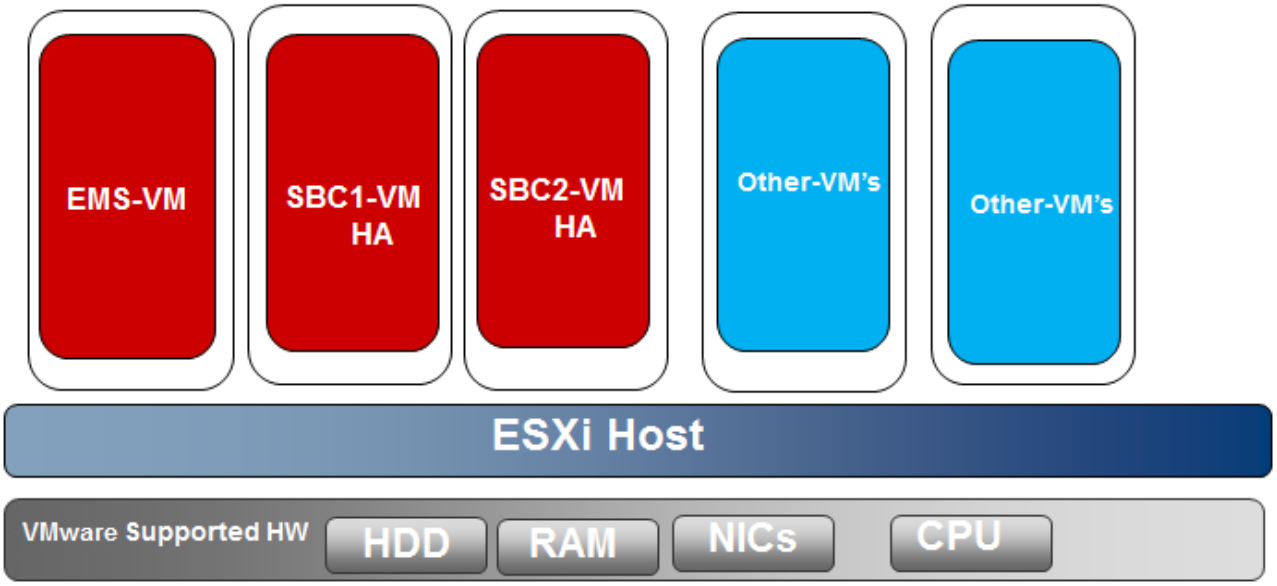
If you select a standalone deployment, the OVA file installs configurations for both Avaya SBCE and EMS.



EMS and SBC in High Availability (HA) mode

For HA mode, deploy the OVA file separately for EMS and Avaya SBCE. From release 7.0, a single OVA file is available to deploy EMS and Avaya SBCE. Therefore, you can use the same OVA file, but choose different configurations to deploy EMS and Avaya SBCE.

Página2587 de 3226.



For more information, see *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*.

Virtual LAN

A Virtual Local Area Network (VLAN) is a logical group of network elements, such as workstations, servers, and network devices spanning various physical networks. A VLAN overlays a virtual layer-2 network on top of a physical layer-2 network by inserting a VLAN tag in the layer-2 header of a packet. VLAN-aware network devices, such as switches, can send packets through the VLAN overlay.

Tag a VLAN to distinctly identify the VLAN as part of a logically different layer-2 network.

The first step for VLAN tagging is to create a VLAN interface. The packets leaving and entering Avaya SBCE on a VLAN use a physical link connected to a physical interface.

The second step is to configure all networks to which Avaya SBCE connects. Each network to which Avaya SBCE connects is defined and attached to an interface.

Note:

A VLAN is supported on data and signaling interface.

SRTP overview

Avaya SBCE supports encrypted audio and multiple video media such as main video, video presentation, and Far End Camera Control (FECC) based on SDP capability negotiation.

If the far-end entity does not support SRTP encryption, Avaya SBCE converts one leg of the call as RTP and the other leg as SRTP by using the SDP negotiation. The conversion between the originating and terminating legs depends on the cipher policy administered on Avaya SBCE.

Avaya SBCE does not use Master Key Index (MKI) and encrypted RTCP for Avaya Scopia® interoperability. Avaya SBCE negotiates the SDP session by using unencrypted RTCP.

Note:

Avaya SBCE supports SRTP calls over SIP, but Avaya Aura® supports SRTP calls only when the call uses the TLS protocol.

SRTP considerations

Avaya SBCE supports:

1. Fallback from SRTP to RTP due to bandwidth limitation or change in call toplogy, such as a media server not supporting SRTP and application of music-on-hold.
2. Upgrade from RTP to SRTP.
3. Conversion from RTP to SRTP between the originating and terminating legs after failover.
4. Modification of keys using REINVITE.
5. Fallback from RTP to SRTP after failover.

Multiple subnet and multiple interfaces

Multiple subnets

With Avaya SBCE, customers can connect to multiple subnets from a single interface. Avaya SBCE supports multiple IP addresses for each subnet and a unique next hop gateway for each IP address. Therefore, you can have multiple subnets on the same interface. The interface can be a physical or a VLAN interface.

Página2589 de 3226.

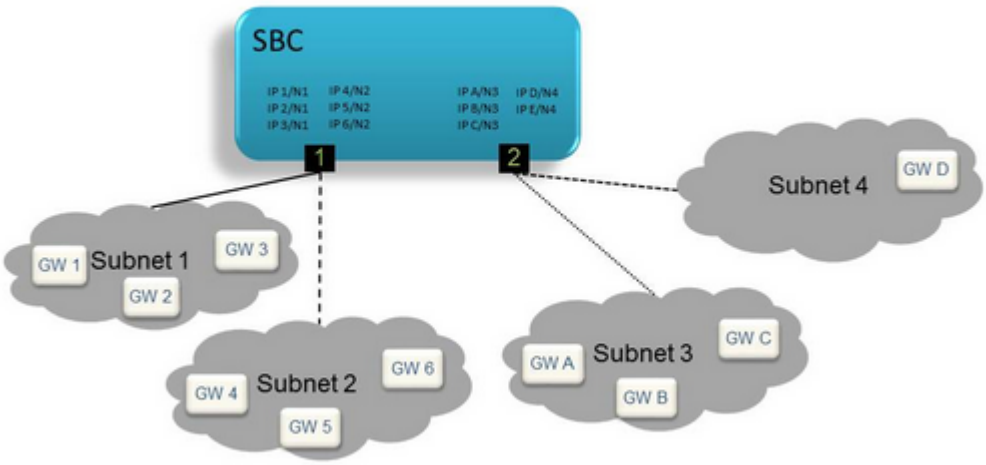


Figure 10: Connectivity to multiple subnets on a single data interface

In Figure 10: Connectivity to multiple subnets on a single data interface on page 49, subnets 1 and 2 are reachable through interface 1, while subnets 3 and 4 are reachable through interface 2.

Overlapping address spaces

You can use multiple subnets to configure cloud-based deployments and multitenancy. In such configurations, Avaya SBCE connects to two or more physically distinct networks that share some or all the IP address space. When you configure overlapped address spaces, multiple endpoints with the same IP address might simultaneously connect toAvaya SBCE. However, Avaya SBCE can distinguish between the connections. Although multiple endpoints use the same IP address, the networks in which the endpoints reside are physically distinct. Avaya SBCE connects to the physically distinct networks by using unique IP addresses in each overlapped address space.

VLAN support

With the virtual LAN (VLAN) capability, a virtual layer-2 network can overlay on a physical layer-2 network by inserting a VLAN tag in the layer-2 header of the packet. Supported network devices can switch such packets through the VLAN overlay. In this release, Avaya SBCE supports VLANs only on the data interfaces.

Página2590 de 3226.

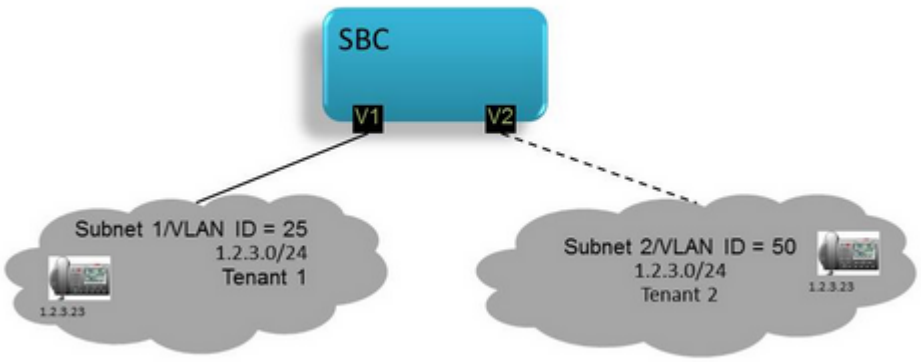


Figure 11: VLAN support

Deployment examples

Avaya SBCE connected to multiple subnets on a single interface

In this scenario, Avaya SBCE connects to multiple subnets on the same data interface.

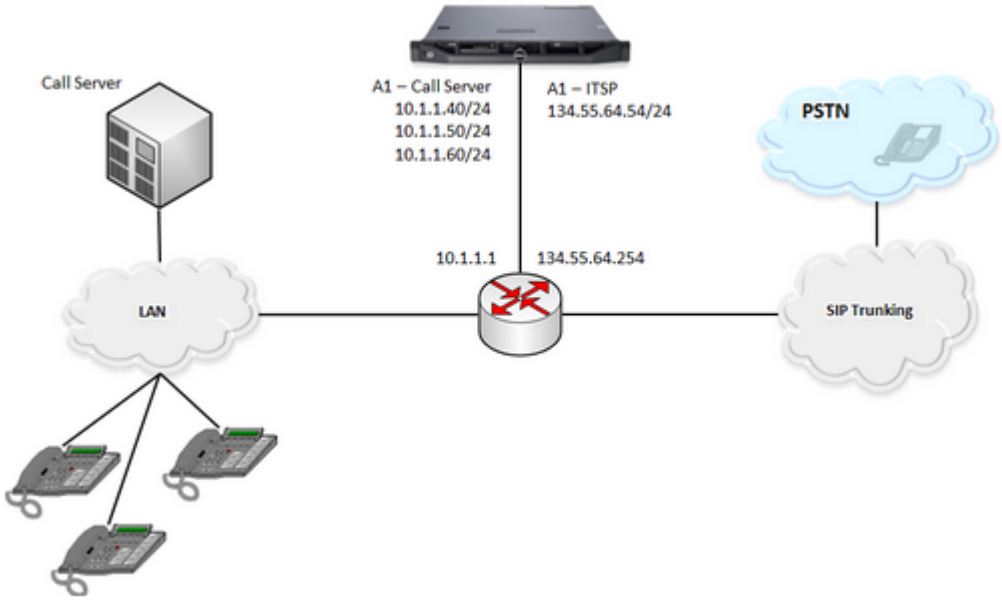


Figure 12: Avaya SBCE connected to multiple subnets on a single interface

Configuration details

- **Interfaces and purposes**: This configuration uses only the A1 Avaya SBCE data interface. With the help of the next-hop router, this data interface provides connectivity to two different

Página2591 de 3226.

networks: the call server network and the ITSP network. This configuration uses three Avaya SBCE IP addresses: two for the call server network and one for the ITSP network.

- **Surrounding networking equipment**: This configuration uses the next-hop router to support multiple gateway addresses on the same physical network connection.
- **Network interfaces**: In this scenario, A1 is enabled. A2, B1, and B2 remain disabled. Enable only one data interface.
- **Networks connected to Avaya SBCE**: In this configuration, two networks are added to the same Avaya SBCE interface. Use the **Device Specific Settings** > **Network Management** > **Networks** tab. Define the call server network first and then define the ITSP network. Thus, to configure multiple networks on the same Avaya SBCE data interface, add the networks to the same interface when you define the networks.

Avaya SBCE connected to multiple subnets on two interfaces

In this scenario, Avaya SBCE connects to a call server on one interface and a trunk server on another.

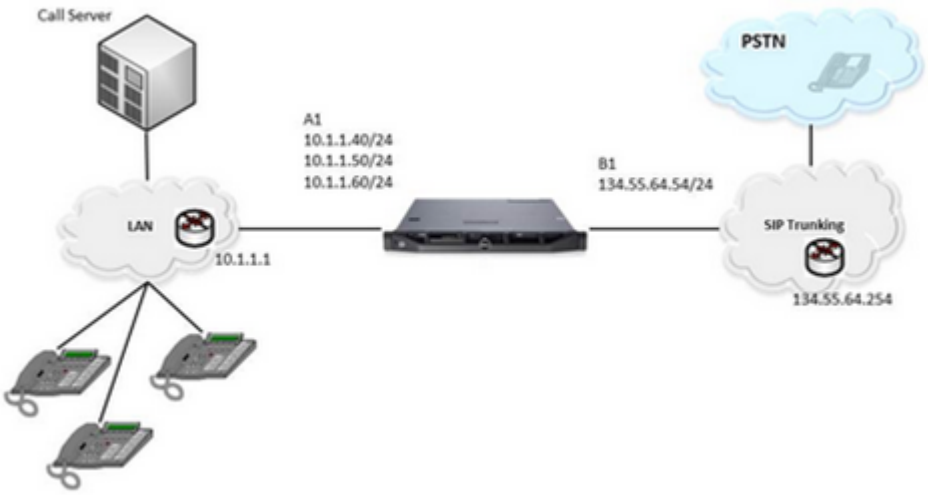


Figure 13: Avaya SBCE connected to multiple subnets on two data interfaces

Configuration details

- **Avaya SBCE interfaces**: This configuration uses four IP addresses: three on the A1 interface and one on the B1 interface.
- **Surrounding networking equipment**: The next-hop routers on both data interfaces do not need to support multiple Avaya SBCE subnets or VLAN tagging.
- **Avaya SBCE network interfaces**: This scenario uses the A1 and B1 interfaces. Ensure that you configure the required interfaces.
- **Networks connected to Avaya SBCE**: In this example, Avaya SBCE connects to two data networks through the A1 and B1 interfaces. Each configured IP address can use a unique next-hop router, if necessary, or the default gateway. Define each network that connects to Avaya SBCE. Use the **Network Management** tab in **Device- Specific Settings** to define the network.

Página2592 de 3226.

- **Other Avaya SBCE setup**: To configure media and signaling interfaces, flows, and routing profiles, see the related sections.

Avaya SBCE connected to multiple subnets by using a single VLAN

In this scenario, Avaya SBCE connects to a combination of VLAN and non-VLAN networks by using a single data interface.

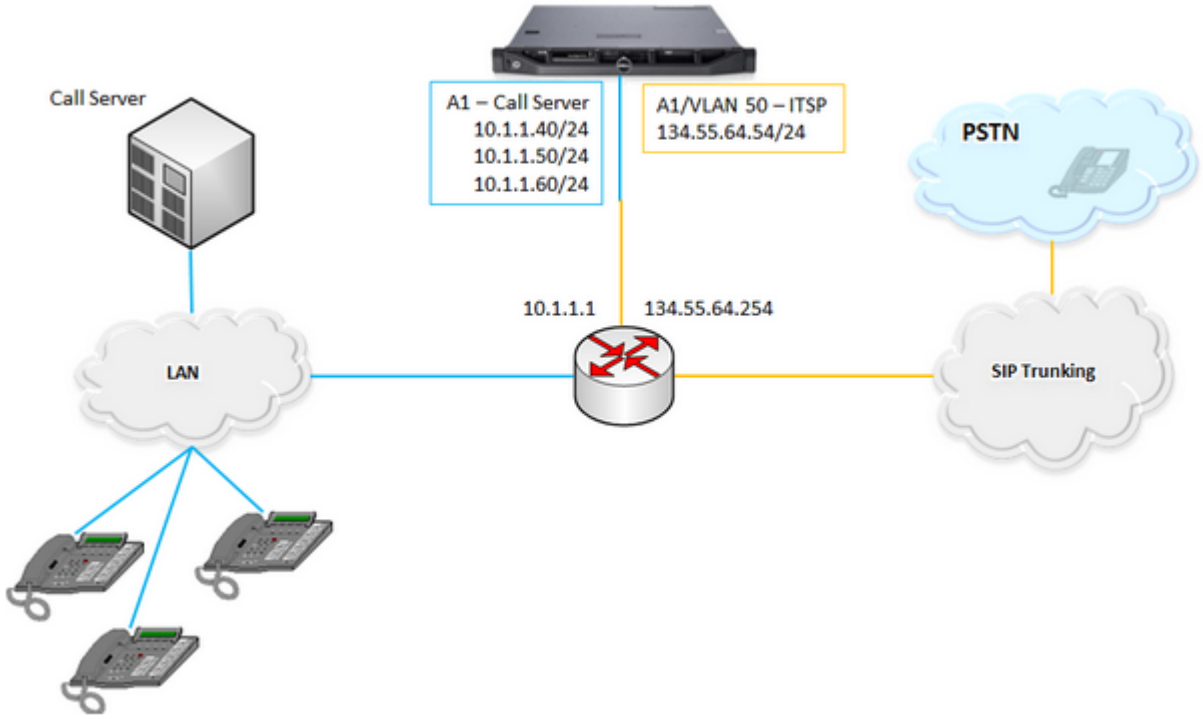


Figure 14: Avaya SBCE connected to multiple subnets, using a single VLAN and a single data interface

Configuration details

- **Interfaces and purposes**: In this scenario, only the A1 Avaya SBCE data interface is used. This data interface provides connectivity to two different networks with the help of the next-hop router: the call server network and the ITSP network. Additionally, one of the networks, the ITSP network, is on a VLAN. Three Avaya SBCE IP addresses are required for the call server network, one VLAN interface on the A1 physical interface, and one Avaya SBCE IP address on the ITSP network.
- **Surrounding networking equipment**: In this example, the next-hop router is configured to support two gateway IP addresses and one VLAN on the same physical port.
- **Network interfaces**: The ITSP network requires VLAN tagging. The ITSP network uses VLAN ID (VID) 50. Packets leaving Avaya SBCE on the ITSP network must contain a VID of 50. To enable VLAN tagging, create a VLAN interface. VLAN interfaces on Avaya SBCE use the underlying facilities of a physical interface A1, A2, B1, or B2. Packets leaving and entering Avaya SBCE on VLAN use the physical link connected to the associated physical interface. Define VLAN interface to connect Avaya SBCE to the ITSP network. Use the **Add VLAN** button located in the **Device Specific Settings** > **Network Management** > **Interfaces**

Página2593 de 3226.

tab. Initially, keep the VLAN interface disabled. Then enable both the A1 and ITSP VLAN interfaces while other interfaces remain disabled.

- **Networks connected to Avaya SBCE**: In this example, the ITSP network connects to the VLAN interface on top of the physical A1 interface. Define the call server network in the same way as in other multiple subnet scenarios. Define the ITSP network and use the new VLAN interface.

Multiple gateways on the same network

This configuration includes two gateway routers and two call servers connected to the call server network. In this configuration, only the second gateway can route calls to the second call server.

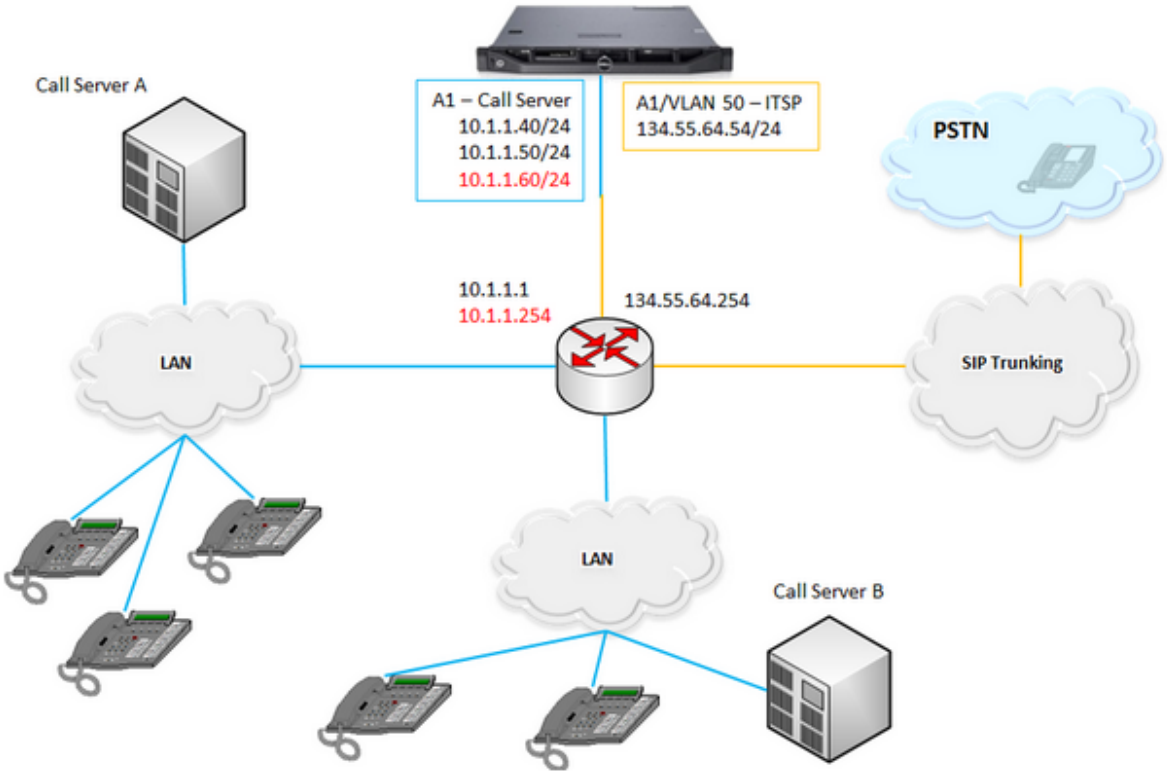


Figure 15: Multiple gateways on the same network

Configuration details

- **Interfaces and purposes**: Only one Avaya SBCE interface connects to both, the call server and ITSP networks. Because the call server network has multiple gateway routers , one of the Avaya SBCE IP addresses on that network provides call routing capabilities to call server B.
- **Surrounding networking equipment**: The next-hop router supports three gateway IP addresses and one VLAN on the same physical port. Two gateway IP addresses are on the call server network, and one is on the ITSP network. The 10.1.1.1 gateway address is the default gateway on the call server network. Additionally, Avaya SBCE uses the 10.1.1.254

Página2594 de 3226.

gateway to reach call server B, as the default gateway in this example is unable to reach the network.

- **SBC Network Interfaces**: The configuration of the call server and ITSP network interfaces is the same as in the earlier scenarios.
- **Networks connected to Avaya SBCE**: The ITSP network configuration is the same as in the earlier examples. For each attached network, define a default gateway router. Each Avaya SBCE IP address on the network can override the default gateway IP address, if necessary. For example, Avaya SBCE uses 10.1.1.254 as the next-hop router instead of 10.1.1.1.

traceSBC tool

The tcpdump tool is the main troubleshooting tool of Avaya SBCE, which can capture network traffic. Using tcpdump is a reliable way to analyze the information arriving to and sent from Avaya SBCE. However, tcpdump has its own limitations, which can make troubleshooting difficult and time consuming. This traditional tool is not useful in handling encrypted traffic and real-time troubleshooting.

SIP and PPM traffic is encrypted especially in Remote Worker configurations. Checking encrypted traffic with a network capture is difficult and time consuming. The delay occurs because the unencrypted private key of the Avaya SBCE is needed to decrypt the TLS and HTTPS traffic.

The traceSBC tool offers solutions for both issues. traceSBC is a perl script that parses Avaya SBCE log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, you can use the tool easily even in case of TLS and HTTPS. traceSBC can parse the log files downloaded from Avaya SBCE. traceSBC can also process log files real time on Avaya SBCE, so that you can check SIP and PPM traffic during live calls. The tool can also work in the noninteractive mode, which is useful for automation.

SIP and PPM logging administration

Starting from Release 6.3, SIP logging is always enabled by default. You can enable PPM, STUN, TLS, and AMS logging, if required.

Log files

Avaya SBCE can log SIP messages as processed by different subsystems and also log PPM messages. The traceSBC utility can process the log files real-time by opening the latest log files in the given directories. traceSBC also checks regularly if a new file is generated, in which case the old one is closed and processing continues with the new one. A new log file is generated every time the relevant processes restart, or when the size reaches the limit of ~10 M.

Log locations:

SIP messages are found at `/archive/log/tracesbc/tracesbc_sip/` and PPM messages can be found at `/archive/log/tracesbc/tracesbc_ppm/`.

Active files are of the following format:

```
-rw-rw---- 1 root root 112445 Aug 21 10:12 tracesbc_sip_1408631651
```

Página2595 de 3226.

Inactive or closed files are of the following format:

```
-rw-rw---- 1 root root 175236 Aug 21 06:33
tracesbc_sip_1408617250_1408620820_1
```
or

```
-rw-rw---- 1 root root 31706 Jul 10 13:34
tracesbc_sip_1436549674_1436553270_1.gz
```

Advantages

Memory

After 10000 captured messages, traceSBC stops processing the log files to prevent exhausting the memory. This check is done during the capture when the tool is parsing the log files. The tool counts the number of SIP and PPM messages in the logs. This number is not the number of messages sent or received on the interfaces. This counter is a summary of messages from all logs, not for each log. Note that this safeguard is present only for real-time mode. When the tool is used in nonreal-time mode, this counter does not stop processing the logs specified in the command line. The counter continues processing the logs specified in the command line to be able to process more files or messages in off-line mode.

Processor

A built-in mechanism is available to prevent high CPU usage. Throttling is not tied to CPU level. In the current implementation, throttling is done by releasing the CPU for a short period after each line of the file is processed. The result is that CPU occupancy is low on an idle system when the tool actively processes large log files. You can disable throttling by the –dt command line parameter which can be useful when processing large log files offline. However, in this case CPU occupancy might go up to 100%, and so you must not use this option on a live system.

Avaya SBCE support for Serviceability Agent

Avaya SBCE contains Serviceability Agent which monitors faults on the system. Serviceability Agent sends SNMPv2c and SNMPv3 notifications to configured destinations through the net-SNMP master agent.

With the support for Serviceability Agent, you can use Avaya SBCE to:

- Manage SNMPv3 users.
- Manage SNMP trap destinations.
- Create, edit, and view SNMP trap profiles.

For optimum security, enable only SNMP v3 with authentication and privacy modes. Customers who have upgraded from a version earlier than 7.1, can enable SNMP versions v1 and v2c, if required. However, customers are responsible for security risks related to using SNMP versions v1 and v2c. From Release 7.1, for new installations of Avaya SBCE, SNMP v1/v2 configuration is unavailable.

To ensure that you can view Avaya SBCE alarms on System Manager, you must upload the common alarm definitions file (cadf) to System Manager. For more information about uploading the cadf file, see *Administering Avaya Session Border Controller for Enterprise*.

Página2596 de 3226.

Multi-tenancy

Avaya SBCE achieves multi-tenancy using multiple tenants, call servers, and Avaya SBCE interfaces.

This scenario uses all four Avaya SBCE data interfaces. Avaya SBCE connects to two tenant networks, each with a unique set of remote workers. Avaya SBCE also connects to three other networks, each with a call server. Each call server is reached through a separate physical interface, which provides a measure of redundancy when one or more call servers stop responding.

Configuration example 1 : Multi-tenancy using multiple tenants, call servers, and Avaya SBCE interfaces

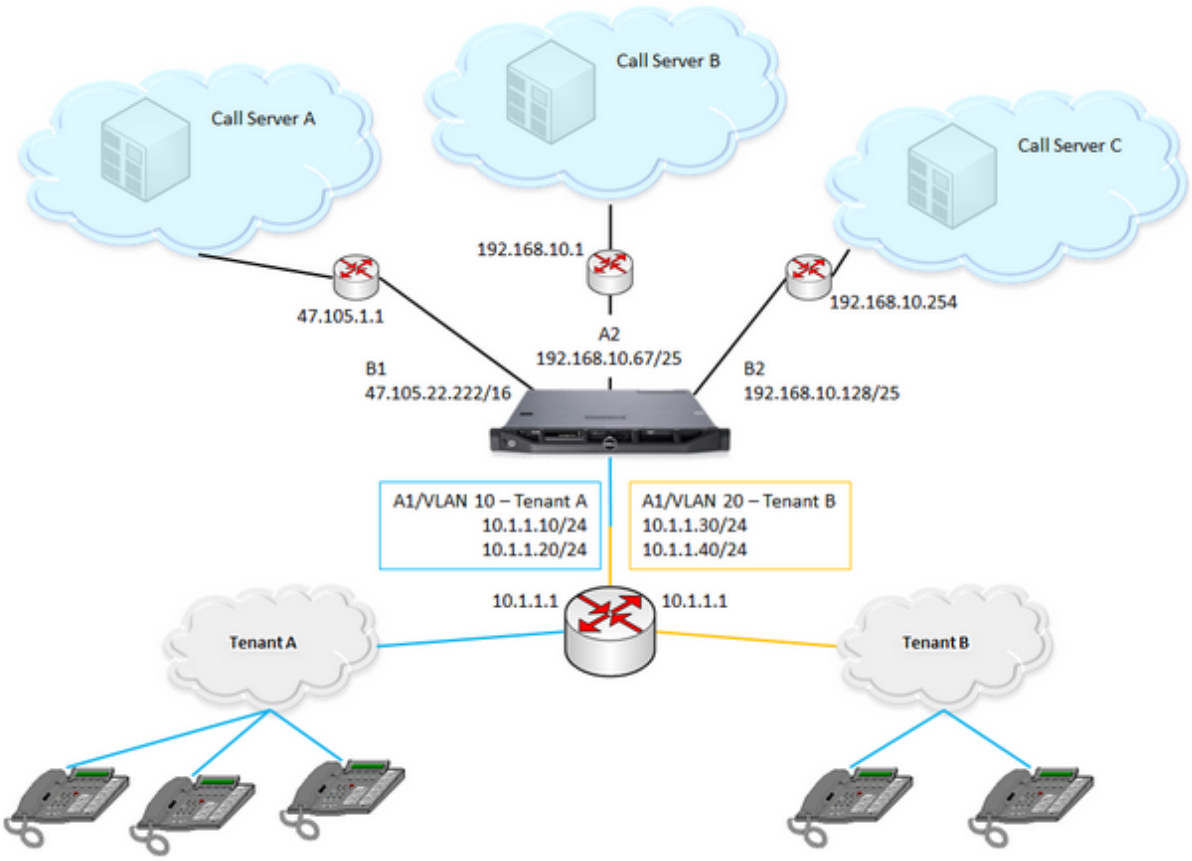


Figure 16: Multiple tenants, call servers, and Avaya SBCE interfaces

- **Interfaces and purposes**: The A1 interface of Avaya SBCE provides connectivity to tenant subnets. Each subnet uses a unique VLAN tag: tenant A (in blue) is on VLAN 10, while tenant B (in orange) uses VLAN 20. The gateway router on the A1 interface provides connectivity to both tenant VLANs.

  The B1 interface provides connectivity to call server A, A2 connects Avaya SBCE to call server B, and B2 connects the network containing call server C.

Página2597 de 3226.

Note:

You can attach tenants to the B1 interface and connect call server A through the A1 interface. The physical ports retain their historical names: A1, A2, B1, and B2.

- **Surrounding networking equipment**: This configuration supports corresponding mapping between SBC NICs and physical server NICs. Configure the gateway on the A1 interface to support VLAN 10 and VLAN 20, and the associated gateway IP addresses. You do not need to configure the other three gateways on A2, B1, or B2 separately. If Avaya SBCE is running on a virtual machine, configure VMWare vSwitch and the physical interfaces on the server. If each physical interface on Avaya SBCE uses a separate vSwitch and each vSwitch connects to a separate physical interface on the server, connect vSwitch to a physical port setup. Configure up to four vSwitches.
- **Avaya SBCE Network interfaces**: When you configure VLANs on Avaya SBCE, the first step is always to create the VLAN interfaces. In this example, two VLAN interfaces are created to support the two tenant networks. First, the VLAN for tenant A on interface A1. Then, the VLAN for tenant B on A1. The remaining networks use physical interfaces on Avaya SBCE. Finally, enable all the interfaces: the two VLANs as well as A2, B1, and B2.
- **Networks connected to Avaya SBCE**: In this example, Avaya SBCE is attached to five networks. For each attached network, define a default gateway router, beginning with tenant A, followed by tenant B, call server A, call server B, and finally call server C.

Configuration Example 2 : Multi-tenancy using the same IP address

Avaya SBCE supports the use of the same IP address on multiple data interfaces in Avaya SBCE. Customers often share the same address space and service IP address while using multitenant and cloud features. With support for using the same IP address more than one time, more than one customer can use the same IP address to connect to Avaya SBCE.

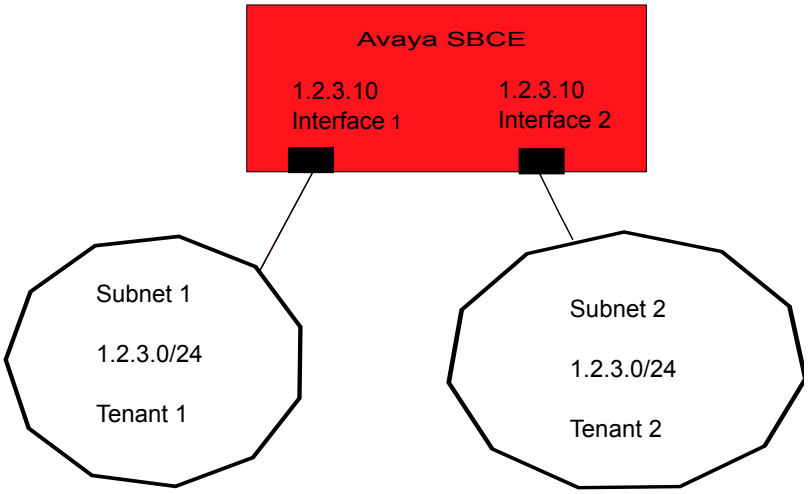


Figure 17: Same IP address used on different interfaces

To permit the use of multiple instances of the same IP, the instances must exist on separate network interfaces, virtual network interfaces, or both. Avaya SBCE separates interface definition from network definition as follows:

- An interface is a combination of a physical port such as A1, A2, B1, and B2, and a vlan ID. A vlan ID can be **no vlan**.

Página2598 de 3226.

- A network ties a set of Avaya SBCE IPs and gateways with an interface.

Therefore, for two instances of 1.2.3.0 on Avaya SBCE, you must define two interfaces and two networks, so that 1.2.3.0 occurs exactly once within each network.

In this scenario, Avaya SBCE connects to two tenant networks, each with a unique set of remote workers. However, the same IP address is assigned on Avaya SBCE on both the tenant networks.

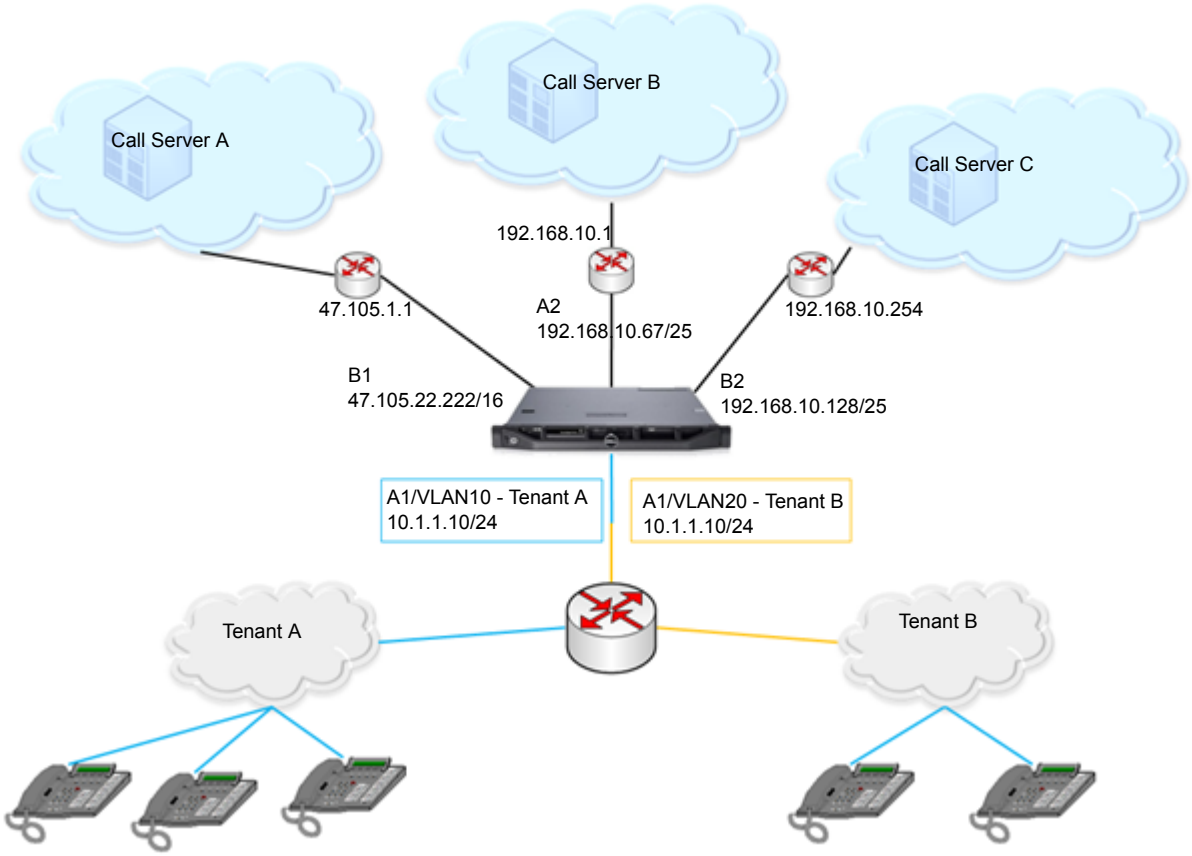


Figure 18: Multiple tenants using the same IP address

The following sections describe the configuration details for this deployment example.

Interfaces and purposes:

The A1 interface of Avaya SBCE provides connectivity to tenant subnets. Each subnet uses a unique VLAN tag: tenant A, highlighted in blue, is on VLAN 10, while tenant B, highlighted in orange, uses VLAN 20. The gateway router on the A1 interface provides connectivity to both tenant VLANs.

The B1 interface provides connectivity to call server A, A2 connects Avaya SBCE to call server B, and B2 connects the network containing call server C.

Surrounding networking equipment:

Configure the gateway on the A1 interface to support VLAN 10 and VLAN 20, and the associated gateway IP addresses. As the Avaya SBCE address on both tenants is the same, the gateway must be able to distinguish between the addresses for both tenant networks.

Página2599 de 3226.

Network interfaces:

To use the same IP address on Avaya SBCE multiple times, select the **Allow Non-unique IPs for Complex Networks** field on the Network Options page. To configure VLANs on Avaya SBCE, create VLAN interfaces. In this example, two VLAN interfaces are created to support the two tenant networks:

- The VLAN for tenant A on interface A1
- The VLAN for tenant B on A1

The remaining networks use physical interfaces on Avaya SBCE. Finally, enable all the interfaces: the two VLANs as well as A2, B1, and B2.

In this example, the Avaya SBCE is attached to five networks. For each attached network, define a default gateway router and Avaya SBCE IP addresses. Begin with tenant A, followed by tenant B, call server A, call server B, and finally call server C.

Support for IP Office trunk from a dynamic IP address

Avaya SBCE supports an IP Office trunk originating from dynamic IP addresses. The external address of the ISP router or firewall at the remote site is based on Dynamic Host Configuration Protocol (DHCP). Therefore, a static external IP address is unavailable for configuration or installation.

Instead, in the server configuration for Remote Branch Office servers, you can administer an FQDN pointing to a Dynamic DNS record. If the TLS connection from the Remote Branch Office drops, Avaya SBCE resolves the FQDN entry again for all Remote Branch Office servers. If the DNS record TTL value expires, Avaya SBCE queries the DNS for all FQDN entries in the server configuration.

Note:

If a DNS lookup fails, Avaya SBCE tries the DNS lookup every 30 seconds for the first 10 failures and then every 3000 seconds.

Reuse of connection established by IP Office for delivering calls

Avaya SBCE reuses the TLS connection from IP Office for SIP signaling towards the IP Office. The routing profile towards the Remote Branch Office must use a routing entry that matches the server configuration for the Remote Branch Office. For Remote Branch Office routing entries, the transport must be TLS and the **Port** field must be empty.

Avaya SBCE rejects the incoming TLS connection from IP Office if the:

- Required TLS Client Certificate is not configured in IP Office.
- Self-Signed Certificate is presented by IP Office during TLS handshake.
- Peer Verification fails in Avaya SBCE with the TLS Client Certificate presented by IP Office.

If the TLS connection from the Remote Branch Office drops, Avaya SBCE rejects calls originating from the enterprise until the connection is reestablished. Meanwhile, Avaya SBCE displays a 500 server internal error message.

Note:

You can provide custom route entries with the IP Office listen port if you administer DNAT rules in the Firewall or the NAT router.

Secure Client Enablement Services proxy

Client Enablement Services (CES) provides access to many Avaya Unified Communications (UC) capabilities, including telephony, mobility, messaging, conferencing, and Presence Services through a single application. Avaya one-X® Mobile communicates with the CES server by using the CES protocol. To provide CES services to Avaya one-X® Mobile clients outside the enterprise network, Avaya SBCE provides a secure proxy that must be deployed in the enterprise DMZ. Avaya SBCE checks all traffic from Avaya one-X® Mobile clients outside the enterprise network to the CES server.

When a new connection is established from an Avaya one-X® Mobile outside the enterprise network:

- Avaya SBCE checks whether the first message from the Avaya one-X® Mobile device is a login request and forwards the message to the CES server. Avaya SBCE drops all messages received from the Avaya one-X® Mobile device before the login request.
- The CES server authenticates Avaya one-X® Mobile or sends an error message to Avaya SBCE. After authentication failure, Avaya SBCE rejects all subsequent messages from the Avaya one-X® Mobile.
- After authentication, Avaya SBCE forwards all messages from Avaya one-X® Mobile to the CES server.

Avaya SBCE maintains statistics for all login attempts. Avaya SBCE supports at least 10,000 Avaya one-X® Mobile clients on Dell R630 and HP DL360 G9.

Support for integrated Dell Remote Access Card and integrated Lights-Out

Dell Remote Access Controller (DRAC) and HP integrated Lights-Out (iLO) are management tools. These tools provide powerful remote server management features, including control to remotely turn a server on or off. You can use DRAC features to troubleshoot and diagnose issues during a remote server restart. From Release 7.0 onwards, Avaya SBCE supports the following features of the iDRAC Express Card:

- System Provisioning: You can install Avaya SBCE ISO by using iDRAC provisioning features.
- System monitoring and management: You can monitor the status of the server by using iDRAC features.

Página2601 de 3226.

You can buy the iDRAC card with or without the server. For Dell servers later than the 600 series, the iDRAC express card is part of the base configuration. For these servers, you need not install, back up, or manage another license for the iDRAC express card. However, to upgrade from the express version to the enterprise version, you must buy another license directly from Dell. Similarly, to upgrade from iLO 3 to iLO 4, you must purchase another license from HP.

For more information about installing and using iDRAC, go to http://www.support.dell.com/ and see *Integrated Dell Remote Access Controller User's Guide*.

Supported hardware platforms

Avaya SBCE supports Dell iDRAC and HP iLO on the following platforms:

Platform	iDRAC and iLO support
Portwell CAD 0208	Does not support iDRAC and iLO.
Dell R210 II and R210 II XL	Does not support iDRAC.
Dell R320	Does not support iDRAC.
Dell R620	Does not support iDRAC.
Dell R630	Supports iDRAC 8 express.
HP DL360 G8	Does not support iLO.
HP DL360 G9	Supports iLO 4.

Important:

Dell R210 II and Dell R320 servers do not support iDRAC interfaces, therefore these servers do not support iDRAC.

Previous generation servers have cipher 0 vulnerabilities. Therefore, do not use iDRAC and iLO when iDRAC and iLO are not included with the platform.

SIPREC-based recording solution

Avaya SBCE supports a SIP-based media recording (SIPREC) solution with the following components:

- Avaya SBCE as the SIP Recording Client (SRC)
- Avaya Contact Recorder as the SIP Recording Server (SRS)
- Application Enablement Services for CTI integration
- Contact Center Application Servers such as Avaya Aura® Contact Center and Call Center Elite
- Media anchor points such as Avaya Aura® Media Server or Communication Manager Media Gateway

Página2602 de 3226.

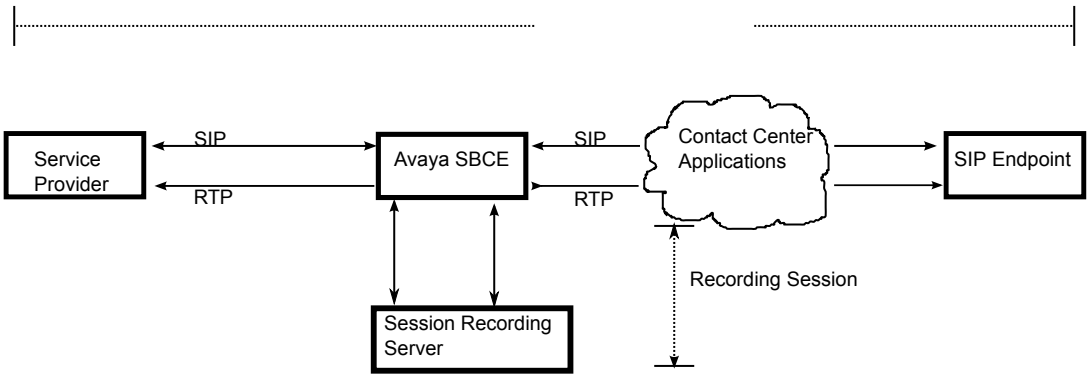


Figure 19: SIPREC-based recording solution architecture

With the SIPREC-based recording solution, Avaya SBCE supports full-time session recording, selective recording, and continuous recording. With full-time session recording, every communication session connected by using Avaya SBCE is recorded.

The recording servers can be colocated with the Avaya SBCE or distributed in different locations. If the SRS and Avaya SBCE are at different locations, ensure that the network does not require Network Address Translation between the SRS and Avaya SBCE devices. You must deploy the Avaya SBCE and Recording Server in a trusted, secured network for privacy and security of the recorded media.

You must have a SIP trunk on Avaya SBCE to ensure that SIPREC functions correctly.

Features for session recording

The following Avaya SBCE features support the recording solution:

- Initiation, modification, and termination of recording session from the SIP Recording Server (SRS) during the recording session.
- Early media clipping avoidance during session setup.
- Wave file played to indicate that the session is being recorded.
- Alternate routing for recording sessions with Round Robin load balancing.

  When a recording session starts, Avaya SBCE starts a timer. When the timer expires, Avaya SBCE triggers alternate routing mechanisms. Avaya SBCE also uses alternate routing mechanisms after receiving the following messages from the recording server: 408,480,486,488, 500, and 503.
- High Availability for the recorder media stream and metadata sent to the Recording Servers.
- Recording Server routing.

  Avaya SBCE communicates with a cluster of Recording Servers. You must administer a URL for each Recording Server in the cluster. Avaya SBCE sends an INVITE message to the Recording Server. When Avaya SBCE sends the Contact URI with the feature tag +sip.src in the INVITE message to the SRS, the SRS identifies a recording session.
- Metadata elements to identify media streams from SRC and SRS.

  Avaya SBCE provides the following metadata elements:

Página2603 de 3226.

Metadata element	Supporting parameter
Call identifier	UCID
Session Identifier	sdp session id
Participant Identifier	PAI
Stream Identifier	Label on media stream
Stream direction	send, recv and inactive
Timestamp for resynchronization	NA

- No controls from the trunk side of the recording sessions.

  Avaya SBCE uses only the controls specified from Avaya SBCE and at the recording server.

- Unique labels that is the media labels for media streams to identify the media stream for participants in the recording session. Media labels are applicable only for the audio recording.

  From Release 7.2.2.2, to identify the trunk and the enterprise, the value of the media stream from a trunk must be less than the value of media stream coming from an enterprise.

- Security options.

  Avaya SBCE supports an SAVP profile for SRTP sessions and an AVP profile for RTP sessions. Avaya SBCE supports TLS and TCP connection. ACR supports TCP connection with SIP uri scheme using RTP/AVP and SAVP profile.

  Note:

  For SIPREC, Avaya SBCE supports SRTP only with hmac80, because ACR does not support any other cryptographic algorithm.

- REFER handling and redirection supported in recording scenarios.
- SIP recording in translator mode. Avaya SBCE receives media streams and relays them to the Recording Server. Avaya SBCE does not change any data in the media streams.

In addition, from Release 7.1, Avaya SBCE provides the following features:

- Support for full-time, selective, and continuous recording.
- Support for call termination on recording failure.

  When Avaya SBCE initiates a session towards every configured recording server, there can be scenarios when none of the servers respond. In such scenarios, Avaya SBCE can terminate the session that is initiated or in progress towards the calling or called party. Call termination on recording failure is not supported for remote worker calls.

- Support for recording a remote worker to remote worker call.
- Support for recording in case of downstream forking.

  If Avaya SBCE received multiple forked dialogs, the first dialog received with early media is recorded. Subsequent early media in forked dialogs is not recorded. For final answer, the media stream between the calling and final answered party is recorded.

Selective recording

From Release 7.1, Avaya SBCE supports selective recording. For selective recording, media is streamed continuously, similar to full-time recording. However, the recording server masks recorded streams until the system detects Computer Telephony Integration (CTI) events. Therefore, only a portion of the communication session is recorded when the Recording Server cuts through the media stream after receiving CTI events.

With selective recording, bandwidth and processing cycles are conserved because media streams do not flow through the network when recording is not required.

Continuous recording

From Release 7.1, Avaya SBCE supports continuous recording if the standby recording server has information about the current state of the active recording server. If the active recording server fails, the standby recording server continues recording the communication session. The recording server requests Avaya SBCE to stream the media and metadata for that communication session to the active recording server.

End-to-end secure indication

Avaya endpoints can display an end-to-end secure indicator for calls that use secure protocols for both halves of the call. From Release 7.0 onwards, Avaya SBCE provides a **Securable** field on the Server Configuration page to indicate whether the server is securable. Avaya SBCE uses the **Securable** field to determine whether the trunk and call server can use secure protocols, and sets appropriate values for the Av-Secure-Indication header.

The Av-Secure-Indicator header in the outgoing INVITE message is set to secured when the following conditions are met:

- The trunk server and call server are securable.
- The incoming and outgoing links use TLS and have a secure Audio-Visual Profile (SAVP) or transaction capabilities application part (tcap) messages with an SAVP profile.
- System Manager sends the Av-Secure-Indication header as secured.

Avaya SBCE sets the Av-Secure-Indication header to unsecured when:

- Any condition required for setting the Av-Secure-Indication header to secured is not met.
- The Answer message has an AVP profile.

Subsequent messages such as Update without SDP, PRACK without SDP, and ACK must keep the secure indication value from the response of the previous request.

To make the Trunk server unsecured, the corresponding trunk link with Session Manager must also be unsecured.

Note:

Avaya SBCE depends on Avaya Aura® 7.0 to support the end-to-end secure indication feature. Avaya Aura® 7.0 makes this feature available to users.

Media encryption by using AES-256

Advanced Encryption Standard (AES) is a widely used specification for data encryption. From Release 7.0 onwards, Avaya SBCE supports media encryption by using AES-256.

The AES standards describe a symmetric key algorithm. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Though AES-128 is adequately secure, highly security conscious users might adopt AES-192 or AES-256. To provision this feature, Avaya SBCE supports the following crypto suites:

- AES_256_CM_HMAC_SHA1_32
- AES_256_CM_HMAC_SHA1_80

The following options are available in the **Preferred Format#1**, **Preferred Format#2**, and **Preferred Format#3** fields on the Media Rule page:

- SRTP_AES_CM_256_HMAC_SHA1_32
- SRTP_AES_CM_256_HMAC_SHA1_80

Transcoding

From Release 7.1, Avaya SBCE supports transcoding. Transcoding translates a media stream encoded by using one codec into a media codec encoded by using another codec. Avaya SBCE performs transcoding when the inbound and outbound entities have incompatible codecs. The Session Description Protocol (SDP) offer contains information about the codecs that the device sending the message prefers. The device that receives the message responds to the SDP offer by using the set of codecs that the receiving device supports.

To enable the transcoding feature, you must go to **Device Specific Settings** > **Advanced Options**, click the **Feature Control** tab, and select the **Transcoding** check box.

By providing transcoding, Avaya SBCE:

- Optimizes bandwidth availability by enforcing the use of different compression codecs.
- Normalizes traffic in the network to a single codec.
- Reduces the usage of multimedia resource function processors and media gateways to support a large number of codecs.

Avaya SBCE supports audio transcoding and transcoding for trunk deployments. All transcoded calls are anchored to Avaya SBCE. Fax transcoding is not supported. If a call has both audio and video m lines, Avaya SBCE only transcodes the audio. Video calls that require transcoding are converted to audio calls.

Página2606 de 3226.

Supported transcoding capacities

Server name	Maximum transcoded sessions	Maximum non-transcoded sessions
Dell R210–II XL	100	5000
HP DL360 G8	200	6000
Dell R620	200	6000
Dell R320	200	6000
Dell R630	1000	10000
HP DL360 G9	1000	10000

These capacities vary from codec to codec because, depending on the codec algorithm, the processing CPU cycles differ for each media stream. The estimated capacities are with G711 and G729 codecs and are based on the 180 sec hold/talk time.

Codecs supported for transcoding

The following codecs are supported for transcoding:

- PCMU
- PCMA
- G722
- G729
- G729AB
- G726–32
- OPUS Constrained Narrow Band
- OPUS Narrow Band
- OPUS Wide Band

Support for IPv6 addresses

From Release 7.1, Avaya SBCE supports IPv6 addresses to SIP trunk servers. To support the transition to IPv6, Avaya SBCE uses dual stack nodes that run both IPv4 and IPv6. Avaya SBCE supports trunk deployments with IPv4 only to the enterprise, and IPv6, dual stack, or IPv4 only towards the trunk or public network.

Avaya SBCE supports the following deployment scenarios:

- Public (untrusted) network: IPv6-only, Dual stack, Mixed mode
- Private/Enterprise (trusted) network: IPv4-only

Avaya SBCE supports:

- IPv6 unique local unicast address and IPv6 global unicast address.
- IPv6 communication with entities such as SIP servers, SIP endpoints, DNS servers, NTP server, syslog server, and Avaya Aura® Media Server.

Página2607 de 3226.

Note:

If the DNS response has both IPv4 and IPv6 addresses, Avaya SBCE relies on configuration policies to determine the address types to be tried.

- IPv6 communication with EMS.

From release 7.2, Avaya SBCE supports:

- IPv6 communication with SIP recording server.
- IPv6 in remote worker deployments.

Avaya SBCE supports the following features over IPv6:

- High availability (HA)
- Access to EMS web interface
- Time synchronization with the configured NTP server
- SIP trunking

Avaya SBCE supports Alternate Network Address Types (ANAT) semantics for SDP to permit alternate network addresses for media streams. ANAT semantics are useful in environments with both IPv4 and IPv6 hosts. When Avaya SBCE receives an SDP offer with ANAT semantics, Avaya SBCE:

- Determines whether the enterprise network uses only IPv4.
- Strips media line grouping and sends only the IPv4 address in the m line if the enterprise network uses IPv4.
- Picks an m line based on ANAT preference configuration and sets the port to 0 in other m lines.

SIP entities that generate an SDP offer with ANAT semantics place the sdp-anat-option-tag in the **Require header** field. Avaya SBCE supports the sdp-anat-option tag. Avaya SBCE supports UDP/RTP, TCP/RTP, TLS/SRTP, and other transport combinations in IPv6-only, dual stack, and mixed mode networks.

If you have an environment with both IPv4 and IPv6 hosts, you must go to **Domain Policies** > **Media Rules**, and select **ANAT Enabled**. For more information, see *Administering Avaya Session Border Controller for Enterprise*.

Edge Server for Converged Conference solution

The Converged Conference solution uses the features of Avaya Scopia® V8.5 and Avaya Aura® Conferencing to provide a converged conferencing and web collaboration solution in a unified architecture.

In the converged conference solution, Avaya SBCE:

- Acts as an Edge Server for the set of converged clients. The Edge Server enables the clients to access enterprise video infrastructure remotely across firewalls that block media ports.

Página2608 de 3226.

- Provides firewall traversal for SIP, HTTP, and WebRTC devices and tunnels media where the firewall blocks media ports. Avaya SBCE allows streams to come in through known ports for TLS/TCP.
- Makes video federation calls across companies possible. These calls can be across video endpoints between two enterprises that are behind a SIP Gateway or an SBC, and connected by a SIP trunk.
- Facilitates unregistered guest users to dial in to a video conference or dial out from a video conference.

The Converged Conference solution comprises the following:

- Converged Application Server: The components that are colocated on the same server or distributed based on deployment topology and scale. The components include a management application, conference focus, SIP back-to-back user agent, H.323 Gatekeeper, and a Unified User Portal.
- Web Service Gateway (WSGW): The HTTP to SIP Gateway for WebRTC and HTTP clients.
- Web Collaboration Server: Avaya Aura® Conferencing leveraged for real time Web Collaboration.
- Converged Media Server: Software-based media processing for transcoding and composition of video, high scale audio, and WebRTC audio/video support. The server uses the Avaya Scopia® Elite Multipoint Control Unit (MCU) framework. You can also use traditional Elite MCU with hardware accelerator blades as an alternative.
- Converged clients: New set of audio/video clients including Meet Me clients, WebRTC-based Thin Clients such as Simple WebRTC Chat (SWC), Avaya Equinox®, and Scopia XT series of clients.
- Edge Server: Avaya SBCE, Path finder (H.323), and Avaya Scopia® Desktop Server. Avaya SBCE provides Session Border Controller functionality for SIP calls, BFCP/FECC for XT series, reverse proxy functionality for HTTP, and TURN/STUN for WebRTC. Avaya Scopia® Desktop Server is required for handling signaling and media for legacy Avaya Scopia® desktop mobile phones.
- Common management infrastructure for all components and devices.
- Conference recording and a content management system using WildCat.

Página2609 de 3226.

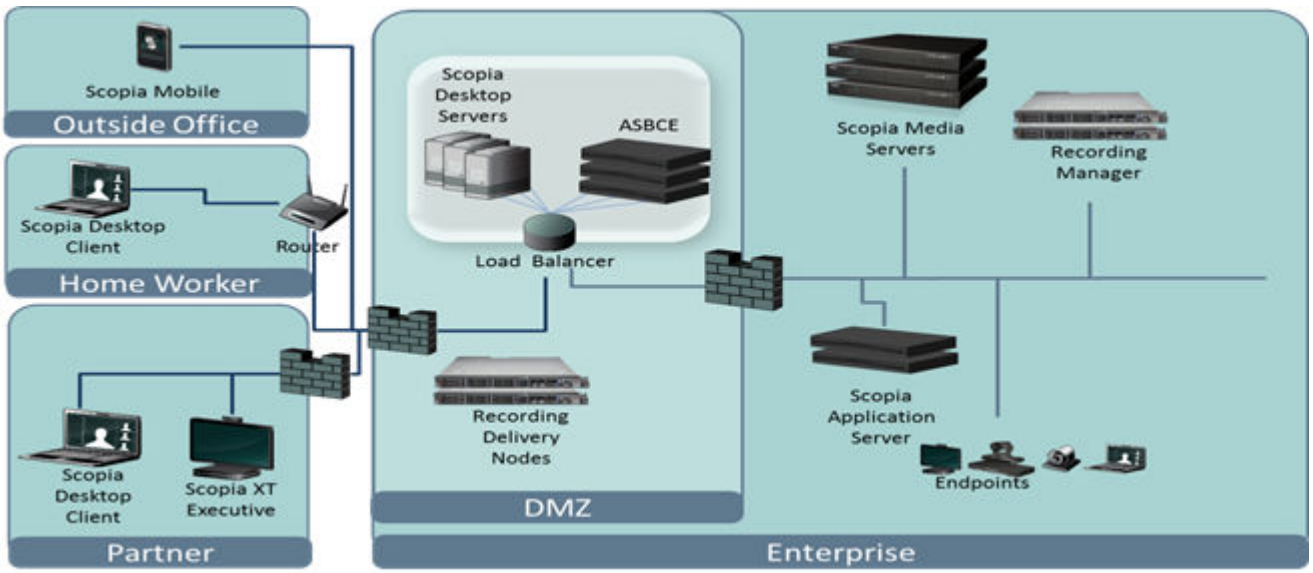


Figure 20: Components of Converged Conference solution with Avaya SBCE as an edge server

The solution supports Avaya Aura®, IP Office, and cloud deployment from small to large distributed deployment, and virtualized deployments on cloud environments.

Avaya SBCE features for the Converged Conference solution

For the Converged Conference solution, Avaya SBCE 7.1 supports the following:

- TURN/STUN control signaling and media relay UDP for WebRTC with symmetric NATing.
- TURN/STUN over TCP for WebRTC.
- Multiplexing and demultiplexing RTP/RTCP or SRTP/SRTCP on TCP or TLS.
- Relaying media through TURN relay using TCP end-to-end without converting to UDP for the TURN relay.
- Load balancing for TURN.
- Sending the status of devices to Avaya Scopia® management and load balancers.
- Calculating bandwidth for all audio/video sessions. Avaya SBCE provides this input to iVIEW load balancer for effective load balancing.
- Detecting DoS and rate limit the http or https signaling request from remote connections.
- Rewriting URL based on redirection.
- Click to conference for unregistered users. The endpoints can call through Avaya SBCE to Avaya Scopia® MCU without being registered to the authorized domain. For dialed out calls, the FQDN is resolved and DNS priority transport is selected as TLS or TCP.

  For this feature to work, the following configuration changes are required:

  - Create a click to call flow.

Página2610 de 3226.

- For dialed-out scenarios, configure a valid DNS server or client on Avaya SBCE. Ensure that the receive interface of the click to call flow matches the signaling interface of the inbound flow selected.

ENUM support

From Release 7.1, Avaya SBCE supports the E.164 Number Mapping (ENUM) protocol. Telephone numbers in the PSTN are organized by using the format specified in the E.164 standard. Conversely, the Internet uses the Domain Name System (DNS) to link domain names to IP addresses. ENUM defines a method to convert a telephone number into a format that can be used with the DNS to look up addressing information such as Uniform Resource Identifiers (URIs). Numbers that conform to the numbering plan defined in E.164 are:

- Limited to 15 digits.
- Prefixed with a plus sign (+) to indicate that the number includes an international country calling code.

ENUM translates E.164 numbers to URIs by using Naming Authority Pointer (NAPTR) records stored in DNS. With ENUM, calls can be completed over the Internet instead of transferring the call to PSTN. Therefore, ENUM provides cost savings for businesses that communicate with other enterprises by using SIP. If the number is unavailable in the ENUM database, Avaya SBCE routes the call to the service provider to send the call to the PSTN.

Process for converting the E.164 number

When a user dials an E.164 number, ENUM constructs an Application Unique String (AUS) from the number by removing all non-digit characters except the plus sign (+). For example, for the dialed number +44-207-946-0148, the AUS is +442079460148.

The AUS is then converted to an initial key, which is a Fully Qualified Domain Name (FQDN), by using the following steps:

1. Remove the leading plus sign (+) from the AUS.
2. Reverse the order of digits and insert dots between the digits. For example, the number 442079460148 is changed to 8.4.1.0.6.4.9.7.0.2.4.4.
3. Append the string .e164.arpa to change the number to a domain name. For example, 8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa.

The domain name is then used to request NAPTR records. The NAPTR records might contain the end result or the NAPTR records generate a new key to request further NAPTR records from the DNS. At the end of this process, a SIP URI is generated, that Avaya SBCE uses to update the request URI, and proceeds with the routing. If a routing entry is not configured in the corresponding routing profile, Avaya SBCE uses this URI to determine the destination.

Página2611 de 3226.

Call preservation

With the Call preservation feature, the dialog context of the SIP user agent can survive a Session Manager failure even when the Session Manager context is lost. The dialog continues with end-to-end signaling of the intact user agent, through an alternate Session Manager. The Call preservation feature is available only for SIP Routing Element (SRE) flows.

For Call preservation, a Session Manager Failover Group comprising a pair of Session Manager servers is associated with peer entities. The peer entities, such as Avaya SBCE, use enhanced SIP timing and recovery techniques to provide signaling path continuity during Session Manager failure. When Avaya SBCE detects that a Session Manager is unreachable, Avaya SBCE routes the SIP traffic through the alternate Session Manager by using the Failover Group Domain Name (FGDN) in the Session Manager Via and Record-route headers. The FGDN is a fully qualified domain name (FQDN) that resolves to an ordered set of Session Manager servers within a Session Manager Failover Group that provides a high availability SRE service. When the preferred Session Manager becomes unresponsive, the peer SIP entity uses the Session Manager Failover Group Domain resolution to identify and communicate with the alternate Session Manager.

The naming convention for the failover group is as follows:

- Failover group name: *Primary SM-Secondary SM*

  For example, sm1–sm2.

- Primary FGDN: *Primary SM-Secondary SM.sip domain*

  For example, sm1–sm2.example.com.

- Secondary FGDN: *Primary SM-Secondary SM-Identifier.sip domain*

  For example, sm1–sm2–2.example.com.

- Session Manager FQDN: *SM.SM IP Domain*

  For example, sm1.example.com.

The Session Manager failover group can contain two or more Session Manager member instances. The primary Session Manager carries the traffic for the failover group in normal conditions. For more information about administering the Call Preservation feature, see *Call Preservation Feature Description and Administration Guide*.

To support the call preservation feature, Avaya SBCE:

- Maintains an affinity to the last preferred Session Manager in the failover group for every dialog.
- Preserves the failover group target set in the dialog context. This caching in the dialog prevents unnecessary duplicate DNS queries.
- Supports requests with an FGDN in the Via, Next Hop Route, or Record-Route headers.
- Resets the TCP or TLS socket to the failed Session Manager if Avaya SBCE detects that the preferred Session Manager is unreachable.

Página2612 de 3226.

- Supports Call Preservation only on TCP and TLS transport types.
- Changes the dialog-scoped affinity to the preferred Session Manager only when the preferred Session Manager instance becomes unreachable. Avaya SBCE reevaluates the affinity by selecting one of the following:
  - The alternate Avaya SBCE with highest priority
  - The alternate Session Manager with highest priority, excluding any alternate Session Manager instances in the FG that are already unavailable.
- Detects that a Session Manager is back in service and reachable within the interval configured in the **Frequency** field on the Server Configuration page in the **Heartbeat** tab.

  Important:

  Heartbeat configuration is mandatory for the Call preservation feature. The heartbeat is used to detect the restored Session Manager.

  Supports provisional response reliability with a 100 rel message and sends PRACK to all received provisional responses.

Support for TILEncore-Gx36 Intelligent Application Adapter

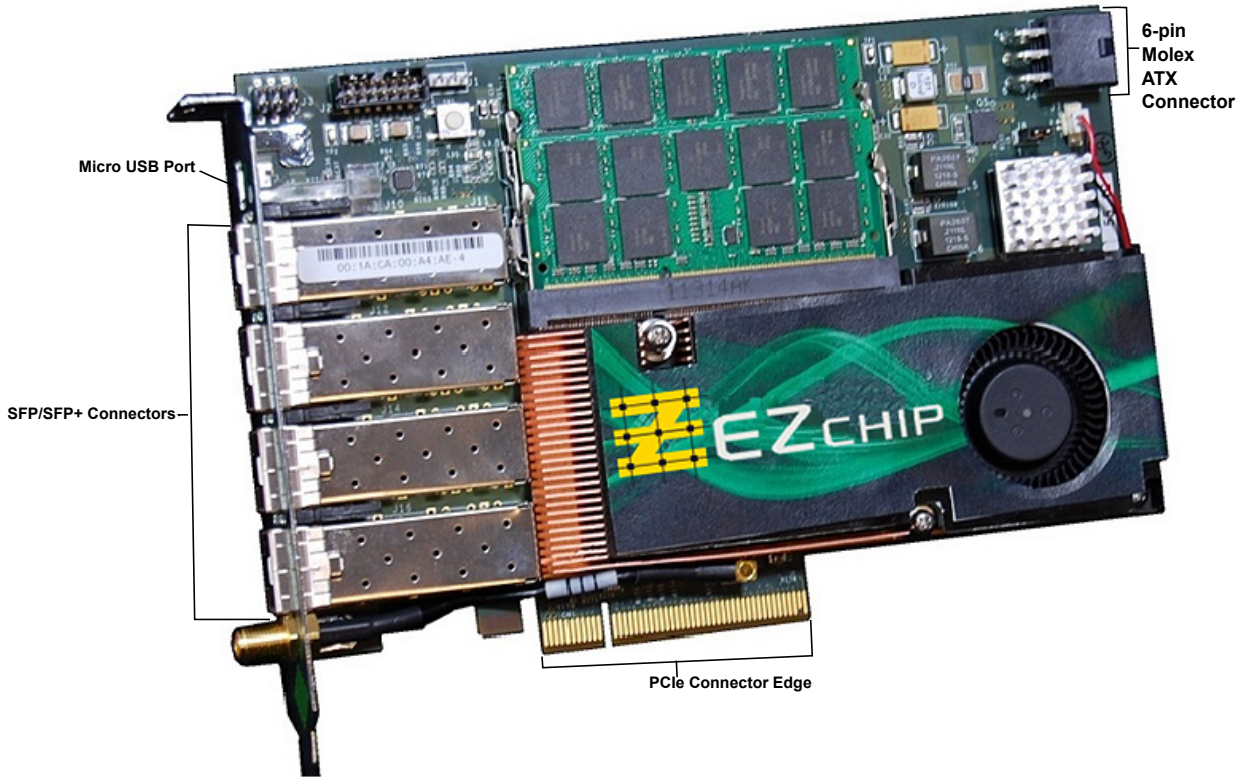
For every session, Avaya SBCE supports signaling and media packets. The number of media packets is significantly higher than the signaling packets. When the number of sessions on the Avaya SBCE increases, the CPU available to process media packets can dominate the host server, even before all network bandwidth is occupied. Increasing the amount of CPU available for media packet processing or dataplane processing helps Avaya SBCE support more simultaneous sessions. The TILEncore-Gx36 Intelligent Application Adapter significantly increases the number of dataplane cores at lower costs without requiring a larger server. Therefore, to provide more capacity, Avaya SBCE 7.1 supports the TILEncore-Gx36 Intelligent Application Adapter.

TILEncore-Gx36 Intelligent Application Adapter overview

TILEncore-Gx36 is a full-height, half-length, single-slot PCIe card comprising a TILEncore-Gx 36-core processor, on-board memory, and other components for packet processing. The adapter requires a single PCIe slot in the host. The adapter functions as a coprocessor within Avaya SBCE. The dataplane software on Avaya SBCE runs on the adapter, and all other software runs on the host server.

This adapter is supported only in HP DL360 G9 and Dell R630.

Página2613 de 3226.



TILEncore-Gx36 features

Feature	Description
TILE-Gx8036 Processor	Provides a 36-core (tile) Gx8036 processor, with each tile running at 1.2 GHz. Wire-speed packet classification and load-balancing engine that performs initial packet inspection, parsing, and distribution to tiles. Two separate cryptographic engines capable of up to 40 Gbps of throughput.
Network Connectivity	Provides four physical SFP/SFP+ ports. You can configure every port as either 1 Gbps or 10 Gbps Ethernet.
Adapter/Host Interface	Operates under host-based software control. Functions as a standard Network Interface Controller (NIC) for packets such as SIP signaling packets, which the card does not process on board. Supports Message Signaled Interrupts (MSI and MSI-X), with which Receive Side Scaling (RSS) can be used on the host.
Memory	Provides 8 GB or 16 GB DDR3 (DDR3-1600) memory.
Virtualization	Supports Single-Root I/O Virtualization (SR-IOV) with which multiple guest operating systems on a single host server can share the adapter.

Table continues…

Página2614 de 3226.

Feature	Description
Power and Thermal	Can be powered either through the PCIe connector or the ATX power connector. Requires 65 W from the PCIe fingers when powered by using PCIe. Airflow requirements vary between 100 and 400 lfm, depending on the internal configuration of the server.
Ports	Provides four physical network ports, a micro-USB port, and several status indicators on the rear panel of the Gx adapter.
Console connectivity	Provides on-board UART that can be used for a serial connection. Micro-USB connection which supports console connectivity is available on the rear panel of the board. PCIe bus can be used to connect to the adapter over a virtual Ethernet link.
DIP Switches	Provides DIP switches located behind the card that can be used to modify: • Whether the board can boot through the UART and USB interfaces. • PCIe x4 or x8 lane operation. • PCIe operational mode (root complex, endpoint, or auto). • Edge connector power usage. • PCIe reference clock source for host or local.
Supported Servers	Can be hosted on HP DL360 G9 and Dell R630 servers in Avaya SBCE Release 7.1.
Capacity increase	Provides capacity gains of up to 20000 simultaneous sessions for Avaya SBCE with TILEncore-Gx36 Adapter.
High Availability	Supports high availability for homogenous server pairs. In homogenous HA pairs, the Avaya SBCEs are the same type, both HP DL360 G9 or both R630, and either both Gx-enabled, or both server-only.
IPv6	Supports IPv6 addresses for Avaya SBCE with TILEncore-Gx36 Adapter.
Media transcoding	Supports media transcoding by using Avaya Aura® Media Server for Avaya SBCE with TILEncore-Gx36 Adapter.

Configuration of TILEncore-Gx36 Adapter installed in Avaya SBCE

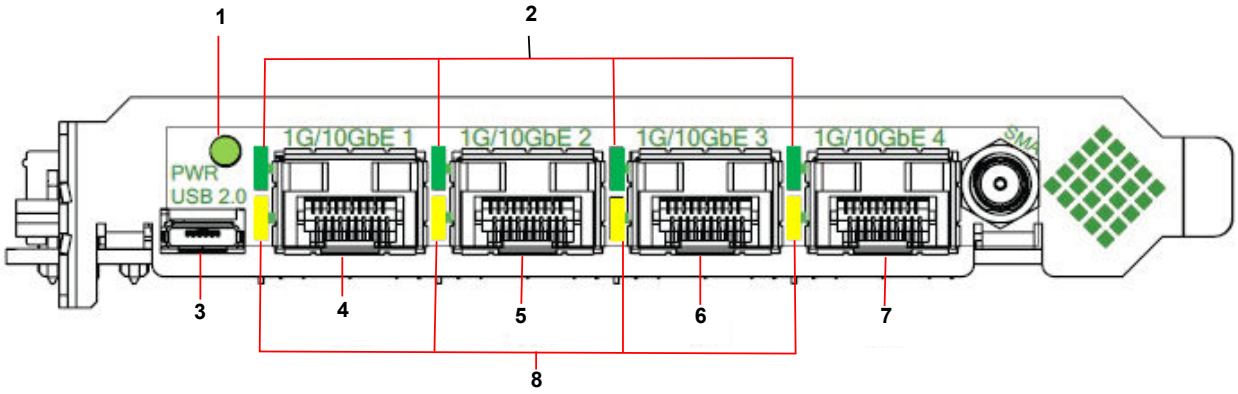
- Four 1Gbps SFP transceivers: In Release 7.1, Avaya SBCE supports maximum 4 Gbps combined bandwidth.
- Boots through the PCIe bus: Adapter software is stored on the disk of the host server. Tools supplied with the Tilera Multicore. Development Environment (MDE) is used to boot the Gx and transfer a bootrom image to the card.
- 8 GB of memory
- Power supplied through the PCIe edge connector: Additional cabling is not required inside the host server chassis.
- Micro-USB serial cable: Avaya SBCEs that use the Gx adapter are shipped with a micro-USB serial cable that can be used to provide console connectivity in the field. The cable is not factory-installed.

Página2615 de 3226.

- DIP switches: Factory default positions, which provide the necessary configuration that Avaya SBCE requires. For DIP switch specifications, see the Gx36 User Guide.
- Four protected data interfaces on Avaya SBCE: The interfaces are named A1, B1, A2, and B2. The adapter is configured so that these interfaces are arranged, beginning from left, as A1, A2, B1, and B2.

For information about installing the adapter, see the Tilera documentation.

TILEncore-Gx36 Intelligent Application Adapter rear panel



Name	Description
1	Power LED The power LED is lit only when all major board components are powered and functional.
2	Link LEDs The green Link LEDs are lit when the Ethernet link is functional.
3	Micro USB port The micro USB port provides a console connection to the card. You can restart the adapter through the micro USB port.
4	A1 network interface Every network port operates at 1 Gbps or 10 Gbps when using an SFP transceiver.
5	A2 network interface
6	B1 network interface
7	B2 network interface
8	Activity LEDs The yellow activity LEDs are lit when the Avaya SBCE network interfaces are enabled.

Página2616 de 3226.

Chapter 3: Interoperability

Product compatibility

For the latest and most accurate compatibility information go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Avaya SBCE supported servers

Server	Processors	System Memory	On-board Storage
Dell R210 II XL (core)	Intel Xeon E3-1220 3.10 GHz Quad Core/4T	4 GB (DDR3 1333MHz)	500 GB (3.5-in SATA 3Gb/s – 7.2K)
Dell R210 II (core)	Intel Xeon E3-1230 3.20 GHz Quad Core/4T	4 GB (DDR3 1333MHz)	500 GB (3.5-in SATA 3Gb/s – 7.2K)
Dell R210 II XL (EMS)	Intel Pentium G850 2.90 GHz Dual Core/2T	2 GB (DDR3 1333MHz)	2 x 500 GB (3.5-in SATA 3Gb/s – 7.2K)
Dell R320	Intel® Xeon® E5-2430v2 2.5 GHz, 6 cores–80W	8 GB (DDR4 1600 MT/s UDIMM)	2 x 300 GB 10K SAS
Dell R330	Intel® Xeon® E3-1200v5 3.6 GHz, 4 cores–80W	16 GB (DDR4 2133 MT/s UDIMM)	Up to four 3.5–inch hot-swap HDDs or Up to eight 2.5–inch hot-swap HDDs
Dell R620	Intel® Xeon® E5-2600, Dual core	32 GB (DDR3 1333)	2.5-in SATA 3Gb/s – 7.2K
Dell R630	2 x Intel® Xeon® E5-2640 2.6 GHz, 8 cores–90W	32 GB (DDR4 2133 MT/s RDIMM)	2 x 300 GB 10K SAS
HP DL360 G8	Intel® Xeon® E5-2400	up to 384GB	(8) SFF SAS/SATA/SSD
HP DL360 G9	2 x Intel® Xeon® E5-2640 2.6 GHz, 8 cores–90W	32 GB (DDR4 2133 MT/s RDIMM)	2 x 300 GB 10K SAS
Portwell CAD-0208 (core)	Intel® Atom D510 1.66GHz - Dual Core	2GB (SO-DIMM DDR2 667MHz)	320GB (2.5-in SATA 3Gb/s – 7.2K)
Portwell CAD-0230	Intel® Atom C2000 1.7GHz - Dual Core	2GB (SO-DIMM DDR3 1333MHz)	One 2.5–inch HDD

Table continues…

Página2617 de 3226.

Server	Processors	System Memory	On-board Storage
Avaya Converged Platform 100 series server with profile 3	Intel Skylake S-4114, two CPUs per server, ten cores per CPU, twenty cores per server, 2.2 Ghz core frequency	12 x 4 GB RDIMM, 6 x 8 GB RDIMM	Up to four 2.5 inch 10K HDD, SAS, 600 GB SAS HDD
Avaya Converged Platform 100 series server with profile 5	Intel Skylake G-6132, two CPUs per server, fourteen cores per CPU, twenty eight cores per server, 2.6 Ghz core frequency	12 x 16 GB RDIMM	Up to six 2.5 inch 10K HDD SAS, 600 GB SAS HDD

Note:

Only Dell R210 II XL, Dell R620, Portwell CAD-0208, Portwell CAD-0230, Dell R320, Dell R330, Dell R630, HP DL 360 G8,HP DL 360 G9, Avaya Converged Platform 100 series server with profile 3, and Avaya Converged Platform 100 series server with profile 5 support new installations.

Avaya products

For the latest compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Third-party product requirements

External SAL gateway

When Secure Access Link (SAL) is used for remote access to the Avaya SBCE for Avaya services, the customer must provide a SAL Gateway. Customers can buy the SAL Gateway from Avaya. Customers can also provide the SAL Gateway if the server complies with the SAL requirements specified on the Avaya Support website at http://support.avaya.com. Sometimes, a System Platform integrated SAL Gateway can be used instead of buying another server. See Product Support Notice PSN003058u.

Operating system compatibility

The Avaya SBCE and EMS use RedHat Enterprise Linux 7.x on all platforms.

Página2618 de 3226.

Chapter 4: Performance specifications

Supported capacity

Server Type	Non-encrypted Sessions with Trunking	Encrypted Remote Worker Users	Encrypted Sessions with Presence	SIPREC with SIP Trunking Replicated Sessions	Scopia Video Sessions	Transcoded Sessions	
	Standard	Advanced		Advanced		Internal	External
Avaya Converged Platform 100 series server with profile 3 (Dell™ PowerEdge™ R640 Server)*	14,000	20,000	8,000	6,000	800	1,000	2,500
Avaya Converged Platform 100 series server with profile 5 (Dell™ PowerEdge™ R640 Server)*	30,000	20,000	10,000	10,000	800	1,000	5,000
Dell R630 with TILEncore Gx36 Intelligent Application Adapter	30,000	20,000	7,500	10,000	800	1000	5,000
HP DL360 G9 with TILEncore Gx36 Intelligent Application Adapter	30,000	20,000	7,500	10,000	800	1000	5,000

Table continues…

Dell R630 (High Capacity)	14,000	20,000	7,500	6,000	800	1,000	2,500
HP DL360 G9 (High Capacity)	14,000	20,000	7,500	6,000	800	1,000	2,500
Dell R330 (Mid-Range Capacity)	6,000	5,000	2,000	3,000	200	300	1,250
HP DL360 G9(Mid-Range Capacity)	6,000	5,000	2,000	3,000	200	300	1,250
VMware ESXi 6.x**	5,000	6,000	3,000	2,500	200	100	1,250
Portwell CAD 0230	600	500	500	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Nutanix***	5,000	6,000	3,000	2,500	200	100	1,250

Note:

- Avaya SBCE supports Avaya Converged Platform 100 series server with profile 3 and profile 5 (Dell™ PowerEdge™ R640 Server) from Release 7.2.2.2 and later.
- ** VMware ESXi 6.x supports Avaya SBCE medium deployment type.
- *** Avaya SBCE supports deployment of KVM using Nutanix from Release 7.2.1 and later.

Note:

For the other supported servers which are not listed in the above table, capacity information published in the previous releases apply.

Redundancy and high availability

Redundancy and High Availability (HA) features are available in EMS and Avaya SBCE servers. Hardware that support these features are Dell R210 II XL, Dell R320, Dell R620, Dell R630, Dell R330, HP DL360 G8, and HP DL360 G9 platforms. These features are also available for TILEncore-Gx-enabled servers and Avaya SBCE deployed in a virtualized environment. These features support HA for homogeneous server pairs. In homogenous HA pairs, Avaya SBCE devices are of the same type.

HA support for both media and signaling ensures that Avaya SBCE security functionality is provided continuously, regardless of hardware or software failures. High availability requires minimum two Avaya SBCE devices and one standalone EMS server.

Página2620 de 3226.

Note:

High availability requires Gratuitous Address Resolution Protocol (GARP) support on the connected network elements. When the primary Avaya SBCE fails over, the secondary Avaya SBCE broadcasts a GARP message to announce that the secondary Avaya SBCE is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBCE IP address. Devices that do not support GARP must be on a different subnet with a GARP-aware router or L3 switch to avoid direct communication. For example, to handle GARP, branch gateways, Medpro, Crossfire, and some PBXs/IVRs must be deployed in a different network from Avaya SBCE, with a router or L3 switch. If you do not put the Avaya SBCE interfaces on a different subnet, after failover, active calls will have a one-way audio. Devices that do not support GARP continue sending calls to the original primary Avaya SBCE.

All IP addresses configured on the Network Configuration screen are shared between both HA devices in HA deployment mode. The HA devices are also configured with private, default IPs that are used to replicate signaling and media data between each other. The configured interfaces are inoperative on the standby or secondary device until the device becomes active or primary. When the devices failover, the active device sends a GARP message to update the ARP tables of the neighboring HA device to begin receiving traffic.

Avaya SBCE high availability

The Avaya SBCE can be deployed as a pair either in the enterprise DMZ or core, or geographically dispersed, where each Avaya SBCE resides in a separate, physical facility.

In either configuration, Avaya SBCE HA pairs can be deployed in an enterprise in a parallel mode configuration. In the parallel configuration, the signaling packets are routed only to the active or primary Avaya SBCE, which performs all data processing. The interface ports on the standby Avaya SBCE do not process any traffic. The management interfaces on the Avaya SBCE appliances have different IP addresses, but the signaling or media interfaces have the same IP address. On failover, the standby Avaya SBCE advertises the new MAC as the L2 address for the common IP address. The Avaya SBCE devices are synchronized through the heartbeat on the dedicated interfaces, and both Avaya SBCE devices are in continuous communication with the Avaya EMS.

When the Avaya EMS detects a failure on the active Avaya SBCE, the active SBC network interface ports are automatically disabled. The ports of the standby SBC are enabled. Failure detection and operational transfer occur without dropping packets or adding any significant amount of latency into the data paths. The EMS reports the change in status to the EMS for action by the system administrator.

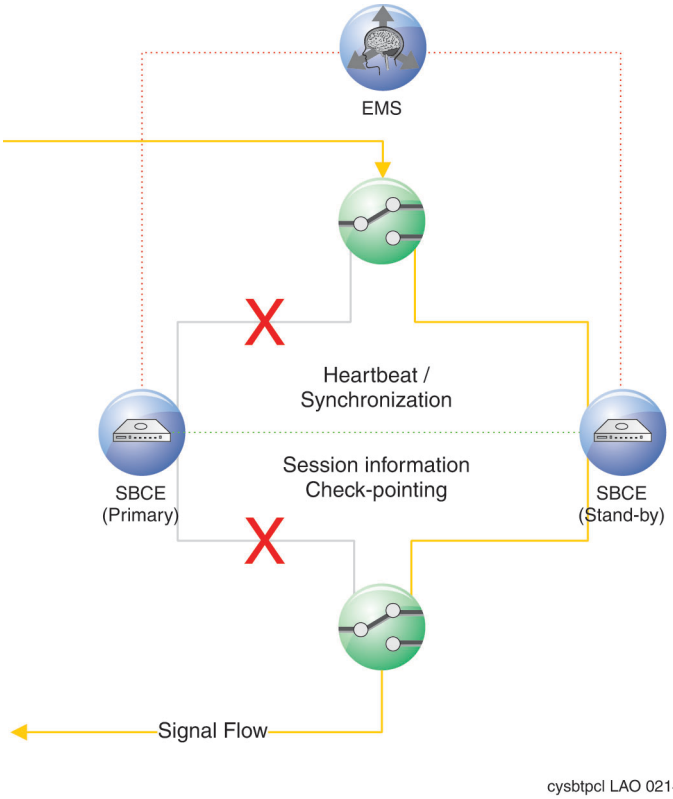


Figure 21: Typical Avaya SBCE HA – Parallel Mode Topology (colocated)

EMS replication

EMS replication gives an enterprise the option of deploying two Avaya EMS servers to ensure uninterrupted network monitoring and control. EMS data is replicated between the servers iteratively as determined by user-defined fields on the EMS GUI interface. These servers can be located in the same facility or in different geographic locations.

Avaya SBCE 7.1 and later support EMS HA active/active configuration. When one EMS fails, the other EMS is usable without any manual intervention or downtime.

Página2622 de 3226.

Chapter 5: Environmental requirements

Altitude requirements

Dell R210 II XL altitude ranges

Range	Operating altitude	Non-operating altitude
Low limit	-50 ft (-15.2 m)	-50 ft (-15.2 m)
High limit	10,000 ft (3048 m)	35,000 ft (10,668 m)

Hardware dimensions

Server	Height	Width	Depth	Weight
Dell R210 II XL (Core)	1.7 in. (4.32 cm)	17.10 in. (43.45 cm)	15.50 in. (39.37 cm)	15.5 lbs. (7.03 kg)
Dell R210 II (Core)	1.7 in. (4.32 cm)	17.10 in. (43.45 cm)	15.50 in. (39.37 cm)	15.5 lbs. (7.03 kg)
Dell R210 II XL (EMS)	1.7 in. (4.32 cm)	17.10 in. (43.45 cm)	15.50 in. (39.37 cm)	15.5 lbs. (7.03 kg)
Dell PowerEdge R320	1.7 in. (4.318 cm)	17.1 in. (43.434 cm)	24 in (60.69 cm)	25 lbs (11.34 kg)
Dell PowerEdge R330	1.68 in. (4.28 cm)	17.09 in. (43.42 cm)	24 in (61.0 cm)	29.54 lbs (13.4 kg)
Dell PowerEdge R620	1.7 in. (4.318 cm)	17.1 in. (43.434 cm)	26.9 in. (68.326 cm)	41.0 lbs (19.1 kg)
Dell PowerEdge R630	1.7 in. (4.318 cm)	19 in. (48.26 cm)	27.6 in (70.104 cm)	43.0 lbs (19.50 kg)
Portwell CAD-0208 (core)	1.65 in. (4.20 cm)	7.10 in. (18.03 cm)	5.90 in. (14.98 cm)	15.5 lbs. (7.03 kg)
Portwell CAD-0230	1.65 in. (4.20 cm)	8.27 in. (21.00 cm)	8.27 in. (21.00 cm)	15.5 lbs. (7.03 kg)
HP Proliant DL360 G8	1.7 in. (4.318 cm)	17.1 in. (43.434 cm)	27.5 in. (69.85 cm)	42.3 lbs (19.19 kg)
HP Proliant DL360 G9	1.7 in. (4.318 cm)	17.2 in. (43.68 cm)	27.5 in (69.85 cm)	44.0 lbs (19.95 kg)

Página2623 de 3226.

Temperature and humidity requirements

Server	Operating Temperature	Storage Temperature	Relative Humidity
Dell R210 II XL (core)	50 ºF to 95 ºF (10 ºC to 35 ºC)	-40 ºF to 149 ºF (-40 ºC to 65 ºC)	20% to 90%, noncondensing
Dell R210 II (core)	50 ºF to 95 ºF (10 ºC to 35 ºC)	-40 ºF to 149 ºF (-40 ºC to 65 ºC)	20% to 90%, noncondensing
Dell R210 II XL (EMS)	50 ºF to 95 ºF (10 ºC to 35 ºC)	-40 ºF to 149 ºF (-40 ºC to 65 ºC)	20% to 90%, noncondensing
Dell R320	50 ºF to 95 ºF (10 ºC to 35 ºC)	-40 ºF to 149 ºF (–40 ºC to 65 ºC)	20% to 80%, noncondensing
Dell R330	41 ºF to 104 ºF (5 ºC to 40 ºC)	23 ºF to 113 ºF (–5 ºC to 45 ºC)	5% to 85%, noncondensing
Dell R620	-40 ºF to 149 ºF (–40 ºC to 65 ºC)	-40 ºF to 149 ºF (–40 ºC to 65 ºC)	5% to 95%
Dell R630	50 ºF to 95 ºF (10 ºC to 35 ºC)	50 ºF to 95 ºF (10 ºC to 35 ºC)	1% to 80%, noncondensing
Portwell CAD-0208 (core)	41 ºF to 95 ºF (5 ºC to 35 ºC)	32 ºF to 158 ºF (0 ºC to 70 ºC)	20% to 90%, noncondensing
Portwell CAD-0230	32 ºF to 104 ºF (0 ºC to 40 ºC)	14 ºF to 158 ºF (–10 ºC to 70 ºC)	20% to 90%, noncondensing
HP DL 360 G8	50 °F to 95 °F (10 °C to 35 °C)	101.7 °F (38.7 °C)	5 to 95% nonoperating 10 to 90% operating
HP DL 360 G9	50 ºF to 95 ºF (10 ºC to 35 ºC)	-22 ºF to 140 ºF (-30 ºC to 60 ºC)	8% to 80%, noncondensing

Note:

For altitudes greater than 900 m or 2952 ft, see Dell documentation for operating temperature ranges.

Power requirements

Server	Input	Nominal (110 V)	AC Power Max
Dell R210 II XL (core)	110–240 VAC auto switch	2 A	250 W
Dell R210 II (core)	110–240 VAC auto switch	2 A	250 W

Table continues…

Página2624 de 3226.

Server	Input	Nominal (110 V)	AC Power Max
Dell R210 II XL (EMS)	110–240 VAC auto switch	2 A	250 W
Dell R320	110–240 VAC		300 W
Dell R330	110–240 VAC		350 W
Dell R620	110–240 VAC	2 A	750 W
Dell R630	110–240 VAC		750 W
Portwell CAD-0208 (core)	110–240 VAC auto switch	2 A	60 Watt Power Adapter
Portwell CAD-0230	12 V DC		40 W
HP DL360p G8	100–240 VAC	15 A	308.95 W
HP DL 360 G9	110–240 VAC		800 W

Physical system protection requirements

The server is equipped with air vents on either side of the equipment chassis, and exhaust vents on the back. Be sure to follow these guidelines:

- Do not block these air vents.
- Do not place the server in a location where dirt or dust might clog the air vents or enter the chassis and damage internal components.
- Do not install the device in or near a source of heat, including proximate high-current or high-power consuming equipment such as switch banks. Excessive heat might cause the server to overheat and fail.

Note:

The customer must ensure that environmental hazards do not interfere with the operation of the Avaya SBCE server. These hazards could include excessive heat, excessive humidity, improper ventilation, or electromagnetic interference from proximate equipment.

Regulatory standards

Avaya SBCE servers conform to the following standards.

Server	Certifications
Dell R210 II XL (core)	CSA, FCC, UL, RoHS

Table continues…

Página2625 de 3226.

Server	Certifications
Dell R210 II (core)	CSA, FCC, UL, RoHS
Dell R210 II XL (EMS)	CSA, FCC, UL, RoHS
Dell R320	CSA, FCC, CE, UL, RoHS
Dell R330	CSA, FCC, CE, UL, RoHS
Dell R620	CSA, FCC, CE, UL, RoHS
Dell R630	CSA, FCC, CE, UL, RoHS
HP DL360 G8	CSA, FCC, CE, UL, RoHS
HP DL360 G9	CSA, FCC, CE, UL, RoHS
Portwell CAD-0208 (core)	CE, FCC, UL
Portwell CAD-0230	CE, FCC

Página2626 de 3226.

Chapter 6: Security

Security specification

Unified communications intrusion protection

Traditional intrusion prevention systems (IPS) monitor network traffic to gather and analyze information from various parts of the network to identify possible security breaches. This information is used for subsequent prevention or mitigation. Unlike traditional IPS, Avaya SBCE security products detect any anomalous event, including day zero attacks. Additionally, also prevents virtually any type of intrusion from outside the enterprise and misuse from within the enterprise. This capability is because of the unparalleled flexibility and fine-grain tuning allowed when network security administrators establish Unified Communications rule sets. The Avaya SBCE IPS security feature includes:

- Flood and Fuzzing Protection: Protection from volume-based Denial-of-Service (DoS) and malformed message or fuzzed attacks. Customized protocol scrubbing rules detect and remove malformed messages that might cause call servers or other critical network components to stop responding. Malformed messages can also make other portions of the communications infrastructure vulnerable because of degraded performance of critical Unified Communications systems components, such as servers and endpoints.
- Media Anomaly Prevention: Selectively enables the media traffic and enforces rules on the traffic carried. The traffic flow is based on the negotiated signaling and other configured policies, such as prevent video or prevent modem/FAX.
- Spoofing Prevention: Various validation techniques are applied to detect and prevent spoofing, including the end-point fingerprints for different message fields to trigger other validations and verifications.
- Stealth Attack Prevention: Based on the learned call behavior patterns of subscriber endpoints, Avaya SBCE can detect any nuisance and annoying calls to a particular destination or user. These products can selectively block the subscribers from whom the calls originate.
- Reconnaissance Prevention: Avaya SBCE detects and blocks application layer scan reports and blocks the attackers that originate them.

Página2627 de 3226.

Attack protection

Avaya SBCE security products ensure the integrity of all real-time IP applications. Avaya SBCE security products maintain the highest level of communications network security, reliability, and availability by performing these three critical functions: monitoring, detection, and protection.

Monitoring

Each Avaya SBCE provides complete network security monitoring and management capabilities. These capabilities encompass each aspect of the UC network, including all endpoints, media gateways, call servers, voice mail (VM) and applications servers. In addition, the monitoring and management capabilities provide a cascaded, multi-layered detection, mitigation, and reporting system that provides real-time information based on user-definable event thresholds. This system supports a detailed graphical user interface (GUI) called the EMS web interface. The EMS can be installed on and run from any Avaya SBCE security device. The EMS can also be installed on a separate server platform and used as a standalone Element Management System (EMS). This EMS monitors and coordinates the security activities of all Avaya SBCE security devices installed in a network.

Note:

Both the EMS and Avaya SBCE can be installed in one box. However, as your network grows and you require more than one Avaya SBCE, the EMS must be installed on a dedicated platform.

Detection

The detection capability of the Avaya SBCE solution uses numerous dynamic and adaptive algorithms to detect any anomalies in the learned caller behavior that are based upon user-definable Time-of-Day (ToD) and Day-of-Week (DoW) criteria. These algorithms are flexible enough to accommodate special circumstances such as weekends, holidays, and other user-specified time periods. Avaya SBCE solution can also learn and apply dynamic trust scores, starting from an unknown score and either increasing or decreasing to different levels depending upon the behavior pattern of the caller, which could be Trusted, Known, Unknown, Suspected, or Spammer. The dynamic trust score is also dependant upon called party feedback, including (Black List and White List, further enhancing the time-critical ability to detect anomalous behavior.

The detection capability is also able to collect and correlate multiple events and activities from different nodes and endpoints in the network to accurately detect attacks. These attacks might otherwise have escaped unnoticed if reported only by a single point in the network. The detection capability can inspect the sequence and content of messages to detect protocol anomalies and any instances of endpoint scanning. Finally, the detection capability of the Avaya SBCE solution can validate the source of a suspected malicious call or attack by implementing a unique detection technique that is based upon learned caller fingerprints.

Avaya SBCE security products can continuously learn call patterns and endpoint fingerprints. These products can also constantly analyze raw event data based on specific user-definable

Página2628 de 3226.

criteria and take automatic action. Therefore, Avaya SBCE security products can evolve and adapt automatically to effectively counter any new or existing threat.

Protection

The Avaya SBCE provides complete network protection by blocking attacks while simultaneously passing legitimate calls through unimpeded. This exceptional level of protection can be extended to an endpoint, a specific group of endpoints, or to all assets in the network. Extending this protection is based on highly flexible user-defined rule sets called Unified Communications Policies. These policies can be implemented to precisely discriminate or normalize any incoming or outgoing signaling or multimedia traffic. Thus all IP communication devices, such as hard-phones, soft-phones, Wi-Fi phones, and smart phones are protected effectively. Call servers, voice mail servers, media servers, media gateways, and application servers are also protected, effectively securing the entire network from all types of attack.

Avaya SBCE hardening

System level Layer 3/Layer 4 security features include IPTable firewall rules to provide restrictions on inbound traffic. The restrictions are effective after content filtering processing for data traffic to protect the Avaya SBCE from IP/ICMP/TCP level attacks.

Outbound traffic is unrestricted.

Protection against layer 3 and layer 4 floods and port scans

ICMP flood prevention

When an ICMP flood from a host is detected, all further requests from that host are blocked for a specified time.

Port scan blocking

When a port scan from a host is detected, all further requests from that host are blocked for a specified time.

Data interface restrictions

- General protection is provided on all data interfaces.
- TCP signaling level flooding control rules are applied dynamically on application-specified listening IP and listening port.

TCP signaling level flood control

Only a specified number of requests are allowed in a specified period for the following request types:

- TCP SYN

Página2629 de 3226.

- FIN
- RST

System-wide security settings

System-wide security settings are supported across the entire Avaya product line.

The Avaya SBCE has the following protection types:

- General Protection
- Management Interface Restrictions
- Data Interface Restrictions

For all products, the management interface is dynamically detected from the system configuration.

For Avaya SBCE, there are no restrictions on the internal Ethernet interface, ethbint, and external Ethernet M1 interface, ethext, on the Com Express coprocessor board in the Avaya SBCE box.

To enable Avaya SBCE HA, TCP 1950 ports are allowed bidirectionally on the data interface.

Avaya SBCE HA does not require any extra rules to enable HA traffic.

Installation security

On installing the application rpm package, rules get added or updated for that version. After restart, ICU invokes the appropriate rules script for that platform.

DoS security features

With the Denial of Service (DoS) security feature of the EMS, you can view and edit DoS and Distributed Denial-of-Service (DDoS) attack response control parameters. These parameters can then be applied either to individual SIP endpoints or their parent domain. Also, the Avaya SBCE supports DoS activity reporting for certain time periods. The server DoS feature and the Domain DoS features are further classified based on traffic types, such as Remote Worker, Trunk and Remote Worker, and Trunk. The following rules describe the input methods:

- For Remote Worker, the input is taken from Number of remote workers and Max Concurrent Sessions.
- For Trunk, the input is taken from Max Concurrent Sessions.
- For Remote Worker and Trunk, the input is taken from Number of remote workers and Max Concurrent Sessions.

Rules for setting threshold values for different types of traffic:

- Server DoS is applicable for initiated thresholds. Initiated threshold is applicable for any SIP request routed to the server irrespective of whether any response is received.
- In calculation of all threshold values, 10% of actual value is considered.

Página2630 de 3226.

- Server DoS can also be applicable for remote worker traffic in case of pending threshold value. Pending threshold means SIP Request for which no corresponding response has come from the server.
- Server DoS feature is also applicable in case of failed threshold value. Failed threshold implies that failure request has come for a SIP request other than 401 and 407.

List of recommended threshold values:

- Recommended threshold value for Single Source DoS feature for remote worker deployment is 300 messages.
- Recommended threshold value for trunk is 15 messages.
- The default threshold value for Avaya remote worker in case of phone DoS is 200 messages.
- The recommended threshold value for Call Walking in case of remote worker deployment: INVITE – 10 messages, Registration – 5 messages, and All – 20 messages.

Protocol scrubber

Protocol scrubbing uses a sophisticated statistical mechanism to thoroughly check incoming SIP signaling messages for various types of protocol-specific events and anomalies. The protocol scrubber verifies certain message characteristics such as proper message formatting, message sequence, field length, and content against templates received from Avaya. Messages that violate the security rules dictated by the scrubber templates are dropped while messages that violate syntax rules are repaired. Messages are repaired by rewriting, truncating, rejecting, or dropping, depending on the processing rules imposed by the templates. Protocol scrubbing rule templates are prepared by Avaya and the user can edit the templates minimally.

Protocol scrubbing for SIP allows you to install a scrubber rules package. You can also enable or disable the scrubber rules contained in the package, and delete the package from the system. In addition, you can view a list of all installed scrubber rules.

Topology hiding

Topology hiding allows you to change key SIP message parameters to hide or mask how your enterprise network appears to an unauthorized or malicious user.

Firewall rules

Firewall rules protect the Avaya SBCE, and communications and signaling for Avaya SBCE. Firewall rules are hard-coded and cannot be configured. Firewall rules can be divided into the following categories:

- Common rules

Página2631 de 3226.

- Management rules
- Data interface rules

Common rules

Common rules are applied to all interfaces. Common rules are divided into the following categories:

- ICMP restrictions
- Portscan detection
- KILLSCAN rules

ICMP restrictions

- Always accept ICMP ping replies.
- Any IP address sending an ICMP ping request is added to the pingflood list.
- When an IP in the pingflood list sends an ICMP ping request, drop the request if that IP has sent five ping requests in one second.
- Accept all other ICMP ping requests.
- ICMP redirect datagrams for the network are rate-limited to one per second.
- ICMP redirect datagrams for the host are rate-limited to one per second.
- ICMP destination unreachable messages are rate-limited to one per second.
- ICMP time exceeded messages are rate-limited to one per second.
- ICMP bad IP header messages are rate-limited to one per second.
- Drop all other ICMP packets.

Detecting Portscan

Procedure

1. Follow KILLSCAN rules.
2. Accept all packets with INVALID state.

KILLSCAN rules

1. Remove the current IP from the portscan list.
2. Any IP address sending packets with FIN, PSH, and URG flags set, but without SYN, RST, or ACK flags is added to the portscan list.
3. Any IP address sending packets with SYN and RST flags set is added to the portscan list.
4. Any IP address sending packets with FIN and SYN flags set is added to the portscan list.
5. Any IP address sending packets with FIN flags set, but without SYN, RST, PSH, ACK, or URG flags is added to the portscan list.
6. Any IP address sending packets with FIN, SYN, RST, PSH, ACK, and URG flags set is added to the portscan list.
7. Any IP address sending packets without any FIN, SYN, RST, PSH, ACK, or URG flags set is added to the portscan list.

Página2632 de 3226.

8. Any IP address sending packets with FIN, SYN, RST, PSH, ACK, and URG flags set is added to the portscan list.
9. Drop all packets from any IP in the portscan list.

Management and MGMTPROTECT rules

Management rules are applied only to management interfaces. The first step in the management rules is to follow the MGMTPROTECT rules, which can be divided into the following categories:

- TCP flood restrictions
- SSH rules
- HTTPS rules
- DNS rules
- Syslog rules
- OpenVPN rules

Management rules

- Follow MGMTPROTECT rules.
- Accept all packets in RELATED or ESTABLISHED state.
- Accept all packets on TCP port 222.
- Accept all packets on TCP port 443.
- Accept all packets on TCP port 53.
- Accept all packets on UDP port 53.
- Accept all packets on TCP port 514.
- Accept all packets on UDP port 514.
- Accept all packets on UDP port 123.
- Drop all other packets.

TCP flood restrictions for all ports

- Any IP address sending packets with FIN flags set, but without SYN, RST, PSH, ACK, or URG flags is added to the finrstlim list.
- Any IP address sending packets with RST flags set, but without FIN, SYN, PSH, ACK, or URG flags is added to the finrstlim list.
- For any IP address in the finrstlim list that sends ten packets in one second, drop the packet.

SSH rules

- Any IP address sending, on port 222, packets with the SYN flag, but without RST or ACK is added to the sshsyn list.
- For any IP address in the sshsyn list that sends, on port 222:

  Fifteen packets with the SYN flag, but without RST or ACK in 1 minute during the TTL of the previous packet sent, drop the packet.

Página2633 de 3226.

Ten packets with the SYN flag, but without RST or ACK in 30 seconds during the TTL of the previous packet sent, reject the packet. An ICMP port unreachable message is sent for the packet.

HTTPS rules

- Any IP address sending, on port 443, packets with the SYN flag, but without RST or ACK, is added to the httpssyn list.
- For any IP address in the httpssyn list that sends, on port 443:
  - Ten packets with the SYN flag, but without RST or ACK in one second during the TTL of the previous packet sent, drop the packet.
  - Five packets with the SYN flag, but without RST or ACK in one second during the TTL of the previous packet sent, reject the packet. Send an ICMP port unreachable message.

DNS rules

- Any IP address sending, on TCP port 53, packets with the SYN flag, but without RST or ACK is added to the dnssyn list.
- For any IP address in the dnssyn list that sends, on TCP port 53:
  - Ten packets with the SYN flag, but without RST or ACK in one second during the TTL of the previous packet sent, drop the packet.
  - Five packets with the SYN flag, but without RST or ACK in one second during the TTL of the previous packet sent, reject the packet. Send an ICMP port unreachable message.

Data interface rules

Data interface rules are applied only to data interfaces. The default DATAIFPROTECT rules are all commented out, although more DATAIFPROTECT rules are dynamically generated by the protect-socket command.

- Follow DATAIFPROTECT rules.
- Accept all packets.

Protect-socket command

The protect-socket command takes a hardware type (1U), add or "del", a protection scheme (a number), an IP address to protect, and a port to protect. From these, it generates a set of firewall rules to protect that IP and port, all added to the DATAIFPROTECT rule list.

- Any IP address sending a packet to the specified IP and port with the SYN flag but not RST or ACK is added to the apprules list.
- For any IP address in the apprules list that sends:
  - Ten packets with the SYN flag, but without RST or ACK to the specified IP and port in one second during the TTL of the previous packet sent, drop the packet.
  - Five packets with the SYN flag, but without RST or ACK to the specified IP and port in one second during the TTL of the previous packet sent, reject the packet. Send an ICMP port unreachable message.

Página2634 de 3226.

- If the protection scheme is given as 1, also follow these rules:
  - For any IP address that sends twenty packets in state ESTABLISHED to the specified IP and port in one second, drop the packet.
  - Keep a record of any IP address that sends a packet in the ESTABLISHED state to the specified IP and port.
  - For any IP address that sends three packets in the NEW state to the specified IP and port in one second, drop the packet.
  - Keep a record of any IP address that sends a packet in the NEW state to the specified IP and port.
- Delete any existing rule for accepting packets.
- Accept all packets.

Port utilization specification

Management interface port restrictions

Only selected ports are allowed on the management interface, and all other TCP/UDP traffic is blocked on the management interface.

Internal – Between one or more Avaya SBCEs and the EMS

- SSH TCP-222.
- HTTPS TCP-443.
- OpenVPN UDP-1194.
- Syslog TCP/UDP-514.
- NTP UDP-123.

External – Between the EMS and Avaya SBCEs and an external device

- SSH TCP-222.
- HTTPS TCP-443.
- Syslog TCP/UDP-514.
- NTP UDP-123.
- DNS TCP/UDP-53 for DNS and the signaling and media ports.
- SNMP Version 2 or 3 UDP-161 + 162. The SNMP agent receives requests on UDP port 161, and the SNMP manager receives notifications for traps and InformRequests on port 162

Página2635 de 3226.

TCP packets

Regardless of TCP ports, only a specified number of TCP packets are allowed from a host within a specified time frame.

SSH port

The following rules apply to the SSH port:

- Only a specified number of connections from a host are allowed within a specified time frame.
- Only a specified number of connection requests are responded with ICMP-unreachable.
- Further connection requests are dropped until new connection requests stop for a specified period.

Additional port assignments

DNS server

If the DNS server is not in the DMZ, open UDP port 53 on Avaya SBCE through the EMS GUI. Then, Avaya SBCE can access the DNS server.

SNMP

If you have your own SNMP, open the SNMP UDP ports 161 and 162 on Avaya SBCE through the EMS GUI. Then, Avaya SBCE can access the SNMP from the DMZ.

Syslog

If you have your own Syslog, open the Syslog UDP port 514 on Avaya SBCE through the EMS GUI. Then, Avaya SBCE can access the Syslog from the DMZ.

Media ports

The default media port range is 35000 to 40000, but other media port ranges can be configured, if a different media port range is required.

SIP signaling ports

The following ports are default ports. Other ports can be configured.

- TCP/UDP 5060
- TLS 5061

Página2636 de 3226.

HTTP/HTTPS ports

These ports are used for Personal Profile Management (PPM) communications and configuration files and firmware downloads. Configure these ports on Avaya SBCE through the EMS GUI. Then, the phones can login and download configuration files from Avaya HTTP server or HTTPS server.

- HTTP port 8080 or port 80
- HTTPS port 443

LDAP/LDAPS ports

- LDAP port 389
- LDAPS port 636

Avaya Aura® Media Server Offloading port

The default port is port 7150.

Shared Control port

In Remote Worker deployments where endpoints are configured in the shared control mode, enable shared control port on the internal interface of Avaya SBCE towards Avaya Aura® network. This port could be any unused TLS port on the internal interface of Avaya SBCE, for example, port 5063 . This port must be enabled on the internal firewall between Avaya SBCE and the Avaya Aura® network.

For more information about port usage, see *Avaya Port Matrix: ASBCE*.

Chapter 7: Licensing requirements

Avaya SBCE uses the Avaya Product Licensing and Delivery System (PLDS) to create Release 7.2 licenses and download Avaya SBCE software. The license file generated by PLDS is downloaded to the EMS. PLDS is not integrated with WebLM. Use PLDS to perform operations such as license activations, license upgrades, license moves and software downloads.

There are two licensed versions of Avaya SBCE:

- Standard Services delivers secure SIP trunking.
- Advanced Services adds Mobile Workspace User, Media Replication and other features to the Standard Services offer.

Avaya Aura® Mobility Suite and Collaboration Suite licenses include Avaya SBCE.

Note:

Licenses and a WebLM server are required for an upgrade to Release 7.2 or a new installation of Avaya SBCE Release 7.2.

Avaya SBCE license features

To use a feature, you must ensure that the license file that you upload to WebLM has the appropriate licenses for the feature. You cannot configure or use a feature if the correct license for that feature is not present in the license file.

License feature	Description
VALUE_SBCE_STD_SESSION_1	Specifies the number of standard session licenses.
VALUE_SBCE_STD_HA_SESSION_1	Specifies the number of standard service HA session licenses.
VALUE_SBCE_ADV_SESSION_1	Specifies the number of session licenses for remote worker, media recording, and encryption. **Note:** You must buy and deploy a standard session license with every advanced license feature.
VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.

Table continues…

Página2638 de 3226.

License feature	Description
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Scopia® video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Scopia® video conferencing HA session licenses.
VALUE_SBCE_CES_SVC_SESSION_1	Specifies the number of Client Enablement Services session licenses.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Specifies the number of Client Enablement Services HA session licenses.
VALUE_SBCE_TRANS_SESSION_1	Specifies the number of transcoding session licenses.
VALUE_SBCE_TRANS_HA_SESSION_1	Specifies the number of transcoding HA session licenses.
VALUE_SBCE_ELEMENTS_MANAGED_1	Specifies the maximum number of Avaya SBCE elements managed.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that download of VMware OVA files is permitted for Avaya SBCE.
VALUE_SBCE_ENCRYPTION_1	Specifies the Avaya SBCE encryption, and is required for advanced licenses.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1	Specifies the configuration of HA for the setup.
FEAT_SBCE_DYNAMIC_LICENSING_1	Specifies that dynamic or pooled licensing is permitted for Avaya SBCE.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies encryption Avaya SBCE encryption only for signaling.

WebLM server details

Avaya SBCE uses WebLM for licensing requirements.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

  The primary host ID of WebLM is used for creating the license file.
- Licensed features
- Licensed capacity

You can install the Avaya SBCE license file on System Manager WebLM, local WebLM, or standalone WebLM server.

Página2639 de 3226.

Do not use IP OfficeWebLM for installing the Avaya SBCE license file. Avaya SBCE does not support IP OfficeWebLM.

Use the following URL formats for installing a license on the System Manager WebLM server or standalone WebLM server:

- System Manager WebLM server: https://<SMGR_server_IP> :52233/WebLM/LicenseServer
- Standalone WebLM server: https://<WEBLM_server_IP> :52233/WebLM/LicenseServer

For installing a license through a local WebLM server on :

- Avaya SBCE in virtualized environment: Download the WebLM OVA file from PLDS and deploy the OVA file on the virtual machine.
- Avaya SBCE hardware device: Select the **Use local WebLM server** check box.

Options for configuring the WebLM server IP address are available on the System Management page of the EMS web interface.

Warning:

Virtual EMS cannot run a local WebLM.

Página2640 de 3226.

Chapter 8: Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com

Title	Description	Audience
Implementation		
Deploying Avaya Session Border Controller for Enterprise	Hardware installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.	Implementation engineers
Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment	Virtual installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.	Implementation engineers
Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading to Avaya SBCE 7.2.	Implementation engineers
Maintenance and Troubleshooting		
Administering Avaya Session Border Controller for Enterprise	Configuration and administration procedures.	Implementation engineers, Administrators
Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	Troubleshooting and maintenance procedures.	Implementation engineers, and Sales engineers
Reference		
Avaya Port Matrix: ASBCE 7.2	Port information.	Implementation engineers, Administrators, and Sales engineers

Related links

Finding documents on the Avaya Support website on page 101

Página2641 de 3226.

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Related links

Documentation on page 100

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Note:

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

Course code	Course title
5U00090E	Knowledge Access: Avaya Session Border Controller
5U00160E	Knowledge Collection Access: Avaya Unified Communications Core Support

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

Página2642 de 3226.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Página2643 de 3226.

Glossary

ARP	Address Resolution Protocol
Codec	Coder/Decoder
Day Zero Attack	See Zero-Day Attack.
DDoS	Distributed Denial-of-Service
Demilitarized Zone (DMZ)	A computer network-related term that refers to the “neutral zone” between an enterprise’s private network and outside public network. Typically, a computer host or small network is inserted into this neutral zone to prevent outside users from getting direct access to the internal network.
Denial-of-Service (DoS)	The objective or end-result of certain types of malicious attacks or other activities against a network, where access to network services, resources, or endpoints is prohibited.
Digest Authentication (DA)	A Hypertext Transport Protocol (HTTP) authentication scheme whereby user passwords are encrypted prior to being sent across the Internet, thus certifying the integrity of the Uniform Resource Locator (URL) data. The downside of DA is that although passwords are encrypted, the data being exchanged is not; it is sent in the clear.
Distributed Denial-of-Service (DDoS)	A more sophisticated type of DoS attack where a common vulnerability is exploited to first penetrate widely dispersed systems or individual end-points, and then use those systems to launch a coordinated attack. Much more difficult to detect than simple DoS attacks.
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DoW	Day-of-Week
EMS	Element Management System
FW	Firewall
GARP	Gratuitous Address Resolution Protocol
GUI	Graphical User Interface

Página2644 de 3226.

HA	High-Availability or Harvest Attack
High-Availability	The SBCE feature that allows two SBCE security devices to be deployed as an integral pair, wherein one of the devices functions as the Primary and the other as an Alternate or Standby. Connected by a heartbeat signal and shared database, the two SBCE security devices provide failover protection in the event one of the devices malfunctions.
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ICMP	Internet Control Message Protocol
IM	Instant Messaging
Intrusion	A malicious user or process deliberately masquerading as a legitimate user or process.
IP	Internet Protocol
IPS	Intrusion Protection System
ITSP	Internet Telephony Service Provider
Latency	The amount of time it takes for a packet to cross a network connection, from sender to receiver. Also, the amount of time a packet is held by a network device (firewall, router, etc.) before it is forwarded to its next destination.
MAC	Message Authentication Code
MCD	Machine Call Detection
NAT	Network Address Translation
NTP	Network Time Protocol
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SBCE	Session Border Controller for Enterprise
Secure Sockets Layer (SSL)	SSL is a commonly-used method for managing the security of a message transmitted via the Internet and is included as part of most browsers and Web server products. Originally developed by Netscape, SSL gained the support of various influential Internet client/server developers and became the de facto standard until evolving into Transport Layer Security (TLS).

Página2645 de 3226.

	The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer (where a “socket” is an endpoint in a connection). SSL uses the Rivest, Shamir, and Adleman (RSA) public-and-private key encryption system, which also includes the use of a digital certificate. If a Web site is hosted on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SPAM	A common term used to describe the deliberate flooding of Internet addresses or voice mail boxes with multiple copies of the same digital or voice message in an attempt to force it on users who would not otherwise choose to receive it. SPAM can be either malicious or simply annoying, but in either case the cost of sending those messages are for the most part borne by the recipient or the carriers rather than by the sender (SPAMMER).
Spoof	A prevalent method of deceiving VoIP endpoints to gain access to and manipulate its resources (for example, faking an Internet address so that a malicious user looks like a known or otherwise harmless and trusted Internet user).
SRTP	Secure Real-Time Transport Protocol
SSL	Secure Socket Layer
STUN	Simple Traversal of UDP through NAT
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
ToD	Time-of-Day
Tromboning	The situation where RTP media traffic originates at a certain point within a network and follows a path out of that network into another network (the

	access network, for example) and back again to a destination close to where it originated. See Anti-Tromboning.
Tunneling	A security method used to ensure that data packets traversing an unsecure public network do so in a secure manner that prevents disruption or tampering.
TURN	Traversal Using Relay NAT
UDP	User Datagram Protocol
VM	Voice Mail
VoIP	Voice-over-Internet Protocol
VPN	Virtual Private Network
Zero-Day Attack	A particular type of exploit that takes advantage of a security vulnerability in a network on the same day that the vulnerability itself becomes generally known. Ordinarily, since the vulnerability isn't known in advance, there is oftentimes no way to guard against an exploit or attack until it happens.
Zombie	An IP network element that has been surreptitiously taken over by an attacker, usually without the user's knowledge.

Página2647 de 3226.

Index

A

ACP 100 series 76
additional network security deployment 19
advanced services offer 11
AES-256 support
    media encryption 65
altitude requirements 82
AMAX server 83, 84
ANAT 66
anomaly detection 11, 12, 87
Avaya Aura® applications on Amazon Web Services
    overview 18
Avaya SBCE
    architecture overview 16, 46
    support for IPO trunk from dynamic IP address 59
    support for transcoding 65
Avaya SBCE connected to multiple subnets, using a single VLAN 52
Avaya SBCE connected to multiple subnets on two interfaces 51
Avaya SBCE deployment models 14

B

BFCP
    architecture 40
    description 38
    overview 38
BFCP architecture 40
border access control 14
borderless UC 10

C

call handling
    WebRTC 45
call pattern detection 87
certifications of server 84
CES
    secure proxy 60
codec validation 13
command
    protect-socket 93
common firewall rules 90
common rules 91
compatibility matrix 77
control center 87
converged conference
    edge server 67
Converged Conference
    features 69

D

data interface firewall rules 90
data interface restrictions 89
Debian Linux 77
debian package install 89
Dell R210 II 76, 83, 84
Dell R320 76
Dell R620 76
Dell R630 76
denial of service 89
deploy
    multiple SBCE in HA mode 45
    multiple SBCE in non-HA mode 44
deployment
    multiple SBCE 44
detecting
    portscan 91
detection 87
DNS rules 93
DNS server port 95
document changes 8
DoS activity reporting 89
DoS attacks 11
dynamic trust scores 87

E

E.164 number mapping 70
edge server
    converged conference 67
element management system 10
EMS 10
EMS takeover 81
end-point fingerprints 87
end-to-end secure indication 64
ENUM 70
    algorithm 70
    processing 70
environmental requirements for server 83, 84
EZChip adapter 72

F

failover 80
far end camera control 37
firewall rules
    common 90
    data interface 90
    management 90
firewall rules, generating 93
flood protection 86
floor 38

Página2648 de 3226.

floor chair 38
floor control 38
floor control server 38
floor participant 38
Forward Error Correction
FEC 42
fuzzing protection 86

G

GARP support 79

H

hardware platforms 10
hardware warranty 9
header manipulation 23
high availability 79
Avaya SBCE 80
HP DL360 G8 76
HP DL360 G9 76
HTTP/HTTPS ports 95
https rules 93

I

ICMP
restrictions 91
ICMP flood 88
ICMP flood prevention 88
identity engine 44
iDRAC
hardware platforms 61
iLO 60
information management subsystem 13
in-line deployment 14
intelligence element 12, 13
IP Office SSL 23
IPTable firewall rules 88
IPv6 addresses 66

K

KILLSCAN
rules 91
KVM overview 19

L

layer 3 and 4 security features 88
license administration
WebLM support 43
license download 97
license feature
SBCE 97
licensing
licensing *(continued)*
advanced services 97
standard services 97
Linux operating system 77
logging 54

M

management and MGMTPROTECT rules 92
management firewall rules 90
management interface port restrictions 94
management interface restrictions 89
master storage repository 13
MDA 29
media
unanchor 22
media anchoring 22
media anomaly prevention 86
media element 12, 13
media ports 95
Medpro TN2302 circuit pack 79
mobile workspace user 22
monitoring 87
monitoring, detection and protection 87
MontaVista Linux 77
multiple gateways on the same network 53
multiple subnet 48
multiple subnet overview 48
multiple subnet scenario
Avaya SBCE connected to multiple subnets on two interfaces 51
multiple subnet scenarios
multiple gateways on the same network 53
multiple subnets on a single interface, using a single VLAN 52
single data interface 50
multiple subnets on a single interface 50
multi-tenancy 56

N

NAT traversal 13
network security 19
new features 21, 22

O

offer and exchange rules for BFCP 38
on-board storage 76
one-wire deployment 14
one-X mobile
secure CES proxy 60

P

parallel mode configuration 80

Página2649 de 3226.

password
policies ... 20
PLDS ... 97
port assignments
DNS ... 95
HTTP/HTTPS ... 95
media ... 95
SIP signaling ... 95
SNMP ... 95
Syslog ... 95
port restrictions ... 94
port scan blocking ... 88
Portwell CAD-0208 ... 76, 83, 84
power requirements of server ... 83
prevention ... 88
processors ... 76
product compatibility ... 76
protection against layer 3 and layer 4 floods and port scans ... 88

R

real time
SIP Server Status ... 43
reconnaissance prevention ... 86
REFER ... 27
registered users
user registrations ... 43
reinvite ... 30
related documentation ... 100
remote user ... 22
remote worker ... 22
replication
EMS ... 81
restrictions
data interface ... 88
reuse of IP Office connection for call delivery ... 59
reverse proxy ... 36
RTCP ... 30
monitoring report generation ... 35
RTP anomaly detection ... 13
rules
data interface ... 93
firewall ... 93

S

safety requirements ... 84
SAL gateway ... 77
SBCE
license feature ... 97
SBC hardening ... 88
scenarios ... 40
Scopia and Avaya SBCE interoperability with SRTP ... 47
screened subnet deployment ... 14
scrubber rules package ... 90
scrubber templates ... 90
securable field ... 64
security life cycle ... 11
security settings ... 89
server
certifications ... 84
dimensions ... 82
environmental requirements ... 83
humidity requirements ... 83
power requirements ... 83
temperature requirements ... 83
servers ... 76
capacity ... 78
Serviceability Agent support ... 55
Session Manager failure
call preservation ... 71
SigMa module ... 10
signaling decryption ... 12
signaling element ... 12
signaling manipulation ... 23
single sign on ... 44
SIP call processing ... 24
SIP decoding ... 12
SIPREC
continuous recording ... 64
features ... 62
selective recording ... 64
SIPREC support
overview ... 61
SIP signaling ports ... 95
SIP trunking ... 24
SIP trunk integration module ... 10
SIP validation ... 12
site requirements
safety ... 84
SNMP ports ... 95
software warranty ... 9
spoofing ... 11, 12, 86
SRTP considerations ... 48
SRTP encryption of media ... 14
SRTP support ... 47
SSH port rules ... 95
SSH rules ... 92
SSL VPN ... 23
standard services
configuration ... 10
offer ... 10
stealth attack prevention ... 86
support ... 102
remote ... 23
support under warranty ... 9
Syslog port ... 95
system configurations ... 10
system memory ... 76
system requirements
altitude ... 82
humidity ... 83
power ... 83

Página2650 de 3226.

system requirements *(continued)*
temperature 83

T

TCP flood restrictions 92
TCP packets restrictions 95
TCP signaling level
flood control 88
TCP signaling level flooding control rules 88
thermal requirements 84
TILEncore-Gx36 72
TILEncore-Gx36 adapter
rear panel 75
Tilera adapter 72
TN2302 circuit pack 79
topology hiding 90
traceSBC
log files 54
overview 54
traceSBC advantages 55
training 101
two-wire deployment 14

U

UCID 25
UC proxying 10
unified communication policies 88
unified communications security 11

V

videos 101
virtual private network TLS encryption 14
VLAN
use 47

W

warranty 9
WebLM 97
server details 98
WebRTC
call handling 45

Página2651 de 3226.

Date and Time Settings

You can change the date and time settings used by the server through the server's web configuration pages. The **System** menu shows the server's current date and time.

To change the server date and time settings:

1. Login to the server's web configuration menus.
2. Select **Settings**.
3. Select **System**.
4. Select the **Date Time** section.
   - **Date**
     For a server not using NTP, this field shows the server's current date and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.
   - **Time**
     For a server not using NTP, this field shows the server's current UTC time and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.
   - **Timezone**
     In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The **Timezone** field determines the appropriate offset applied to the UTC time above. Note that changing the timezone can cause a *"Session expired"* message to appear in the browser in which case you need to login again.
   - **Enable Network Time Protocol**
     When selected, the server obtains the current date and time from the NTP servers listed in the **NTP Servers** list below. It then uses that date and time and makes regular NTP requests for updates.
     - **NTP Servers**
       With **Enable Network Time Protocol** selected, use this field to enter the IP address of an NTP server or servers to use. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at http://support.ntp.org/bin/view/Servers/WebHome. However, it is your responsibility to comply with the usage policy of the chosen server. Choose several unrelated NTP servers in case one of the servers becomes unreachable or its clock unreliable. The server uses the responses it receives from each NTP server to determine reliability.
       - The IP Office system can also use NTP to obtain its system time.
     - **Synchronize system clock before starting service**
       Use this option to synchronize the system clock to an NTP time server before starting other services. Do not use this option if the time server cannot be reliably reached. Waiting for synchronization to occur may block use of the system until a timeout has passed.
     - **Use local time source**
       When not selected, external NTP takes priority over the internal system clock. If selected, the local system clock is used as the time source. Only use this option if system clock is synchronized with another reliable source, for example a radio controlled clock device.
5. Click **Save**.

AVAYA

Engage The Power of We™

Avaya Session Border Controller for Enterprise

A security solution for SIP-based networks implementing unified communications applications

"Customer service is at the heart of what we do, and as a leader in outsourced contact center services, our clients count on us to ensure superior functions and secure service. The Avaya SBCE helps us deliver this, and does so with an eye towards cost-savings. We can reduce our hardware expenses, simplify implementations, and use fewer resources, saving us time and money. Avaya SBCE is critical in helping protect our network, while delivering the cost-saving benefits of SIP trunking."

–Richard Blake, Manager, IT Telecom, Teleperformance

To benefit from the latest communication and collaboration solutions, businesses are increasingly turning to SIP-based networks.

Whether it's to lower costs using IP telephony or to take advantage of the latest multimedia messaging, conferencing and unified communications (UC) applications, SIP is emerging as the industry standard.

Advantages of SIP

Because they are designed for high-fidelity voice, high-definition video and other real-time collaboration applications, carriers are increasingly offering SIP trunks (Session Initiation Protocol). SIP trunks cost-effectively support more telephone extensions and help reduce local, toll-free, domestic and international long-distance communications costs.

With the support of a SIP network, a growing business can more easily and cost effectively roll out the latest UC applications to employees regardless of where they are working: in the office, at home or on the road. The productivity that results from these collaborative, real-time applications can be a major competitive advantage.

SIP Trunk Security

However, SIP trunks also present a security challenge: there is vulnerability at the point where the SIP trunk connects to the public network, which can leave a business exposed to hacker attacks including spoofing, call hijacking, eavesdropping and toll fraud. In addition to potential damage to business operations, privacy and security mandates such as those for credit and health information (e.g., PCI and HIPAA) require that these vulnerabilities be addressed, imposing significant financial and legal penalties for non-compliance.

VPN-less Remote Worker Security

Business customers are now facing an evolving world where users are no longer confined inside the walls of the enterprise. Trends towards mobile access to system resources, telecommuting, and BYOD are creating the need to deliver SIP-based UC and collaborative services to these remote users in a flexible yet secure manner. Avaya Session Border Controller for Enterprise delivers a new solution for this need with security in mind.

Página2654 de 3226.

Security for SIP-based networks

- A clear line of defense where the SIP trunk meets the public network
- Supporting communications applications that drive competitive advantage
- Protection against:
  - Denial of Service (DoS) attacks
  - Spoofing
  - Call Hijacking
  - Toll-fraud blocking
  - Eavesdropping and theft of information
- Multiple vendor compatibility
  - Cisco 8.x & 9.x (CUCM)
  - Mitel
  - Shoretel
  - Microsoft Lync
- Fine-grained policy enforcement

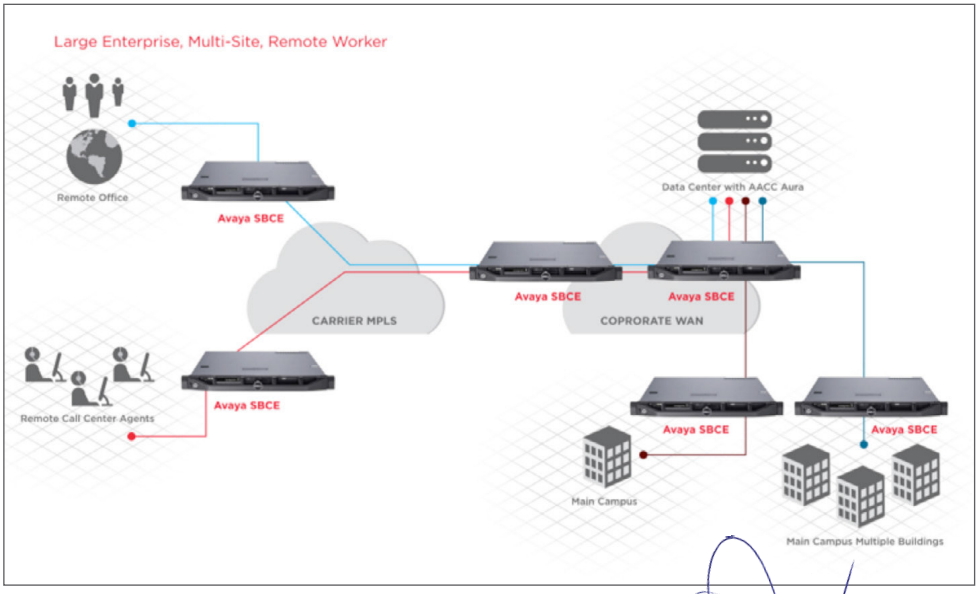
Multi Domain Security

Network support for multiple users connecting via multi-tiered networks, both private and public cloud based, is a necessity. This is especially true for large multinational enterprises or large scaled government communication installations. The criticality of maintaining secure access regardless of location is understood, but the solution is not always as obvious. Avaya Session Border Controller for Enterprise helps provide the necessary functions for network-to-network security as well as network-to-user security. This means that for a large

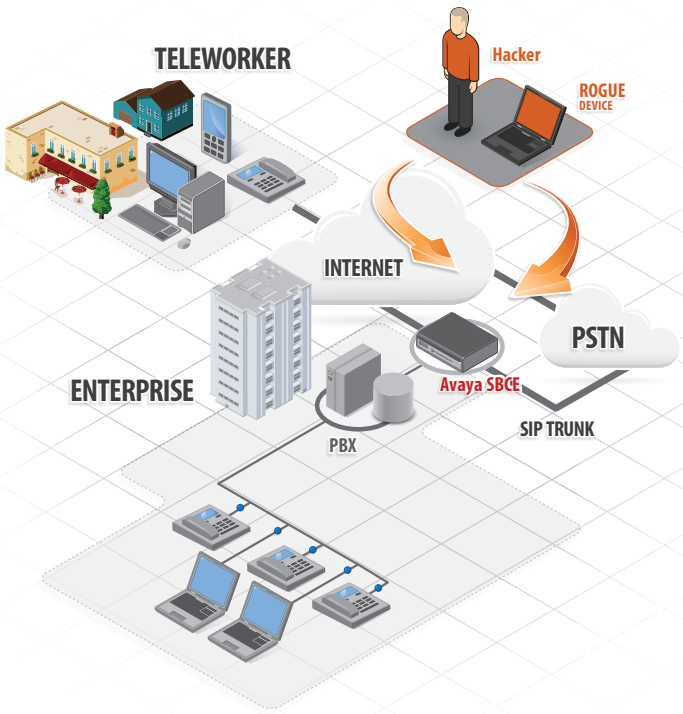
scale, geographically extended network, all layers of network access can be kept secure. The back-to-back-to-back capabilities of the Avaya Session Border Controller for Enterprise will help ensure secure user access no matter how extended and diverse.

Cloud

As more enterprises are looking at hosted alternatives for their collaboration environments, it becomes even more critical for the interfaces between enterprise and host to be secure and manageable. The Session Border Controller for Enterprise offers an interface that helps to support network protection and enterprise control of VOIP traffic. Avaya sees increased interest in configurations that are a hybrid architecture, hosted applications as well as enterprise on premise applications. The Session Border Controller for Enterprise is the protection needed to help address proper protocol support and a truly integrated and secure network infrastructure.



Página2655 de 3226.



A Solution for Growing Businesses

The Avaya Session Border Controller for Enterprise (Avaya SBCE) helps address the security vulnerabilities in SIP networks in a cost-effective, easily-implemented, single-box solution.

Easily operated from an intuitive graphical user interface (GUI), the Avaya SBCE establishes a precise demarcation where the SIP trunks meet the enterprise network, presenting a clear line of defense. It helps deliver enterprise-class security that helps mitigate the risks of Denial of Service (DoS) and application-layer threats as well as toll-fraud. Fine-grained policy enforcement helps support ongoing compliance.

With Avaya SBCE in place, growing businesses can adopt the collaborative and unified communications applications that drive competitive advantage.

Single-box Solution for SIP Network Security

Avaya Session Border Controller for Enterprise provides an advanced application-layer security architecture in one device: SIP Firewall, Session Border Controller, Intrusion Detection System and Intrusion Prevention System (IDS/IPS), Access Controller, Authentication, Unified Communications Proxy and Policy Enforcement for all real-time unified communication applications.

Help Secure and Support BYOD

Consumer devices are pouring into the enterprise. Businesses can leverage BYOD—Bring Your Own Device—as a way to reduce costs, increase productivity, and enhance communication and collaboration. The challenge is how to say yes to BYOD while maintaining control of the network.

Avaya Session Border Controller for Enterprise with IP Office

Avaya IP Office is the solution many growing businesses turn to for comprehensive, easily implemented unified communications.

With more than 300,000 systems installed worldwide, IP Office is an industry standard-bearer, delivering the communications and productivity tools today's employees need to perform at their best.

When Avaya IP Office is implemented in conjunction with SIP trunks, the Avaya Session Border Controller for Enterprise works hand in hand to help protect against security threats.

Página2656 de 3226.

As more enterprises are looking at hosted alternatives for their collaboration environments, it becomes even more critical for the interfaces between enterprise and host to be secure and manageable.

The Session Border Controller for Enterprise is the protection needed to help support proper protocol support and a truly integrated and secure network infrastructure.

Every enterprise is impacted by and talking about BYOD, but what can get lost in the conversation is the fact that BYOD is more than just device management. Avaya supports BYOD with a combination of security, authentication, networking, and policies. The Avaya solution includes device authentication, access control for wired and wireless devices, secure remote access, and support via a range of services.

The Avaya Session Border Controller for Enterprise is designed to securely enable many deployments, including:

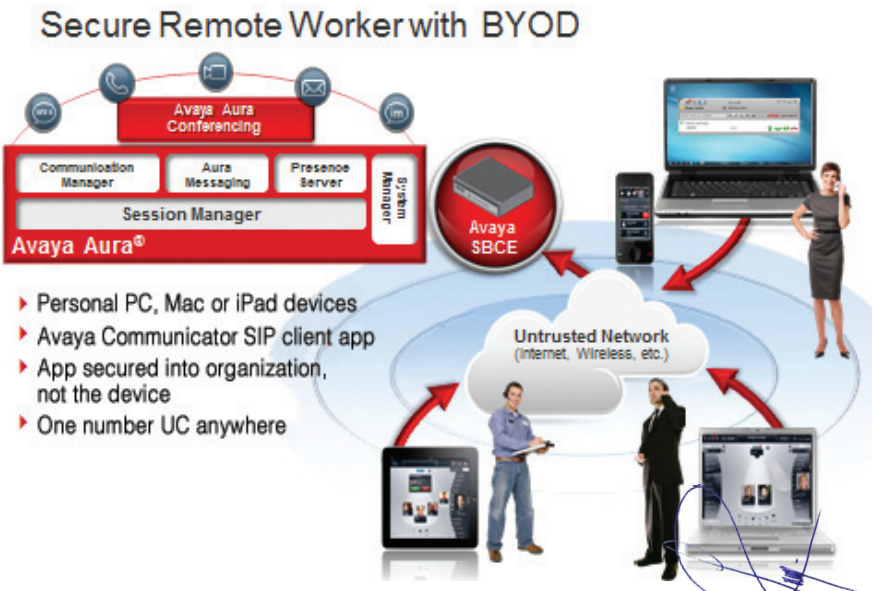
- Enabling remote workers to connect without VPN, offering support of Bring Your Own Device (BYOD) without the administrative overhead of a Virtual Private Network (VPN) solution
- Help secure UC applications entering the enterprise core
- Help secure Border Access for incumbent and competitive local exchange

Support for Legacy Communications

Security for remote access is not just an issue for new systems; even legacy call systems see requirements to add secure mobile collaboration. The Avaya Session Border Controller for Enterprise has been extensively tested for compatibility with Avaya Aura® and Avaya IP Office installations as well as to support the legacy systems of our customers. The Avaya Session Border Controller for Enterprise will support:

- Avaya Aura platform Release 6.1 and higher
- Avaya IP Office 9.0
- Avaya Communication Server 1000 Release 7.6

Maintaining secure remote access is our goal for all collaboration solutions and enterprise mobility requirements.



Página2657 de 3226.

Virtualization

The need to reduce CapEx and consolidate the network environment has led many enterprises to utilize a virtual application solution for real-time collaboration. Extending the benefits of infrastructure virtualization offers a less costly implementation. In addition, the move to virtualization can provide ongoing savings in IT operating expenses due to support for a common system architecture. The secure access requirements for SIP based communications can also significantly reduce the hardware requirements for system design. The Avaya Session Border Controller for Enterprise offers a virtualized solution for the management as well as the core appliance. This will support the overall move to a virtualized collaboration solution for all customers as they fulfill the enterprise requirements for SIP access and remote worker security.

Avaya Session Border Controller for Enterprise core application software and EMS are available as OVA files for installation on VMware. More details are available in the Avaya Session Border Controller for Enterprise VMware deployment guide available on the **Avaya Support website**.

Avaya SBCE VMware Resources	EMS	EMS & SBCE
vCPU	3 vCPU	4
Min Processor	2.4 GHz (Xeon x5670 or equivalent)	2.4 GHz
CPY reservation	7200 MHz	9600 MHz
Virtual memory	4G	8G
Virtual Storage	80G	80G
Shared NICs	2@100Mbps or 1000 Mbps	4@100Mbps or 1000 Mbps

The Avaya Session Border Controller for Enterprise offers a virtualized solution for the management as well as the core appliance, supporting the overall move to a virtualized collaboration solution for any enterprise.

As part of the Avaya support for a virtualized collaboration solution, Avaya Aura Virtualized Environment provides a complete set of UC and Collaboration applications all compatible with VMware and ready for installation on a customer provided virtualized infrastructure.

Página2658 de 3226.

Specification	Low Range SBCE Portwell (Core)	Mid Range SBCE		Mid Range SBCE (Dual PSU)	
		Dell (Core)	Dell EMS	Dell (Core/EMS)	HP (Core/EMS)
Product Type	Avaya SBCE	Avaya SBCE	Avaya EMS	Avaya SBCE, EMS	Avaya SBCE, EMS
SIP Trunk Sessions	250	6000	NA	6000	NA
Remote Worker Sessions	250	1200	NA	1200	NA
Part Number	271023	271021	271022	308596	308597
Platform Type	CAD-0208-3402-900	PE R210 II XL (OEM)	PE R210 II XL (OEM)	PE R620 (CR2 OEM)	DL 360pG8 (CR2 OEM)
BIOS	08.00.15	1.1.1	1.1.1	2.2.2	P71 03/01/2013
Main Processor	ATOM D510 – 1.66GHz	Xeon E3-1220 - 3.1GHz (Quad core - 80W)	Pentium G850 2.9 GHz (Dual core)	Xeon E5-2630 2.3 GHz (Hex Cores)	Xeon E5-2630 2.3 GHz (Hex Cores)
Memory	2GB DDR2 667MHz SODIMM	4GB (2 X 2GB) DDR3 1333MHz, UDIMM	2GB (1 X 2GB) DDR3 1333MHz, UDIMM	16GB (4 x 4GB) DDR3 1600MHz, RDIMMS	16GB (4 x 4GB) DDR3 1600MHz, RDIMM
RAID	No	No	RAID 1	RAID 1	RAID 1
Hard Drives	320GB (SATA)	250/500GB (SATA)	2 X 500 GB (SATA)	2 X 300 GB (SAS)	2 X 300 GB (SAS)
Optical Drive	No	No	No	DVD+/-RW	DVD+/-RW
Compact Flash	No	No	No	No	No
PCI Cards	-	1 X Quad Port NICP-CIe-4	1 X H200 (SAS/SATA) RAID Controller	1 X Dual 1GbE Port NIC	1 X Dual 1GbE Port NIC
TPM	No	No	No	No	No
LED Display	No	Yes	Yes	Yes	Yes
Interfaces (Ports)					
Data	4 X 1GbE	6 X 1GbE	2 X 1GbE	6 X 1GbE	6 X 1GbE
USB	2	2	2	2	2
Console	1 (RJ-45)	1 (DB 9 - Female)	1 (DB 9 - Female)	1 (DB 9 - Female)	1 (DB 9 - Female)
VGA	Yes	Yes	Yes	Yes	Yes
Replaceable Fan	No	No	No	No	No
Replaceable Hard Drive	No	No	No	Yes	Yes
Redundant PSU	No	No	No	Yes	Yes
Port Bypass	No	No	No	No	No
Form Factor	1U (Desk or Rack Mount)	1U	1U	1U	1U
Bezel	-	Dell OEM - Avaya Branded	Dell OEM - Avaya Branded	Dell OEM - Avaya Branded	HP OEM - Avaya Branded

Specification	Low Range SBCE Portwell (Core)	Mid Range SBCE		Mid Range SBCE (Dual PSU)	
		Dell (Core)	Dell EMS	Dell (Core/EMS)	HP (Core/EMS)
Dimensions					
Height	1.7 in	1.7 in	1.7 in	1.7 in	1.7 in
Width	11.75 in	17.1 in	17.1 in	17.1 in	17.1 in
Depth	5.75 in	15.5 in	15.5 in	26.9 in	27.5
Boxed					
Height	7.5 in	10 in	10 in	11.5	8.8
Width	12 in	24 in	24 in	24.25	23.31
Depth	15 in	32 in	32 in	36.25	38.69
Weight					
Unit	3 lbs.	15.5 lbs.	16.2 lbs.	41 lbs.	42.3 lbs.
Boxed	6 lbs.	30 lbs.	31 lbs.	48 lbs.	49 lbs.
Input	100/240V AC Adaptor (12V DC)	100/240V AC	110/240V AC	110/240V AC	110/240V AC
Nominal Current (110V)	0.2 A	1.1A	1.1A	1.5A	1.5A
Maximum Current (110V)	0.5 A	2 A	2 A	4.5A	4.5A
AC Power (Max)	40 Watts	250 Watts	250 Watts	500 Watts	500 Watts
Environmental					
Nominal Operating Temp	20oC	20oC	20oC	20oC	20oC
Operating Temp Range	5oC ~ 35oC	10oC ~ 35oC	10oC ~ 35oC	10oC ~ 35oC	10oC ~ 35oC
Relative Humidity	20% ~ 90%	10% ~ 90%	10% ~ 90%	10% ~ 90%	10% ~ 90%
Storage Temp	0oC ~ 75oC	-40oC ~ 65oC	-40oC ~ 65oC	-40oC ~ 65oC	-30oC ~ 60oC
Certifications & Compliances	FCC, CE, UL & RoHS	FCC, CE, CSA, UL & RoHS	FCC, CE, CSA, UL & RoHS	FCC, CE, CSA, UL & RoHS	FCC, CE, CSA, UL & RoHS
HTS	8517.62.0050				
ECCN's	H/W = 5A002 (A.1), S/W = 5D002 (C.1)				
Export License	Exception: ENC - Restricted to "Non - Government" End Users. Ref: Section 740.17(A), (B)(1) and (B)(2)				
CCATS	G072860				

About Avaya

Avaya is a leading, global provider of customer and team engagement solutions and services available in a variety of flexible on-premise and cloud deployment options. Avaya's fabric-based networking solutions help simplify and accelerate the deployment of business critical applications and services. For more information, please visit **www.avaya.com**.

© 2015 Avaya Inc. All Rights Reserved.
Avaya and the Avaya logo are trademarks of Avaya Inc. and are registered in the United States and other countries. All other trademarks identified by ®, TM, or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc.
02/15 • UC4834-09

Provide FEEDBACK for this document

IP Office™ Platform 11.0

Deploying IP Office Essential Edition (IP500 V2)

Contents

1. System Overview

1.1 Changes for Release 11.0 9
1.2 Additional Documentation 11
1.3 Equipment Availability 12
1.4 Repair 12
1.5 RoHS 12
1.6 IP Office Modes 13
1.6.1 System SD Cards 13
1.6.2 Overall Capacity 14
1.6.3 Hardware Support Summary 15
1.6.4 Feature Support Summary 16
1.7 The Control Unit 18
1.8 IP500 V2 System Components 19
1.9 System SD Card 21
1.10 Licensing 21
1.11 Control Unit Cards 22
1.11.1 IP500 Base Cards 22
1.11.2 IP500 Trunk Cards 25
1.12 External Expansion Modules 26
1.12.1 IP500 External Expansion Modules 27
1.12.2 IP400 External Expansion Modules 28
1.12.3 Connecting External Expansion Modules 29
1.13 Power Supplies and Cables 30
1.13.1 Power Supplies 30
1.13.2 Power Supply Cords 31
1.13.3 Power Supply Backup 32
1.13.4 Cabling and Cables 33
1.13.5 Grounding 35
1.13.6 Lightning Protection/Out-of-Building Connections 36
1.14 Wall and Rack Mounting 37
1.14.1 Wall Mounting Kits 37
1.14.2 Rack Mounting Kits 38
1.15 IP Office Phones 39
1.16 VoIP 40
1.16.1 Voice Compression Channels 41
1.17 Supported Country Locales 42
1.18 IP Office Software Applications 42
1.18.1 Programming Applications 43
1.18.2 User Applications 44
1.18.3 Voicemail Applications 44
1.18.4 Call Logging Applications 45
1.18.5 Call Center Applications 45
1.18.6 CTI Applications 45
1.19 Training 46
1.20 Web Sites 46
1.21 Emergency and Power Failure Ports 47

2. Installation Overview

2.1 Environmental Requirements 51
2.2 Space Requirements 53
2.2.1 Control Unit 53
2.2.2 External Expansion Modules 54
2.2.3 Wall Mounting 55
2.2.4 Rack Space Requirements 57
2.3 Tools and Parts Required 59
2.4 Documentation 60
2.5 Unpacking 60

3. Installing the Administrator Software

3.1 Downloading the Software 63
3.2 Installing the Administrator Applications 64
3.3 Installer PC Connection 67
3.4 Starting IP Office Manager 68
3.5 Starting System Status Application 69
3.6 Starting System Monitor 70
3.7 Starting IP Office Web Manager 71

4. Preparing the System SD Card

4.1 Upgrade the Card Firmware 75
4.2 Creating an Offline Configuration File 76
4.3 Importing and Exporting Settings 77
4.4 Adding a Pre-Built Configuration File 78
4.5 Adding a License File 78
4.6 Adding Security Certificates 78
4.7 Adding a 9600 Series Screen Saver File 79
4.8 Adding Music on Hold Files 79

5. Installing the Control Unit Cards

5.1 Fitting IP500 Daughter Cards 83
5.2 Inserting IP500 Base Cards 84

6. Installing the Physical System

6.1 Wall Mounting 87
6.1.1 Wall Mounting Kit V3 88
6.2 Rack Mounting 89
6.3 Connecting External Expansion Modules 91
6.4 Grounding 93
6.5 Starting the System 94
6.6 Checking the LEDs 95
6.7 Connecting Phones 97
6.7.1 Analog Phones 97
6.7.2 ETR Phones 97
6.7.3 DS Digital Station Phones 97
6.7.4 IP/SIP Phones 97
6.7.5 TCM/BST Phones 98

7. Initial Configuration using Manager

7.1 Network Connection 101
7.2 Initial Configuration 103
7.3 Extension Numbering 104
7.4 Disable Unused Trunks 105
7.5 Setting the Digital Trunk Clock Source 107
7.6 Setting the Trunk Prefixes 109
7.7 DS16B/30B Port Mode Selection 110
7.8 Uploading the License File 111
7.9 Saving the Configuration 112

8. Initial Configuration Using IP Office Web Manager

8.1 The System's Initial IP Address 114
8.2 New System Install 115
8.3 Existing System 118

Página2663 de 3226.

8.4 Dashboard Wizard Menus ... 119
8.4.1 System Settings ... 120
8.4.2 VoIP Settings ... 122
8.4.3 Voicemail Settings ... 123
8.4.4 Licensing Settings ... 124
8.4.5 Users and Extensions ... 125
8.4.6 Groups ... 126
8.4.7 Lines ... 127
8.4.8 Incoming Call Routes ... 128
8.4.9 Outgoing Call Routes ... 129

9. System Security

9.1 Changing the Default Security Settings ... 133
9.2 Changing the Remote User Password ... 135
9.3 Disabling SIP Trunk Support ... 135
9.4 Disabling H.323 Telephone Support ... 135

10. On-Boarding

10.1 On-Boarding ... 139

11. SD Card Management

11.1 Booting from the SD Cards ... 144
11.2 Creating an IP Office SD Card ... 146
11.3 Viewing the Card Contents ... 148
11.4 Backing Up to the Backup Folder ... 149
11.4.1 Backup to the Backup Folder Using IP Office Manager ... 149
11.4.2 Backup to the Backup Folder Using System Status Application ... 149
11.4.3 Backup to the Backup Folder Using a System Phone ... 149
11.4.4 Backup to the Backup Folder Using a IP Office Web Manager ... 149
11.5 Restoring from the Backup Folder ... 150
11.5.1 Restoring from the Backup Folder Using IP Office Manager ... 150
11.5.2 Restoring from the Backup Folder Using System Status Application ... 150
11.5.3 Restoring from the Backup Folder Using a System Phone ... 150
11.5.4 Restoring from the Backup Folder Using IP Office Web Manager ... 150
11.6 Backing Up to the Optional SD Card ... 152
11.6.1 Backing Up to the Optional SD Using IP Office Manager ... 152
11.6.2 Backing Up to the Optional SD Using System Status Application ... 152
11.6.3 Backing Up to the Optional SD Using IP Office Web Manager ... 152
11.6.4 Backing Up to the Optional SD Using a System Phone ... 152
11.7 Restoring a Configuration from an Optional Card ... 153
11.7.1 Restoring from the Optional SD Using IP Office Manager ... 153
11.7.2 Restoring from the Optional SD Using a System Phone ... 153
11.8 Loading Software from an Optional SD Card ... 154
11.8.1 Loading Software from the Optional SD Using IP Office Manager ... 154
11.8.2 Loading Software from the Optional SD Using a System Phone ... 154
11.9 Backing Up to a PC ... 155
11.10 Restoring from a PC ... 155
11.11 Upgrading Card Software ... 156
11.12 Memory Card Shutdown/Removal ... 157
11.12.1 Shutdown a Card Using IP Office Manager ... 157
11.12.2 Shutdown a Card Using System Status Application ... 157
11.12.3 Shutdown a Card Using IP Office Web Manager ... 157
11.12.4 Shutdown a Card Using a System Phone ... 157
11.13 Memory Card Startup ... 158
11.13.1 Startup a Card Using IP Office Manager ... 158
11.13.2 Startup a Card Using System Status Application ... 158
11.13.3 Startup a Card Using IP Office Web Manager ... 158
11.13.4 Startup a Card Using a System Phone ... 158

12. Additional Processes

12.1 Changing an IP Office Basic Edition System to Standard Mode ... 161
12.2 Automating the Change to Standard Mode ... 162
12.3 Switching Off a System ... 163
12.3.1 Shutdown a System Using IP Office Manager ... 163
12.3.2 Shutdown a System Using System Status Application ... 164
12.3.3 Shutdown a System Using a System Phone ... 164
12.3.4 Shutdown a System Using the AUX Button ... 164
12.3.5 Shutdown a System Using IP Office Web Manager ... 164
12.4 Rebooting a System ... 165
12.4.1 Reboot a System Using IP Office Manager ... 165
12.4.2 Reboot a System Using IP Office Web Manager ... 166
12.4.3 Reboot a System Using the Reset Button ... 166
12.4.4 Rebooting a System Using a System Phone ... 166
12.5 Changing Components ... 167
12.5.1 Like for Like Replacement ... 168
12.5.2 Higher Capacity Replacement ... 168
12.5.3 Lower Capacity Replacement ... 168
12.5.4 Adding a New Component ... 168
12.5.5 Permanent Removal ... 169
12.5.6 Replacemnt with a Different Type ... 169
12.6 Defaulting the Configuration ... 170
12.6.1 Defaulting the Configuration Using IP Office Manager ... 170
12.6.2 Defaulting the Configuration Using IP Office Web Manager ... 170
12.6.3 Defaulting the Configuration Using the Reset Button ... 170
12.6.4 Defaulting the Configuration Using Debug ... 171
12.6.5 Default the Configuration Using a System Phone ... 172
12.6.6 Defaulting the Configuration Using Boot Loader ... 172
12.7 Defaulting Security Settings ... 173
12.7.1 Defaulting Security Using IP Office Manager ... 174
12.7.2 Defaulting Security Using IP Office Web Manager ... 174
12.7.3 Defaulting Security using the RS232 Port ... 175
12.7.4 Defaulting Security Using the Boot Loader ... 176
12.8 Loading a Configuration ... 177
12.8.1 Creating an Offline Configuration File ... 178
12.8.2 Loading a Configuration Using IP Office Manager ... 179
12.8.3 Loading a Configuration Using IP Office Web Manager ... 179

Página2664 de 3226.

12.8.4 Loading a Configuration onto a System SD Card ... 179
12.9 Upgrading systems ... 180
12.9.1 Upgrade Using the Upgrade Wizard ... 181
12.9.2 Locally Upgrade the SD System Card Using Manager ... 183
12.9.3 Upgrading Using an Optional SD Card ... 184
12.9.4 Upgrading Using IP Office Web Manager ... 185
12.10 Swapping Extension Users ... 186
12.11 Out of Building Telephone Installations ... 187
12.11.1 DS Phones ... 188
12.11.2 Analog Phone Barrier Box ... 189
12.11.3 Rack Mounting Barrier Boxes ... 190
12.12 Using the External Output Port ... 191
12.12.1 Port Connection ... 191
12.13 SNMP ... 192
12.13.1 Installing the IP Office MIB Files ... 193
12.13.2 Enabling SNMP and Polling Support ... 195
12.13.3 Enabling SNMP Trap Sending ... 195
12.14 Refreshing the System Files from Manager ... 196
12.15 Reset Button ... 197
12.16 AUX Button ... 197
12.17 RS232 Port Maintenance ... 198
12.18 Erasing the Core Software ... 199
12.18.1 Erasing Core Software Using the Reset Button ... 199
12.18.2 Erasing Core Software Using Debug ... 200
12.18.3 Erasing Core Software Using the Boot Loader ... 201
12.19 Enabling IP Office Web Manager ... 202

13.System Components

13.1 IP500 V2 Control Unit ... 205
13.2 IP500 V2 System SD Cards ... 208
13.3 IP500 Base Cards ... 209
13.3.1 4-Port Expansion Card ... 212
13.3.2 Analog Phone ... 213
13.3.3 ATM Combination Card ... 214
13.3.4 BRI Combination Card ... 216
13.3.5 Unified Communications Module ... 217
13.3.6 Digital Station ... 218
13.3.7 ETR6 Card ... 219
13.3.8 TCM8 Digital Station ... 220
13.3.9 VCM ... 221
13.4 IP500 Trunk Daughter Cards ... 223
13.4.1 Analog Trunk Card ... 224
13.4.2 BRI Trunk Cards ... 226
13.4.3 PRI Trunk Cards ... 227
13.5 IP500 External Expansion Modules ... 228
13.5.1 Analog Trunk 16 ... 229
13.5.2 DS16/30 ... 231
13.5.3 DS16A/30A ... 233
13.5.4 DS16B/30B, DS16B2/30B2 ... 236
13.5.5 Phone 16/30 ... 238
13.6 IP400 Expansion Modules ... 240
13.6.1 Analog Trunk 16 ... 241
13.6.2 Digital Station V2 ... 243
13.6.3 Phone V2 ... 245
13.7 Mounting Kits ... 247
13.7.1 IP500 Wall Mounting Kits ... 247
13.7.2 Rack Mounting Kit ... 247
13.7.3 Barrier Box Rack Mounting Kit ... 248
13.8 Phones ... 249
13.9 Phone Button Modules ... 250
13.10 Applications ... 251
13.10.1 IP Office Application Server ... 252
13.10.2 IP Office Manager ... 253
13.10.3 Media Manager ... 253
13.10.4 Avaya IX Workplace Client (Equinox) ... 254
13.10.5 IP Office Web Client ... 254
13.10.6 Monitor ... 255
13.10.7 one-X Portal for IP Office ... 255
13.10.8 Avaya Communicator ... 256
13.10.9 SoftConsole ... 257
13.10.10 System Status Application ... 257
13.10.11 TAPI ... 258
13.10.12 Voicemail Pro ... 259
13.10.13 Web Collaboration ... 260
13.10.14 IP Office Ports ... 260
13.11 Operating System Support ... 261
13.11.1 Windows Support ... 261
13.11.2 Android Support ... 262
13.11.3 Apple Support ... 262
13.11.4 Linux Support ... 262
13.11.5 Browser Support ... 263
13.12 Physical Ports ... 264
13.12.1 Cables ... 265
13.12.2 ANALOG Port ... 267
13.12.3 AUDIO Port ... 267
13.12.4 BRI Port (So) ... 268
13.12.5 BRI Port (To) ... 269
13.12.6 BST Port (RJ21) ... 270
13.12.7 BST Port (RJ45) ... 270
13.12.8 DC I/P Port ... 271
13.12.9 DS Ports (RJ45) ... 271
13.12.10 EF Port ... 272
13.12.11 ETR Port ... 272
13.12.12 EXPANSION Port ... 273
13.12.13 EXT O/P Port ... 273
13.12.14 LAN Port ... 274
13.12.15 PF Port ... 275
13.12.16 PHONE (POT) Port ... 276
13.12.17 PRI Port ... 277
13.12.18 RS232 Port (DTE) ... 278
13.13 Licences ... 279
13.13.1 System Edition Licenses ... 279
13.13.2 Upgrade Licenses ... 280
13.13.3 Trunk Licensing ... 280
13.13.4 Telephone/Endpoint Licenses ... 281
13.13.5 User Licenses ... 282
13.13.6 Voicemail Pro Licenses ... 284
13.13.7 Trial Licenses ... 285
13.13.8 CTI Licenses ... 285
13.13.9 Other Licenses ... 285
13.14 Hardware/Software Compatibility ... 286
13.14.1 Control Units and Control Unit Components ... 287

Página2665 de 3226

13.14.2 Server Platforms 289
13.14.3 Phones 290
13.14.4 Applications 295
13.15 PCS Levels 296
13.16 TAA 296

14. Safety Statements

14.1 Lightning Protection/Hazard Symbols 298
14.2 Trunk Interface Modules 299
14.3 Further Information and Product Updates 300
14.4 Port Safety Classification 300
14.5 EMC Directive 301
14.6 Regulatory Instructions for Use 302
14.6.1 Australia 302
14.6.2 Canada 302
14.6.3 China 303
14.6.4 Japan 304
14.6.5 European Union 304
14.6.6 New Zealand 304
14.6.7 FCC Notification 305
14.6.8 Compliance with FCC Rules 307

15. Document History

Index 315

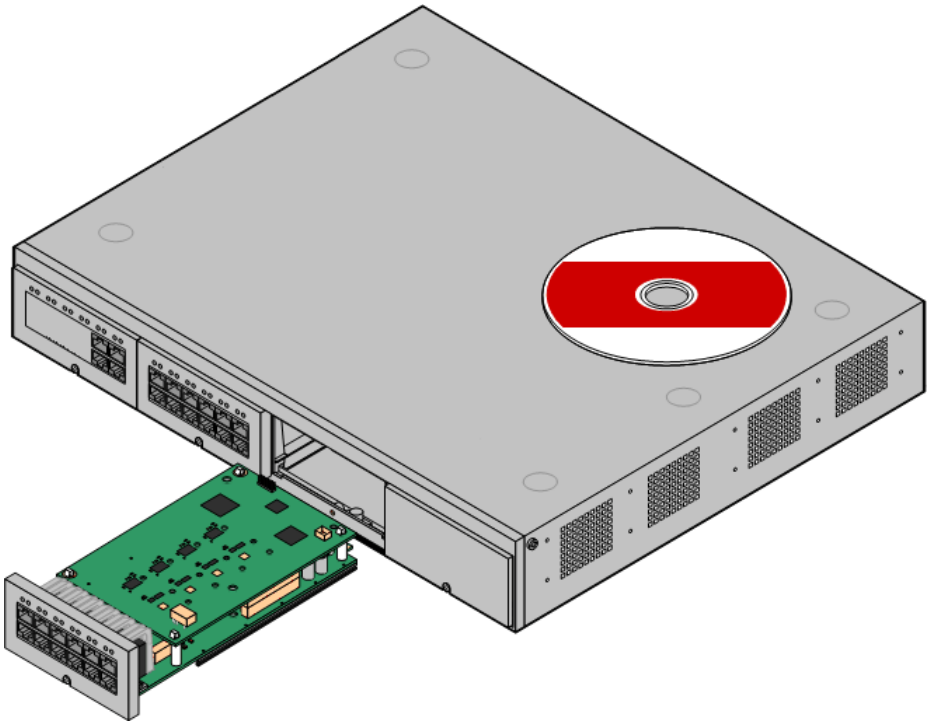
Chapter 1.
System Overview

1. System Overview

This document is intended to assist with the installation of an IP Office system running in IP Office standard mode (IP Office Essential Edition or IP Office Preferred Edition) using an IP500 V2 control unit.

This documentation does not cover installation of IP Office Basic Edition, IP Office Basic Edition - Norstar Mode or IP Office Basic Edition - PARTNER® Mode systems which each have their own separate installation documentation. Nor does it cover the addition of an IP500 V2 system as an IP500 V2 Expansion System system in a Server Edition or IP Office Select network. However, the hardware compatibility notes for the IP500 V2 in this manual remain applicable unless stated otherwise.

- Installers familiar with the installation of previous releases should refer to the Changes for Release 11.0 9 section.



- The IP Office is a converged voice and data communications system. It should therefore only be installed by persons with telephony and IP data network experience.
- Installers must be trained on IP Office systems. Through its Avaya University 46 (AU), Avaya provides a range of training courses including specific IP Office implementation and installation training. It also provides certification schemes for installers to achieve various levels of IP Office accreditation.
- It is the installer's responsibility to ensure that all installation work is done in accordance with local and national regulations and requirements. It is also their responsibility to accurately establish the customer's requirements before installation and to ensure that the installation meets those requirements.
- You should read and understand this documentation before installation. You should also obtain and read the Avaya Technical Bulletins relevant to recent software and hardware releases to ensure that you are familiar with any changes to the IP Office equipment and software.
- The Avaya IP Office IP500 V2 is also known as "IPO IP500 V2 Cntrl Unit", "IP Office IP 500 v2", "IPO IP500 v2", "IP 500 V2", "IP500 V2", "IPO 500v2 System Unit Assembly" or "IP Office 500 v2". Throughout this documentation the term IP500 V2 is used.

1.1 Changes for Release 11.0

The following is a summary of the major changes affecting IP500 V2 installation with IP Office Release 11.0:

- **Using IP Office Web Manager for Initial Configuration** 114
  Using web browser access, initial system configuration can now be performed through a series of menu wizards. These menus replace the IP Office Web Manager dashboard display.
- **IP Office Web Client** 254
  The IP Office Web Client, previously available in R10.1 for customer feedback only, is now full supported and has been enhanced with a range of call, video and conference control features. This is a WebRTC client useable through the Chrome browser (Windows and macOS) by any user configured for one-X Portal for IP Office running on an IP Office Application Server. It can also be installed on Windows PCs as a thick-client. A Chrome extension is available that allows click-to-dial of numbers shown in the browser.
- **J169/J179 SIP Phones**
  These new Avaya SIP phones are now supported. These provide IP Office features similar to those shown on 1400, 1600, 9500 and 9600 Series phones. Both phones are physically similar, supporting 24-programmable buttons through a display with 8 physical dual-LED buttons. The J169 has a grayscale display, the J179 a colour display.
  - **JBM24 Button Module**
    Up to 3 of these button modules are supported by both J169 and J179 phones. Each module provides the phone with an additional 24 programmable dual-LED buttons.
  - **J100 Wireless Module**
    The J179 has a slot for additional optional modules. The J100 wireless module allows the J179 to connect to the customer network via WiFi. This allows the phone to be used in locations where a wired Ethernet connection is not available or not desired.
- **Vantage K100 Series Phones**
  These Avaya SIP phones are supported. The phone consists of an Android tablet device integrated into a desk phone. The phone is available in a modular format:
  - **Vantage K165 Phone**
    An Android tablet desk phone with an RJ11 telephony headset port. This version of the phone does not include a integrated camera.
  - **Vantage K175 Phone**
    This phone is similar to the K165 but also includes includes an integrated camera to support video calls.
  - **J1B1 Wired Handset Module**
    Useable with both the K100 phones, this module adds a standard telephone handset.
  - **J1B2 Bluetooth Handset Module**
    Useable with both the K100 phones, this module add a Bluetooth handset to the desk phone.
- **Avaya IX Workplace Client** 254
  This is a unified communications application supported on a wide range of operating systems on both PCs and mobile devices.

Service Pack 1

As part of R11.0 Service Pack 1, the following are also now supported:

- **H200 Series Phones**
  A range of hospitality phones intended for hotel environments and similar: H229, H239 and H249.
- **K155 Vantage Phone**
  Similar to the K175 but using a smaller screen to allow inclusion of a regular telephone dial pad.

Service Pack 2

As part of R11.0 Service Pack 2, the following are now also supported:

- **Avaya IX Workplace Client Shared Control Mode**
  The Avaya IX Workplace Client application on Windows and macOS PCs can be used in desk phone control mode. In that mode, the application can be used to make and answer calls on the user's associated desk phone.

Feature Pack 4

As part of R11.0 Feature Park 4 (11.0.4.0), the following are now also supported:

- **J100 Series 40.0 Firmware**
  The service pack includes J100 Series 4.0 SIP firmware. That firmware enables support for the following:
  - **J179 Bluetooth**
    The updated firmware supports Bluetooth headset connect to J179 phones which have the optional J100 wireless module installed.

- **JEM24 Button Module**
  This type of button module is supported on J169/J179 phones. The JEM24 has 24 dual-LED buttons with adjacent button label display. A single JEM24 supports 72 programmable button slots. These are arranged in 3-pages, with pages accessed using the module's page scroll button. When multiple JEM24 modules (up to 3) are connected to a phone, each module only supports a single page of 24 programmable button slots. JEM24 and JBM24 button modules cannot be combined on the same phone.

- **Avaya IX Workplace Client on Vantage**
  The Avaya IX Workplace Client client is now supported as a dialer application on Vantage K165/K175 phones.

Feature Pack 4 - Service Pack 2 (R11.0.4.2)

As part of this service pack, the following are now also supported:

- **J159 Telephone**
  These phones are now supported (using J100 R4.0.3 or higher firmware).

- **Equinox Rebrand**
  This release support Equinox R4.3 clients, which are now rebranded as Avaya IX Workplace Client.

No Longer Supported

The following options are no longer supported on IP Office R11.0 and higher:

- **T3 Series Telephones**
  The T3 Series telephones (VoIP and non-VoIP) are not supported.

- **IP DECT**
  The older (pre-R4) IP DECT solution is not supported. IP DECT R4 is still supported.

- **Contact Recorder for IP Office**
  The Contact Recorder for IP Office service (for an IP500 V2, provided by an IP Office Application Server) is no longer supported. The replacement, Media Manager, introduced in R10.1 includes options to assist with migrating any existing Contact Recorder for IP Office archives to Media Manager.

- **IP Office Video SoftPhone**
  The macOS version of this application is no longer supported. The Windows version was already not supported.

- **Integrated Contact Reporter**
  This application is not supported.

- With the release of IP Office Release 11.0, Avaya no longer directly supports IP Office Releases 10.0 and R9.1 systems and related applications.

1.2 Additional Documentation

This manual only covers the basic system installation necessary to result in a configurable IP500 V2 system. IP Office applications and ancillary products, including IP telephones, are outside the range of this manual.

If those applications and products are to be part of the system installation, the separate documentation for those products should be obtained, read and understood prior to installation.

- **! IP Office Technical Bulletins**
  You must obtain and read the IP Office Technical Bulletin relating to the IP Office software release which intend to install. The bulletin contains important information that may not have been included in this manual. IP Office Technical Bulletins are available from the Avaya support website *(http://support.avaya.com)*.

To download documentation:

1. Browse to ***https://support.avaya.com***.
2. Select **Support by Product** and then **Documents**.
3. Enter ***IP Office*** in the **Enter Product Name** box and select the matching option from the displayed list.
4. Use the **Choose Release** drop-down to select the required IP Office release.
5. Select the type of documents required from the list and click **ENTER**.

1.3 Equipment Availability

SAP codes and details of specific items within this documentation are for reference only. Items available in any specific locale should be confirmed against the local Avaya IP Office price list for that locale. The local price list may also include additional items relative to the installation requirements of that locale.

This documentation covers the equipment supported by IP Office 11.0. That includes equipment supported but no longer available as new from Avaya.

1.4 Repair

IP Office systems do not contain any user serviceable or repairable components. If a faulty unit is suspected, the whole unit should be replaced.

IP Office control units should not be opened under any circumstances except the insertion of IP500 base cards 82.

1.5 RoHS

RoHS is a European Union directive for the Removal of Certain Hazardous Substances from Electrical and Electronic Equipment. Similar legislation has been or is being introduced in a number of other countries. Avaya has decided to make its global product range compliant with the requirements of RoHS.

The actions taken vary:

- In some cases equipment has been discontinued and is no longer available from Avaya.
- In some cases new manufactured stock has been made RoHS compliant and keeps its existing SAP code.
- In other cases the equipment has been replaced by a new RoHS compliant alternative with new SAP codes.
- The SAP codes within this document are for RoHS compliant equipment unless otherwise stated.

1.6 IP Office Modes

IP Office systems can run in a number of modes. For IP Office Release 10.0, only the following modes are supported for IP500 V2 control units:

IP Office Basic Edition Modes

The following operating modes are collectively referred to as IP Office basic mode.

- **IP Office Basic Edition**
  This is the default operating mode for IP500 V2 control units.
- **IP Office Basic Edition - Norstar Mode**
  This mode operates the same as the IP Office Basic Edition mode. This mode is sold in Middle East and North African locales.
- **IP Office Basic Edition - PARTNER® Mode**
  This mode operates the same as the IP Office Basic Edition mode. This mode is sold in North American locales.

IP Office Standard Modes

The following operating modes are collectively referred to as IP Office standard mode.

- **IP Office Essential Edition**
  For IP Office Release 11.0, IP500 V2 systems run in this mode if an **Essential Edition** license is added to the configuration. Systems set to this mode without a license will not support any telephony functions.
- **IP Office Preferred Edition**
  This mode is similar to IP Office Essential Edition but adds support for the Voicemail Pro application. This mode is enabled by adding a **Preferred Edition (Voicemail Pro)** license to a system already licensed for **Essential Edition**.

Other Modes

- **Server Edition**
  This IP Office mode is not covered by this documentation. It uses IP Office servers running on Linux servers including virtual servers. Refer to the separate Server Edition documentation. Physical IP500 V2 systems can be used in a Server Edition network as an IP500 V2 Expansion System system. Therefore, the hardware compatibility notes for the IP500 V2 control unit in this manual remain applicable for Server Edition usage unless stated otherwise.
- **IP Office Select**
  This mode enabled additional capacity and features to a Server Edition network. All systems in the network need to be configured as IP Office Select systems. Again, IP500 V2 control units can be employed as expansion systems in a IP Office Select network.

1.6.1 System SD Cards

IP500 V2 control unit must be fitted with a System SD card. The default mode of the system is determined by the type of System SD card present. By using IP Office Manager and adding licenses the mode of the system can be changed.

The different System SD cards are:

- **IP Office U-Law SD Card**
  A system fitted with this type of card defaults to U-Law telephony and IP Office Basic Edition ***Key System*** operation. Intended for North American locales.
- **IP Office A-Law SD Card**
  A system fitted with this type of card defaults to A-Law telephony and IP Office Basic Edition ***PBX System*** operation. Intended for locales outside North America.

1.6.2 Overall Capacity

The following table is a summary only. Support for particular types of extension, trunk and user ports also depends on other factors such as local support variations. For example, BRI trunks are not supported in North American locales.

		IP Office Basic Edition - PARTNER® Mode	IP Office Basic Edition - Norstar Mode	IP Office Basic Edition	IP Office Essential Edition IP Office Preferred Edition
Extensions	Maximum Extensions	100 [1]	100 [1]	100 [1]	384
Trunks	Maximum Trunks	64	64	64	[5]
	- Maximum Analog Trunks	32	32	32	204
	- Maximum BRI Channels [3]	–	12	12	32
	- Maximum PRI Channels [4]	24	30	30	240
	- Maximum SIP Channels [2]	20	20	20	[5]
	- Maximum H323 IP Channels	–	–	–	[5]

1. 100 Extensions in 3-digit extension numbering mode. 48 extensions in 2-digit extension numbering mode.
   - For IP Office Basic Edition modes, the system assumes that the base control unit is always fully populated with up to 32 extensions, either real or phantom or a mix, to which it assigns extension numbers in sequence.
     - It does this before assigning extension numbers to any real extensions on attached external expansion modules up to the system extension limit. If the system extension limit has not been exceeded, any remaining extension numbers are assigned to additional phantom extensions.
     - For DS ports, the control unit can only host up to 3 DS8 cards plus a Combo card with 6 DS ports and 2 analog phone ports. This means that with external expansion modules, the maximum DS extensions achievable is 98 in 3-digit extension numbering mode, 46 in 2-digit extension numbering mode.
2. In all modes, voice compression hardware resources are also required for SIP support.
3. IP Office Basic Edition mode systems do not support both BRI and PRI trunks in the same system. They are also restricted to 12 BRI channels regardless of the BRI hardware installed. IP Office standard mode systems support both BRI and PRI trunks in the same system.
4. IP Office Basic Edition mode systems are limited to 1 single-port PRI card.
5. Capacity is dependent on licenses, voice compression resources and available bandwidth.

1.6.3 Hardware Support Summary

Note that even where indicated as supported, the availability and support of equipment may still be subject to local restrictions. The table below is a summary for IP Office Release 11.0, refer to Hardware Software Compatibility[286] for a more historical summary and for a listing of supported telephones.

	IP Office Basic Edition modes	IP Office standard modes
IP500 V2 Control Unit	✓	✓
IP500 Base Cards		
IP500 Digital Station Card	✓ 3	✓ 3
IP500 Analog Phone 2/8	✓ 4	✓ 4
IP500 TCM8 Card	✓ 4	✓ 4
IP500 VCM 32/64 Cards	–	✓ 2
IP500 4-Port Expansion	–	✓ 1
IP500 BRI Combo[2][4]	✓ 2	✓ 2
IP500 ATM Combo[2]	✓ 2	✓ 2
IP500 ATM Combo V2[2]	✓ 2	✓ 2
IP500 ETR6[1][6]	✓ 3	–
Unified Communications Module[6]	–	✓
Trunk Daughter Cards		
Analog Trunk Card	✓	✓
Analog Trunk Card V2	✓	✓
BRI Trunk Cards[4]	✓	✓
PRI Trunk Card[4][5]	✓ 1	✓ 4
Expansion Modules		
Number of Modules[3]	8	12
Digital Station 16/30	✓	✓
Digital Station 16A/30A	✓	✓
Digital Station 16B/30B	✓	✓
Phone 8/16/30	✓	✓
Analog Trunk 16	✓	✓
Telephone Types		
ETR Phones *(ETR ports)*	✓	–
BST Phones *(BST ports)*	✓	✓
DS Phones *(DS ports)*	✓	✓
H323 IP Phones *(LAN)*	–	✓
SIP IP Phones *(LAN)*	–	✓
DECT R4 *(LAN)*	–	✓
DECT DMS *(BST ports)*	✓	✓
Voicemail Types		
Embedded Voicemail	✓	✓
Voicemail Pro	–	✓

1. The ETR6 card is only supported by IP500 V2 systems in IP Office Basic Edition - PARTNER® Mode or IP Office Basic Edition U-Law modes.
2. Only 2 combinations cards are supported in a control unit, regardless of combination card type.
3. External expansion modules can be added so long as the overall limit for extensions and trunks is not exceeded. On IP Office Basic Edition mode systems, a maximum of one Analog Trunk 16 module is supported.
4. IP Office Basic Edition mode systems do not support a mix of BRI and PRI trunks and only supports a maximum of 12 BRI channels.
5. IP Office Basic Edition mode systems only support a single-port PRI card.

Página2676 de 3226.

1.6.4 Feature Support Summary

The table below is a general summary only. For more specific details refer to the installation documentation for the specific application.

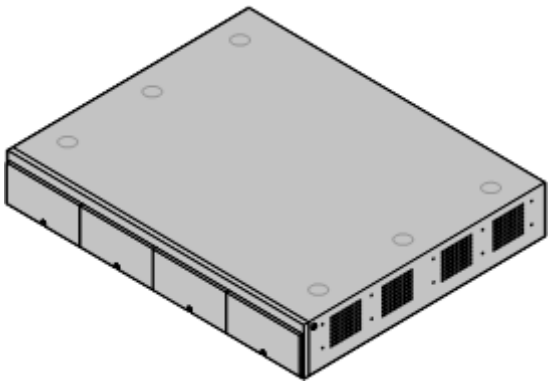
		IP Office Basic Edition			IP Office Essential Edition	IP Office Preferred Edition
		PARTNER Mode	Norstar Mode	Quick Mode		
Admin Applications	Phone Based Admin	✓	✓	✓	–	–
	IP Office Web Manager	✓	✓	✓	✓	✓
	IP Office Manager	✓	✓	✓	✓	✓
	Monitor (System Monitor)	✓	✓	✓	✓	✓
	System Status Application	✓	✓	✓	✓	✓
Applications	one-X Portal for IP Office	–	–	–	–	✓
	IP Office Web Client					✓
	one-X Mobile					✓
	Avaya Communicator					✓
	SoftConsole	–	–	–	✓	✓
	TAPI (1st Party)	–	–	–	✓	✓
	TAPI (3rd Party)	–	–	–	✓	✓
	Voicemail Pro	–	–	–	–	✓
	Media Manager	–	–	–	–	✓

		IP Office Basic Edition			IP Office Essential Edition	IP Office Preferred Edition
Locales		Canada, Mexico, United States.	Bahrain, Egypt, Kuwait, Morocco, Oman, Pakistan, Qatar, Saudi Arabia, South Africa, Turkey, United Arab Emirates.	Argentina, Australia, Bahrain, Belgium, Brazil, Canada, Chile, China, Colombia, Czech, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Italy, Korea, Kuwait, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Norway, Oman, Pakistan, Peru, Philippines, Poland, Portugal, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, United Kingdom, United States, Venezuela.	Argentina, Australia, Bahrain, Belgium, Brazil, Canada, Chile, China, Colombia, Czech, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Italy, Japan, Korea, Kuwait, Malaysia, Mediterranean, Mexico, Morocco, Netherlands, New Zealand, Norway, Oman, Pakistan, Peru, Philippines, Poland, Portugal, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, United Kingdom, United States, Venezuela.	
Voicemail Languages	**Embedded Voicemail**	• **Arabic**, **Cantonese**, **Danish**, **Dutch**, **English (UK)**, **English (US)**, **Finnish**, **French**, **French (Canada)**, **German**, **Hebrew**, **Italian**, **Japanese**, **Korean**, **Mandarin**, **Norwegian**, **Polish**, **Portuguese**, **Portuguese (Brazil)**, **Russian**, **Spanish**, **Spanish (Argentina)**, **Spanish (Latin)**, **Spanish (Mexico)**, **Swedish**, **Turkish**.				
	Voicemail Pro	–	–	–	–	As above plus: **Greek**, **Hungarian**. Minus: **Arabic**, **Spanish (Mexico)**.

1.7 The Control Unit

The base of any IP Office system is the control unit. It stores the system configuration and controls the system operation. Each control unit can be customized by inserting various base card 22 onto which trunk daughter cards 25 can also be added. External expansion modules 26 can also be connected to add additional extension and trunk ports.

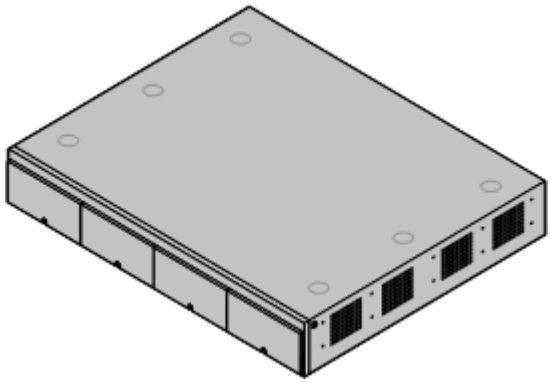
IP Office Release 11.0 supports the following IP Office control units. Other previous types of IP Office control units are not supported by IP Office Release 11.0 and are not covered by this documentation.



- **IP500 V2 Control Unit** 205
  This control unit has four front slots for IP500 base cards. It has an internal power supply unit and uses a mandatory System SD card. It includes a 2 port ethernet LAN switch (layer 3 managed) on the rear.
  - The type of System SD card fitted to the system determines its default operation mode 13 of the system.
    - **IP Office Basic Edition**
    - **IP Office Basic Edition - PARTNER® Mode**
    - **IP Office Basic Edition - Norstar Mode**
    - **IP Office Essential Edition**

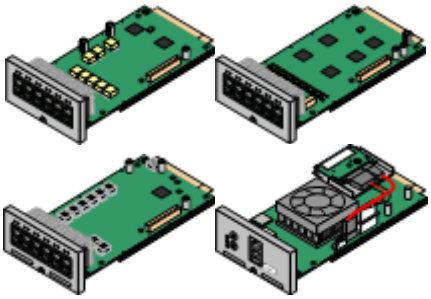
1.8 IP500 V2 System Components

The following are the typical components of a system based on an IP500 V2 control unit.

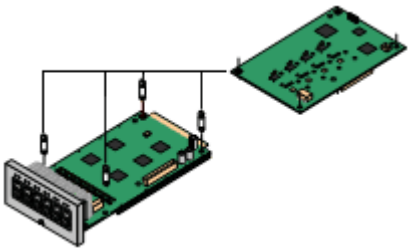


- **IP Office IP500 V2 System Unit** 205
  The control unit holds the main configuration and performs the routing and switching for telephone calls and data traffic. Each control unit includes 4 slots for optional base cards to support trunk and phone extension ports.
  - **Avaya SD Card** 21
    This card holds the firmware and other files used by the system when it starts. An Avaya System SD card is mandatory for correct system operation. The card also provides storage for embedded voicemail if that is used.

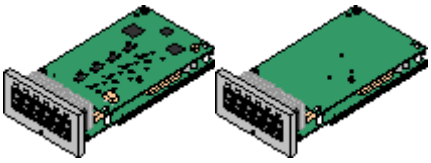
- **License Keys** 279
  Various features and applications require licenses in the system's configuration. These are entered by uploading a PLDS XML file containing all the system's license. The file and its licenses are specific to the unique serial number of the System SD card installed in the system.



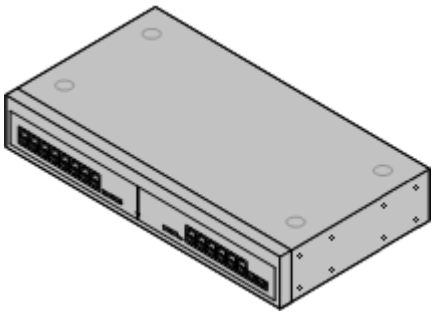
- **IP500 Base Cards** 22
  The IP500 V2 control unit has slots for up to 4 IP500 base cards. These can be used to add ports for analog extensions, digital extensions, voice compression channels and other resources.
  - **IP500 Digital Station Base Card** 218
  - **IP500 Analog Phone Base Card** 213
  - **IP500 VCM Base Card** 221
  - **IP500 4-Port Expansion Base Card** 212
  - **IP500 TCM8 Base Card** 220
  - **IP500 ETR6 Base Card** 219
  - **Unified Communications Module** 217



- **IP500 Trunk Daughter Cards** 25
  Many of the IP500 base cards can be fitted with an IP500 daughter card in order to support various types of trunk connections.
  - **IP500 Analog Trunk Card** 224
  - **IP500 Analog Trunk Card V2** 224
  - **IP500 BRI Trunk Card** 226
  - **IP500 PRI Trunk Card** 227



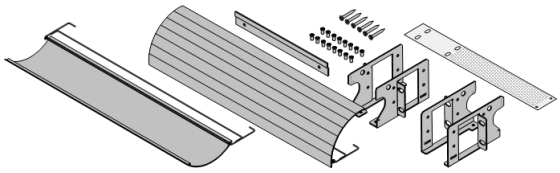
- **IP500 Combination Cards** 22
  These card are pre-paired base and daughter cards. They provide 6 digital station ports, 2 analog phone ports, 10 voice compression channels and either 4 analog trunk ports or 4 BRI channels (2 ports). The trunk daughter card cannot be removed or replaced with another type.
  - **IP500 BRI Combination Card** 216
  - **IP500 ATM Combination Card** 214
  - **IP500 ATM Combination Card V2** 214



- **IP500 External Expansion Modules** 26
  Additional ports can be added using a number of IP500 external expansion modules.
  - Systems running in IP Office standard modes support 8 external expansion modules as standard. If fitted with an IP500 4-Port Expansion Base Card, up to 12 external expansion modules are supported.

- **Power Supplies** 30
  The IP500 control unit has an internal power supply unit. Each external expansion module is supplied with an external power supply unit. Additional power supply units may also be required for IP phones and some phone add-ons.
- **Power Cords** 31
  Depending on the locale, different power cords need to be ordered for each control unit, external expansion module and any phones or devices using external power supply units.

- **Cables** 33
  The system is designed primarily for connection to a structured cabling system using CAT3 UTP cabling. This approach allows telephone and data traffic to share the same wiring infrastructure and simplifies equipment moves.



- **Mounting Kits** 37
  The control unit can be used free-standing, with external expansion modules stacked above it. With optional rack mounting kits, the control unit and external expansion modules can also be rack mounted. Alternatively with an optional wall mounting kit the IP500 control unit can be wall mounted. IP500 external expansion modules can also be wall mounted.

- **Surge Protectors and Barrier Boxes** 36
  Where the installation includes extensions in other buildings additional protective equipment is required. This equipment may also be required in areas where the lightning risk is high.
- **Phones** 39
  IP Office systems support a variety of Avaya digital and IP phones plus analog phones.

- **Application DVDs** 42
  The IP Office applications can be ordered on a number of DVDs. In addition they can be downloaded from the IP Office section of the Avaya support web site (*http://support.avaya.com*).

1.9 System SD Card

The IP Office system requires an Avaya System SD card[208] in order to operate. This card carries the firmware and various other files that the system loads when it powers up. Once the system is operational, the System SD card holds a copy of the system configuration, licenses file and, if being used, embedded voicemail files. The card is inserted into the System SD slot on the rear of the control unit before the system is started.

If the system is using a PLDS XML file for licensing, the feature key serial number of the SD card is used as the unique value against which the licenses are issued and validated.

Setting the System's Original Software Level

For a new IP Office control unit, the version of IP Office software that it loads from the system SD card when it is first powered up becomes its base or original software level. That value is written into the control units permanent memory and cannot be changed.

Therefore, it is important to ensure that the System SD card has been loaded with the correct version of software before the system is first powered up. This is done by using IP Office Manager to load the required level of software onto the SD card[75].

1.10 Licensing

The IP Office system requires licensing for some features, see Licenses[279]. The license file can be either uploaded manually or pre-loaded onto the System SD card[78].

How is the system licensed?

- An XML file containing the full set of PLDS licenses is uploaded to the system. The license file is unique to the feature key serial number of the System SD card installed in the system.
    - The PLDS host ID used for the license file must match that shown by the 12 digit **PLDS ID** printed on the SD card label. Older cards have an 10 digit feature key serial number shown by **FK** or **FK SN**. For those cards add the prefix ***11*** to obtain the card's PLDS ID.

Minimum License Requirements

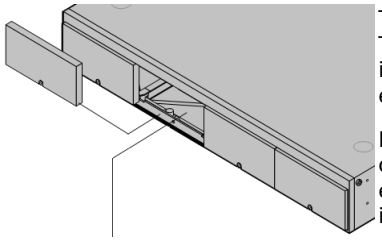
For IP Office Essential Edition, the system requires an **Essential Edition** system license for the specific IP Office release you want it to run.

Página2682 de 3226.

1.11 Control Unit Cards

The following control unit cards are supported.

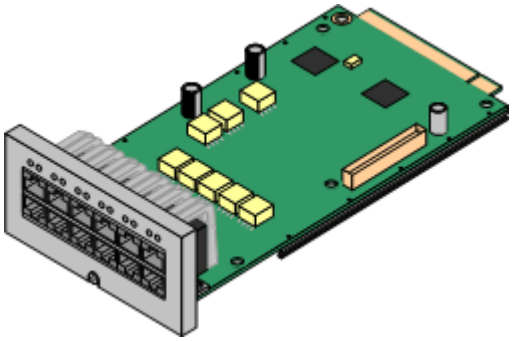
1.11.1 IP500 Base Cards



The IP500 V2 control unit has 4 slots for the insertion of IP500 base cards. The slots are numbered 1 to 4 from left to right. Normally they can be used in any order, however if the capacity for a particular type of card is exceeded, the card in the rightmost slot will be disabled.

Each base card includes an integral front panel with ports for cable connections. Typically the first 8 ports on the left are for connection of extension devices. The 4 ports on the left are used for connection of trunks if a trunk daughter card[25] is added to the base card.

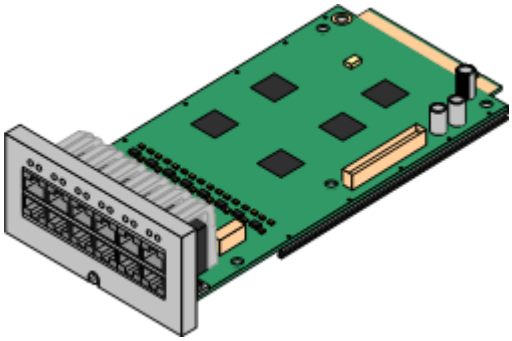
IP500 Digital Station Base Card[218]



This card provides 8 DS (digital station) ports for the connection of Avaya digital phones.

- The card can be fitted with an IP500 trunk daughter card[25] which uses the base card ports for trunk connection.
- **Maximum:** 3 per control unit.
    - Connections for 4100, 7400, M-Series and T-Series phones use the IP500 TCM8 Digital Station card.

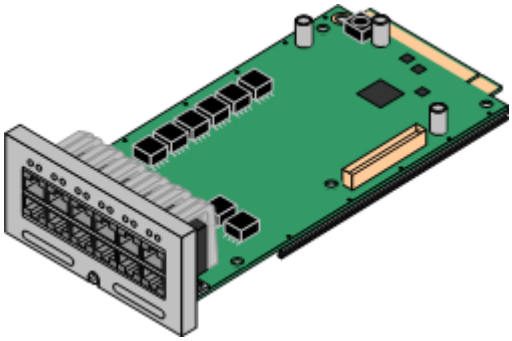
IP500 Analog Phone Base Card[213]



The card is available in two variants, supporting either 2 or 8 analog phone ports.

- The card can be fitted with an IP500 trunk daughter card[25] which uses the base card ports for trunk connection.
- **Maximum:** 4 per control unit.
    - The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors.
    - If fitted with an IP500 Analog Trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12.

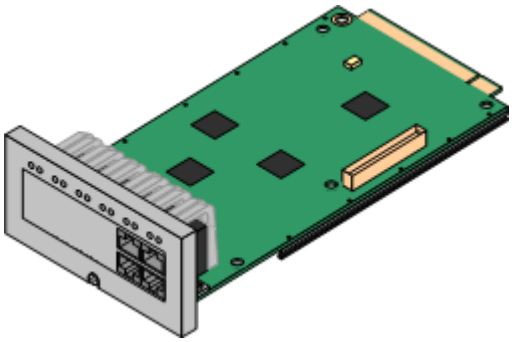
IP500 TCM8 Digital Station Card[220]



This card provides 8 BST (digital station) ports for the connection of Avaya 4100, 7400, M-Series and T-Series phones.

- The card can be fitted with an IP500 trunk daughter card[25] which uses the base card ports for trunk connection.
- **Maximum:** 4 per control unit per IP500 V2 control unit.

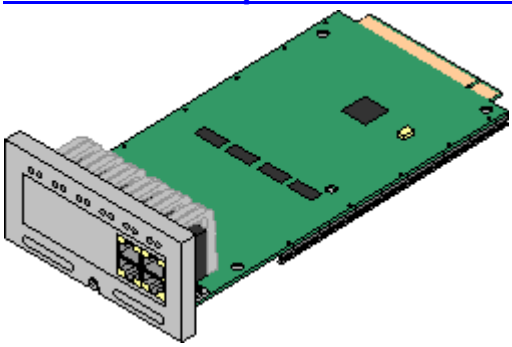
IP500 VCM Base Card [221]



This card is available in variants supporting either 32 or 64 voice compression channels for use with VoIP calls.

- The card can be fitted with an IP500 trunk daughter card [25] which uses the base card ports for trunk connection.
- **Maximum:** 2 per control unit.

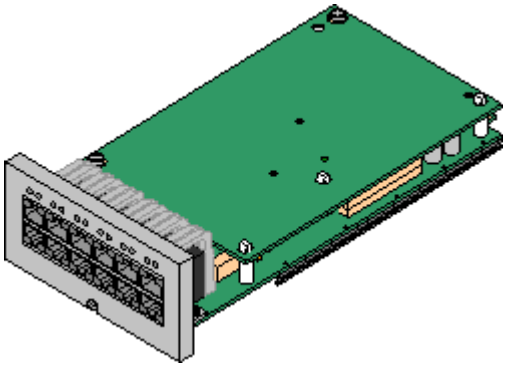
IP500 4-Port Expansion Base Card [212]



This card adds an additional 4 expansion ports for external expansion modules. The card is supplied with four 2m yellow interconnect cables.

- This card does not accept any IP500 trunk daughter card.
- **Maximum:** 1 per control unit (Right-hand slot 4 only).
- **Supported Expansion Modules:** The following external expansion modules are supported:
  - IP500 Analogue Trunk Module
  - IP500 BRI So Module
  - IP500 Digital Station Module
  - IP500 Digital Station Module
  - IP500 Digital Station Module
  - IP500 Phone Module

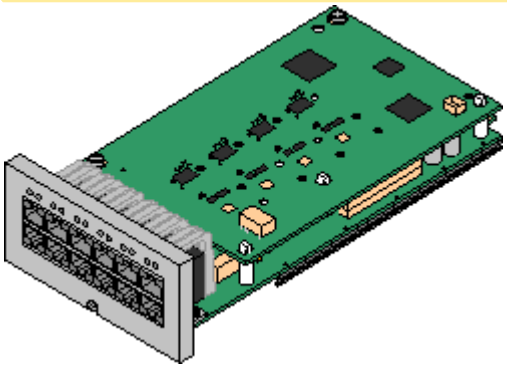
IP500 BRI Combination Card [216]



This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 2 BRI trunk ports (9-10, 4 channels). The card also includes 10 voice compression channels.

- **Maximum:** 2 combination cards per IP500 V2 control unit, regardless of type.
  - IP500 Combination cards are pre-fitted with a trunk daughter card which cannot be removed or changed for another type/capacity trunk daughter card.
  - IP Office Basic Edition - Norstar Mode and IP Office Basic Edition systems are limited to a maximum of 12 BRI channels using BRI Combination and or BRI trunk daughter cards.

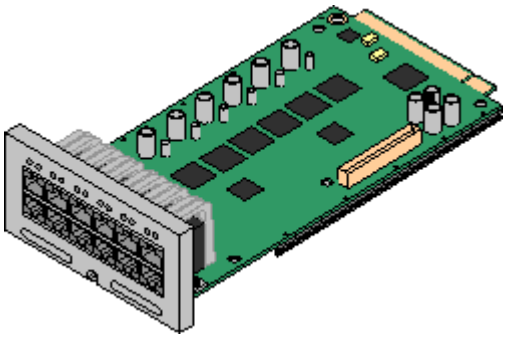
IP500 ATM Combination Card/IP500 ATM Combination Card V2 [214]



This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 4 analog trunk ports (9-12). The card also includes 10 voice compression channels.

- **Maximum:** 2 combination cards per IP500 V2 control unit, regardless of type.
  - IP500 Combination cards are pre-fitted with a trunk daughter card which cannot be removed or changed for another type/capacity trunk daughter card.
  - The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors.
  - During power failure phone port 8 is connected to analog trunk port 12.

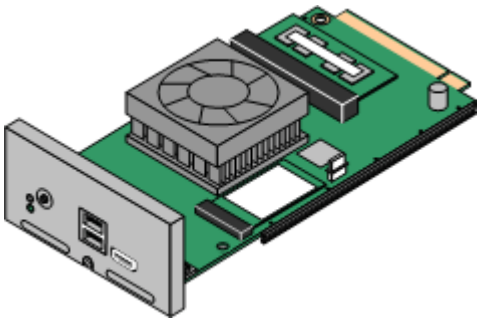
IP500 ETR6 Base Card [219]



This card is only supported in an IP500 V2 control unit running in IP Office Basic Edition - PARTNER® Mode or IP Office Basic Edition. It provides 6 ETR ports for connection of ETR phones. 2 Analog extension ports are also provided for emergency use only with an analog trunk card.

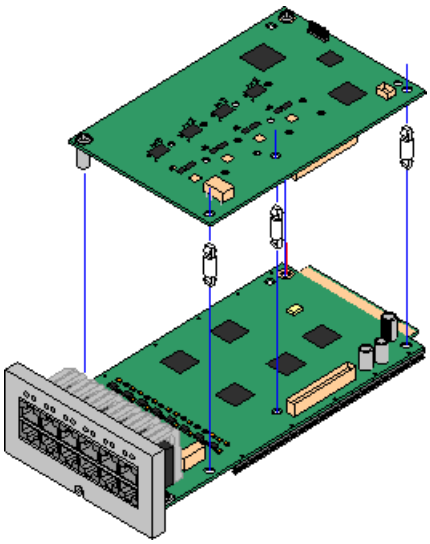
- The card can be fitted with an IP500 trunk daughter card which uses the base card ports for trunk connection.
- **Maximum:** 3 per IP500 V2 control unit.
- The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors.
- If fitted with an IP500 Analog Trunk daughter card, during power failure phone ports 7 and 8 are connected to analog trunk port 12. However during normal operation analog phone ports 7 and 8 are not useable.

Unified Communications Module [217]



This card acts as an embedded Linux server for the one-X Portal for IP Office and/or Voicemail Pro applications.

1.11.2 IP500 Trunk Cards

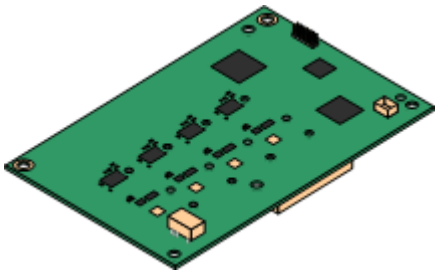


Many IP500 base cards[22] can be fitted with an IP500 trunk daughter cards to support the connection of trunks to the base card.

Each daughter card is supplied with the stand off pillars required for installation and a label to identify the daughter cards presence on the front of the base card after installation.

- IP500 Combination cards are pre-fitted with a trunk daughter card which cannot be removed or changed for another type of trunk daughter card.

IP500 Analog Trunk Card/IP500 Analog Trunk Card V2[224]

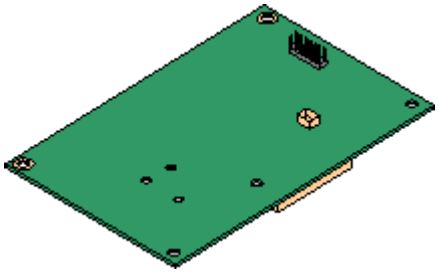


These cards allow the base card to support 4 analog loop-start trunks.

  - The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors.
  - If fitted base card with analog phone ports, during power failure phone port 8 is connected to analog trunk port 12.

- **Maximum:** 4 per control unit. The IP500 Analog Trunk Card V2 is only supported in the IP500 V2.

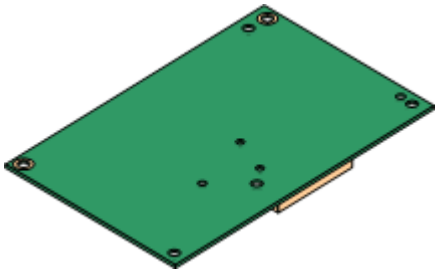
IP500 PRI-U Trunk Card[227]



This card allows the base card to support up to 2 PRI trunk connections. The card is available in single and dual port variants. The card can be configured for E1 PRI, T1 robbed bit, T1 PRI or E1R2 PRI trunks. A T1(J) variant for use in Japan is also available.

- **Maximum:** 4 per control unit.
- The IP Office system supports 8 unlicensed B-channels on each IP500 PRI-U port fitted. Additional B-channels, up to the capacity of ports installed and PRI mode selected require **IP500 Universal PRI (Additional Channels)**[280] licenses added to the configuration. These additional channels consume the licenses based on which additional channels are configured as in-service from port 9 of slot 1 upwards. D-channels are not affected by licensing.

IP500 BRI Trunk Card[226]

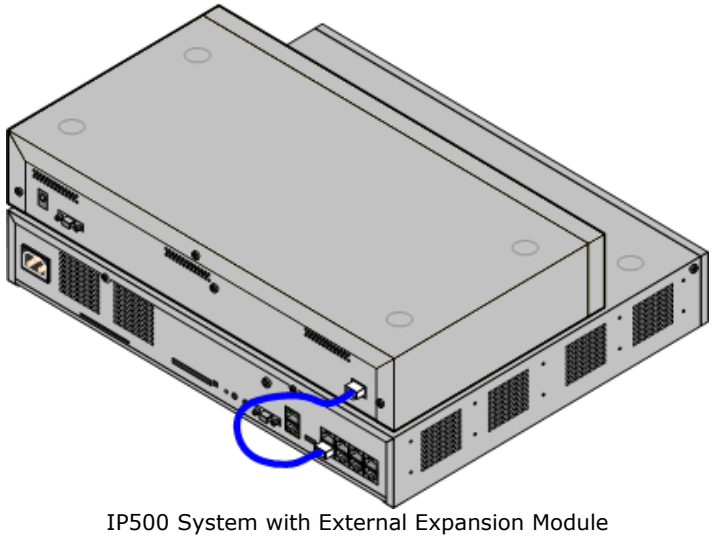


This card allows the base card to support up to 4 BRI trunk connections, each trunk providing 2B+D digital channels. The card is available in 2 port (4 channels) and 4 port (8 channels) variants.

- **Maximum:** 4 per control unit.
- **S-Bus Connection**: The card can be switched from To trunk mode to So mode. This mode requires additional terminating resistors and an ISDN crossover cable connection, see BRI Port (So)[268].
  - IP Office Basic Edition - Norstar Mode and IP Office Basic Edition systems are limited to a maximum of 12 BRI channels using BRI Combination and or BRI trunk daughter cards.

1.12 External Expansion Modules

These modules can be used to add additional ports to an IP Office systems. The number of external expansion modules supported depends on the control unit type. Each module uses an external power supply unit[30] supplied with the module. A locale specific power cord[31] for the PSU must be ordered separately.



IP500 System with External Expansion Module

- Systems running in IP Office standard modes support 8 external expansion modules as standard. If fitted with an IP500 4-Port Expansion Base Card, up to 12 external expansion modules are supported.
  - Each external expansion module is supplied with a blue 1 meter (3'3'') expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
  - When connecting to expansion ports on an IP500 4-Port Expansion card, a yellow 2 meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. 4 Yellow cables are supplied with the IP500 4-Port Expansion card.
- **! Important: External Expansion Module Power**
  In order to be detected and operated correctly, external expansion modules must start before the IP Office control unit. Normally this achieved by connected all expansion modules to the same power strip as the control unit. The control unit applies a short delay to its own start-up process to ensure that expansion modules powered on at the same time as it are detected.

IP500 External Expansion Modules

Expansion modules include an external power supply unit (PSU) and a 1m blue interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

Variant	Country	SAP Code
Digital Phones (Non-IP)		
IPO 500 Digital Station 16[231]	All	700449499
IPO 500 Digital Station 30[231]	All	700426216
IPO 500 Digital Station 16A (RJ21)[233]	All	700500699
IPO 500 Digital Station 30A (RJ21)[236]	All	700500698
IPO 500 Digital Station 16B[236]	All	700501585
IPO 500 Digital Station 30B[236]	All	700501586
Analog Phones		
IPO 500 Phone 16[238]	All	700449507
IPO 500 Phone 30[238]	All	700426224
Others		
IPO 500 Analog Trunk 16[229]	US	700449473

Página2687 de 3226.

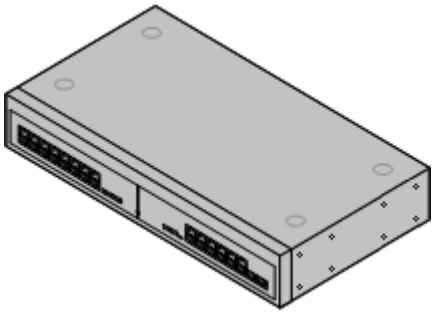
1.12.1 IP500 External Expansion Modules

The following IP500 external expansion modules are supported by IP Office Release 11.0. Each module uses an external power supply unit[30] supplied with the module. A locale specific power cord[31] for the PSU must be ordered separately.

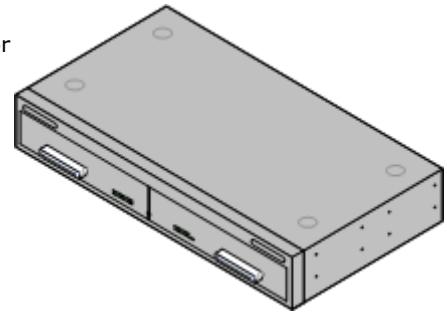
The external module can be stacked on top of the control unit. They can also be wall or rack mounted using one of the IP Office mounting kits[247].

- Systems running in IP Office standard modes support 8 external expansion modules as standard. If fitted with an IP500 4-Port Expansion Base Card, up to 12 external expansion modules are supported.

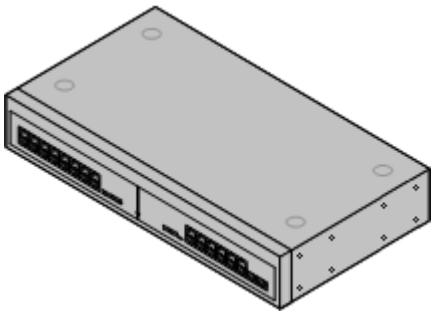
- **IP500 Digital Station Modules**[231]
  Provides, depending on variant, an additional 16 or 30 RJ45 DS[271] ports for supported Avaya DS digital phones[39].



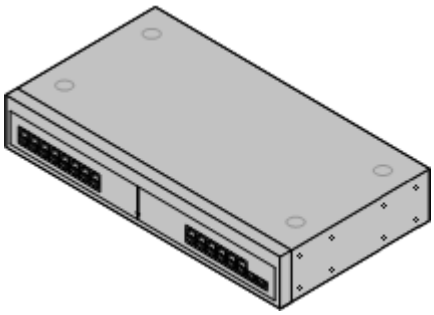
- **IP500 Digital Station A Modules**[233]
  Provides, depending on variant, RJ21 ports for connection of an additional 16 or 30 Avaya BST digital phones[39]. Supported by IP500 V2 only.



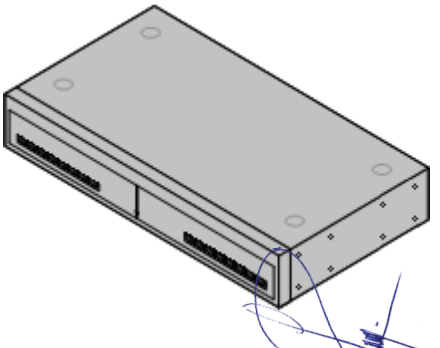
- **IP500 Digital Station B/B2 Modules**[236]
  Provides, depending on variant, an additional 16 or 30 RJ45 ports. These can be used as either DS[271] ports for supported Avaya DS digital phones[39] or BST[270] ports for supported Avaya BST digital phones[39]. However, the module can only support one port type at any time. For IP Office Release 10.1 the DS16B/DS30B modules have been superseded by the DS16B2/DS30B2 modesl.



- **IP500 Phone Modules**[238]
  Provides, depending on variant, an additional 16 or 30 PHONE[276] ports for connecting analog phones.



- **IP500 Analog Trunk Module**[229]
  Provides an additional 16 ANALOG[267] ports for connection of analog trunks. Supports both loop-start and ground-start trunks.
  - Use with ground start trunks requires that the trunk module and the IP Office control unit are grounded.
  - In IP Office Basic Edition - PARTNER® Mode, IP Office Basic Edition - Norstar Mode and IP Office Basic Editions, only 1 Analog Trunk module is supported.



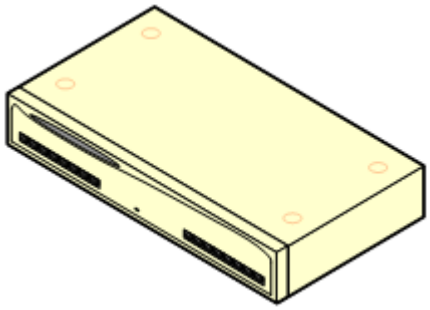
Página2688 de 3226.

1.12.2 IP400 External Expansion Modules

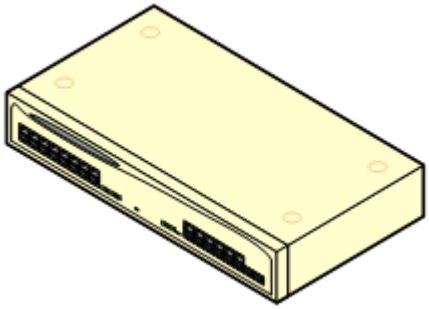
The following IP400 external expansion modules are supported by IP Office Release 11.0 and can be used with IP500 V2 control units. Each module uses an external power supply unit[30] supplied with the module. A locale specific power cord[31] for the PSU must be ordered separately.

If being rack mounted these units use the IP400 rack mounting kit. If being rack mounted, these units use the IPO IP500 RACK MNTG KIT. They cannot be wall mounted.

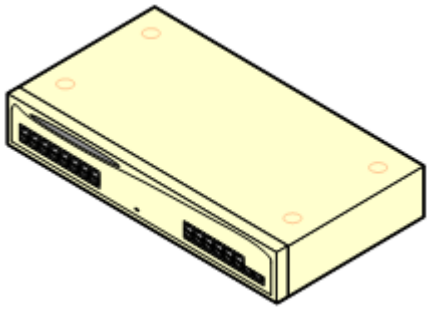
- **IP400 Analog Trunk Module (ATM16)**[241]
  Provides an additional 16 ANALOG[267] ports for connection of analog trunks. Supports both loop-start and ground-start trunks.
  - Available in a number of variants for different locales.
  - Use with ground start trunks requires that the trunk module and the IP Office control unit are grounded.



- **IP400 Digital Station Module V2**[243]
  Provides, depending on variant, an additional 16 or 30 DS[271] ports for supported Avaya digital phones[39]. Supersedes the previous Digital Station module.



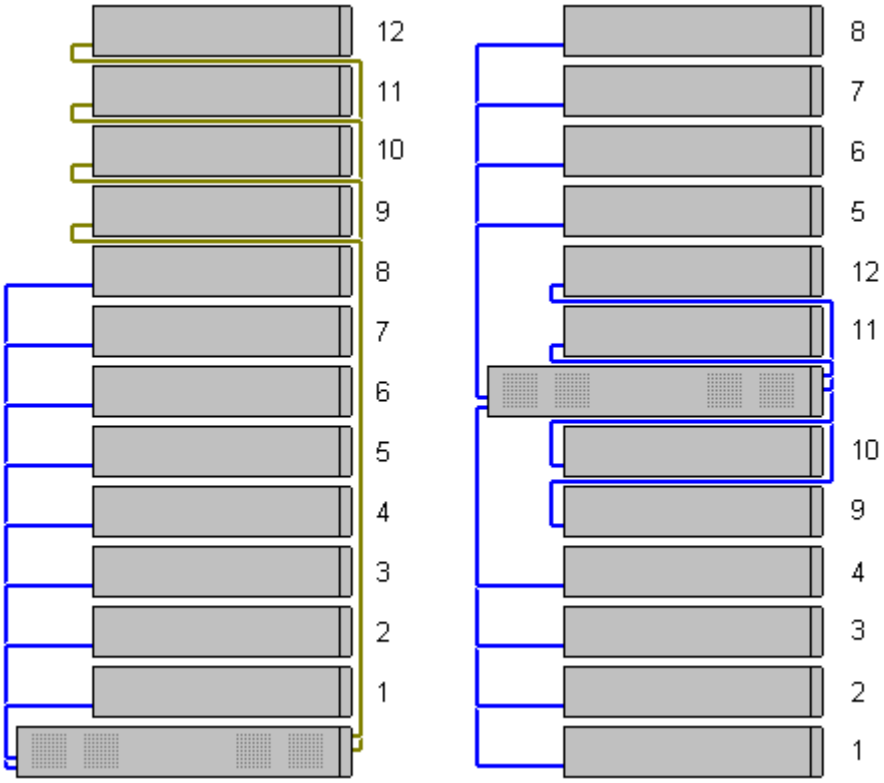
- **IP400 Phone Module V2**[245]
  Provides, depending on variant, an additional 16 or 30 PHONE[276] ports for analog phones. Supersedes the previous Phone module. With IP Office 3.1, the Phone V2 supports a wider range of message waiting indication (MWI) options than Phone V1 modules.



1.12.3 Connecting External Expansion Modules

The integral expansion ports on a control unit are located on the rear of the unit. An additional 4 expansion ports can be added to the front of the control unit by installing an IP500 4-Port Expansion card.

- Each external expansion module is supplied with a blue 1 meter (3'3'') expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on an IP500 4-Port Expansion card, a yellow 2 meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. 4 Yellow cables are supplied with the IP500 4-Port Expansion card.



1.13 Power Supplies and Cables

All IP Office control units and external expansion modules either have an internal power supply unit or are supplied with an external power supply unit.

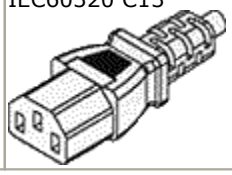
1.13.1 Power Supplies

IP500 V2 control units have an internal power supply unit and so only require a suitable locale specific power cord[31] and a power outlet that includes a switch. Note that if the power cord includes an earth lead, the power outlet must be connected to a protective earth.

External expansion modules are all supplied with an external power supply unit (PSU). These PSUs include an integral 1.5 meter lead for connection to the control unit or expansion module. A power cord[31] for connection from the PSU to the power outlet is not included as this varies by locale. The appropriate power cord must be ordered separately or sourced locally.

- **! Important: External Expansion Module Power**
  In order to be detected and operated correctly, external expansion modules must start before the IP Office control unit. Normally this achieved by connected all expansion modules to the same power strip as the control unit. The control unit applies a short delay to its own start-up process to ensure that expansion modules powered on at the same time as it are detected.

Additional power supply units are required for phone button modules and may also be required for Avaya IP phones.

Area	Type	Used on:	Connector Type
IP Office Control Units and External Expansion Modules	**60W Earthed PSU**	Analog Trunk Module, IP500 Phone 30, IP500 Digital Station 30, IP500 Digital Station 16A, IP500 Digital Station 30A.	IEC60320 C13 

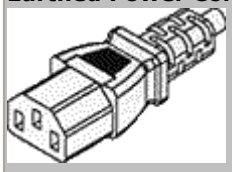
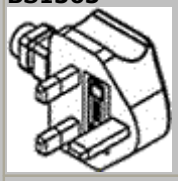
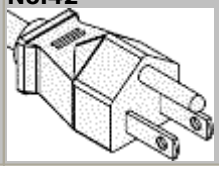
- Avaya IP phones can use IEEE 802.3af Power over Ethernet (PoE) power supplies. Refer to the IP Office IP Phone Installation Manual for full details.

1.13.2 Power Supply Cords

Each control unit and expansion module requires a switched power outlet socket rated at 110-240V ac, 50-60Hz. Connection from that power outlet socket requires an appropriate locale specific power cord which is not supplied with the unit and must be ordered separately. Note that if the power cord includes an earth lead, the power outlet must be connected to a protective earth.

Power cords must not be attached to the building surface or run through walls, ceilings, floors and similar openings. Installation measures must be taken to prevent physical damage to the power supply cord, including proper routing of the power supply cord and provision of a socket outlet near the fixed equipment or positioning of the equipment near a socket outlet.

For locales not detailed below an appropriate power cord must be obtained locally.

Power Cord Type	Power Outlet Plug Type	Locales	SAP Codes
Earthed Power Cords (IEC60320 C13) 	**CEE7/7 (Schuko)**	Europe and South Africa.	700289762
	BS1363 	Czech Republic, Ireland, United Kingdom.	700289747
	NEMA5-15P / CS22.2 No.42 	North, Central and South America.	700289770

1.13.3 Power Supply Backup

The use of an Uninterrupted Power Supply (UPS) with any telephone system is strongly recommended. Even at sites that rarely lose electrical power, that power may occasionally have to be switched off for maintenance of other equipment. In addition, most UPSs also provide an element of power conditioning, reducing spikes and surges.

The capacity of UPS systems and the total equipment load the UPS is expected to support are usually quoted in VA. Where equipment load is quoted in Watts, multiply by 1.4 to get the VA load.

The calculation of how much UPS capacity is required depends on several choices.

- **What equipment to place on the UPS?**
  Remember to include server PCs such as the voicemail. It is recommended that the total load on a new UPS is never greater than 75% capacity, thus allowing for future equipment.
- **How many minutes of UPS support is required?**
  Actual UPS runtime is variable, it depends on what percentage of the UPS capacity the total equipment load represents. For example, a 1000VA capacity UPS may only support a 1000VA (100%) load for 5 minutes. This relationship is not linear, the same UPS may support a 500VA (50%) load for 16 minutes. Therefore, the lower the percentage of maximum capacity used, the increasingly longer the UPS runtime, for example up to 8 hours.
- **How frequent are the power loses?**
  You also need to include allowance for the UPS recharge time. For most UPS's the ratio of discharge to full recharge time is 1:10.
- **How many output sockets does the UPS provide?**
  Multiple UPS units may be required to ensure that every item of supported equipment has its own supply socket.

Example Values

The dominate factor in the power consumption of an IP Office system is the telephones attached to the control unit and any external expansion modules. This does not include IP telephones which require their own separate power supplies. If any server PCs are being used by the system, the requirements of those PCs should also be included in the assessment. Similarly support for adjunct systems such as DECT should be considered.

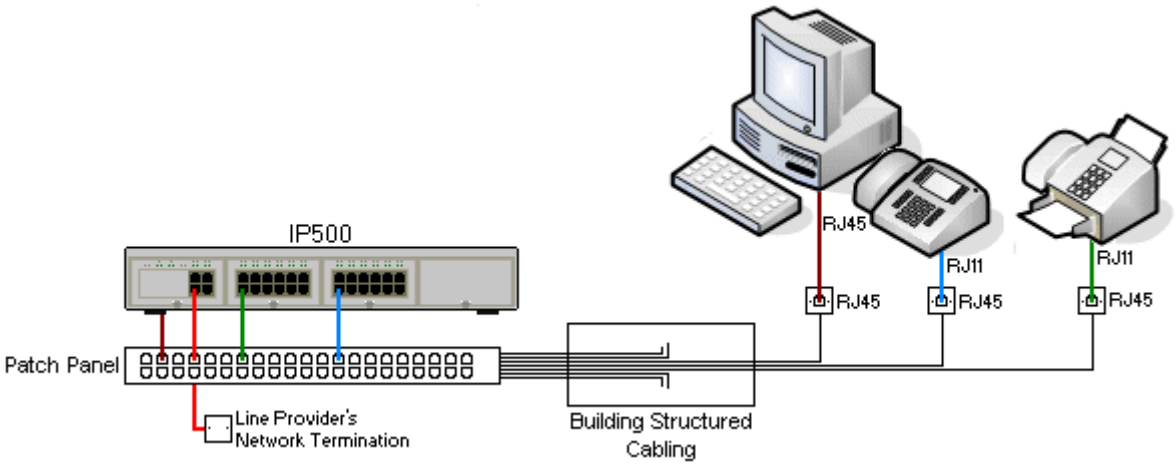
The following are worst case figures tested found using fully populated control units and external expansion modules:

- **IP500 V2 Control Unit:** 115W.
- **IP500 Digital Station 16 External Expansion Module:** 31W.
- **IP500 Digital Station 30 External Expansion Module:** 56W.
- **IP500 DS16A Digital Station RJ21 External Expansion Module:** 34W.
- **IP500 DS30A Digital Station RJ21 External Expansion Module:** 60W.
- **IP500 Phone 16 External Expansion Module:** 25W.
- **IP500 Phone 30 External Expansion Module:** 45W.
- **IP500 Analog Trunk Module 16 External Expansion Module:** 8.8W.

1.13.4 Cabling and Cables

The IP Office systems are designed primarily for use within an RJ45 structured cabling system using CAT3 unshielded twisted-pair (UTP) cabling and RJ45 sockets.

A structured cabling system is one where cables are run from a central RJ45 patch panel in the communications/data room to individual RJ45 sockets at user locations. All wires in each cable between the patch panel and the desk socket are connected straight through. This arrangement allows devices connected at the patch panel to be swapped to match the type of device that needs to be connected at the user socket. For example, making one user socket a phone port and another user socket a computer LAN port, without requiring any rewiring of the cables between the patch panel and the user location.



- **Traditional IDC Punchdown Wiring Installations**
  Where necessary, the far end RJ45 plug can be stripped from IP Office cables and wired into traditional wiring systems using punch-block connectors. This type of installation should be performed by an experienced wiring technician.
- **Trunk Connections**
  The majority of IP Office trunk ports use RJ45 connectors for acceptance of an RJ45-to-RJ45 cable. However, connection at the line provider's end may require use of a different plug type in order to match the line providers equipment.
- **RJ11 Phone Connectors**
  Many phones use RJ11 sockets and are supplied with RJ11-to-RJ11 cables. RJ11 plugs can be inserted into RJ45 sockets and in many case the connection will work. However this is not recommended or supported as the connection lock is not truly positive and may become disconnected. An RJ45-to-RJ11 cable[271] is available for these connections.

Standard IP Office Cables

The following are Avaya standard cables available for use with IP Office systems. The maximum length is applicable if the standard Avaya cable is replaced with an alternate cable.

Cable	Description	SAP Code	Standard Length	Maximum Length
9-Way DTE Cable 278	Connects to control unit RS232 DTE port. 9-Way D-type plug to 9-way D-type socket.	–	2m/6'6''.	2m/6'6''.
Structured Cabling DS Line Cable 271	Connects from RJ45 sockets to RJ11 socketed DS and analog phones.	TT700047871	4m/13'2''.	See table below.
BRI/PRI Trunk Cable 269	Connects BRI/PRI trunk ports to the line provider's network termination point. RJ45 to RJ45. Red.	700213440	3m/9'10''.	–
Expansion Interconnect Cable 273	Connects the control unit to expansion modules. RJ45 to RJ45. Blue. May be replaced by a yellow interconnect cable (2m (6'6") - 700472871) supplied with the IP500 4-Port Expansion 212 card when using that card.	700213457	1m/3'3''.	1m/3'3''.
LAN Cable 274	Connects from IP Office LAN ports to IP devices. RJ45 to RJ45. Grey.	700213481	3m/9'10''.	100m/328'.

The table below details the maximum total cable distances for DS and analog extensions using different cable thicknesses. Cabling should be Category-1 unshielded twisted pair cable or better.

Telephone	Unshielded Twisted-Pair (UTP) - 50nf/Km		
	AWG22 (0.65mm)	AWG24 (0.5mm)	AWG26 (0.4mm)
1400 Series	1200m/3937'	1000m/3280'.	670m/2200'
9500 Series	1200m/3937'	1000m/3280'	670m/2200'
BST	580m/1900'	365m/1200'	228m/750'
Analog Phones	1000m/3280'	1000m/ 3280'	400m/1312'
ETR Phones	305m/1000'	305m/1000'	122m/400'

1.13.5 Grounding

All IP Office control units and external expansion modules must be connected to a functional ground. Where the unit is connected to a power outlet using a power cord with an earth lead, the power outlet must be connected to a protective earth.

Use of ground connections reduces the likelihood of problems in most telephony and data systems. This is especially important in buildings where multiple items of equipment are interconnected using long cable runs, for example phone and data networks.

In some cases, such as ground start trunks, in addition to being a protective measure, this is a functional requirement for the equipment to operate. In other cases it may be a locale regulatory requirement and or a necessary protective step, for example areas of high lightning risk.

- **WARNING**
  During installation do not assume that ground points are correctly connected to ground. Test ground points before relying on them to ground connected equipment.

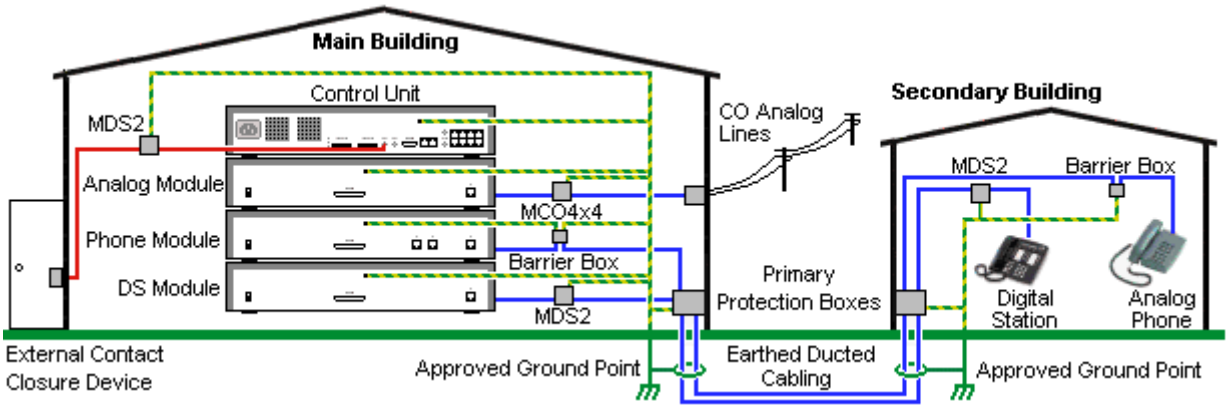
The ground point on IP Office control units and external expansion modules are marked with a or symbol. Ground connections to these points should use a 14 AWG solid wire with either a green sleeve for a functional ground or green and yellow sleeve for a protective ground.

- **Additional protective equipment**
  In addition to grounding, additional protective equipment will be required in the following situations. Refer to "Out of Building Telephone Installations 36".
  - On any Digital Station or Phones external expansion module connected to an extension located in another building.
  - In the Republic of South Africa, on all Analog Trunk external expansion modules (ATM16) and on any control units containing an analog trunk cards (ATM4/ATM4U).

1.13.6 Lightning Protection/Out-of-Building Connections

The following are the only supported scenarios in which wired extensions and devices outside the main building can be connected to the IP Office system. In these scenarios, additional protection, in the form of protective grounding and surge protectors, must be fitted.

- **WARNING**
  The fitting of additional protection does not remove the risk of damage. It merely reduces the chances of damage.



- Only ports on IP Office external expansion modules are supported. Out-of-building connection to ports on base cards in the control unit is not supported.
- Cables of different types, for example trunk lines, phone extensions, ground and power connections, should be kept separate.
- All cabling between buildings should be enclosed in grounded ducting. Ideally this ducting should be buried.
- A Primary Protection Box must be provided at the point where the cables enter the building. This should be three point protection (tip, ring and ground). Typically this would be gas tube protection provided by the local telephone company. The ground wire must be thick enough to handle all the lines being affected by indirect strike at the same time.

Connection Type	Protection Device Type	Requirement
Analog Phone Extensions Phones External expansion module (POT[276] or PHONE[276]) ports only.	**IP Office Barrier Box**[189] Supports a single connection. Maximum of 16 on any expansion module.	• Connection from the expansion module to the phone must be via a surge protector at each end and via the primary protection point in each building. • The IP Office external expansion modules, control unit and IROB devices must be connected to the protective ground point in their building. • The between building connection must be via earthed ducting, preferable underground. The cable must not be exposed externally at any point.
DS Phone Extensions	**ITW Linx MDS2**[188] Supports up to 4 connections. This device was previously referred to as the Avaya 146E.	
BST Phone Extensions	None	Currently not supported.
Analog Trunks	**ITW Linx MCO4x4**[188] Supports up to 4 two-wire lines. This device was previously referred to as the Avaya 146C.	For installations in the Republic of South Africa, the fitting of surge protection on analog trunks is a requirement. For other locations where the risk of lightning strikes is felt to be high, additional protection of incoming analog trunks is recommended.
External Output Switch	**ITW Linx MDS2**[188] Supports up to 4 connections. This device was previously referred to as the Avaya 146E.	Connections from an IP Office Ext O/P port to an external relay device must be via a surge protector. When using the MDS2 on the Ext O/P port, use only the Line 1 and Equipment 1 jacks, do not use the Line 2 or Equipment 2 jacks.

The towerMAX range of devices are supplied by ITWLinx (http://www.itwlinx.com).

1.14 Wall and Rack Mounting

All the IP Office control units are designed to be free-standing. On systems with external expansion modules, the control unit and modules are intended to be stacked.

Using additional option mounting kits, some systems can be wall or rack mounted.

Control/Expansion Unit	Wall Mount	Rack Mount
IP500 V2 Control Unit	✓	✓
IP500 External Expansion Modules	✓	✓

1.14.1 Wall Mounting Kits

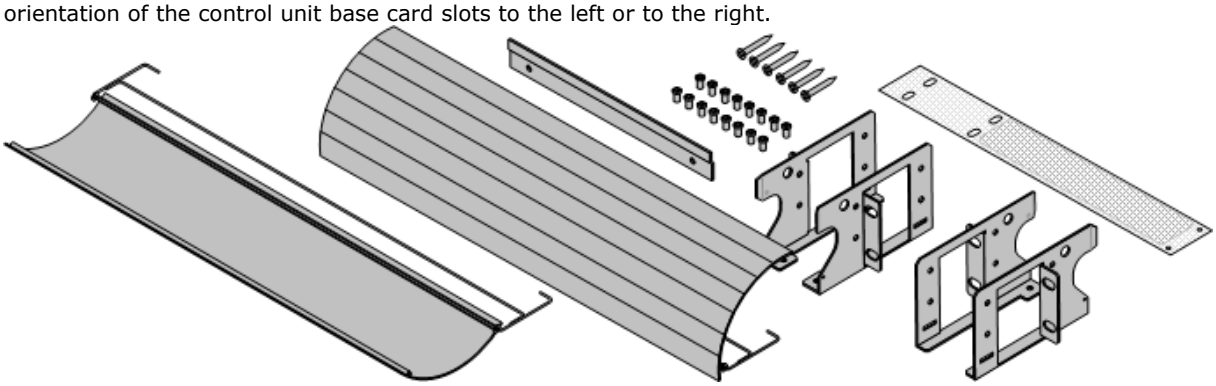
IP500 V2 control units and IP500 external expansion modules can be wall or rack mounted. To do this, a wall mounting kit is required in addition to suitable wall fixings.

In addition to the existing environmental requirements[51] for an IP Office system, the following additional requirements apply when wall mounting a unit:

- The wall surface must be vertical, flat and vibration free. Attachment to temporary walls is not supported.
- Only the screws provided with the mounting kit should be used to attach the brackets to the control unit or expansion modules.
- The installation must be done by a service person.
- Ensure that the system has been shut down and power has been removed from all the units. Shut down the system using a shutdown command and then remove the power. Do not simply remove the power.
- A suitable plywood mounting surface of at least 1m x 1m x 19mm (39” x 39” x 0.75”) is required. If an expansion box is being mounted as well a plywood mounting surface of at least 1.2m x 1.2m x 19mm (48” x 48” x 0.75”) is required.
- A minimum of 6 x 45mm long 5mm/6mm (1.75” #10/#12) pan head screws must be used to secure the plywood to the wall studs.
- The supplied 20mm long 4mm (#8 ¾”) wood screws must be used to secure the brackets to the plywood mounting surface

The following kit is currently available:

- **IPO IP500 WALL MNTG KIT V3** *(SAP Code 700503160)*
  This kit can be used for wall and rack mounting of IP500 V2 control units and IP500 external expansion modules. The kit incorporates cable routing at the front and rear of the unit. For wall mounted control units, it allows orientation of the control unit base card slots to the left or to the right.

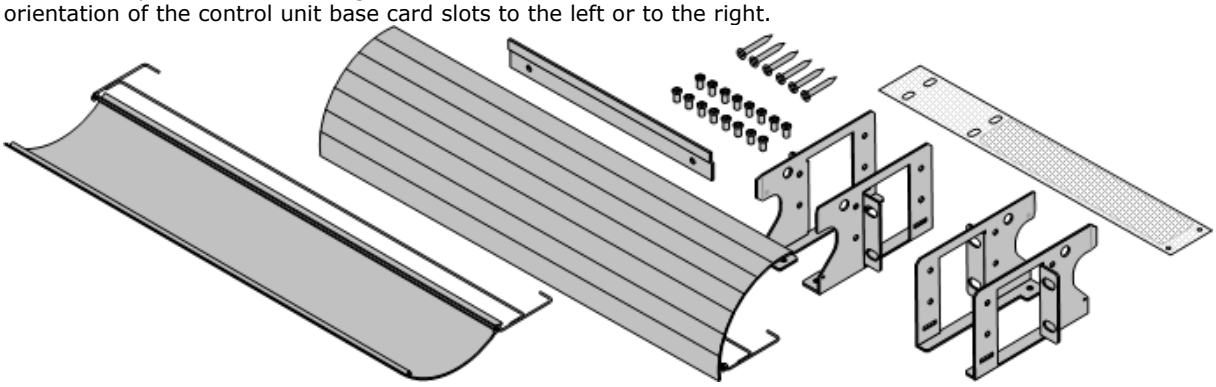


1.14.2 Rack Mounting Kits

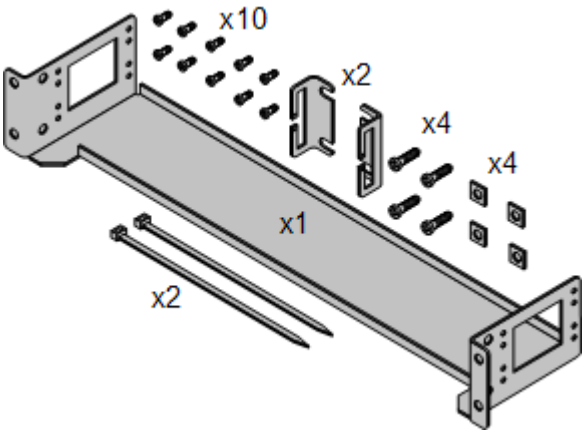
All IP Office control units and external expansion modules can be rack mounted into standard 19" rack systems. Each unit requires a 2U slot space within the rack. Rack mounting requires a kit for each control unit and external expansion module.

Where systems are being rack mounted, the effect of conditions within the rack cabinet must be considered. For example, the rack temperature may be above the room temperature and airflow within the rack is restricted. The environmental requirements 51 for the individual IP Office units are still applicable inside the rack cabinet.

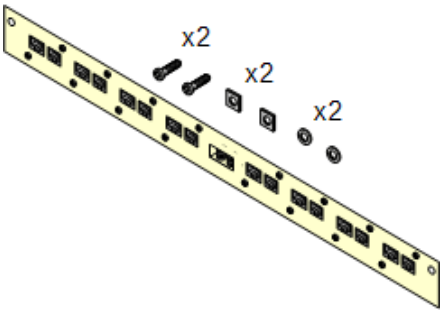
- **IPO IP500 WALL MNTG KIT V3** *(SAP Code 700503160)*
  This kit can be used for wall and rack mounting of IP500 V2 control units and IP500 external expansion modules. The kit incorporates cable routing at the front and rear of the unit. For wall mounted control units, it allows orientation of the control unit base card slots to the left or to the right.



- **IPO IP500 RACK MNTG KIT** *(SAP Code 700429202)*
  This kit contains all the components required for the rack mounting of a single IP500 V2 control unit or IP500 external expansion module. This includes screws for fixing of the brackets to the module, bolts for securing the module in the rack and cable tidy brackets..



Barrier Box Rack Mounting Kit



- **Barrier Box Rack Mounting Kit** *(SAP 700293905)*
  Barrier boxes must be used for out-of-building analog phone extensions 36. This bracket allows up to 8 IP Office barrier boxes to be rack mounted and simplifies the number of connections to the protective ground point in the rack. This kit must be used when more than 3 barrier boxes are in use and supports a maximum of 16 barrier boxes for a single external expansion module.

1.15 IP Office Phones

IP Office Release 11.0 supports the following phones and phone add-ons. Availability may depend on location and may be subject to local restrictions. For historic phone support, see Hardware/Software Compatibility[290].

Enhanced Tip and Ring (ETR Ports)

These phones are only supported on an ETR6 card in a IP500 V2 systems. They are only supported in IP Office Basic Edition - PARTNER® Mode and IP Office Basic Edition systems running a North American locale and U-Law companding.

- **ETR Series:** ETR6, ETR6D, ETR18, ETR18D, ETR34D *(ETR 34D phones are limited to a maximum of 2 per card and 4 in total)*

Avaya DS Digital Telephones (DS Ports)

These digital stations connect to the IP Office via DS[271] ports. They are supported by all IP Office modes.

- **1400 Series:** 1403, 1408, 1416
- **9500 Series:** 9504, 9508

The following additional DS port phones are only supported in IP Office standard modes:

- **2400 Series:** 2402, 2410, 2420.

Avaya BST Digital Telephones (BST Ports)

These digital stations connect to the IP500 V2 IP Office system via BST ports.

- **4100 Series:** 4135, 4136, 4145, 4145EX, 4146, 4146EX - Connection to IP Office BST ports via a Digital Mobility Solution system.
- **7400 Series:** 7420, 7430, 7434, 7439, 7440, 7444, 7449 - Connection to IP Office BST ports via a Digital Mobility Solution system.
- **ACU:** Audio Conferencing Unit
- **M-Series:** M7100, M7100N, M7208, M7208N, M7310, M7310N, M7324, M7324N.
- **T-Series:** T7000, T7100, T7208, T7316, T7316E, T7406, T7406E

Analog Telephones

Analog phones and devices connect to PHONE[276] ports with the IP Office system. However due to the variety of analog phones and device available no guarantee of operation is given. It is the responsibility of the IP Office installer and maintainer to test and verify the operation of proposed analog equipment.

- **6200 Series:** 6211, 6219, 6221 *(North America)*.
- **B100 Series:** B149, B159, B169*.
- **Interquartz Gemini:** 9330-AV, 9335-AV, 9281-AV *(Europe, Middle East, Africa, Asia-Pacific)*.

IP Telephones

IP Phones (SIP and H323) connect to the IP Office system via the RJ45 LAN or WAN. These device require an Avaya IP Endpoint license and voice compression resources.

H323:

- **1600 Series:** 1603IP/SW, 1608, 1608-I, 1616, 1616-I
- **3600 Series:** 3641, 3645
- **3700 Series:** 3701, 3711 - Connection via DECT base stations. 3720, 3725, 3730, 3735, 3740, 3745, 3749 - Connection via DECT R4 base stations.
- **9600 Series:** 9608, 9608G, 9611G, 9620L, 9620C, 9621G, 9630G, 9640, 9640G, 9641G, 9641GS, 9650, 9650C.

SIP:

- **1000 Series:** 1010, 1040
- **1100 Series:** 1120E, 1140E
- **1200 Series:** 1220, 1230
- **B100 Series:** B169*, B179, B199.
- **D100 Series:** These DECT handsets (up to 8) use a base station that connects to the IP Office system using a SIP trunk and appear on the IP Office as SIP extensions.
- **E129:** A simple SIP telephone, the E129 support auto-answer, handsfree and headset operation.
- **H175:** SIP video telephone.
- **H200:** H229, H239, H249.
- **J100 Series:** J129, J139, J159, J169, J179.
- **K100 Series:** K155*, K165, K175.

*The B169 is a DECT phone that connects to a DECT base station. The base station connects to the IP Office. Analog and SIP base stations exist.

Página2700 de 3226.

1.16 VoIP

IP Office is a converged telephony system, that is it combines aspects of traditional PABX telephone systems and IP data and telephony systems. This works at various levels.

- Individual phone users can control the operation of their phone through applications running on their PC.
- Data traffic can be routed from the LAN interface to a telephony trunk interface, for example a dial-up ISP connection.
- Voice traffic can be routed across internal and external data links. This option is referred to as voice over IP (VoIP).

The VoIP mode of operation can include external SIP trunks, IP trunks between customer systems and/or H.323 or SIP IP telephones for users. In either case the following factors must be considered:

- The IP Office control unit must be fitted with voice compression channels[41]. These are used whenever an IP device (trunk or extension) needs to communicate with a non-IP device (trunk or extension) or to a device that uses a different codec.
- A network assessment is a mandatory requirement for all systems using VoIP. For support issues with VoIP, Avaya may request access to the network assessment results and may refuse support if those are not available or satisfactory.

A network assessment would include a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies, and setting voice quality objectives.
- The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support H.323, DHCP, TFTP and jitter buffers in H.323 applications.
- An outline of the expected network assessment targets is:

Test	Minimum Assessment Target
Latency	Less than 150ms.
Packet Loss	Less than 3%.
Duration	Monitor statistics once every minute for a full week.

1.16.1 Voice Compression Channels

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. For IP Office systems this conversion is done by voice compression channels. These support the common IP audio codecs G.711, G.723 and G.729a. For IP Office Release 8.0 and higher, IP500 VCM and IP500 Combination cards also support G.722.

For IP500 V2 control units, channels can be added using IP500 VCM cards[221] and IP500 Combination Cards[214].

The voice compression channels are used as follows:

Call Type	Voice Compression Channel Usage
IP Device to Non-IP Device	These calls require a voice compression channel for the duration of the call. If no channel is available, busy indication is returned to the caller.
IP Device to IP Device	Call progress tones (for example dial tone, secondary dial tone, etc) do not require voice compression channels with the following exceptions: • Short code confirmation, ARS camp on and account code entry tones require a voice compression channel. • Devices using G723 require a voice compression channel for all tones except call waiting. When a call is connected: • If the IP devices use the same audio codec no voice compression channel is used. • If the devices use differing audio codecs, a voice compression channel is required for each.
Non-IP Device to Non-IP Device	No voice compression channels are required.
Music on Hold	This is provided from the IP Office's TDM bus and therefore requires a voice compression channel when played to an IP device.
Conference Resources and IP Devices	Conferencing resources are managed by the conference chip which is on the IP Office's TDM bus. Therefore, a voice compression channel is required for each IP device involved in a conference. This includes services that use conference resources such as call listen, intrusion, call recording and silent monitoring.
Page Calls to IP Device	IP Office 4.0 and higher only uses G729a for page calls, therefore only requiring one channel but also only supporting pages to G729a capable devices.
Voicemail Services and IP Devices	Calls to the IP Office voicemail servers are treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.
Fax Calls	These are voice calls but with a slightly wider frequency range than spoken voice calls. IP Office only supports fax across IP between IP Office systems with the Fax Transport option selected. It does not currently support T38.
T38 Fax Calls	Each T38 fax call uses a VCM channel. Within a Small Community Network, a T38 fax call can be converted to a call across an H323 SCN lines using the IP Office Fax Transport Support protocol. This conversion uses 2 VCM channels. In order use T38 Fax connection, the **Equipment Classification** of an analog extension connected to a fax machine can be set ***Fax Machine***. Additionally, a new short code feature **Dial Fax** is available.

Measuring Channel Usage

The System Status Application can be used to display voice compression channel usage. Within the **Resources** section it displays the number of channel in use. It also displays how often there have been insufficient channels available and the last time such an event occurred.

The IP500 VCM cards, channel usage is also indicated by the LEDs (1 to 8) on the front of the IP500 VCM card[221].

Página2702 de 3226.

1.17 Supported Country Locales

When a new or defaulted system's configuration is first opened in IP Office Manager, the value set in the **Locale** field should always be checked and changed if necessary.

The system's locale sets factors such as the default ringing patterns and caller display settings. The locale also controls the language that a voicemail server will attempt to use for prompts by default.

- The supported countries are: ***Argentina***, ***Australia***, ***Bahrain***, ***Belgium***, ***Brazil***, ***Canada***, ***Chile***, ***China***, ***Colombia***, ***Czech Republic***, ***Denmark***, ***Egypt***, ***Finland***, ***France***, ***Germany***, ***Greece***, ***Hong Kong***, ***Hungary***, ***Iceland***, ***India***, ***Ireland***, ***Italy***, ***Japan***, ***Korea***, ***Kuwait***, ***Malaysia***, ***Mediterranean***, ***Mexico***, ***Morocco***, ***Netherlands***, ***New Zealand***, ***Norway***, ***Oman***, ***Pakistan***, ***Peru***, ***Philippines***, ***Poland***, ***Portugal***, ***Qatar***, ***Russia***, ***Saudi Arabia***, ***Singapore***, ***South Africa***, ***Spain***, ***Sweden***, ***Switzerland***, ***Taiwan***, ***Turkey***, ***United Arab Emirates***, ***United States***, ***Venezuela***.

1.18 IP Office Software Applications

The IP Office applications are available on a number of DVDs. These can be ordered at a nominal cost to cover order processing and delivery. Separate installation packages for IP Office applications can also be downloaded[63] from the Avaya support website at http://support.avaya.com.

Title	Discs	Description	SAP Code
IP Office Release 11.0 Admin and User DVD Set	2	These DVDs contain installation packages for all the main IP Office administration and user applications. They also contain documentation for IP Office. • **DVD 1:** Contains the IP Office Administrator Applications suite, IP Office Documentation, IP Office User Applications, IP Office Voicemail Pro. • **DVD 2:** Contains the one-X Portal for IP Office application.	700513659
Voicemail Pro ScanSoft TTS DVD Set	2	Contains text to speech engines for use with Voicemail Pro's TTS functions. Supports the same languages as Voicemail Pro pre-recorded prompts except Hungarian.	700478068
IP Office Release 11.0 Server Edition Installation DVD	2	Installation DVD for Server Edition servers and IP Office Application Server. The second DVD contains open source material used for the first DVD.	700513657
Virtualized IP Office Server Edition DVD	1	Installation DVD for virtualized Server Edition servers and virtualized IP Office Application Server.	700513658
IP Office Linux Server TTS DVD Set	3	Contains text to speech engines for use with Linux based Voicemail Pro's TTS functions.	700502693

- It is acceptable to make copies of the Avaya IP Office DVDs listed above. However the content must remain intact, unaltered and without change or addition. Avaya does not accept any liability and responsibility for damage or problems arising from the use of such copies.

Página2703 de 3226.

1.18.1 Programming Applications

The following applications are used to program and maintain an IP Office system. Typically they run on a PC connected to the IP Office system via its LAN interface. These applications are all provided on the IP Office Administrator Applications DVD and don't require any licenses.

Due to the nature of the applications, if installed on a PC at the customer site, this should be a secure PC or the PC of a trusted user. If a voicemail server PC is also being installed with the IP Office system, the same PC can be used for the programming and maintenance applications.

For maintainers, these applications can also be run remotely if a route for data connections to the customer's IP Office exists from the maintainer's location.

- **IP Office Manager Version**
  It is important to download and install the correct version of the IP Office administration suite including IP Office Manager.
  - For system installation, you should use the version of IP Office Manager that matches the IP Office release required on the system. This sets the version of software loaded when recreating the System SD card 75.
  - For system maintenance, the version of IP Office Manager used sets the version of software uploaded to a system when upgrading the system 180.
  - For system configuration IP Office Manager is backward compatible. IP Office Manager Version 11.0 is backwards compatible for configuring systems running software from IP Office Release 6.0 upwards. IP Office Manager cannot load the configuration of an IP Office system running a higher version of software.
    - **Admin Lite Not Supported**
      Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).
- **! IP Office Technical Bulletins**
  You must obtain and read the IP Office Technical Bulletin relating to the IP Office software release which intend to install. The bulletin contains important information that may not have been included in this manual. IP Office Technical Bulletins are available from the Avaya support website *(http://support.avaya.com)*.

Applications

- **IP Office Manager** 253
  This tool is used to access all parts of the IP Office configuration. Different levels of access can be defined to control which parts of the configuration the IP Office Manager user can view and alter. IP Office Manager is also used to upgrade the software files used by an IP Office system.
  - **Admin Lite Not Supported**
    Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).
- **IP Office Web Manager** 71
  The configuration for an IP500 V2 system can be accessed via web browser using the same service user accounts as used for IP Office Manager. Currently, for IP Office standard mode systems, IP Office Web Manager can only be used to configure users, groups and service users (security accounts) and to perform basic maintenance actions. Therefore, IP Office Manager is still required for full system installation and maintenance.
- **System Status Application** 257
  This application can be used to inspect the current status of IP Office lines and extensions and to view records of recent alarms and events. It runs as a Java application.
- **SNMP MIBs** 192
  Not an application as such. Using IP Office SNMP MIB files the status of the IP Office system to be monitored by 3rd-party SNMP applications such as Castlerock and HP OpenView. When configured for SNMP operation, the IP Office can also send alerts for potential problems. IP Office systems also support the sending of the same alerts to SMTP email or Syslog addresses.
  - The alarms configurable for output via SNMP can also be output to SMTP email and or Syslog.
- **Monitor (SysMon)** 255
  Monitor is a tool that can show a trace of all activity on the IP Office system in detail. As a consequence, interpretation of Monitor traces requires a high-level of data and telephony protocol knowledge. Despite that however, all IP Office installers and maintainers need to understand how to run Monitor when necessary as Avaya may request copies of Monitor traces to resolve support issues.

1.18.2 User Applications

The IP Office supports a number of applications that operate in parallel with users telephones. These applications are installed from the IP Office Applications DVD. The one-X Portal for IP Office server can also be installed as part of the IP Office Application DVD installation.

Some of them require licenses to be entered into the IP Office system's configuration to enable features or to set the number of simultaneous users.

- **one-X Portal for IP Office** [255]
  This application is installed on a server PC connected to the IP Office. Users can access the one-X portal from their own PC using a web browser. The application allows the user to control their phones, access voicemail messages, call logs and phone directories.
  - **IP Office Web Client**
    This is a WebRTC client supported in a browser. It allows the user to make, answer and control audio and video calls from their PC. It is useable by users configured for one-X Portal for IP Office. Requires an IP Office Application Server with the WebRTC Gateway service configured.
- **SoftConsole** [257]
  This is a licensed application. It is intended for telephone system operators or receptionists. It displays details of calls and allows them to quickly see the status of the callers required destination and transfer the call. The SoftConsole user is able to access a range of details about the status of users and groups on the IP Office system. Up to 4 simultaneous SoftConsole users can be licensed.
- **Avaya IX Workplace Client** [254]
  This is a unified communications application that runs on Windows, macOS, iOS and Android devices.
- **Avaya Communicator** [256]
  This is a licensed application that runs on a various Windows, iPad and Android devices. Depending on configuration, a user can either use it in conjunction with their own phone to control calls or they can use it as their phone.
- **one-X Mobile**
  This is a set of clients supported on Apple iOS and Android mobile telephone devices. These allow the user to access the IP Office directory, personal contact and messages and to make and receive calls via the telephone system.
- **Web Collaboration** [260]
  Share documents and messages in a conference. Web Collaboration provides the user with functions to share documents, applications and their desktop in a web collaboration conference. This runs in parallel with an audio conference hosted by the IP Office system. Internal users licensed for web collaboration can use WebRTC to stream audio via the web collaboration conference rather than having to make a parallel telephone call to the audio conference.
- **TAPILink Lite** [258]
  The Microsoft Telephony Application Program Interface (TAPI) allows TAPI compliant applications to interact with IP Office phones by installing an IP Office TAPI driver. TAPILink Lite does not require any licenses entered into the IP Office system's configuration. It allows TAPI compliant applications such as Outlook to make and answer calls. The speech part of the calls is still via the user's physical phone.

1.18.3 Voicemail Applications

The IP Office supports a range of applications for the recording and playing of voicemail messages.

- **Embedded Voicemail**
  Embedded Voicemail supports basic voicemail mailbox operation, simple auto-attendants and hunt group announcements. For IP500 V2 controls units, Embedded Voicemail is provided by the Avaya SD card fitted by default.
- **Voicemail Pro** [259]
  This voicemail application runs on a server PC connected to the IP Office. It requires various licenses entered into the IP Office configuration to control the features it offers and the number of simultaneous connections. The operation of Voicemail Pro can be customized to provide special services. The application can be installed on a Windows server or be provided by an IP Office Application Server (which can also run one-X Portal for IP Office and Media Manager).
- **Media Manager** [253]
  Voicemail Pro can be used for manual and automatic call recording. Those recording are placed into mailboxes. Media Manager allows those recordings to be redirected to a separate store where details of each recording are maintained in a searchable database. This allows recordings to be archived, searched and played back separately from mailbox messages. This application requires entry of a additional licenses into the IP Office configuration. This application requires an IP Office Application Server including additional hard disk for storage of recordings.

1.18.4 Call Logging Applications

A wide range of 3rd -party applications exist to provide call logging and accounting for telephone systems. To support these the IP Office provides an SMDR output.

- **SMDR Output**
  For IP Office Release 5.0 and higher, the IP Office control unit directly outputs SMDR records to a specified IP address. This is configure using IP Office Manager.

1.18.5 Call Center Applications

The IP Office supports a number of contact center solutions.

- **IP Office Contact Center**
  This application suite supports a range of module allowing calls to be routed to agents based on a range of factors.
- **Avaya Contact Center Select**
  This is a large contact center solution for up to 250 agents.

1.18.6 CTI Applications

- **TAPILink Pro**
  Using the same software as TAPILink Lite, TAPILink Pro provides all of the features and functionality of TAPILink Lite, but additionally provides third party CTI operation. This means that a single server can control and monitor any number of telephone devices. This requires entry of a CTI Link Pro license. TAPILink Pro also provides the ability to monitor and control groups. This allows an application to be notified when a call enters a queue, and can also redirect it to another location.
- **TAPI WAV driver**
  Provides software-based support for voice processing. Purchasing the CTI Link Pro RFA license key also enables 4 ports of voice processing; additional ports can be purchased in 4 port increments. The TAPI-WAV driver is for use with TAPI 2.1 only; for TAPI 3.0, IP Office supports the Media Service Provider (MSP) interface, defined by Microsoft in TAPI 3.0.
- **DevLink Pro**
  Provides a real-time event stream in addition to the SMDR interface provided in IP Office SMDR (see below). The real-time event stream takes the form of a call record, which is issued whenever the state of any endpoint of a call changes (typically there are two endpoints on a call, but for some circumstances, such as conference calls, intruded calls there may be more).

1.19 Training

Avaya University provides a wide range of training courses for IP Office and its associated applications. This includes courses necessary for IP Office resellers to become Avaya Authorized Channel Partners and for individuals to achieve IP Office certification.

Details of courses can be found on the Avaya University web site (http://www.avaya-learning.com). The site can be used to check course availability and to book course. It also includes on-line courses and on-line course assessments. The site requires users to setup a user name and password in order to track their personal training record.

1.20 Web Sites

Information to support the IP Office can be found on a number of web sites.

- **Avaya** *(http://www.avaya.com)*
  The official web site for Avaya. The front page also provides access to individual Avaya web sites for different countries.
- **Avaya Enterprise Portal** *(http://partner.avaya.com)*
  This is the official web site for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the site portal can be individually customized for what products and information types you wish to see and to be notified about by email.
- **Avaya Support** *(http://support.avaya.com)*
  Contains documentation and other support materials for Avaya products including IP Office. Copies of the IP Office CD images are available from this site and updated core software .bin files.
- **Avaya IP Office Knowledge Base** *(https://ipofficekb.avaya.com)*
  Access to an on-line regularly updated version of the IP Office user guides and technical manuals.
- **Avaya University** *(http://www.avaya-learning.com)*
  This site provides access to the full range of Avaya training courses. That includes both on-line courses, course assessments and access to details of classroom based courses. The site requires users to register in order to provide the user with access to details of their training record.
- **Avaya Community** *(http://www.aucommunity.com)*
  This is the official discussion forum for Avaya product users. However it does not include any separate area for discussion of IP Office issues.
- **Avaya Product Compatibility Matrix** *(https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml)*
- **Avaya Product Port Matrix Documents** *(https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003)*
- **Other Non-Avaya Web Sites**
  A number of third-party web forums exist that discuss IP Office. These can act as useful source of information about how the IP Office is used. Some of these forums require you to be a member and to register. These are not official Avaya forums and their content is not monitored or sanctioned by Avaya.
  - **Tek-Tips** *(http://www.tek-tips.com)*
  - **IP Office Info** *(http://www.ipofficeinfo.com)*
  - **Yahoo Groups** *(http://groups.yahoo.com/group/ipoffice)*
  - **PBX Tech** *(http://www.pbxtech.info/forumdisplay.php?f=8)*

1.21 Emergency and Power Failure Ports

IP Office systems provide 2 types of analog extension power failure ports. In all cases these only work with loop-start analog trunks. Any phones connected to these ports should be clearly labeled as power fail extensions in accordance with the appropriate national and local regulatory requirements.

Switching Power Failure Ports

During normal operation, these ports can be used for normal analog phone connection. During power failure, the ports connect directly to an analog trunk port.

This type of power failure port is provided by the following cards:

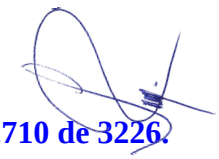
- **IP500 Analog Phone 8 Card**
  When an IP500 Analog Phone 8 base card is fitted with an IP500 Analog Trunk daughter card, during power failure extension port 8 is connected to analog trunk port 12.
- **IP500 ATM Combination Card/IP500 ATM Combination Card V2**
  On this card, during power failure, extension port 8 is connected to analog trunk port 12.

Emergency Only Power Failure Ports

During normal operation, these ports cannot be used. During power failure, the ports connect directly to an analog trunk port.

- **IP500 Analog Trunk Daughter Card/IP500 Analog Trunk Daughter Card V2**
  Regardless of the IP500 card hosting it, during power failure pins 4 and 5 of port 12 are connected to pins 7 and 8.
- **IP500 ETR6 Card**
  On this card, during normal operation extension ports 7 and 8 are not useable. However, if the card is fitted with an IP500 Analog Trunk daughter card, during power failure extension ports 7 and 8 are connected to analog trunk port 12.

Chapter 2.
Installation Overview



2. Installation Overview

This installation process is a simple outline. Many steps can be completed before the actual installation at the customer site.

Installation process summary

1. **Prepare for installation** 50
   a. **Environmental Requirements** 51
      Check that the installation area meets the system environmental requirements.
   b. **Space Requirements** 53
      Check that the installation area meets the system space requirements.
   c. **Tools and Parts Required** 59
      Check that you have the tools and additional parts required.
   d. **Documentation** 60
      Ensure that you have obtained and read all the relevant documentation.
   e. **Unpacking** 60
      Check that all the required equipment has been delivered and that there is no damage.
2. **Admin Software Installation** 62
   For system installation you need a PC with the IP Office administrator software installed. This must include a copy of IP Office Manager that matches the IP Office software level required.
   a. **Downloading the Software** 63
   b. **Installing the Administrator Applications** 64
3. **Preparing the System SD card** 74
   Upgrade the System SD card to the required releaser of IP Office software. In addition add any other files available such as the license file, pre-built configuration, music-on-hold file.
   - **! WARNING: Installing PCS14 and earlier control units**
     PCS 296 14 or lower units must first install Release 8.1(65) (or higher 8.1) or any Release 9.0 and then upgrade to Release 9.1. Care should be taken to ensure that no calls are made before the upgrade to Release 10.0, otherwise the system will require an 10.0 upgrade license despite being "new". The PCS of the control unit is printed on the label on the back of the control unit.
4. **Install the control unit cards** 82
   Attach any trunk daughter cards to their IP500 base cards and insert the base cards into the control unit.
5. **Install the system** 86
   a. **Wall Mounting** 87
      If wall mounting, attach the brackets and fit the unit to the wall.
   b. **Rack Mounting** 89
      If rack mounting, attach the brackets and fit the control unit into the rack.
   c. **Connect the External Expansion Modules** 91
      Connect the external expansions modules to the control unit.
   d. **Ground the system** 93
      Attach required ground cables to the control unit and external expansion modules.
   e. **Starting the System** 94
      Insert the System SD card and power up the system.
   f. **Connecting Phones** 97
      Connect the Avaya digital phones.
6. **Initial Configuration**
   Once the physical system is started, it can be configured. This can be done using either IP Office Manager 100 or IP Office Web Manager 114 .

Página2711 de 3226.

2.1 Environmental Requirements

The planned location must meet the following requirements. If being installed into a rack system, these are requirements for within the rack:

1. ☐ Temperature: Operating 5°C to 40°C (Storage -40°C to 70°C).
2. ☐ Relative Humidity: Operating 10% to 90% (Storage 5% to 95%).
3. ☐ Check there are no flammable materials in the area.
4. ☐ Check there is no possibility of flooding.
5. ☐ Check that no other machinery or equipment needs to be moved first.
6. ☐ Check that it is not an excessively dusty atmosphere.
7. ☐ Check that the area is unlikely to suffer rapid changes in temperature and humidity.
8. ☐ Check for the proximity of strong magnetic fields, sources of radio frequency and other electrical interference.
9. ☐ Check there are no corrosive chemicals or gasses.
10. ☐ Check there is no excessive vibration or potential of excessive vibration, especially of any mounting surface.
11. ☐ Check that where telephones are installed in another building, that the appropriate protectors and protective grounds are fitted (see Out of Building Telephone Installation 36).
12. ☐ Check there is suitable lighting for installation, system programming and future maintenance.
13. ☐ Check that there is sufficient working space for installation and future maintenance.
14. ☐ Ensure that likely activities near the system will not cause any problems, e.g. access to and maintenance of any other equipment in the area.
15. ☐ Where ventilation holes are present on any of the IP Office units, those holes should not be covered or blocked.
16. ☐ The surface must be flat horizontal for free-standing or rack mounted installations.

Rack Mounting

1. Rack Positioning - Ensure compliance with the rack manufacturers safety instructions. For example check that the rack legs have been lowered and fixing brackets have been used to stop toppling.
2. Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
   - ☐ Operating Temperature: 5°C (40°F) to 40°C (104°F).
   - ☐ Operating Humidity: 10% to 95% non-condensing.
3. Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised. Proper ventilation must be maintained. The side ventilation slots on the IP500 control unit should not be covered or blocked.
4. Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
5. Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
6. Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
7. ⚠ Only the screws provided with the mounting kit should used to attach the brackets to the control unit.

Wall Mounting

In additional to the requirements above, the following are applicable to IP Office units that support wall mounting.

1. Units must only be mounted onto permanent wall surfaces.
2. The surface must be vertical and flat.
3. Orientation of the unit must be as shown in the section on IP500 Wall Mounting 87.
4. The appropriate Avaya wall mounting kits must be used.

Página2712 de 3226.

IMPORTANT SAFETY INSTRUCTIONS

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.
4. Use only the power cord and batteries indicated in this manual.

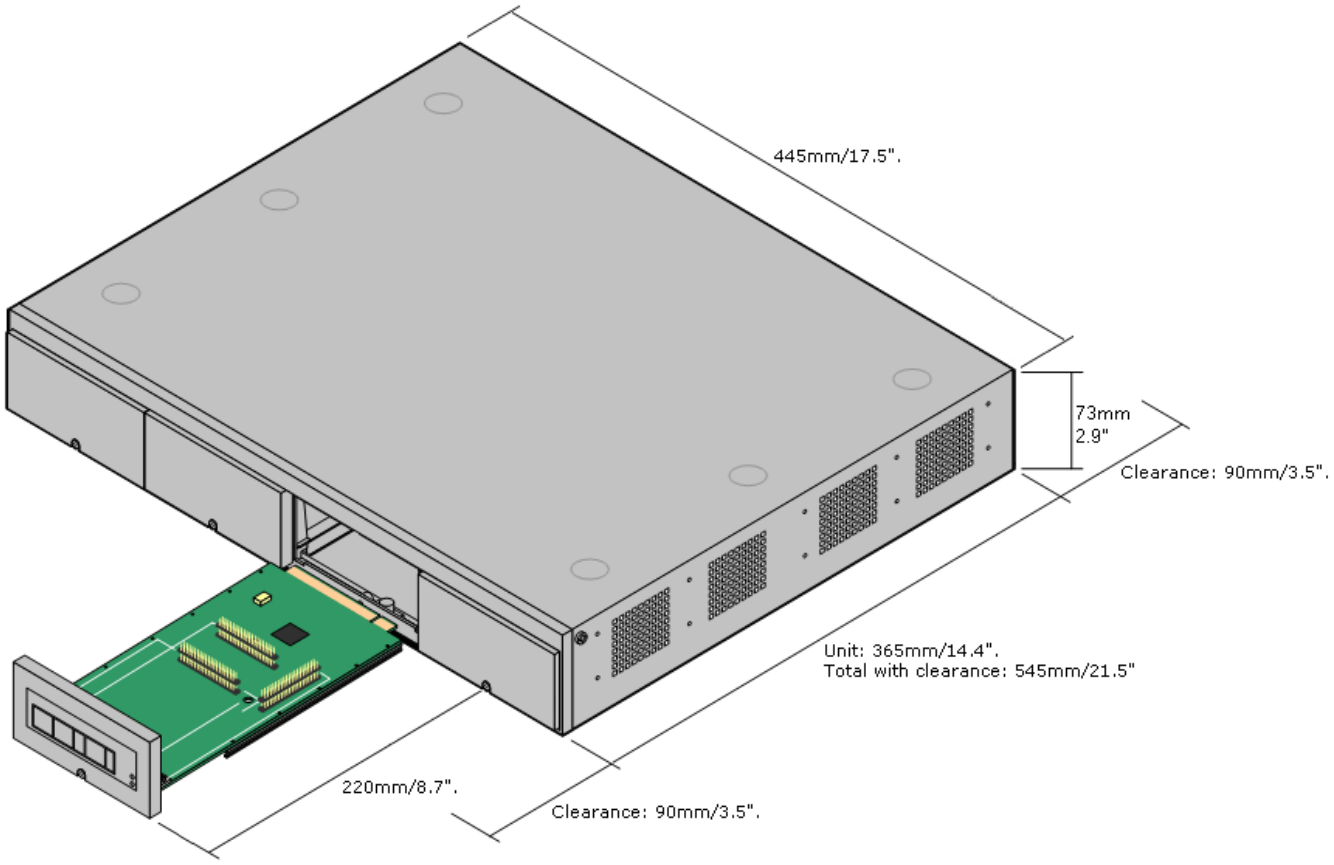
2.2 Space Requirements

IP Office control units and modules are designed to be installed either in a free-standing stack or into a 19" rack system. Rack installation requires a rack mounting kit[37] for each control unit and expansion module.

- **Cable Clearance**
  Clearance must be provided at the front and rear of all modules for cable access. On IP500 V2 systems allow a minimum clearance of 90mm (3.5 inches).
- **Additional Clearance**
  Care should be taken to ensure that the positioning of the modules does not interrupt air flow and other factors that may affect environmental requirements[51]. This is especially important on IP500 V2 control units which have ventilation slots at the side.
- **Cable Access**
  Power cords must not be attached to the building surface or run through walls, ceilings, floors and similar openings. Installation measures must be taken to prevent physical damage to the power supply cord, including proper routing of the power supply cord and provision of a socket outlet near the fixed equipment or positioning of the equipment near a socket outlet.

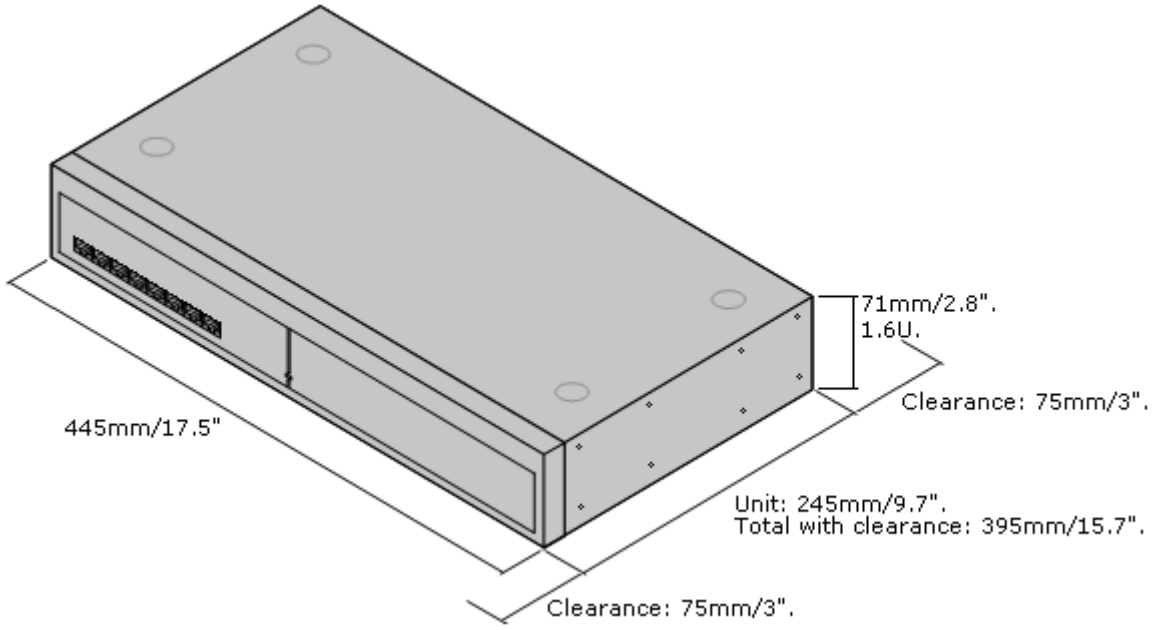
2.2.1 Control Unit

The ventilation slots on the rear and sides should not be covered or blocked.



2.2.2 External Expansion Modules

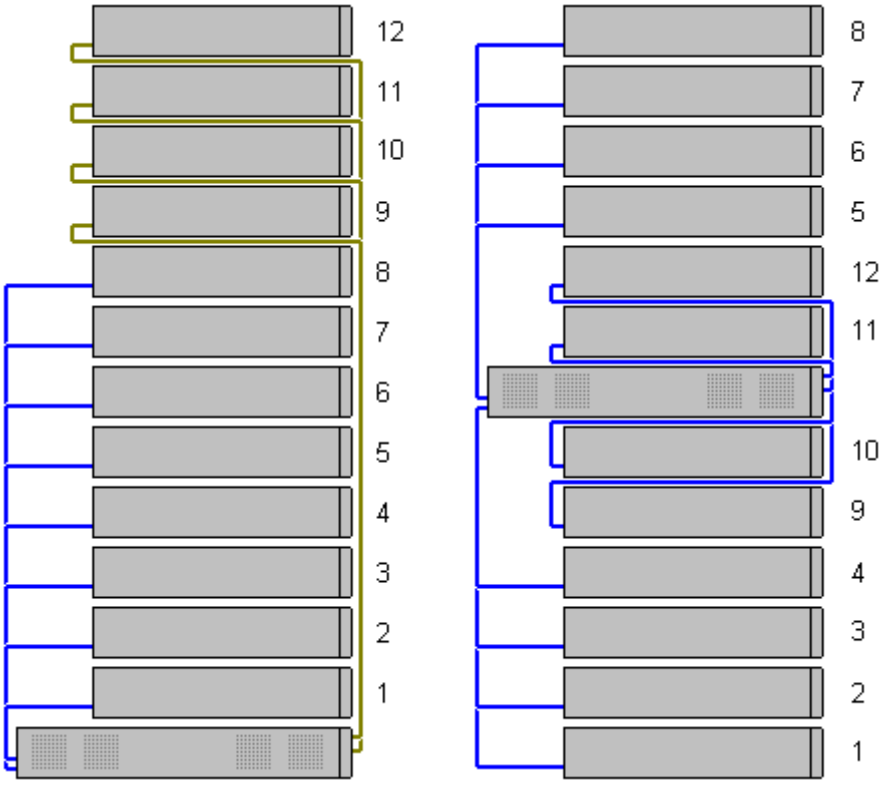
The dimensions below are applicable to all IP Office external expansion modules.



For free-standing systems, the external expansion modules can be stacked on top of the control unit. For that, and for rack mounted systems, the diagram below shows the recommended options to accommodate the length of the module interconnect cable.

The integral expansion ports on a control unit are located on the rear of the unit. An additional 4 expansion ports can be added to the front of the control unit by installing an IP500 4-Port Expansion card.

- Each external expansion module is supplied with a blue 1 meter (3'3'') expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on an IP500 4-Port Expansion card, a yellow 2 meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. 4 Yellow cables are supplied with the IP500 4-Port Expansion card.



2.2.3 Wall Mounting

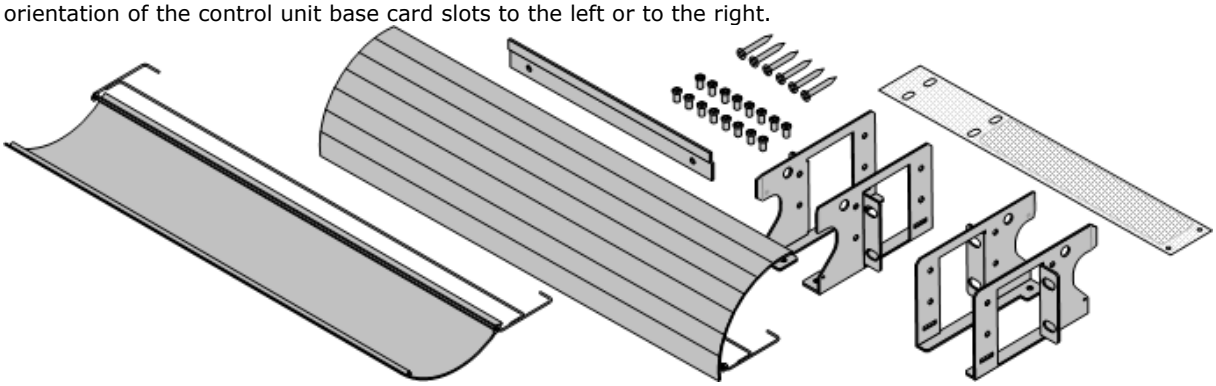
IP500 V2 control units and IP500 external expansion modules can be wall or rack mounted. To do this, a wall mounting kit is required in addition to suitable wall fixings.

In addition to the existing environmental requirements[51] for an IP Office system, the following additional requirements apply when wall mounting a unit:

- The wall surface must be vertical, flat and vibration free. Attachment to temporary walls is not supported.
- Only the screws provided with the mounting kit should be used to attach the brackets to the control unit or expansion modules.
- The installation must be done by a service person.
- Ensure that the system has been shut down and power has been removed from all the units. Shut down the system using a shutdown command and then remove the power. Do not simply remove the power.
- A suitable plywood mounting surface of at least 1m x 1m x 19mm (39" x 39" x 0.75") is required. If an expansion box is being mounted as well a plywood mounting surface of at least 1.2m x 1.2m x 19mm (48" x 48" x 0.75") is required.
- A minimum of 6 x 45mm long 5mm/6mm (1.75" #10/#12) pan head screws must be used to secure the plywood to the wall studs.
- The supplied 20mm long 4mm (#8 ¾") wood screws must be used to secure the brackets to the plywood mounting surface

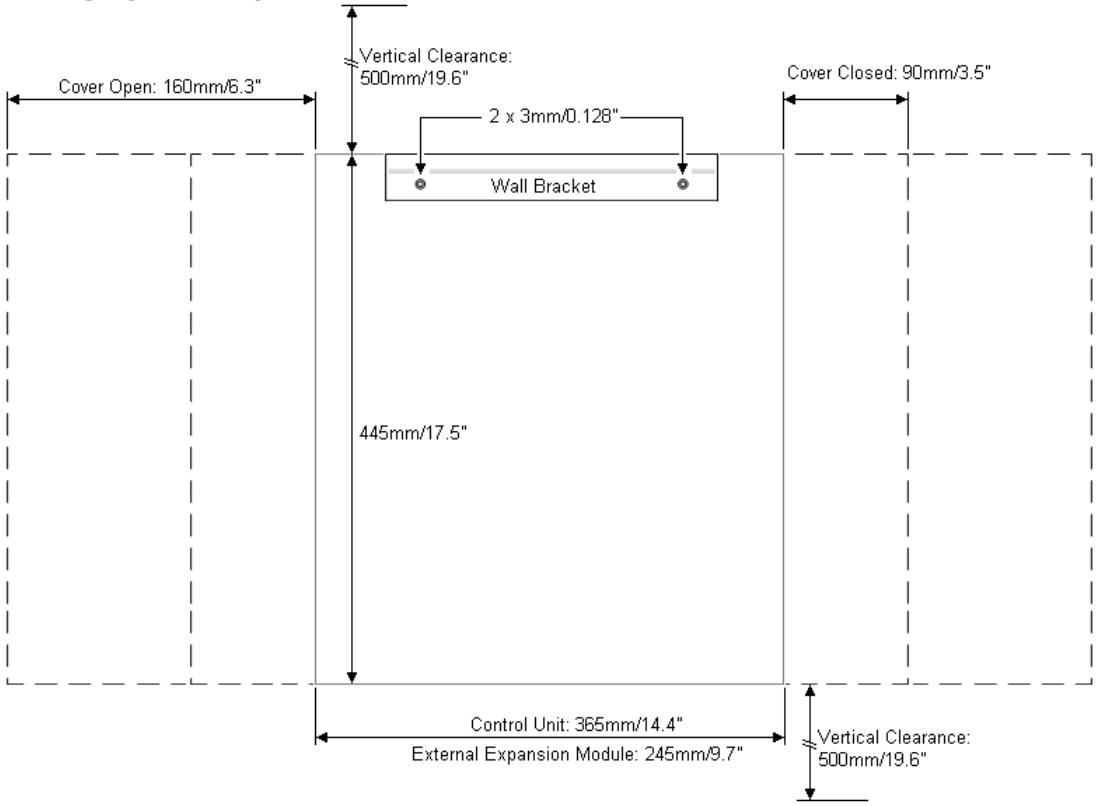
The following kit is currently available:

- **IPO IP500 WALL MNTG KIT V3** *(SAP Code 700503160)*
  This kit can be used for wall and rack mounting of IP500 V2 control units and IP500 external expansion modules. The kit incorporates cable routing at the front and rear of the unit. For wall mounted control units, it allows orientation of the control unit base card slots to the left or to the right.



Página2716 de 3226.

Wall Mounting Space Requirement

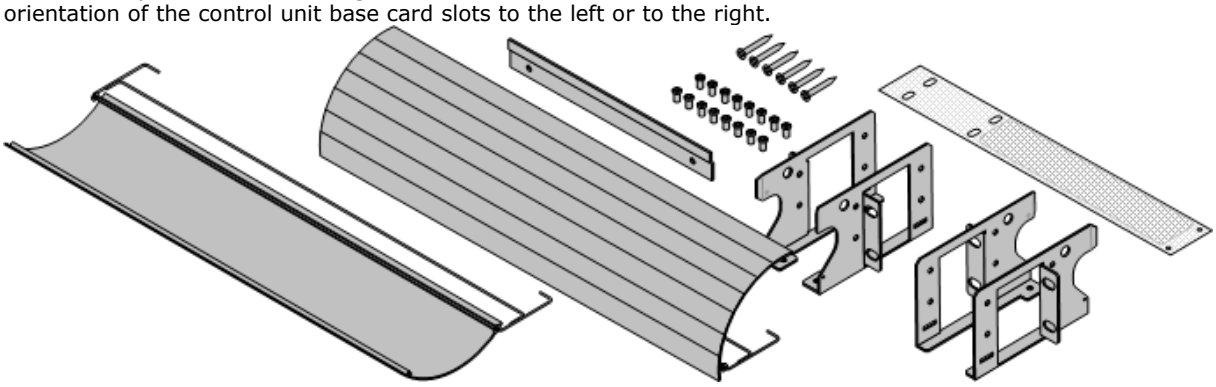


2.2.4 Rack Space Requirements

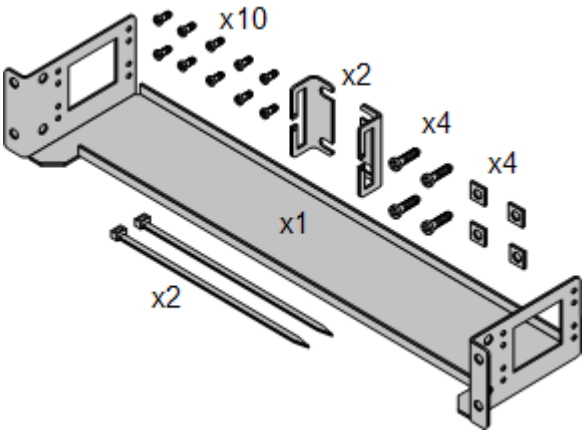
All IP Office control units and external expansion modules can be rack mounted into standard 19" rack systems. Each unit requires a 2U slot space within the rack. Rack mounting requires a kit for each control unit and external expansion module.

Where systems are being rack mounted, the effect of conditions within the rack cabinet must be considered. For example, the rack temperature may be above the room temperature and airflow within the rack is restricted. The environmental requirements 51 for the individual IP Office units are still applicable inside the rack cabinet.

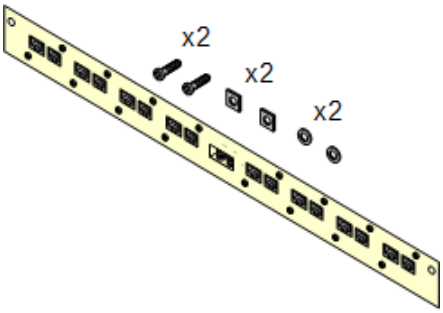
- **IPO IP500 WALL MNTG KIT V3** *(SAP Code 700503160)*
  This kit can be used for wall and rack mounting of IP500 V2 control units and IP500 external expansion modules. The kit incorporates cable routing at the front and rear of the unit. For wall mounted control units, it allows orientation of the control unit base card slots to the left or to the right.



- **IPO IP500 RACK MNTG KIT** *(SAP Code 700429202)*
  This kit contains all the components required for the rack mounting of a single IP500 V2 control unit or IP500 external expansion module. This includes screws for fixing of the brackets to the module, bolts for securing the module in the rack and cable tidy brackets..



Barrier Box Rack Mounting Kit



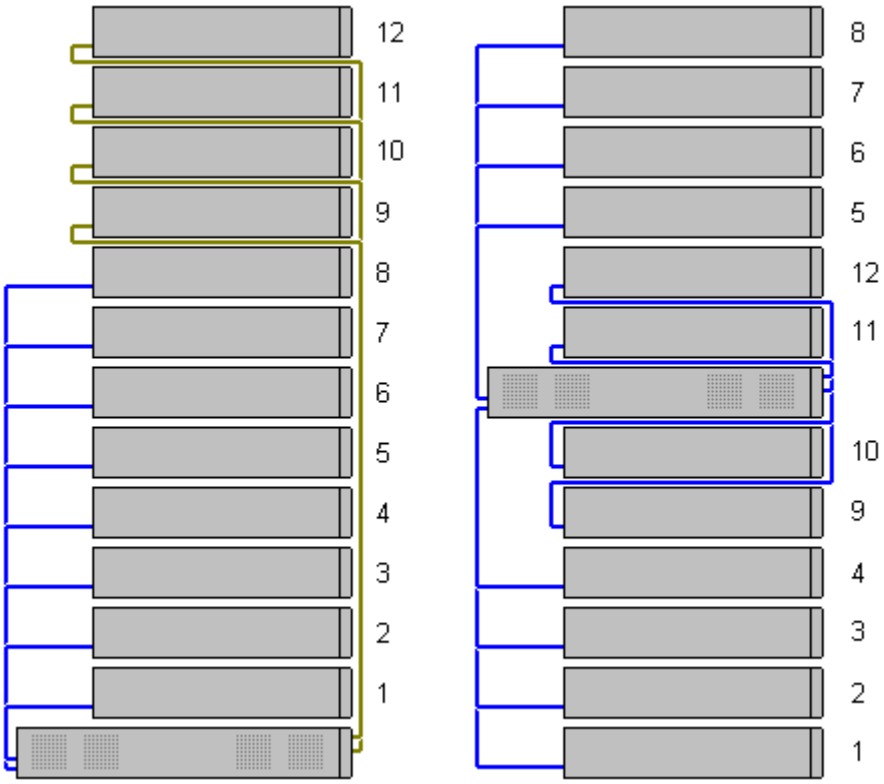
- **Barrier Box Rack Mounting Kit** *(SAP 700293905)*
  Barrier boxes must be used for out-of-building analog phone extensions 36. This bracket allows up to 8 IP Office barrier boxes to be rack mounted and simplifies the number of connections to the protective ground point in the rack. This kit must be used when more than 3 barrier boxes are in use and supports a maximum of 16 barrier boxes for a single external expansion module.

Página2718 de 3226.

Rack Module Positioning

The integral expansion ports on a control unit are located on the rear of the unit. An additional 4 expansion ports can be added to the front of the control unit by installing an IP500 4-Port Expansion card.

- Each external expansion module is supplied with a blue 1 meter (3'3'') expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on an IP500 4-Port Expansion card, a yellow 2 meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. 4 Yellow cables are supplied with the IP500 4-Port Expansion card.



2.3 Tools and Parts Required

The following is a general summary of the tools required. Additional tools and equipment will be required for wall and or rack mounting and to fashion ground cable connections suitable to local requirements.

IP Office Parts

The minimum parts required are:

- ☐ IP500 V2 Control Unit [205]
- ☐ Avaya SD Card [208]
- ☐ PLDS License File [279]
  - The PLDS host ID used for the license file must match that shown by the 12 digit **PLDS ID** printed on the SD card label. Older cards have an 10 digit feature key serial number shown by **FK** or **FK SN**. For those cards add the prefix ***11*** to obtain the card's PLDS ID.
- ☐ The file must be appropriate for the release of software being licensed.
- ☐ The file must contain an **Essential Edition** license appropriate to the target IP Office release.

Tools Required

- ☐ 5mm Flat-blade screwdriver.
- ☐ Crosshead screwdriver.
- ☐ Anti-static wrist strap and ground point.
- ☐ RJ45-RJ45 Ethernet LAN Cable.
- ☐ M4 Cross-Head Screwdriver.
- ☐ Tools suitable for crimping a cable spade.
- ☐ If wall mounting, drills and tools for wall mounting fixtures.

System Administration

- ☐ Windows PC with:
  - ☐ IP Office Admin suite installed [64].
  - ☐ RJ45 Ethernet LAN port.
  - ☐ SD Card reader.

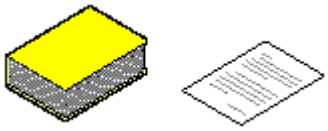
Additional Parts Required

In addition to orderable IP Office equipment, the following items will be required.

- ☐ 14AWG Solid copper wire for ground connection of control units and expansion modules.
- ☐ Cable sleeve matching local regulator requirements for ground wires. Typically green for a functional ground and green/yellow for a protective ground.
- ☐ If wall mounting, additional fixtures and fittings suitable for the wall type and mounting kit being used.
- ☐ Cable ties and labels for tidying and identifying cables.

Página2720 de 3226.

2.4 Documentation



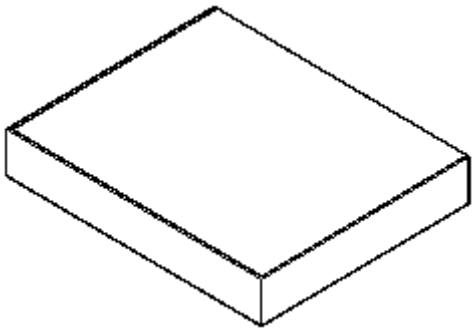
Ensure that you have read this manual in full before starting installation. Also include the installation documentation for any other equipment and applications being installed as part of the IP Office system.

IP Office documentation is available from the following web sites.

- **Avaya Support** *(http://support.avaya.com)*
  Contains documentation and other support materials for Avaya products including IP Office. Copies of the IP Office CD images are available from this site and updated core software .bin files.
- **Avaya IP Office Knowledge Base** *(https://ipofficekb.avaya.com)*
  Access to an on-line regularly updated version of the IP Office user guides and technical manuals.

- **! IP Office Technical Bulletins**
  You must obtain and read the IP Office Technical Bulletin relating to the IP Office software release which intend to install. The bulletin contains important information that may not have been included in this manual. IP Office Technical Bulletins are available from the Avaya support website *(http://support.avaya.com)*.

2.5 Unpacking



Use the following procedure when unpacking any equipment supplied by Avaya or an Avaya reseller or distributor.

Information Required

- ☐ **Equipment Checklist**.
  An installation checklist of the parts and equipment ordered for the installation.

Procedure

1. ☐ **Check for Packaging Damage**
   Before unpacking any equipment, check for any signs of damage that may have occurred during transit. If any damage exists bring it to the attention of the carrier.
2. ☐ **Check the Correct Parts Have Been Delivered**
   Check all cartons against the packing slip and ensure that you have the correct items. Report any errors or omissions to the equipment supplier.
3. ☐ **Retain All Packaging and Documentation**
   While unpacking the equipment, retain all the packaging material. Fault returns are only accepted if repackaged in the original packaging. If performing a staged installation, the original packaging also assists when repacking equipment to move it to the final installation site.
4. ☐ **Ensure that Anti-Static Protection Measures are Observed**
   Ensure that anti-static protection measures are observed at all times when handling equipment with exposed electrical circuit boards.
5. ☐ **Check All Parts**
   Visually inspect each item and check that all the necessary documentation and accessory items have been included. Report any errors or omissions to the dealer who supplied the equipment.
6. ☐ **Check All Documentation**
   Ensure that you read and retain any documentation included with the equipment.

Chapter 3.

Installing the Administrator Software

3. Installing the Administrator Software

In order to install and maintain an IP Office system you must be familiar with using the following applications.

- **IP Office Manager**
  This is a Windows based application. IP Office Manager is used to access all parts of the IP Office configuration. Different levels of access can be defined to control which parts of the configuration the user can view and alter. IP Office Manager is also used to upgrade the software files used by an IP Office system.
  - **IP Office Manager Version**
    It is important to download and install the correct version of the IP Office administration suite including IP Office Manager.
    - For system installation, you should use the version of IP Office Manager that matches the IP Office release required on the system. This sets the version of software loaded when recreating the System SD card 75.
    - For system maintenance, the version of IP Office Manager used sets the version of software uploaded to a system when upgrading the system 180.
    - For system configuration IP Office Manager is backward compatible. IP Office Manager Version 11.0 is backwards compatible for configuring systems running software from IP Office Release 6.0 upwards. IP Office Manager cannot load the configuration of an IP Office system running a higher version of software.
    - **Admin Lite Not Supported**
      Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).
- **IP Office Web Manager**
  Following installation, the configuration for an IP500 V2 system can also be accessed via web browser using the same service user accounts as used for IP Office Manager.
- **System Status Application**
  System Status Application (SSA) is a reporting tool that provides a wide range of information about the current status of an IP Office system. It reports the available resources and components within the system and details of calls in progress. Details of alarms current and historical alarms are shown. When required for diagnostics escalation, SSA can take a snap shot image of the IP Office system's status including a copy of its current configuration.
- **Monitor (System Monitor)**
  System Monitor is a tool that can show the activity on the IP Office system in great detail. As a consequence, interpretation of traces requires a high-level of data and telephony protocol knowledge. However, all IP Office installers and maintainers must know how to run Monitor to capture a trace as Avaya may request those traces to investigate support issues.

3.1 Downloading the Software

The IP Office administration suite of software is available as an orderable DVD 42. However, the software can also be downloaded from the Avaya support website (http://support.avaya.com).

- **IP Office Manager Version**
  It is important to download and install the correct version of the IP Office administration suite including IP Office Manager.
  - For system installation, you should use the version of IP Office Manager that matches the IP Office release required on the system. This sets the version of software loaded when recreating the System SD card 75.
  - For system maintenance, the version of IP Office Manager used sets the version of software uploaded to a system when upgrading the system 180.
  - For system configuration IP Office Manager is backward compatible. IP Office Manager Version 11.0 is backwards compatible for configuring systems running software from IP Office Release 6.0 upwards. IP Office Manager cannot load the configuration of an IP Office system running a higher version of software.
  - **Admin Lite Not Supported**
    Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).
- **! IP Office Technical Bulletins**
  You must obtain and read the IP Office Technical Bulletin relating to the IP Office software release which intend to install. The bulletin contains important information that may not have been included in this manual. IP Office Technical Bulletins are available from the Avaya support website *(http://support.avaya.com)*.

To download Avaya software:

1. Browse to ***http://support.avaya.com*** and log in.
2. Select **Support by Product** and click **Downloads**.
3. Enter ***IP Office*** in the **Enter Product Name** box and select the matching option from the displayed list.
4. Use the **Choose Release** drop-down to select the required IP Office release.
5. Click **Downloads**. The page lists the most recently available downloads.
6. Click **View Downloads** for the full list of downloads.
7. Select the required software package for download.
8. The page displayed in a new tab or windows details the options for downloading that software. For IP500 installation, download the full administration package, not the separate binary files or the Admin lite download packages.
9. Also download the documents listed under the **RELATED DOCUMENTS** heading if shown.

Página2724 de 3226.

3.2 Installing the Administrator Applications

The IP Office Administration suite consists of a number of applications for IP Office installers and maintainers.

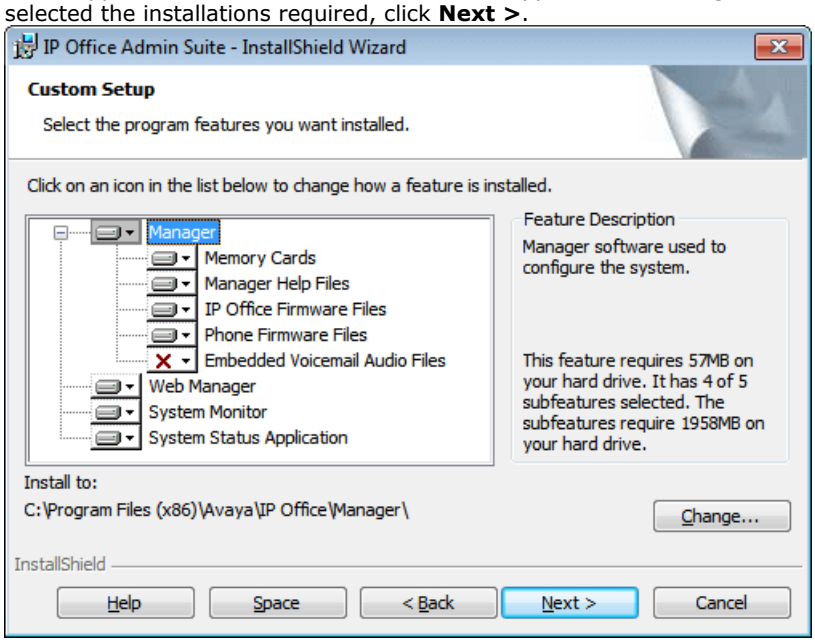
- ☐ **System Monitor** - *Install* ✓
- ☐ **IP Office Manager** - *Install* ✓
- ☐ **System Status Application** - *Install* ✓

Requirements

- ☐ **IP Office Release 11.0 User/Admin DVD Set (2) (700513659)**
  Alternatively the IP Office Administrator Applications suite can be downloaded from Avaya's support website (*http://support.avaya.com*).
- ☐ **Windows PC Requirements**
  The specifications below are the minimum requirements for IP Office Manager. If other applications are to be installed on the PC their individual requirements should also be meet. The supported versions of Windows are listed in the Operating Systems 261 section.
  - **Standard Manager:** Core i3 CPU, 4GB RAM, 32/64-bit OS
  - **Server Edition Manager:** Core i5 CPU, 6GB RAM , 32/64-bit OS
  - **Server Edition Select Manager:** Core i5 CPU, 8GB RAM, 64-bit OS
  - IP Office Manager is only supported on Windows set to 100% font size display.

To install the IP Office administrator applications:

1. Using the **Add or Remove Programs** option in the Windows Control Panel, check that the PC does not already have a version of the IP Office Admin suite installed.
   - If 'yes' and the suite is a pre-IP Office 3.2 version, remove the existing IP Office Admin suite via Add/Remove Programs.
   - If the existing suite is IP Office 3.2 or higher, it is possible to upgrade without removing the previous installation.
2. Insert the IP Office Administrator Applications DVD. Select the option for the IP Office Administration Suite. A folder window will display the installation files for the administration suite.
3. Right-click on setup.exe and select **Run as administrator**.
4. Select the language for the installation process. This does not affect the language used by IP Office Manager when running. Click **Next >**.
5. Click **Next >**.
6. If you agree, click **I accept the terms in the license agreement** and then click **Next >**.
7. If required, change the destination to which the applications should be installed. We recommend that you accept the default destination. Click **Next >**.
8. The next screen is used to select which applications should be installed. Clicking on each will display a description of the application. Click on the ▼ next to each application to change the installation selection. When you have selected the installations required, click **Next >**.



- **Manager**
  Install the basis IP Office Manager application required for editing system configurations plus any of the following:
  - **Memory Cards**
    Install the files needed to recreate an Avaya System SD card.
  - **Manager Help Files**
    Install the application help files in all available languages. If not selected, only English is installed.
  - **IP Office Firmware Files**
    Install the firmware files used by IP Office external expansion modules. These files are only need if IP Office Manager is to be used for system upgrades.
  - **Phone Firmware Files**
    Install the firmware files used by the various Avaya IP telephones supported by IP Office. These files are only need if IP Office Manager is to be used for system upgrades.
  - **Embedded Voicemail Audio Files**
    Install the voicemail prompts used by Embedded Voicemail. These files are only need if IP Office Manager is to be used for system upgrades.
- **Web Manager**
  Install a copy of the files that need to be loaded onto a system for it to run IP Office Web Manager.
- **System Monitor**
  Install the System Monitor application.

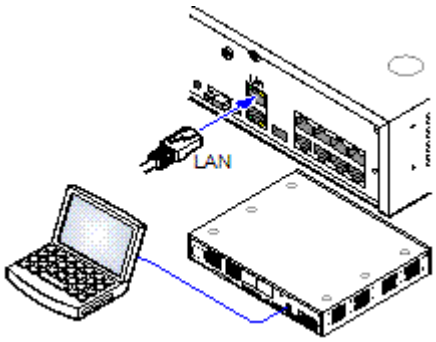
Página2726 de 3226.

- **System Status Application**
  Install the System Status Application application.

9. Ensure that at minimum **System Monitor** and **Manager** are selected. Click **Next >**.
10. Click **Install**. If the installation requires other components such as Windows .Net, follow the prompts to install those components.
11. If requested, reboot the PC.
12. Click **Finish**.

Página2727 de 3226.

3.3 Installer PC Connection



During installation it is recommended that the IP Office control unit is started without it being connected to any network. That ensures that the IP Office defaults to a known set of IP address settings.

If the IP Office is started connected to a network with a DHCP server, the programming PC will need to be connected to the same network as either a DHCP client or with an IP address valid for that network.

This section covers connecting your installation PC directly to the IP Office control unit.

Requirements

- ☐ **IP Office Administration PC**
  A Windows PC with the IP Office Administrator Application suite installed 64.
- ☐ **LAN Cable**

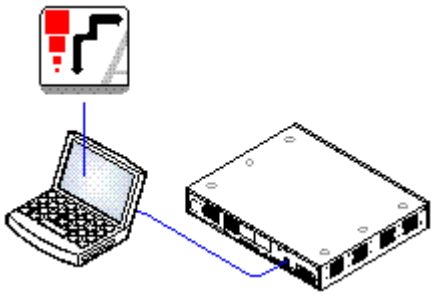
To connect directly to a defaulted IP Office system:

1. The default address for the IP Office control unit LAN port is 192.168.42.1/255.255.255.0. To directly connect a PC, change the TCP/IP properties for the PCs LAN port to the following:

Fixed IP address	192.168.42.203
Subnet mask	255.255.255.0
Default gateway	192.168.42.1.

   - While setting the PC to be a DHCP client could be used, this is not recommended for performing more advanced functions such as firmware upgrades.
2. Connect the LAN cable from the PCs LAN port to the LAN port on the IP Office control unit.
3. Check that the orange LED lamp on the IP Office LAN port is on. The green LED may also be flickering as it indicates traffic across the LAN connection.
4. To test the connection before running IP Office Manager or System Status Application:
   - Select **Start | Run** and enter ***cmd***.
   - In the command window that appears enter ping **192.168.42.1**. The results should show a number of ping replies from the IP Office. This confirms basic communication between the IP Office Manager PC and the IP Office.
   - If there are no ping replies enter **ipconfig**. The results should list the IP address settings of the IP Office Manager PC as required above. If they do enter **exit** and check the cable connection.
5. You can now start IP Office Manager 68, System Status 69 or System Monitor 70.

3.4 Starting IP Office Manager



IP Office Manager is used to access all parts of the IP Office configuration. IP Office Manager can also be used to upgrade the software files used by an IP Office system.

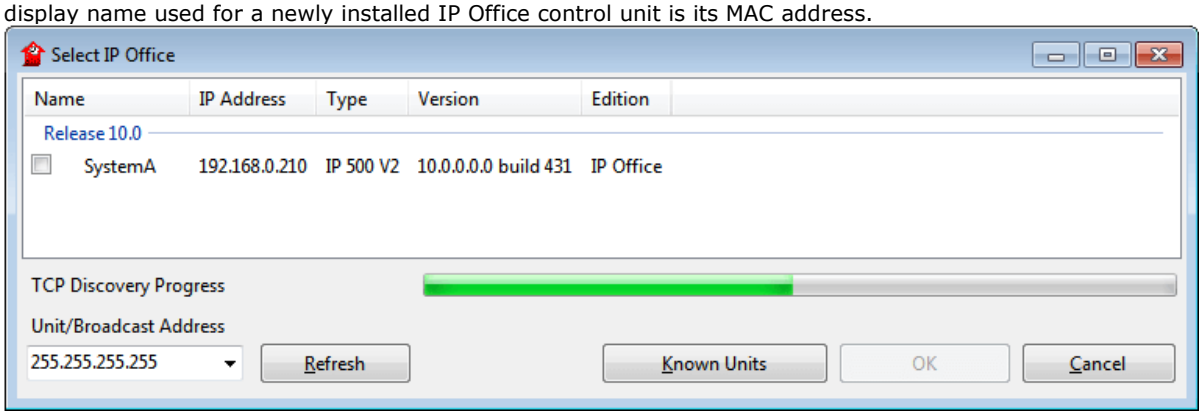
- **IP Office Manager Version**
  It is important to download and install the correct version of the IP Office administration suite including IP Office Manager.
  - For system installation, you should use the version of IP Office Manager that matches the IP Office release required on the system. This sets the version of software loaded when recreating the System SD card 75.
  - For system maintenance, the version of IP Office Manager used sets the version of software uploaded to a system when upgrading the system 180.
  - For system configuration IP Office Manager is backward compatible. IP Office Manager Version 11.0 is backwards compatible for configuring systems running software from IP Office Release 6.0 upwards. IP Office Manager cannot load the configuration of an IP Office system running a higher version of software.
  - **Admin Lite Not Supported**
    Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).

Requirements

- ☐ **IP Office Administration PC**
  A Windows PC with the IP Office Administrator Application suite installed 64.
- ☐ **LAN Cable**

To login to a system using IP Office Manager:

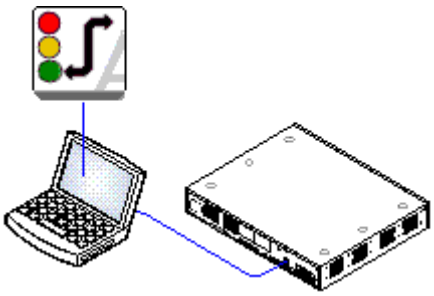
1. Select **Start | All Programs | IP Office | Manager**.
2. If the PC has firewall software installed, you may be prompted as to whether you want to allow this program to access the network. Select **Yes** or **OK**.
3. Select **File | Open Configuration** from the menu bar.
4. The **Select IP Office** window appears. After a few seconds it should list the IP Office control unit. The default display name used for a newly installed IP Office control unit is its MAC address.



   - If the system required was not found, the address used for the search can be changed. Enter or select the required address in the **Unit/Broadcast Address** field and then click **Refresh** to perform a new search.
5. Click the check the box next to the system and then click **OK**.
6. The name and password request is displayed. The name and password must match one of those setup through the the system's security settings.

Página2729 de 3226.

3.5 Starting System Status Application

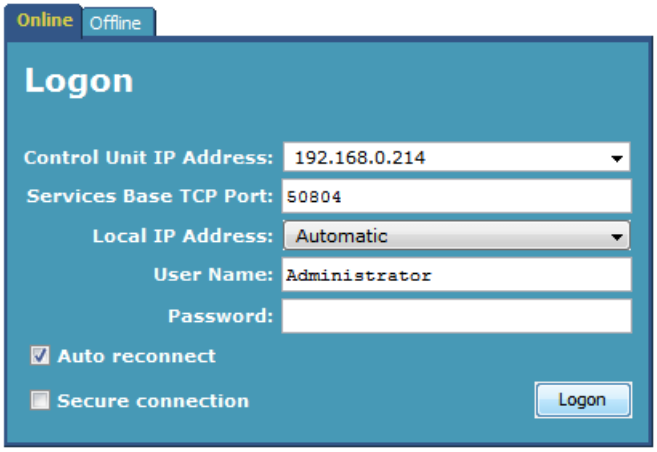


The System Status Application (SSA) is a reporting tool that provides a wide range of information about the current status of an IP Office system. Its can report the available resources and components within the system and details of calls in progress. Details of the number of alarms are recorded and the time date of the most recent alarms.

When required for diagnostics escalation, SSA is able to take a snap shot image of the IP Office system's status including a copy of its current configuration. Use of SSA requires an IP Office service user name and password that has been configured for System Status access in the IP Office's security settings.

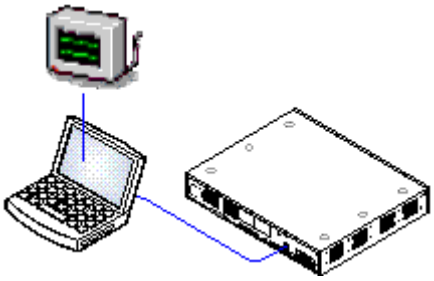
To start System Status:

1. There are several methods that can be used to start the System Status Application.
   - On a PC where System Status has been installed 64, select **Start | Programs | IP Office | System Status**.
   - If IP Office Manager is also installed on the PC and is running, select **File | Advanced | System Status**.
   - For IP500 V2 controls units, start a web browser and enter the IP address of the control unit. Select the link for the **System Status**.
   - If already running IP Office Web Manager, select **Monitoring** and click **System Status**.
2. Once System Status has started, it will request the details of the IP Office system to which you want it to connect.



   - **Control Unit IP Address**
     Enter the IP address of the IP Office control units LAN interface or use the drop down to select a previously used address.
   - **Services Base TCP Port**
     This should match the Services Base TCP Port setting of the IP Office system, set in that systems security settings. The default is 50804.
   - **Local IP Address**
     If the PC has more than one IP address assigned to its network card or multiple network cards, the address to use can be selected if necessary.
   - **User Name/Password**
     Enter a user name and password that has been provided for System Status usage. By default this is the same as the user name and password used with IP Office Manager. This must be the name of an IP Office service user name that has been configured for system status access in the IP Office's security settings.
   - **Auto Reconnect**
     If selected, System Status will attempt to reconnect using the same settings if connection to the IP Office is lost.
   - **Secure Connection**
     Use an encrypted TLS connection to the system. If selected and the system is not configured for secure access, System Status Application offers to reattempt connection using unsecure access instead.
3. Enter the required details for the IP Office and click **Logon**.

3.6 Starting System Monitor



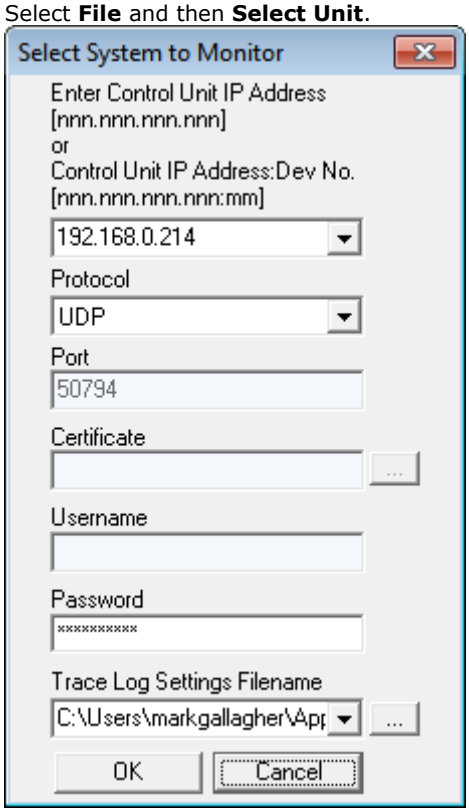
System Monitor is a tool that can show all activity on the IP Office system in great detail. As a consequence, interpretation of Monitor traces requires a high-level of data and telephony protocol knowledge. However, all IP Office installers and maintainers must understand how to run Monitor when necessary as Avaya may request copies of Monitor traces to resolve support issues.

Requirements

- ☐ **IP Office Administration PC**
  A Windows PC with the IP Office Administrator Application suite installed 64.
- ☐ **LAN Cable**

1. To start System Monitor:

1. Select **Start | Programs | IP Office | System Monitor**.
2. Select **File** and then **Select Unit**.



3. Enter the **IP Address** and **Password** of the system that you want to monitor.
   - **Protocol**
     The default **Protocol** , is ***UDP***. The application also supports TCP, HTTP and HTTPS connection. For full details refer to the manual "Using IP Office System Monitor".
   - **Which Password?**
     Using IP Office Manager, it is possible to set a specific **Monitor Password**. If the system does not have a **Monitor Password** set, System Monitor uses the system's **System Password**. The **Monitor Password** and **System Password** are set within a system's security configuration settings.
4. If you want System Monitor to start with a previously saved set of trace options, use the **Trace Log Settings Filename** browse button to select the trace options settings file.
5. Click **OK**.

3.7 Starting IP Office Web Manager

Web browser access to the system can be used to run IP Office Web Manager. Enter the system's IP address and then select the **IP Office Web Manager** link. For full details, refer to the IP Office Web Manager Manual.

To use IP Office Web Manager requires the application files to be present on the system's SD card. This is done by selecting the option to include the web manager files when recreating the SD card 75.

Avaya supports the following browsers for IP Office Web Manager:

- **Microsoft Internet Explorer 10** and **11**.
- **Microsoft Edge**
- **Mozilla Firefox**
- **Google Chrome**
- **Safari**

To login to a system using IP Office Web Manager:

1. Enter the IP address of the IP Office system. From the menu that appears, click on **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
2. The login menu for IP Office Web Manager appears.

3. Enter the name and password for system administration. The default name and password are both ***Administrator***.
   - **Offline Mode**
     Some configuration changes can only be applied to a system using a reboot, for example changing line settings. To edit those settings you need to select **Offline Mode**. In that mode, the top of the browser windows displays a **Save to IP Office** link which, when clicked, displays a menu for the system reboot.
     - You can also switch to offline mode after having logged in by clicking on the and selecting **Offline Mode**.
4. Click **Login**.
   a. You are prompted to change any default password.
   b. For a new system, the initial configuration menu 103 appears.

Chapter 4.

Preparing the System SD Card

4. Preparing the System SD Card

New IP500 V2 control units are supplied with no installed firmware or configuration. When first powered up, the control unit loads and installs the necessary firmware from the Avaya **System SD** 208 card installed in the control unit. It then creates a default configuration matching the physical cards already installed in the control unit and any external expansion modules already attached to it.

You can perform a number of additional actions prior to installing the System SD card in order to pre-configure the system. These can greatly speed up the physical installation at the customer site as they can all be done in advance.

- **Upgrade the Card Firmware** 75
- **Add a Configuration File** 78
- **Add a License File** 78
- **Adding Security Certificates** 78
- **Add a 9600 Screen Saver Image File** 79
- **Add Music on Hold Files** 79

Additional actions that can be performed on SD cards are detailed in the SD Card Management 142 section.

Página2735 de 3226.

4.1 Upgrade the Card Firmware

You can use IP Office Manager to update the set of files on an System SD card to match those expected for the particular IP Office release. This can be used to upgrade the card from an existing system or to prepare the card for a new system.

IP Office Manager updates the card with the binary firmware files for the control unit, external expansion modules and phones. It also includes the prompt files for embedded voicemail operation and an option for the web manager application files.

Existing files such as the system configuration, PLDS license file and embedded voicemail messages and greetings are retained.

- For the card to be used in an control unit's **System SD** card slot it must be Avaya System SD card. The card must be correctly formatted (that can be done using IP Office Manager), however a reformat of an existing working card is not necessary before using recreate to update the card contents.
- The source for the files copied to the SD card are the sub-folders of the ***\Memory Cards*** folder under Manager's applications **Working Directory** (normally ***C:\Program Files(x86)\Avaya\IP Office\Manager***). However, if the **Working Directory** is changed to a location without an appropriate set of ***\Memory Cards*** sub-folders, the required set of files will not be copied onto the SD card.
    - **! WARNING: Installing PCS14 and earlier control units**
      PCS[296] 14 or lower units must first install Release 8.1(65) (or higher 8.1) or any Release 9.0 and then upgrade to Release 9.1. Care should be taken to ensure that no calls are made before the upgrade to Release 10.0, otherwise the system will require an 10.0 upgrade license despite being "new". The PCS of the control unit is printed on the label on the back of the control unit.

Setting the Initial System Software Level

When the control unit makes its first call, the version of software it is running is written to a permanent record on the control unit. This becomes the base level of the control unit when considering the future requirements for upgrade licenses, etc. Therefore, for a new system it is important that you upgrade the System SD card to the required software version before starting the system.

Determining the System SD card software level

On the SD card, in the ***system/primary*** folder, locate and open the ***filelist.txt*** file. The header section at the start of the file ends with the version of the set of files previously copied onto the card. The remainder of the file lists the actual files.

To upgrade/recreate a System SD card

1. Once started do not interrupt this process, for example by removing the SD card. This process takes approximately 20 minutes.
2. Insert the SD card into a card reader on the IP Office Manager PC.
3. Using IP Office Manager, select **File | Advanced | Recreate IP Office SD Card**.
4. Select **IP Office A-Law** or **IP Office U-Law**. This selection affects how the IP Office systems operates when defaulted with this card present in its **System SD** card slot.
5. Browse to the card location and click **OK**.
6. IP Office Manager will prompt whether you want to include Avaya IP Office Web Manager files as part of the recreate process. Those files are necessary if you want to run IP Office Web Manager[71] to manage the IP Office system into which the card is loaded or if you want to use on-boarding[138].
7. IP Office Manager will start creating folders on the SD card and copying the required files into those folders. This process will take approximately 20 minutes.
8. Do not remove the SD card during the process. Wait until the IP Office Manager displays a message.

4.2 Creating an Offline Configuration File

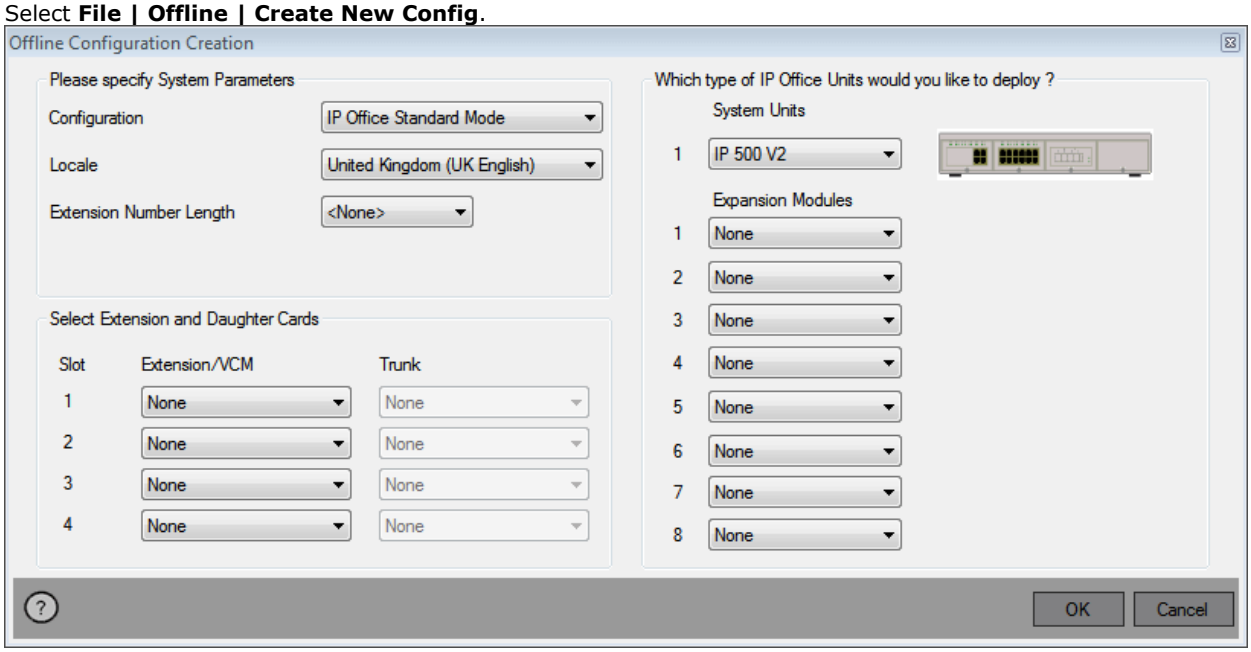
IP Office Manager can be used to create a new configuration without connecting to an IP Office system. During the process, you can specify the locale of the system, what type of trunk cards it uses and what type of control unit and expansion modules to include.

This allows the creation of a configuration prior to installation of system. The configuration file can then be placed onto the System SD card before it is installed into the system. Otherwise the configuration can be uploaded to the system after initial installation of the system.

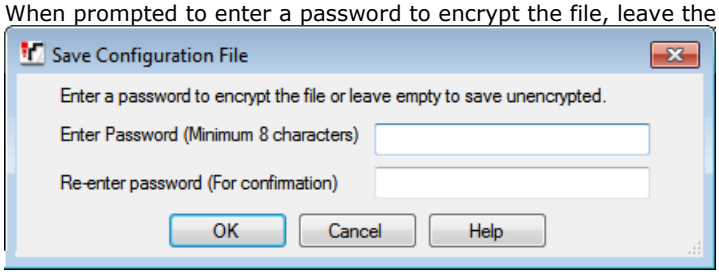
- The configuration created must match the physical equipment in the IP Office system onto which it is loaded. Doing otherwise may cause the IP Office system to reset and experience other problems.

To create an offline configuration file

1. Start IP Office Manager with no configuration loaded into IP Office Manager
2. Select **File | Offline | Create New Config**.



3. Select the type of configuration that you want to create. The equipment and settings are restricted to those supported in the selected mode.
4. When completed click **OK**.
5. IP Office Manager creates and loads the configuration.
6. Edit the configuration to match the customer requirements. This can include importing information from preprepared CSV files 77.
   - Note that since this configuration is being done offline and without licensing, you can configure features that may become unsupported once the configuration is loaded into the live system.
7. When completed, select **File | Save Configuration As**.
8. When prompted to enter a password to encrypt the file, leave the fields blank and click **OK**.



4.3 Importing and Exporting Settings

IP Office Manager can import configuration settings created elsewhere. This can be useful when setting up a new system or sharing common settings such as a directory between systems. Settings are imported and exported in two formats:

- **Comma Separated Variable Text Files (.csv)**
  These are plain text files. These files can be created and edited using programs such as WordPad or Excel. The format is CSV using commas as field separator, no text delimiters and no header row. The simplest way to check the required format for a CSV file prior to import, is to export and study the settings from an existing system.

File Name	Fields in Order	Notes
Directory	*Name, Number.*	
HuntGroup	*Name, Extension, Group, Hunt, Rotary, Idle, Queuing On, Voicemail On, Broadcast, Voicemail Email.*	Apart from Name, Extension and Voicemail Email, the fields use a 1 or 0 value for on or off.
License	*License, License Key*	The License field is for information only and is ignored during import.
ShortCode	*Code, Telephone Number, Feature.*	
User	*Name, Extension, User Restriction/Rights, Voicemail Email.*	
Configuration	The format of this CSV is too complex to be described. It is a full export of all the IP Office system's configuration settings. This file format should only be used for export and import between systems and not for any offline editing.	

- **UTF-8 Character Encoding**
  IP Office Manager imports and exports CSV files using UTF-8 character encoding which uses a double byte to support characters with diacritic marks such as ä. Other applications, such as Excel, may, depending on the user PC settings, use different encoding which will cause such characters to be removed or corrupted. Care should be taken to ensure that any tool used to create or edit the CSV supports all the characters expected and uses UTF-8 format.
  - **Importing into Manager from Excel**
    From Excel save the file as a .csv. This file will use ANSI character encoding. Open the file in Notepad and use the **Save As** option to rename the file and select UTF-8 encoding. Import the UTF-8 version of the file into IP Office Manager.
  - **Exporting from IP Office Manager into Excel**
    Do not double-click on the file exported from IP Office Manager. Start Excel and use **File | Open** to select the file. Excel will recognize that the file uses UTF-8 encoding and will start its text file importation wizard. Follow the wizard instructions and select comma as the field delimiter.

Exporting Settings

1. Within IP Office Manager load the IP Office configuration. Select **File | Import/Export...** from the menu bar.
2. Select **Export**.
3. Select the type of file. The list of exportable entry types will change to match the file type.
4. Select the types of items that should be exported.
5. Use the **Save In** path to select the location for the exported files. The default location used is sub-directory of the IP Office Manager application directory based on system name of the currently loaded IP Office system.
6. Click **OK**.

Importing Settings

Importing settings will overwrite any existing entries that match an entry being imported.

1. Within IP Office Manager select **File | Import/Export...** from the menu bar.
2. Select **Import**.
3. Select the type of file. The list of items will change to match the type of file selected and whether a matching file or files is found in the current file path.
4. Use **Look In** to adjust the file path. The default location used is sub-directory of the IP Office Manager application directory based on system name of the currently loaded IP Office system.
5. Select the types of items that should be imported.
6. Click **OK**.

4.4 Adding a Pre-Built Configuration File

IP Office Manager can be used to create an offline configuration file 76. The pre-created configuration file can be placed on the system's System SD card prior to installation. That file is then loaded when the new IP Office system is started.

- The configuration created must match the physical equipment in the IP Office system onto which it is loaded. Doing otherwise may cause the IP Office system to reset and experience other problems.

To load a pre-built offline configuration onto a System SD card

1. Using IP Office, create an offline configuration that matches the customer requirements and the equipment that will be installed in the IP Office.
2. Rename the configuration file ***config.cfg***.
3. Using a card reader, copy the file into the ***/system/primary*** folder on the System SD memory card.

4.5 Adding a License File

The XML file containing the systems PLDS licenses is stored on the System SD card. This file can be added to the system SD card prior to installation. The license are then automatically imported into the system configuration when the system is started.

- The PLDS host ID used for the license file must match that shown by the 12 digit **PLDS ID** printed on the SD card label. Older cards have an 10 digit feature key serial number shown by **FK** or **FK SN**. For those cards add the prefix ***11*** to obtain the card's PLDS ID.

Minimum License Requirements

For IP Office Essential Edition, the system requires an **Essential Edition** system license for the specific IP Office release you want it to run.

To load a License File onto a system SD card

1. Rename the supplied .XML license file to ***PLDSkeys.xml***.
2. Using a card reader, copy the file into the ***/system/primary*** folder on the System SD memory card.

4.6 Adding Security Certificates

The IP Office system can use security certificates to validate the connections between itself, applications and other IP Office systems. Certificates can also be used for IP telephony communications.

Certificates can be placed onto the System SD card. Those certificates are then loaded into the system's certificate store when the system is started. The certificate file name extension must indicate the type of encoding; PEM encoded files should end with ***.pem***, DER encoded files should end with ***.der***.

To load a certificate to add:

1. Using a card reader, copy the file into the ***/system/primary/certificates/tcs/add*** folder on the System SD memory card.

To load a certificate to remove:

The mechanism above can adapted to also remove an existing certificate.

1. Using a card reader, copy the file into the ***/system/primary/certificates/tcs/remove*** folder on the System SD memory card. If the matching certificate already exists in the system certificate store, that certificate is removed.

Página2739 de 3226.

4.7 Adding a 9600 Series Screen Saver File

When idle, 9600 Series phones can timeout to displaying a screen saver image. Various ***.jpg*** files are present in the cards ***/system/primary*** folder by default.

You can replace these files with your own branded files. The files should be smaller than the screen size on 9600 Series phones in order to then be moved around the screen.

Phone	Maximum Size	Phone	Maximum Size	Phone	Maximum Size
9611	160x160	**9621G**	320x160	**9650**	320x240
9620	320x160	**9630**	320x240	**9650C**	320x240
9620L	320x160	**9640**	320x240		
9620C	320x160	**9641G**	320x240		

- Color Displays: Color depth is 16 bit. A separate color image will look best.
- Non-Color Displays: Best results are achieved with a single grayscale logo image. 2 levels of grayscale are also supported.
- To invoke transparent backgrounds with logos, use a background color of 0,255,0 (brightest possible green).

4.8 Adding Music on Hold Files

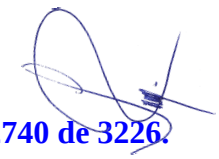
By default the IP Office will use internal music on hold by uploading a music file from the IP Office Manager PC. For IP500 V2 systems, you can load a file onto the System SD card prior to installing it in the IP Office.

The file must be of the following format and must be called ***holdmusic.wav***.

Property	Value	Property	Value
File Type	WAV	**Audio Sample Rate**	8kHz
Bit Rate	128kbps	**Audio Format**	PCM
Audio sample size	16 bit	**Length**	Up to 90 seconds.
Channels	1 (mono)		

To loading a music on hold file onto a System SD card

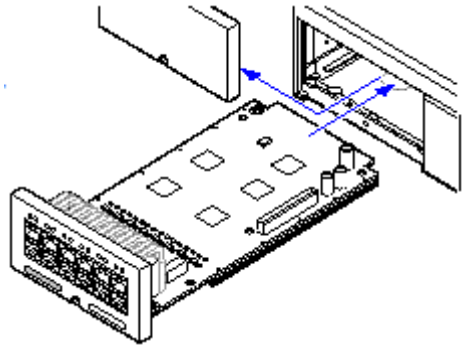
1. Rename the music file ***holdmusic.wav***.
2. Using a card reader, copy the file into the ***/system/primary*** folder on the System SD memory card.
3. If the IP Office is or will be configured for additional hold music files (up to 3 additional files), copy those files to the same location. The name of the additional files must match those specified in the IP Office system's configuration.



Chapter 5.

Installing the Control Unit Cards

5. Installing the Control Unit Cards



The IP500 base cards and trunk daughter cards should be fitted before power is applied to the control unit. Ensure that cards are inserted in the order that matches the planned or pre-built configuration.

This process has 2 stages:

1. Fit the IP500 trunk daughter cards onto the IP500 base cards.83
2. Insert the IP500 Base Cards into the Control Unit.84

⚠ Warnings

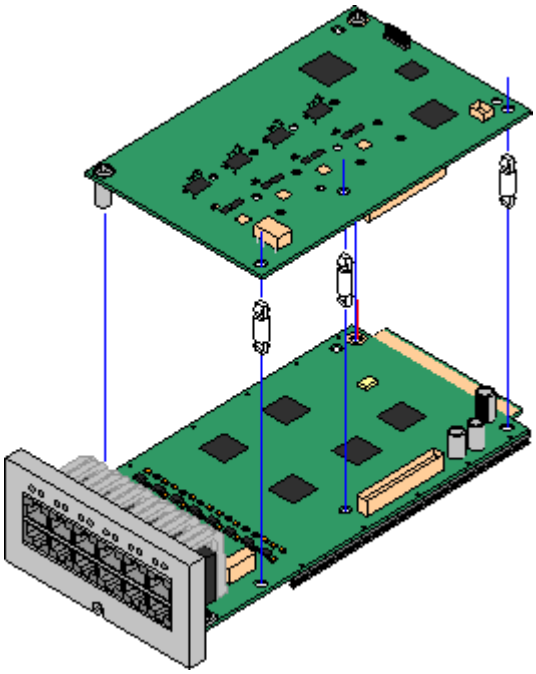
- Correct anti-static protection steps should be taken before handling circuit boards.
- **! IMPORTANT:**
  You Must Switch Off the Control Unit Before Adding, Removing or Swapping Components
  Base cards, trunk cards and external expansions modules must only be removed and added to an IP Office system when that system is switched off163. Failure to do so will result in the new component not loading the correct firmware and not operating or not operating correctly. This applies even when swapping like for like components.

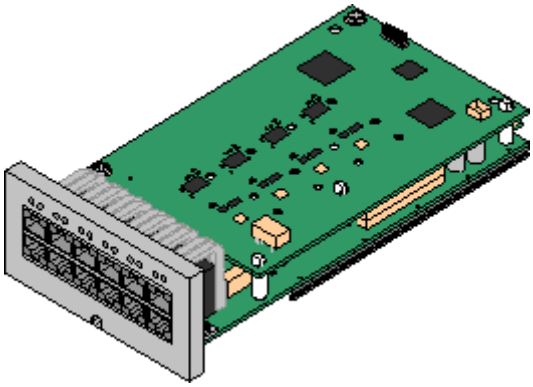
General Notes

- Cards can be fitted in any order into any available slots. The only exception is the IP500 4-Port Expansion card which can only be installed in right hand slot 4.
- It is recommended that cards are fitted from left to right.
- There are restrictions to the number of supported cards of some types. When such a limit is exceed, the right-most card of that type will not function.
- Ensure that you use the labels supplied to identify the card fitted into the control unit.

5.1 Fitting IP500 Daughter Cards

IP500 trunk daughter cards can be fitted to any IP500 base card except the Unified Communications Module and 4-Port Expansion card. For IP500 Combination cards, the trunk daughter card is pre-installed and cannot be changed.





⚠ Warnings

- Correct anti-static protection steps should be taken while handling circuit boards.

Parts and Equipment Required

1. ☐ **IP500 Base Card**
2. ☐ **IP500 Trunk Daughter Card**
3. ☐ **3 Stand Off Pillars**
   These are supplied with the trunk daughter card.

Tools Required

1. ☐ 5mm Flat-blade screwdriver.
2. ☐ Anti-static wrist strap and ground point.

Procedure: Installing a Trunk Daughter Card

1. Check that correct cards have been supplied.
2. Ensure that you are wearing an anti-static wrist strap connected to a suitable ground point.
3. On the base card identify the position of 3 holes for the plastic pillars for the IP500 card. These are along the same edge as the card connector.
4. Fit the stand off pillars to the IP500 base card.
5. If there is a clip-on metal shield over the connector block on the base card, remove it.
6. Using minimal force and checking that the pins are correctly located, push the IP500 trunk card onto its connector block and the stand off pillars.
7. Check that the card connector has snapped into position.
8. Using the washers and screws provided, secure the metal stand off pillars to the base card.
9. A set of labels are supplied with the trunk daughter card. Fit the appropriate label to the front of the base card.

5.2 Inserting IP500 Base Cards

Having prepared each IP500 base card by adding any trunk daughter card[83], the base card can be inserted into the control unit.

⚠ Warnings

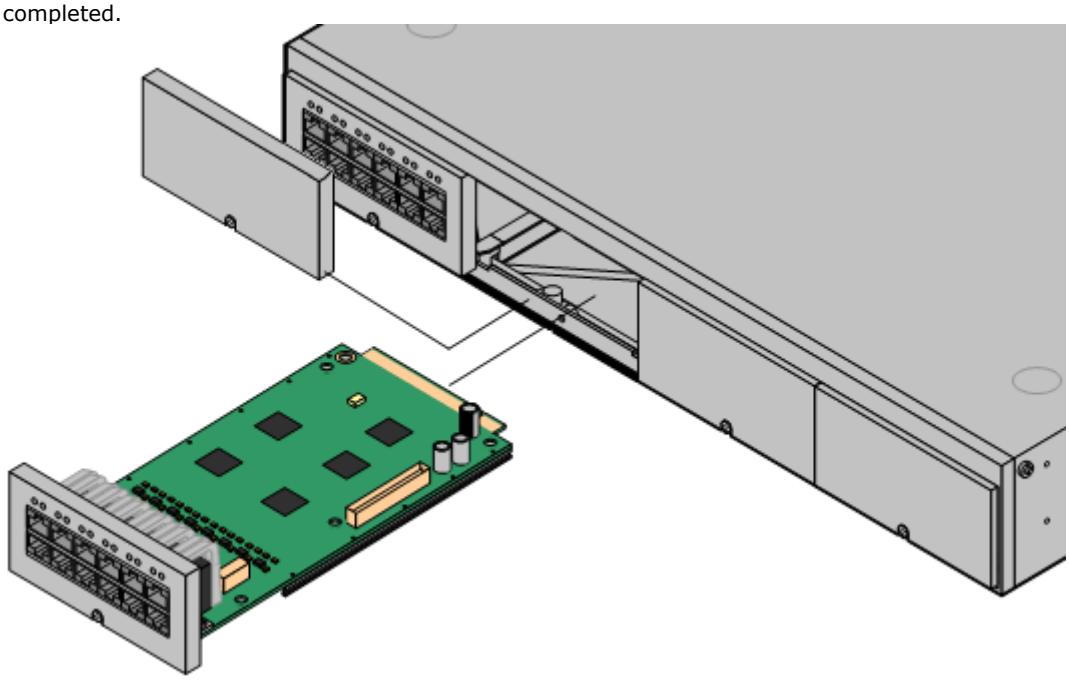
- Correct anti-static protection steps should be taken while handling circuit boards.
- **! IMPORTANT:**
  You Must Switch Off the Control Unit Before Adding, Removing or Swapping Components
  Base cards, trunk cards and external expansions modules must only be removed and added to an IP Office system when that system is switched off[163]. Failure to do so will result in the new component not loading the correct firmware and not operating or not operating correctly. This applies even when swapping like for like components.

Tools Required

- ☐ 5mm Flat-blade screwdriver.
- ☐ Anti-static wrist strap and ground point.

Installing an IP500 Card

1. Check that there is no power to the control unit.
2. Using a flat-bladed screwdriver, remove the cover from the slot on the front of the control unit that will be used for each card being installed. This cover is no longer required but should be retained until installation has been completed.



3. Allowing the card to rest against the bottom of the slot, begin sliding it into the control unit. When half inserted, check that the card rails have engaged with the slot edges by trying to gently rotate it. If the card rotates remove it and begin inserting it again.
4. The card should slide in freely until almost fully inserted. At this point apply pressure at the base of the front of the card to complete insertion.
5. Using a flat-bladed screwdriver secure the card.

Chapter 6.

Installing the Physical System

6. Installing the Physical System

Having prepared for installation, this section covers the basic on-site installation.

Summary

1. **Prepare for installation** 50
   a. **Environmental Requirements** 51
      Check that the installation area meets the system environmental requirements.
   b. **Space Requirements** 53
      Check that the installation area meets the system space requirements.
   c. **Tools and Parts Required** 59
      Check that you have the tools and additional parts required.
   d. **Documentation** 60
      Ensure that you have obtained and read all the relevant documentation.
   e. **Unpacking** 60
      Check that all the required equipment has been delivered and that there is no damage.
2. **Admin Software Installation** 62
   For system installation you need a PC with the IP Office administrator software installed. This must include a copy of IP Office Manager that matches the IP Office software level required.
   a. **Downloading the Software** 63
   b. **Installing the Administrator Applications** 64
3. **Preparing the System SD card** 74
   Upgrade the System SD card to the required releaser of IP Office software. In addition add any other files available such as the license file, pre-built configuration, music-on-hold file.
   - **! WARNING: Installing PCS14 and earlier control units**
     PCS 296 14 or lower units must first install Release 8.1(65) (or higher 8.1) or any Release 9.0 and then upgrade to Release 9.1. Care should be taken to ensure that no calls are made before the upgrade to Release 10.0, otherwise the system will require an 10.0 upgrade license despite being "new". The PCS of the control unit is printed on the label on the back of the control unit.
4. **Install the control unit cards** 82
   Attach any trunk daughter cards to their IP500 base cards and insert the base cards into the control unit.
5. **Install the system** 86
   a. **Wall Mounting** 87
      If wall mounting, attach the brackets and fit the unit to the wall.
   b. **Rack Mounting** 89
      If rack mounting, attach the brackets and fit the control unit into the rack.
   c. **Connect the External Expansion Modules** 91
      Connect the external expansions modules to the control unit.
   d. **Ground the system** 93
      Attach required ground cables to the control unit and external expansion modules.
   e. **Starting the System** 94
      Insert the System SD card and power up the system.
   f. **Connecting Phones** 97
      Connect the Avaya digital phones.
6. **Initial Configuration**
   Once the physical system is started, it can be configured. This can be done using either IP Office Manager 100 or IP Office Web Manager 114 .

6.1 Wall Mounting

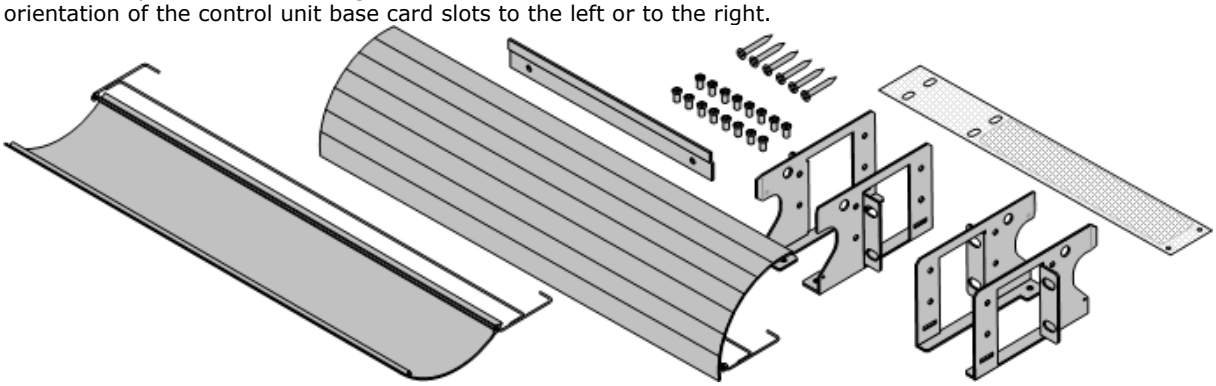
IP500 V2 control units and IP500 external expansion modules can be wall or rack mounted. To do this, a wall mounting kit is required in addition to suitable wall fixings.

In addition to the existing environmental requirements[51] for an IP Office system, the following additional requirements apply when wall mounting a unit:

- The wall surface must be vertical, flat and vibration free. Attachment to temporary walls is not supported.
- Only the screws provided with the mounting kit should be used to attach the brackets to the control unit or expansion modules.
- The installation must be done by a service person.
- Ensure that the system has been shut down and power has been removed from all the units. Shut down the system using a shutdown command and then remove the power. Do not simply remove the power.
- A suitable plywood mounting surface of at least 1m x 1m x 19mm (39" x 39" x 0.75") is required. If an expansion box is being mounted as well a plywood mounting surface of at least 1.2m x 1.2m x 19mm (48" x 48" x 0.75") is required.
- A minimum of 6 x 45mm long 5mm/6mm (1.75" #10/#12) pan head screws must be used to secure the plywood to the wall studs.
- The supplied 20mm long 4mm (#8 ¾") wood screws must be used to secure the brackets to the plywood mounting surface

The following kit is currently available:

- **IPO IP500 WALL MNTG KIT V3** *(SAP Code 700503160)*
  This kit can be used for wall and rack mounting of IP500 V2 control units and IP500 external expansion modules. The kit incorporates cable routing at the front and rear of the unit. For wall mounted control units, it allows orientation of the control unit base card slots to the left or to the right.



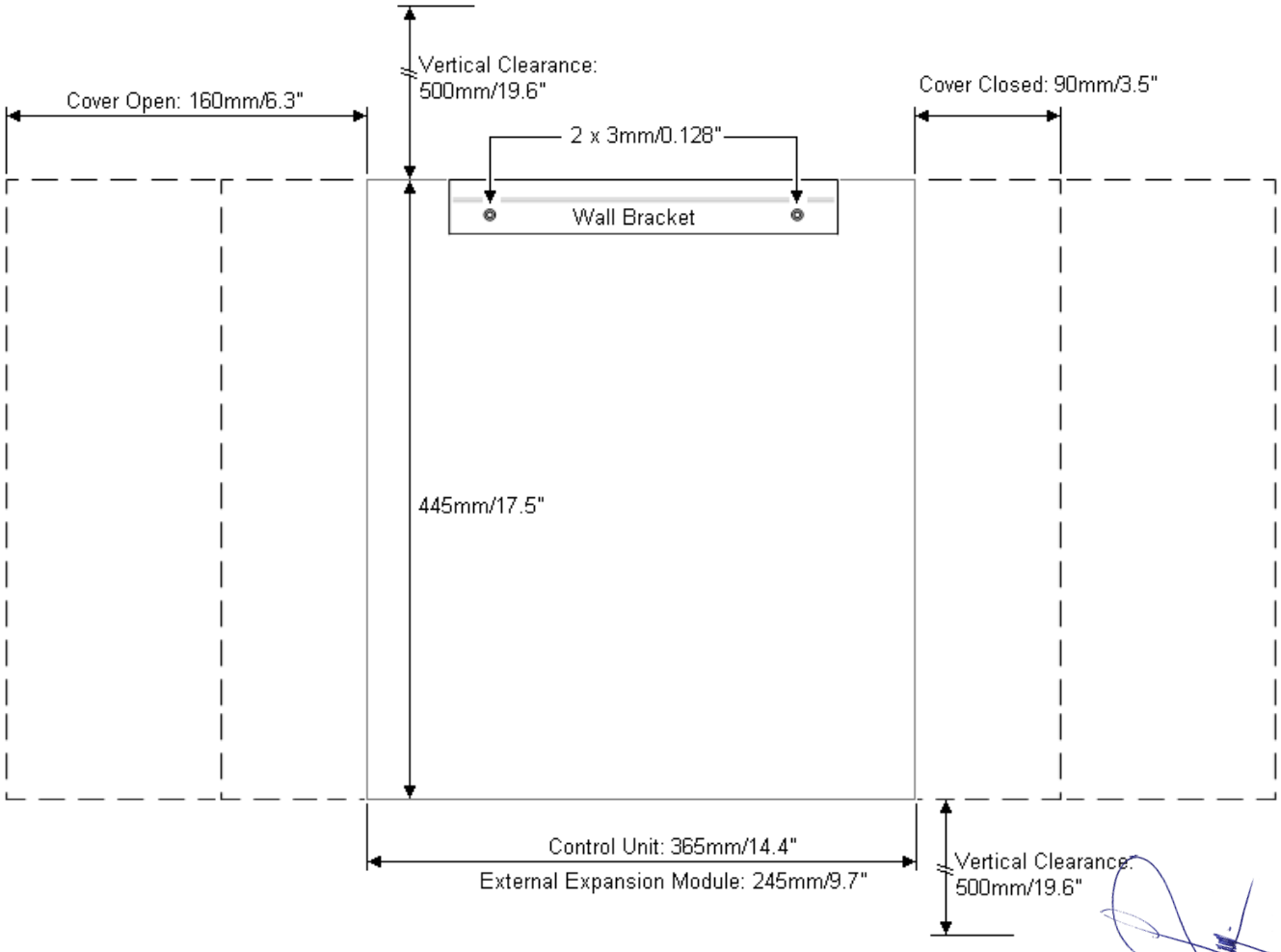
6.1.1 Wall Mounting Kit V3

These notes relate to the **IPO IP500 WALL MNTG KIT V3** *(SAP 700503160)*. This kit can be used to wall or rack mount IP500 V2 control units and IP500 external expansion modules.

The kits includes all components necessary for wall mounting onto a plywood surface. The use of the cable covers is optional.

In addition to the existing environmental requirements 51 for an IP Office system, the following additional requirements apply when wall mounting a unit:

- The wall surface must be vertical, flat and vibration free. Attachment to temporary walls is not supported.
- Only the screws provided with the mounting kit should be used to attach the brackets to the control unit or expansion modules.
- The installation must be done by a service person.
- Ensure that the system has been shut down and power has been removed from all the units. Shut down the system using a shutdown command and then remove the power. Do not simply remove the power.
- A suitable plywood mounting surface of at least 1m x 1m x 19mm (39" x 39" x 0.75") is required. If an expansion box is being mounted as well a plywood mounting surface of at least 1.2m x 1.2m x 19mm (48" x 48" x 0.75") is required.
- A minimum of 6 x 45mm long 5mm/6mm (1.75" #10/#12) pan head screws must be used to secure the plywood to the wall studs.
- The supplied 20mm long 4mm (#8 ¾") wood screws must be used to secure the brackets to the plywood mounting surface
- The installation must be done by a service person only.
- For control units, the mesh flame screen must be installed on the bottom edge of the control unit before mounting. The flame screen attaches to the outside of the control unit.
- Ensure that the system has been shutdown and power has been removed from all the units. Shutdown the system using a shutdown command and then remove power. Do not simply remove the power.
- Full installation instructions are included with the kit.



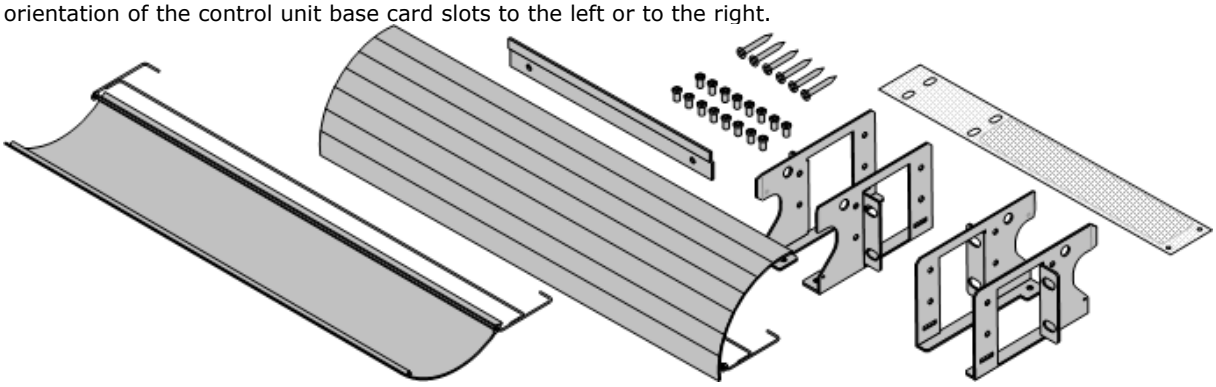
Página2749 de 3226.

6.2 Rack Mounting

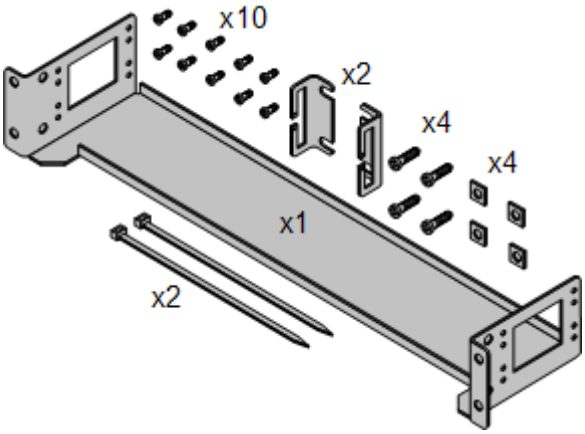
All IP Office control units and external expansion modules can be rack mounted into standard 19" rack systems. Each unit requires a 2U slot space within the rack. Rack mounting requires a kit for each control unit and external expansion module.

Where systems are being rack mounted, the effect of conditions within the rack cabinet must be considered. For example, the rack temperature may be above the room temperature and airflow within the rack is restricted. The environmental requirements 51 for the individual IP Office units are still applicable inside the rack cabinet.

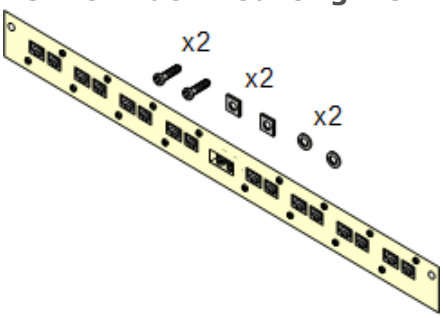
- **IPO IP500 WALL MNTG KIT V3** *(SAP Code 700503160)*
  This kit can be used for wall and rack mounting of IP500 V2 control units and IP500 external expansion modules. The kit incorporates cable routing at the front and rear of the unit. For wall mounted control units, it allows orientation of the control unit base card slots to the left or to the right.



- **IPO IP500 RACK MNTG KIT** *(SAP Code 700429202)*
  This kit contains all the components required for the rack mounting of a single IP500 V2 control unit or IP500 external expansion module. This includes screws for fixing of the brackets to the module, bolts for securing the module in the rack and cable tidy brackets..



Barrier Box Rack Mounting Kit



- **Barrier Box Rack Mounting Kit** *(SAP 700293905)*
  Barrier boxes must be used for out-of-building analog phone extensions 36. This bracket allows up to 8 IP Office barrier boxes to be rack mounted and simplifies the number of connections to the protective ground point in the rack. This kit must be used when more than 3 barrier boxes are in use and supports a maximum of 16 barrier boxes for a single external expansion module.

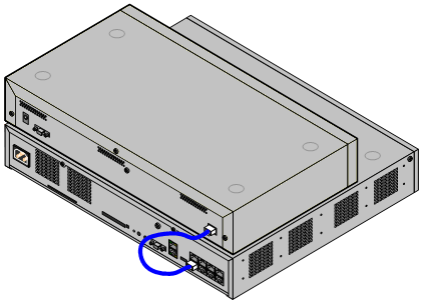
Página2750 de 3226.

Environmental Requirements

In addition to the existing environmental requirements[51] for an IP Office system, the following additional factors must be considered when rack mounting a unit:

1. Rack Positioning - Ensure compliance with the rack manufacturers safety instructions. For example check that the rack legs have been lowered and fixing brackets have been used to stop toppling.
2. Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
   - ☐ Operating Temperature: 5°C (40°F) to 40°C (104°F).
   - ☐ Operating Humidity: 10% to 95% non-condensing.
3. Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised. Proper ventilation must be maintained. The side ventilation slots on the IP500 control unit should not be covered or blocked.
4. Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
5. Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
6. Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
7. ⚠ Only the screws provided with the mounting kit should used to attach the brackets to the control unit.

6.3 Connecting External Expansion Modules



Any external expansion modules should be connected to the control unit before power is applied to the control unit. Ensure that modules are attached in the order that matches the planned or pre-built configuration.

External expansion modules connect to the IP Office control unit using an expansion interconnect cable. Each module is supplied with an expansion connect cable and a power supply unit 30. An appropriate locale specific power cord 31 for the power supply unit must be ordered separately.

- Each external expansion module is supplied with a blue 1 meter (3'3'') expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on an IP500 4-Port Expansion card, a yellow 2 meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. 4 Yellow cables are supplied with the IP500 4-Port Expansion card.
- **! IMPORTANT:**
  You Must Switch Off the Control Unit Before Adding, Removing or Swapping Components
  Base cards, trunk cards and external expansions modules must only be removed and added to an IP Office system when that system is switched off 163. Failure to do so will result in the new component not loading the correct firmware and not operating or not operating correctly. This applies even when swapping like for like components.

Installation Requirements

- ☐ Installation space either on or under the existing IP Office control unit. See Rack Space Requirements 57 for the positioning of multiple stacked modules.
- ☐ Switched power outlet socket.
  The power outlet used must include a switch and in cases where the power cord 31 includes an earth lead, that outlet must have a protective earth connection.
- **! Important: External Expansion Module Power**
  In order to be detected and operated correctly, external expansion modules must start before the IP Office control unit. Normally this achieved by connected all expansion modules to the same power strip as the control unit. The control unit applies a short delay to its own start-up process to ensure that expansion modules powered on at the same time as it are detected.
- ☐ Available EXPANSION port on the control unit.
- ☐ Grounding Requirements
  - ☐ **Functional Grounding**
    Connection of a functional earth 35 is:
    - ☐ Recommend for all modules.
    - ☐ Connection of a functional ground is mandatory for Analog Trunk modules.
  - ☐ **Protective Grounding**
    Connections of a protective ground via surge protection equipment 36 is:
    - ☐ Mandatory for Analog trunk modules in the Republic of South Africa.
    - ☐ Mandatory for Digital Station and Phone modules connected to out of building extensions.
    - ☐ Mandatory for Digital Station V2 and Phone V2 modules.

Tools Required

- ☐ IP Office Manager PC.
- ☐ Tools for rack mounting 89 (optional).

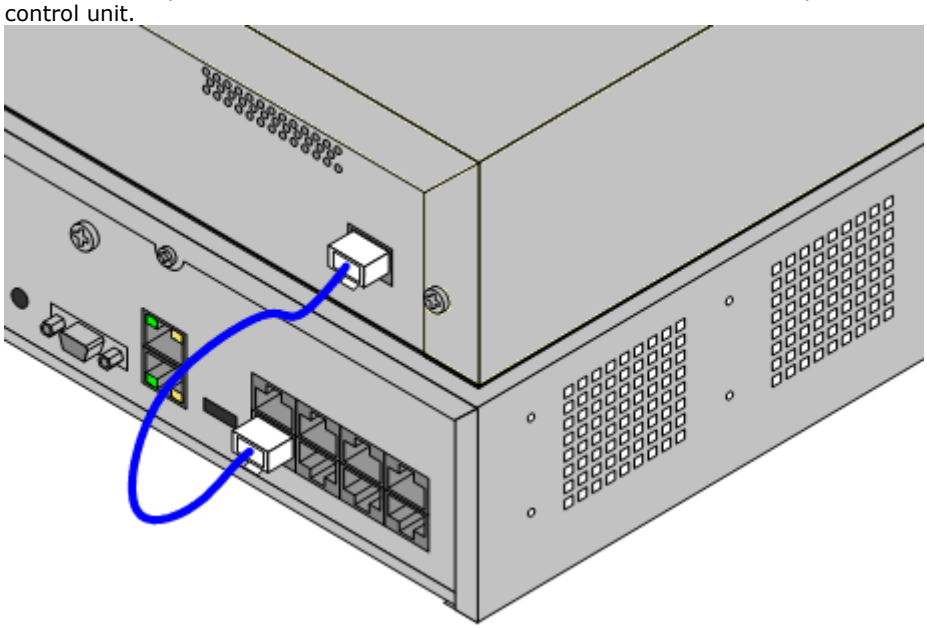
Parts and Equipment Required

- ☐ **External Expansion Module**.
  Each module is supplied with a suitable external power supply unit and a 1m blue interconnect cable. 2m Yellow interconnect cables are supplied with the IP500 4-Port Expansion card and should only be used with that card.
- ☐ Power cord for the power supply unit 31.
- ☐ Rack mounting kit 37 *(optional)*.
- ☐ Wall mounting kit 87 *(optional - IP500 external expansion modules only)*.
- ☐ Cable labeling tags.

Página2752 de 3226.

Procedure

1. External expansion modules should not be attached to a control unit that has power. If adding a new module to an existing system, shutdown the system[163].
2. If the IP Office system is being installed in a rack, attach the rack mounting kit[89] to the expansion module.
3. Attach the external expansion module's power supply but do not switch power on.
4. Connect the expansion interconnect cable from the module's EXPANSION port to the EXPANSION port on the control unit.



- **Note**
  It is recommended to connect modules from port 1 upwards, using each port in sequence.

5. Make careful note of the port used and include this detail on the cable label and any other system records.
6. Attach any other external expansion modules being added.
7. You can now attach the grounding cabling[93] for the external expansion modules.

a. Once the expansion modules are connected and grounded you can start the system[94]. Ensure that the external expansion module's are started before the control unit.

6.4 Grounding

Use of ground connections reduces the likelihood of problems in most telephony and data systems. This is especially important in buildings where multiple items of equipment are interconnected using long cable runs, for example phone and data networks.

All IP Office control units and external expansion modules must be connected to a functional ground. Where the unit is connected to a power outlet using a power cord with an earth lead, the power outlet must be connected to a protective earth.

In some cases, such as ground start trunks, in addition to being a protective measure this is a functional requirement for the equipment to operate. In other cases it may be a locale regulatory requirement and or a necessary protective step, for example areas of high lightning risk.

- **WARNING**
  During installation do not assume that ground points are correctly connected to ground. Test ground points before relying on them to ground connected equipment.
- **Additional protective equipment**
  In addition to grounding, additional protective equipment will be required in the following situations.
  - On any Digital Station or Phones external expansion module connected to an extension located in another building. Refer to "Out of Building Telephone Installations 36".
  - In the Republic of South Africa, on all Analog Trunk external expansion modules (ATM16) and on any control units containing an analog trunk cards (ATM4/ATM4U).

Tools Required

- ☐ M4 Cross-Head Screwdriver.
- ☐ Tools suitable for crimping a cable spade.

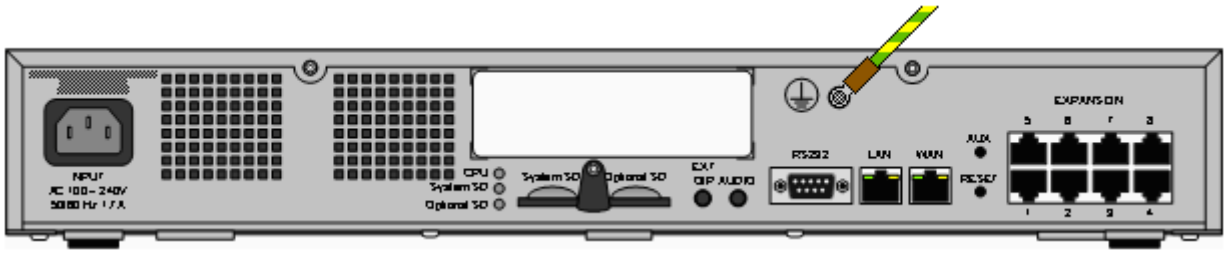
Parts and Equipment Required

- ☐ 14AWG Solid copper wire for ground connection.
- ☐ Cable sleeve matching local regulator requirements. Typically green for a functional ground and green/yellow for a protective ground.

The ground point on IP Office control units and expansion modules are marked with a ⏚ or ⏚ symbol. Ground connections to these points should use a 14 AWG solid wire with either a green sleeve for a functional ground or green and yellow sleeve for a protective ground.

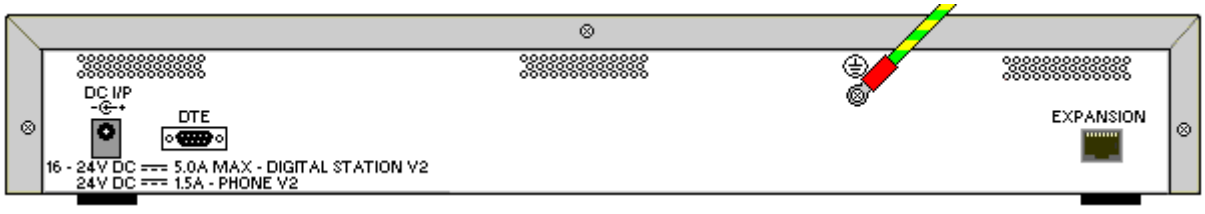
IP500 V2 Control Unit

On IP500 V2 control units the ground point is located above the RS232 DTE port.



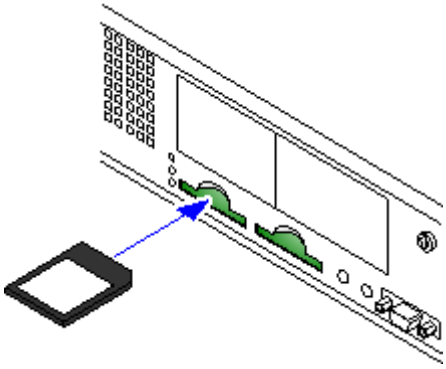
External Expansion Modules

On expansion modules, the ground point is a 4mm screw located towards the right on the rear of the module.



- On some older modules, the dedicated ground point screw is not present. In those cases, the top-center cover fixing screw (3mm) can be used as an alternative ground connection point. A toothed washer should be added to ensure good contact.

6.5 Starting the System



1. Before inserting the System SD card:
   a. Ensure that you have the correct type of Avaya System SD card 208.
   b. Ensure that the card has the required level of software. If necessary, upgrade the card using IP Office Manager 75.
2. With the control unit shut down or unpowered:
   a. The SD card slots are covered by a plastic tab. Partially release the screw holding the tab so that it can be moved clear of the required card slot.
   b. Insert the card into the **System SD** slot on the rear of the control unit.
3. Apply power to any external expansion modules.

   - **! Important: External Expansion Module Power**
     In order to be detected and operated correctly, external expansion modules must start before the IP Office control unit. Normally this achieved by connected all expansion modules to the same power strip as the control unit. The control unit applies a short delay to its own start-up process to ensure that expansion modules powered on at the same time as it are detected.

4. Apply power to the control unit. The power outlet used must include a switch and the power outlet must have a protective earth connection.
5. The control unit loads firmware from the System SD card with which it upgrades itself and its internal components. This takes approximately a minute. The end of this process is indicated by LED1 on each base card flashing every 5 seconds. LED9 on each base card fitted with a trunk daughter card also flashes.
6. The control unit then begins upgrading the external expansion modules if necessary. This is indicated by the center LED on the module flashing red. This process is completed when the LED changes to steady green.
7. If a configuration file is already present on the System SD 78 card it is loaded by the IP Office. If not, new systems create a default configuration and copy that configuration onto the System SD card.
8. It should be possible now to use IP Office Manager to access the configuration of the IP Office.

Control Unit Startup LEDs

Rear

The LEDs on the rear of the control unit go through the following sequence during a normal start up. Note that the times are approximately only:

LED	4s	4s	12s	5s	2s	5s	5s	10s	10s	Finished
CPU	Orange	Green	Green	Green Red	Green	Green	Green	Green	Green	Green
System SD	Orange	Off	Green	Green	Green	Off	Green	Green	Green Flash	Green
Optional SD If present.	Orange	Off	Green	Green	Green	Off	Off	Green	Green	Green

Front

On the front of the control unit, LED1 on any IP500 base cards fitted is used as follows. LED9 is also used for any trunk daughter cards fitted.

LED	30s	30s	Finished
LED1/LED9	Red	Red	Red
		Fast Flash	Flash every 5 seconds

6.6 Checking the LEDs

Control Unit LEDs

LED	Description
Optional SD **System SD**	• **Off** = Card shutdown. • **Green on** = Card present. • **Green flashing** = Card in use. • **Orange steady** = Reset imminent. • **Red flashing** = Card initializing or shutting down. • **Red fast flashing** = card full • **Red steady** = Card failure/wrong type.
CPU	• **Alternate red/green** = Starting up. • **Green on** = Okay. • **Red on** = No software. • **Flashing Red** = Error/Shutdown.

Base Card LEDs

Note: Cards not supported in IP Office Basic Edition mode (4-Port Expansion, VCM32 and VCM64) will display a solid red LED until the system is licensed and configured for Preferred Edition or higher.

Base Card	LEDs 1 to 8 Usage

All Cards	• LED1 is also used for base card status:
	  • **Red On** = Error/Not supported.
	  • **Red Slow Flash** = Initializing.
	  • **Red Flash every 5 seconds** = Card okay.
	  • **Red Fast Flash** = System shutdown.

IP500 Analog Phone	• No status LEDs are used for analog phone extensions.
IP500 Digital Station	• **Green Flashing** = Phone detected. • **Green On** = Phone active.
IP500 TCM8	• **Green On** = Phone detected.

IP500 Combination	• LEDs 1 to 6
	  • **Green Flashing** = Phone detected.
	  • **Green On** = Phone active.

IP500 VCM	• LEDs 1 to 8 are unlabelled. They are used to indicate voice compression channel usage. Each LED lit represents 12.5% of the available voice compression channel capacity in use (total card capacity rather than licensed capacity).
IP500 4-Port Expansion	• LEDs 1 to 8 are used for the expansion ports on the rear of the control unit. LEDs 9 to 12 are used for the card's own expansion ports.

Green	**On**	Expansion module present.
Red	**Flashing**	Initializing.
Red	**On**	Error.
Orange	**Regular Flash**	Base card okay.

Trunk Daughter Card LEDs

Trunk Daughter Card	LEDs 9 to 12 Usage
All cards	• LED 9 is also used for daughter card status. • **Red On** = Error • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.
Analog Trunk	• **Green on** = V1: Card installed. V2: Line connected to the port but idle. • **Green flashing** = Line in use.
PRI Trunk	• **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use. • **Red/Green Fast Flash** (port 9) or **Green Fast Flash** (port 10) = Alarm indication signal (AIS) from the trunk remote end. • **Red with Green Blink** (port 9) or **Green Blink** (port 10) = Port in loopback mode (set through IP Office System Monitor).
BRI Trunk	• **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use.

External Expansion Module LEDs

Module	LEDs
All	The center LED on all external expansion modules is used to indicate the overall state of the module as follows: • **Red flashing** = Module starting up/Loading firmware. • **Red on** = Error. • **Green on** = Module okay. • **Green flashing** = Module starting up/Loading firmware (IP500 DS16A/30A module only).
Analog Trunk 16	• None.
BRI So8	• **Green On** = Connected. • **Green Flashing** = Activity.
Digital Station 16/30	• **Green Flashing** = Phone detected. • **Green On** = Phone active.
Digital Station 16A/30A	• **Green On** = Phone detected.
Phone	• None.

6.7 Connecting Phones

During initial power up, the IP Office automatically creates extension and user entries for all analog and digital extension ports (DS and BST) in the system. This allows those devices to be connected without any additional programming.

- **! Warning**
  If the system has been upgraded from a previous release of IP Office software, all phones are restricted from making any calls until a upgrade license has been entered. For Release 10.0 and higher than means the appropriate release specific **Essential Edition** 279 license. The dialing restriction includes not being able to make emergency calls.
- This section does not cover the installation of DECT, H323 and SIP telephones. For installation of those devices refer to the appropriate supplementary installation manuals.

6.7.1 Analog Phones

Connect any analog phones to their appropriate Phone 276 ports. Ensure that those connected to power failure ports 47 are clearly labeled as such.

6.7.2 ETR Phones

Connect any ETR phones to their appropriate ETR 272 ports. These phones do not need to load additional firmware.

6.7.3 DS Digital Station Phones

Connect any digital phones to their appropriate DS 271 ports. These phones may need to upgrade their firmware to match that supported by the IP Office core software. The appropriate firmware is supplied with the IP Office Manager software and copied onto the System SD card for IP500 V2 systems.

The phones will automatically load the firmware from the IP Office system if necessary.

- The upgrade process takes approximately 10 minutes during which time the phone will display a warning. The phone should not be disconnected during this process.
- Once the phone connected to a port has been upgraded, the IP Office will not check whether the phone on that port needs to be upgraded again except following a system reboot, i.e. multiple phones cannot be upgraded by swapping the connected phones on the same port.

6.7.4 IP/SIP Phones

The installation and configuration of H323 and SIP IP telephones is not covered by this document. Refer to the appropriate IP Office installation manual for the type of phone being installed.

6.7.5 TCM/BST Phones

Connect any BST phones to their appropriate BST ports. These phones do not need to load additional firmware.

DS30B Module

The IP500 DS16B and DS30B external expansion modules support either BST or DS ports. The port type for a whole module is configured using IP Office Manager. See DS16B/30B Port Mode Selection 110.

Default Buttons

For system's with BST phone ports, when a phone is first connected to the port, the button programming of the associated user is overwritten with the default button programming appropriate for the phone model.

If the new system is being installed with a pre-staged configuration that include user button programming, the automatic defaulting of buttons to match the phone type will overwrite the user button settings. This behavior can be prevented by adding the following short code to the user's setup in the pre-programmed configuration:

- **Code:** *DCP
- **Feature:** Dial
- **Telephone Number:** 84000004,1,1,0
  The 4000004 part of the string above can also be used to adjust the defaults for the following phone settings:
  - The first digit sets the phone contrast = 1 (low) to 9 (high).
  - The last digit sets the ringer volume = 0 (high) to 7 (low).

Note that subsequently removing this short code will cause the buttons to return to defaulting according to the phone type.

Phone Type Setting

For some phones, the phone can only report its general type to the system rather than its specific model. It is recommended that after connecting all the phones, the phone types should be correctly set in the IP Office configuration.

- **! Important**
  The default types cannot be changed after installation without defaulting the configuration. Therefore you must ensure that you connect the correct type of phone to each port. If you need to swap phones, uses the process for exchanging extension numbers 186 rather than swapping wiring.

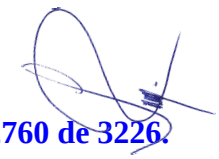
1. Using IP Office Manager, receive the configuration from the system.
2. Select **Extension**.
3. Selecting each extension in turn, on the **Extn** tab, check that the **Device Type** field is set to the correct phone model.

Default Type	Possible Phone Models
T7100	T7100, M7100, M7100N, Audio Conferencing Unit.
T7208	T7208, M7208, M7208N.
M7310	T7406E, T7406, M7310, M7310N
M7310BLF	T7316, M7310BLF
M7324	M7324, M7324N

4. Save the configuration back to the IP Office system.

Chapter 7.

Initial Configuration using Manager



7. Initial Configuration using Manager

This section covers basic configuration changes required for IP Office systems using the IP Office Manager application. This covers just the basic configuration, the full range of configuration possible through IP Office Manager is covered in the IP Office Manager manual 11 .

Summary

1. **Network Connection** 101
   Use IP Office Manager to connection to the new system.
2. **Initial Configuration** 103
   The **Initial Configuration** menu is shown the first time that IP Office Manager or IP Office Web Manager connects to a new system.
3. **Set the Extension Numbering** 104
   Renumber all the user extensions if required.
4. **Disable any Unused Trunks** 105
   Disabling the use of trunks and trunk channels that are not available.
5. **Select the Clock Source for Digital Trunks** 107
   Altering which digital trunk is used to provide the IP Office with its clock signal for call synchronization.
6. **Enter Trunk Prefixes** 109
   On systems where a prefix is being used for external dialing, ensure that the same prefix is added to incoming numbers in order to allow return calls.
7. **DS16B/30B Port Mode Selection** 110
   These modules can support Avaya T-Series and M-Series phones by providing BST ports or other Avaya digital phones by providing DS ports. The port type selection for the whole module is done using IP Office Manager.
8. **Uploading the License File** 111
   Upload the license file provided for the system and check the license status for the licenses.

Basic Security Configuration

After completing the basic configuration, you should follow the processes in the System Security 132 chapter.

Página2761 de 3226.

7.1 Network Connection

The section below details how a new IP Office system determines what IP address it should use.

IP Address and DHCP Mode Resolution

When a defaulted or new IP Office control unit is switched on, it requests IP address information from a DHCP Server. This occurs regardless of whether a LAN cable is connected or not. The process below is done separately for both the LAN port (LAN1 in the configuration) and the WAN port (LAN2 in the configuration) on the back of the IP Office control unit.

- The system makes a DHCP request for what IP address information it should use.
- If a DHCP server responds within approximately 10 seconds, the control unit defaults to being a DHCP client and uses the IP address information supplied by the DHCP server.
- If no DHCP Server responds, the control unit still defaults to being the DHCP client but assumes the following default addresses:
  - LAN Port (LAN1): 192.168.42.1/255.255.255.0.
  - WAN Port (LAN2): 192.168.43.1/255.255.255.0.
  - Note that the IP Office does not check that these addresses are valid and or available on the network.
- Systems running in IP Office standard modes can be configured as a DHCP server. They can also be configured to only provide DHCP for Avaya IP phones and or for remote access dial-in connections. DHCP Server options are not supported for systems running in IP Office Basic Edition modes.
- **!** Once an IP500 V2 control unit has obtained IP address and DHCP mode settings, it will retain those settings even if rebooted without a configuration file present on the System SD card. To fully remove the existing IP address and DHCP mode settings, you must default the system configuration 170.

PC Connection

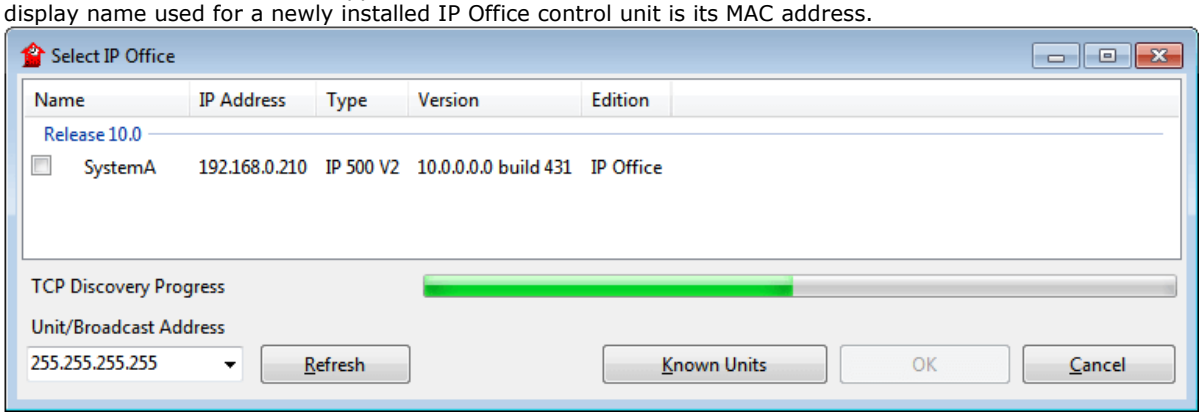
Depending on the conditions that applied when the IP Office control unit was first started, a PC can be connected as follows:

- **If the IP Office is not connected to a network:**
  Connect the PC directly to the IP Office. The PC must be set to an address valid on the same network as the IP Office defaults above.
- **If the IP Office is connected to a network with no DHCP server:**
  Connect the PC directly to the IP Office. The PC must be set to an address valid on the same network as the IP Office defaults above.
- **If the IP Office is connected to a network with a DHCP server:**
  Connect the PC to the network. The PC must be set to be a DHCP client or to an address that is valid for the network. The address being used by the IP Office system will have to be determined from the DHCP server. Most servers list the IP addresses of the clients registered to them.
- **If the IP Office used a pre-built configuration:**
  Use the IP addresses as set in that config. Ensure that the PC is on the same subnet or on a network able to route to that subnet.

Página2762 de 3226.

To login to a system using IP Office Manager:

1. Select **Start | All Programs | IP Office | Manager**.
   - If the PC has firewall software installed, you may be prompted as to whether you want to allow this program to access the network. Select **Yes** or **OK**.
2. Check the default settings for the application:
   a. Click **File | Preferences**.
   b. If you don't expect to ever manage any IP Office Basic Edition systems, select **Default to Standard Mode**. and unselect **Set Simplified View as default**.
   a. Click **OK**.
3. Select **File | Open Configuration** from the menu bar.
4. The **Select IP Office** window appears. After a few seconds it should list the IP Office control unit. The default display name used for a newly installed IP Office control unit is its MAC address.



   - If the system required was not found, the address used for the search can be changed. Enter or select the required address in the **Unit/Broadcast Address** field and then click **Refresh** to perform a new search.
5. Click the check the box next to the system and then click **OK**.
6. The name and password request is displayed. The default name and password are ***Administrator***.
7. You are now prompted to go through the initial configuration menu. See Initial Configuration 103.

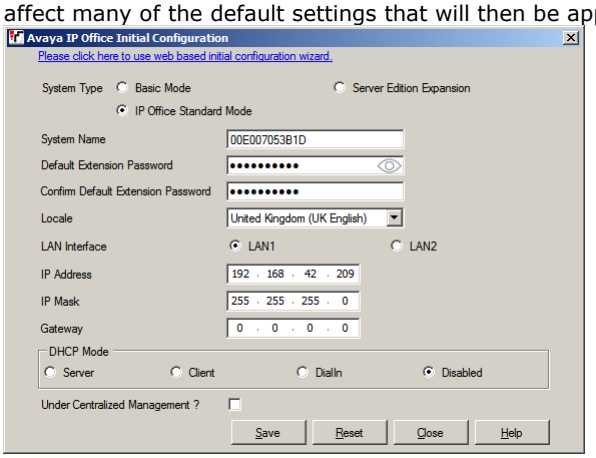
7.2 Initial Configuration

The initial configuration menu appears the first time IP Office Manager connects to a new or defaulted system.

- The initial configuration menu can be re-run at any time by selecting **File | Advanced | Initial configuration** in IP Office Manager or **Actions | Service Commands | Initial Configuration in** IP Office Web Manager. Note however that this erases most of the existing system configuration.

To start the initial configuration using IP Office Manager:

1. Using IP Office Manager, connect to the system 101 .
2. You are prompted to change the default passwords.
   - **Administrator Password**
     This password is used for access to the system's telephony configuration.
   - **Security Administrator Password**
     This password is used for access to the system's security configuration. Note that by default the administrator password above can also be used for security configuration.
   - **System Password**
     This password is used for system upgrades using IP Office Manager and can also be used for connecting System Monitor.
3. Enter the new passwords and click **OK**.
4. The **Initial Configuration** menu prompts you to confirm the required operating mode for the system. For the **System Type** select ***IP Office Standard Mode*** and click **Save**. This mode covers both IP Office Essential Edition and IP Office Preferred Edition systems.
5. The menu also prompts you for additional settings. It is important that you check and set these correctly as they affect many of the default settings that will then be applied to the new system:



   - **System Name:** Used to help identify and access the system.
   - **Default Extension Password:** This password is applied to the initial registration of IP extensions.
   - **Locale:** Set a range of default settings to match the telephony requirements of that country. Also sets the default language for the system and all users.
   - **IP Address Settings:** Check that these settings, especially the **DHCP Mode**, match the requirements for the customer network. Switch between **LAN1** and **LAN2** to check the settings settings of the LAN and WAN ports respectively.
   - **Under Centralized Management:** This setting is used for branch systems in a Avaya Aura network. Refer to the separate branch installation documentation 11.
6. Click **Save**. The new configuration is opened in IP Office Manager. The new configuration has currently not been saved to the system. Either:
   - **Continue basic configuration:**
     Continue the basic configuration using the following sections of this chapter and then save the configuration when finished.
   - **Save and then continue basic configuration:**
     Save the configuration 112 as it currently is. This may cause the system to reboot to use the new settings, the save menu will indicate if that is required. After saving the configuration, and once the system has rebooted if necessary, reload the configuration and continue with the basic configuration.
7. Continue with the basic configuration or click on the save icon to save the updated configuration 112 and then continue.

Página2764 de 3226.

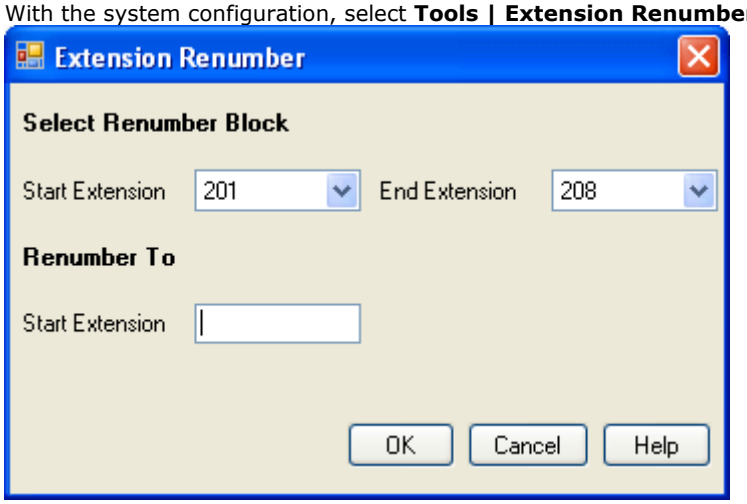
7.3 Extension Numbering

IP Office standard mode systems can use a mix of extension numbers up to 15 digits in length. By default, hunt groups and extensions are given 3-digit extension numbers starting from 200 upwards.

To renumber all user extensions using IP Office Manager:

IP Office Manager can be used to renumber all extensions on the system. This will also update any references to the extension number in other configuration fields.

1. With the system configuration, select **Tools | Extension Renumber**.



2. Select the range of existing user extensions you want renumber and enter the new starting extension number for that range.
3. Click **OK**.
4. Either:
   - **Continue basic configuration:**
     Continue the basic configuration using the following sections of this chapter and then save the configuration when finished.
   - **Save and then continue basic configuration:**
     Save the configuration 112 as it currently is. This may cause the system to reboot to use the new settings, the save menu will indicate if that is required. After saving the configuration, and once the system has rebooted if necessary, reload the configuration and continue with the basic configuration.
5. Continue with the basic configuration 105 or click on the save icon to save the updated configuration 112 and then continue.

7.4 Disable Unused Trunks

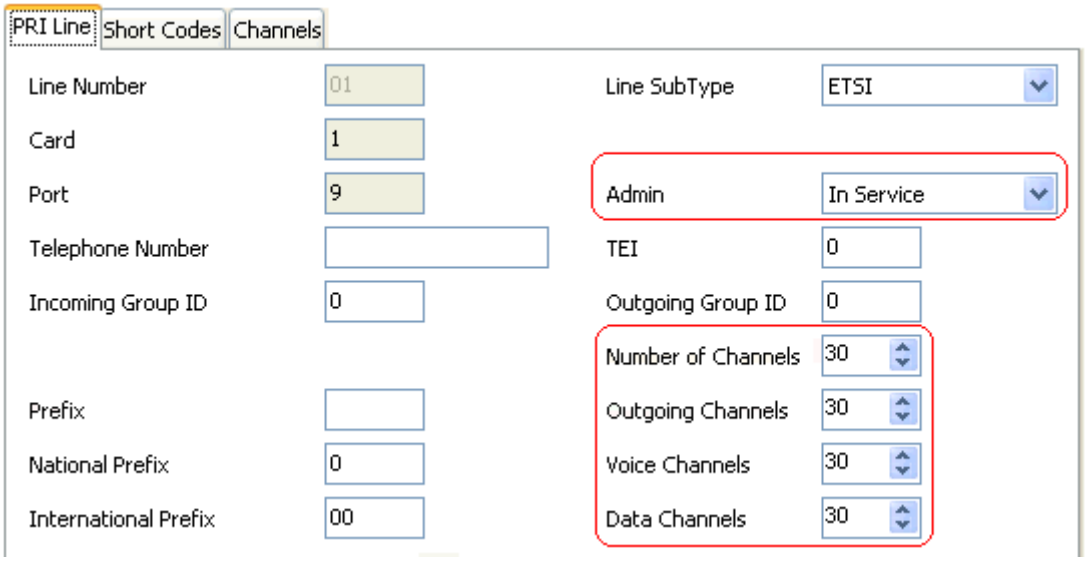
Each IP Office trunk card provides a fixed number of trunk ports with digital trunk ports supporting a fixed number of digital channels. By default the IP Office configuration has configuration entries for all the possible trunks and channels.

In cases where the number of trunks or trunk channels in use or licensed is lower than the number supported by the trunk card, the unused trunks and channels must be disabled.

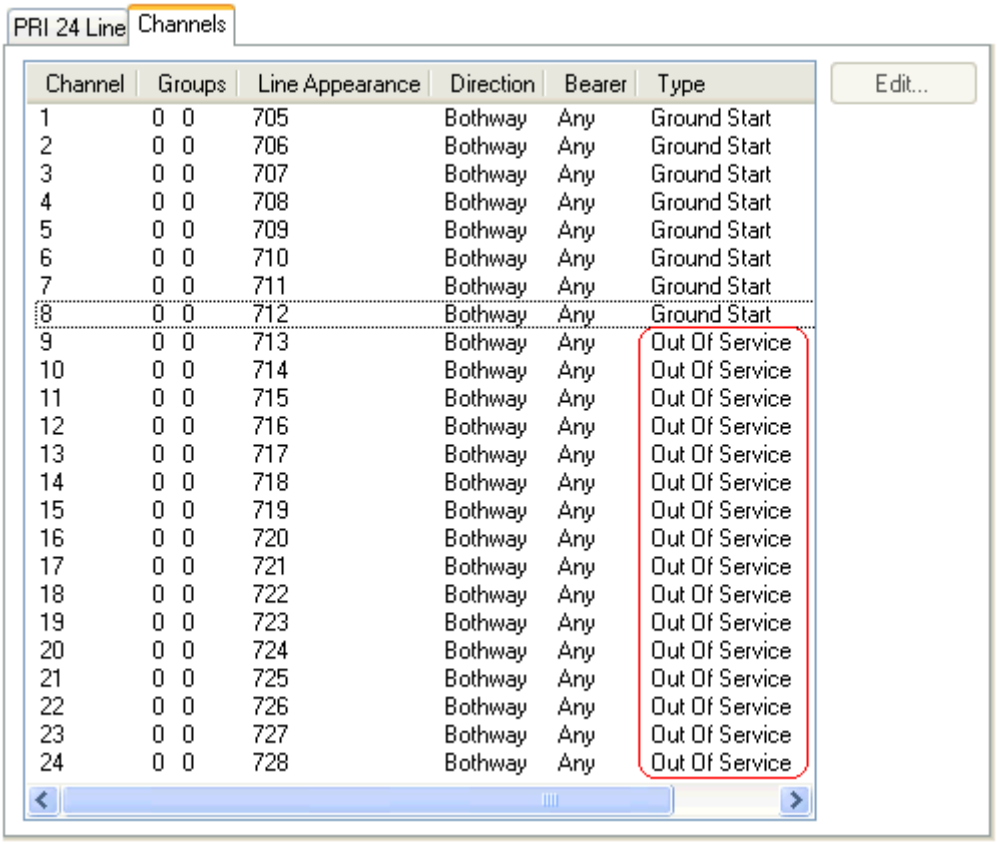
- ⚠ Failure to do this will cause problems with outgoing calls. For example, on a system with an ATM4 trunk card fitted but only two analog trunks actually connected, failure to disable the other two trunks within the IP Office configuration will cause 50% of outgoing call attempts to fail. This is because the system cannot automatically detect the service status of individual analog trunks.
  - For IP Office Release 8.1 Feature Pack 1 and higher with IP500 Analog Trunk 4 V2 cards and ATM4 Combination V2 cards, the system can detect with analog trunks are connected and so can automatically treat unconnected trunk ports as out of service.
- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

To disable unused trunks using IP Office Manager:

1. Within the IP Office configuration, select Line.
2. For each line, set those lines or channels that are not connected or being used as out of service. The location of the relevant setting varies for each trunk type.
   - **Analog Trunks**
     To disable the whole trunk, on the main form set the **Admin** option to ***Out of Service***.
   - **BRI, E1 PRI, S0 and QSIG Trunks**
     To disable the whole trunk, on the main form set the **Admin** option to ***Out of Service***. Otherwise set the number of channels to match the actual subscribed channels.



- **T1, T1 PRI and E1R2 Trunks**
  To disable the whole trunk, on the main form set the **Admin** option to ***Out of Service***. Otherwise select the Channels tab and set those channels that are not used to **Out of Service**.



Channel	Groups	Line Appearance	Direction	Bearer	Type
1	0 0	705	Bothway	Any	Ground Start
2	0 0	706	Bothway	Any	Ground Start
3	0 0	707	Bothway	Any	Ground Start
4	0 0	708	Bothway	Any	Ground Start
5	0 0	709	Bothway	Any	Ground Start
6	0 0	710	Bothway	Any	Ground Start
7	0 0	711	Bothway	Any	Ground Start
8	0 0	712	Bothway	Any	Ground Start
9	0 0	713	Bothway	Any	Out Of Service
10	0 0	714	Bothway	Any	Out Of Service
11	0 0	715	Bothway	Any	Out Of Service
12	0 0	716	Bothway	Any	Out Of Service
13	0 0	717	Bothway	Any	Out Of Service
14	0 0	718	Bothway	Any	Out Of Service
15	0 0	719	Bothway	Any	Out Of Service
16	0 0	720	Bothway	Any	Out Of Service
17	0 0	721	Bothway	Any	Out Of Service
18	0 0	722	Bothway	Any	Out Of Service
19	0 0	723	Bothway	Any	Out Of Service
20	0 0	724	Bothway	Any	Out Of Service
21	0 0	725	Bothway	Any	Out Of Service
22	0 0	726	Bothway	Any	Out Of Service
23	0 0	727	Bothway	Any	Out Of Service
24	0 0	728	Bothway	Any	Out Of Service

  - For T1 set the **Type** to ***Out of Service***.
  - For T1 PRI set the **Admin** field to ***Out of Service***.
  - For E1R2 trunks set the **Line Signalling Type** to ***Out of Service***.

3. Either:
   - **Continue basic configuration:**
     Continue the basic configuration using the following sections of this chapter and then save the configuration when finished.
   - **Save and then continue basic configuration:**
     Save the configuration 112 as it currently is. This may cause the system to reboot to use the new settings, the save menu will indicate if that is required. After saving the configuration, and once the system has rebooted if necessary, reload the configuration and continue with the basic configuration.
4. Continue with the basic configuration 107 or click on the save icon to save the updated configuration 112 and then continue and then continue.

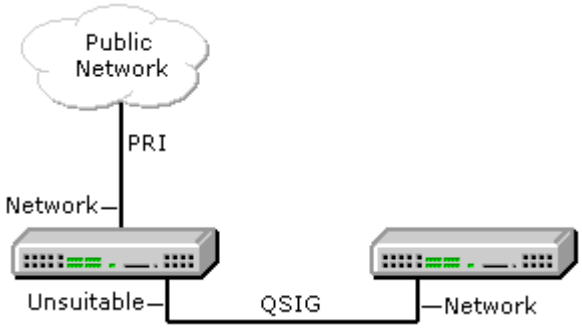
7.5 Setting the Digital Trunk Clock Source

Digital trunks require the telephone system at each end of the trunk to share a clock signal to ensure synchronization of call signalling. The IP Office can obtain and use the clock signal from any of its digital trunks. Typically the clock signal provided by a digital trunk from the central office exchange is used as this is usually the most accurate and reliable clock source.

If no trunk clock source is available, the system can use its own internal clock if necessary. However, an external trunk source is preferred. To do this, the **Clock Quality** setting on each line in the IP Office configuration is set to one of the following:

- ***Network***
  If available, the clock signal from this trunk should be used as the clock source for call synchronization. If several trunk are configured with this setting, the trunk used is determined in the order of slots 1 to 4 and then by port on each slot.
- ***Fallback***
  If available, the clock signal from this trunk can be used as the clock source if none of the trunks set as ***Network*** are providing a clock source. If several trunk are configured with this setting, the trunk used is determined in the order of slots 1 to 4 and then by port on each slot.
- ***Unsuitable***
  The clock source from this trunk will not be used as the clock source.

In the example below the first IP Office is set to use the public network trunk as its clock source and ignoring the possible clock source from the QSIG trunk. The other IP Office system is using the clock signal received from the first IP Office on its QSIG trunk as its clock source. Thus both IP Offices are using the same clock source and that clock source is the public network exchange.

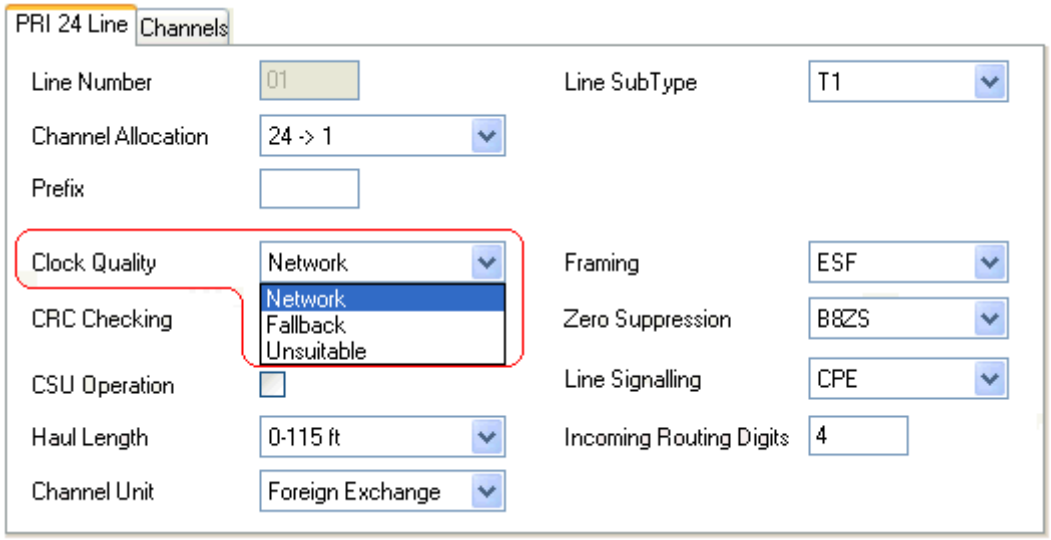


Viewing the Current Clock Source

The current clock source being used by an IP Office system is shown on the **Resources** page within the System Status Application.

To set a trunk's clock quality source using IP Office Manager:

1. Within the IP Office configuration, select **Line**.
2. For each digital line, select the line and on the Line tab select whether that trunk should provide the clock source for the network or whether the trunk is unsuitable. For E1R2 trunks the **Clock Quality** setting is on the **Advanced** tab.



3. Ensure that only one trunk is set to ***Network***. This should preferably be a direct digital trunk to the central office exchange.
4. One other trunk can be set a ***Fallback*** should the selected Network trunk connection be lost. If possible this should be a trunk from a different provider since that reduces the chances of both sources failing at the same time.
5. Ensure that all other digital trunks are set as ***Unsuitable***.
6. Either:
   - **Continue basic configuration:**
     Continue the basic configuration using the following sections of this chapter and then save the configuration when finished.
   - **Save and then continue basic configuration:**
     Save the configuration 112 as it currently is. This may cause the system to reboot to use the new settings, the save menu will indicate if that is required. After saving the configuration, and once the system has rebooted if necessary, reload the configuration and continue with the basic configuration.
7. Continue with the basic configuration 109 or click on the save icon to save the updated configuration 112 and then continue.

Página2769 de 3226.

7.6 Setting the Trunk Prefixes

By default, systems with a U-Law System SD card default to using a 9 prefix for external calls. Systems started with an A-Law System SD card default to no prefix (any dialing that doesn't match an internal number is assumed to be an external number).

Where a prefix is used for outgoing calls, that same prefix needs to be added to trunk settings. That trunk prefix is then used as follows:

- **Incoming Calls**
  On incoming calls, the trunk's set prefix is added to any incoming caller ID received with the call and stored in the call log on phones, etc. The prefix should be such that the resulting caller UD can be used by the systems phones and applications to make return calls. For example, if the system is configured to require a 9 to indicate an outgoing call, the trunk needs to add a 9 to the incoming caller ID so that that ID can be used for return calls.
- **Outgoing Calls**
  On outgoing calls, the short codes used to route the call to a trunk must remove any external dialing prefix (for example 9) so that the number dialed from the system to the trunk is suitable for routing by the trunk provider.

To set trunk prefixes using IP Office Manager:

1. Within the IP Office configuration, select Line.
2. For each line enter the prefix. The location of the prefix settings varies for each trunk type. Some trunk types have a single prefix field. Other trunk types may have separate prefix fields for national, international and other calls.
3. Either:
   - **Continue basic configuration:**
     Continue the basic configuration using the following sections of this chapter and then save the configuration when finished.
   - **Save and then continue basic configuration:**
     Save the configuration 112 as it currently is. This may cause the system to reboot to use the new settings, the save menu will indicate if that is required. After saving the configuration, and once the system has rebooted if necessary, reload the configuration and continue with the basic configuration.
4. Continue with the basic configuration 110 or click on the save icon to save the updated configuration 112 and then continue.

7.7 DS16B/30B Port Mode Selection

Each IP500 DS16B/DS30B and DS16B2/DS30B2 external expansion module in a system can support either DS phone ports[271] or BST phone ports[270]. The modules default to DS phone port operation. The mode of any particular module can be changed though the system configuration.

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.
- **DS16B/DS30B Upgrade Behavior:**
  For DS16B/DS30B modules the process of loading the appropriate firmware for the selected mode or upgrading takes up to 10 minutes during which time the module is not available.
- **DS16B2/DS30B2 Upgrade Behavior:**
  The behavior of DS16/30B2 during firmware upgrade or switching modes differs from other external expansion units:
  - During the firmware upgrade, the unit remains operational and can make and receive calls.
  - Once the upgrade is completed (approximately 9 minutes) the unit reboots and takes about 45 seconds to return to normal operation.

To change the IP500 DS16B/30B module port mode:

1. Within the IP Office configuration, select **Control Unit**. The control unit and external expansion modules are listed.
2. The IP500 DS16B and IP500 DS30B modules are listed as ***DIG ADPx16 RJ45*** and ***DIG ADPx30 RJ45***.
3. Select one of the external expansion modules. In the unit details, the **Operating Mode** drop-down list is used to select what type of phones the module supports. Select the required mode.
   - For DS ports, select ***DS - 1400, 9500, 5400, 2400, T3, 4400 Series Phones***.
   - For BST ports, select ***BST - T7000, M7000 Series Phones***.
4. Click **OK**.
5. Continue with the basic configuration[111] or click on the save icon to save the updated configuration[112] and then continue.

7.8 Uploading the License File

The IP Office system requires licensing for some features, see Licenses[279]. The license file can be either uploaded manually or pre-loaded onto the System SD card[78].

How is the system licensed?

- An XML file containing the full set of PLDS licenses is uploaded to the system. The license file is unique to the feature key serial number of the System SD card installed in the system.
  - The PLDS host ID used for the license file must match that shown by the 12 digit **PLDS ID** printed on the SD card label. Older cards have an 10 digit feature key serial number shown by **FK** or **FK SN**. For those cards add the prefix ***11*** to obtain the card's PLDS ID.

Minimum License Requirements

For IP Office Essential Edition, the system requires an **Essential Edition** system license for the specific IP Office release you want it to run.

To upload the license file using IP Office Manager:

1. Within the system configuration click on **License**.
2. The field **PLDS Host ID** shows the serial number of the System SD card fitted to the system. Check that this number matches the one against which the licenses have been issued.
   - The PLDS host ID used for the license file must match that shown by the 12 digit **PLDS ID** printed on the SD card label. Older cards have an 10 digit feature key serial number shown by **FK** or **FK SN**. For those cards add the prefix ***11*** to obtain the card's PLDS ID.
3. Click **Add...** .
4. For the license type select **PLDS** and click **OK**.
5. Browse to the location of the XML file supplied containing the licenses. Select the file and click **Open**.
6. Continue with the basic configuration[112] or click on the save icon to save the updated configuration[112] and then continue.

7.9 Saving the Configuration

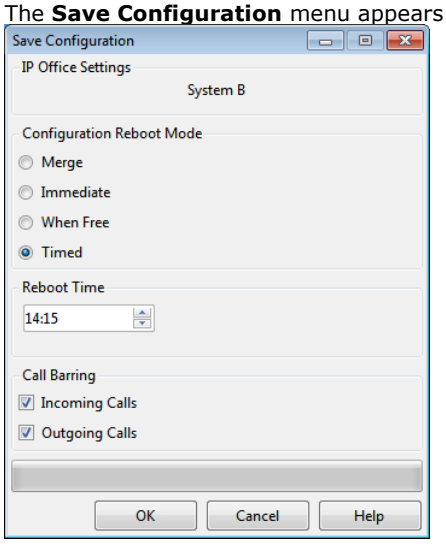
Having completed the basic configuration, the new configuration needs to be saved back to the system. This will very likely require the system to reboot.

After saving the configuration, reload it into IP Office Manager;

- If the IP address settings were changed, you may need to change your PC settings to reload the configuration.
- After reloading the configuration, any licenses should now be listed as ***Valid***.

To save configuration changes using IP Office Manager:

1. Click **OK** to save any changes to the current menu.
2. Click on the icon.
3. The **Save Configuration** menu appears.



- **Merge**
  This method is automatically selected if none of the configuration changes made require a system reboot. If this method is used for a configuration that includes changes that do require a reboot, those changes are not applied until the system is manually rebooted.
- **Immediate**
  This method saves the new configuration changes and then restarts the system. Any current calls and services in progress are ended. This method is automatically selected if any of the changes made so far require a reboot before they are applied to the system.
- **Free**
  This method allows the **Incoming Call Barring** and **Outgoing Call Barring** options to be used. The system reboots when the criteria for the selected options are matched.
- **Timed (HH:MM)**
  This method reboots the the system at the selected time. It can also be used with the call barring options to only reboot after the set time when the selected options are matched.
- **Incoming Call Barring**
  This option can be used with the **Free** and **Timed** reboot methods. When selected, the system bars any further incoming calls. However, it allows existing calls to continue until they are ended.
- **Outgoing Call Barring**
  This option can be used with the **Free** and **Timed** reboot methods. When selected, the system bars any further outgoing calls. However, it allows existing calls to continue until they are ended.
  - **! WARNING**
    This option also bars the making of emergency calls. It should therefore only be used with caution.

4. Select the options required and click **OK**.

Basic Security Configuration

After completing the basic configuration, you should follow the processes in the System Security 132 chapter.

Página2773 de 3226.

Chapter 8.

Initial Configuration Using IP Office Web Manager

8. Initial Configuration Using IP Office Web Manager

You can your web browser to configure an IP500 V2 system through its IP Office Web Manager menus. For new IP500 V2 systems, that includes running a series of initial wizard configuration menus to cover key settings for a new system.

8.1 The System's Initial IP Address

In order to connect to a new system using a browser, you first need to determine what IP address the system has adopted.

The section below details how a new IP Office system determines what IP address it should use.

IP Address and DHCP Mode Resolution

When a defaulted or new IP Office control unit is switched on, it requests IP address information from a DHCP Server. This occurs regardless of whether a LAN cable is connected or not. The process below is done separately for both the LAN port (LAN1 in the configuration) and the WAN port (LAN2 in the configuration) on the back of the IP Office control unit.

- The system makes a DHCP request for what IP address information it should use.
- If a DHCP server responds within approximately 10 seconds, the control unit defaults to being a DHCP client and uses the IP address information supplied by the DHCP server.
- If no DHCP Server responds, the control unit still defaults to being the DHCP client but assumes the following default addresses:
  - LAN Port (LAN1): 192.168.42.1/255.255.255.0.
  - WAN Port (LAN2): 192.168.43.1/255.255.255.0.
  - Note that the IP Office does not check that these addresses are valid and or available on the network.
- Systems running in IP Office standard modes can be configured as a DHCP server. They can also be configured to only provide DHCP for Avaya IP phones and or for remote access dial-in connections. DHCP Server options are not supported for systems running in IP Office Basic Edition modes.
- **!** Once an IP500 V2 control unit has obtained IP address and DHCP mode settings, it will retain those settings even if rebooted without a configuration file present on the System SD card. To fully remove the existing IP address and DHCP mode settings, you must default the system configuration 170.

PC Connection

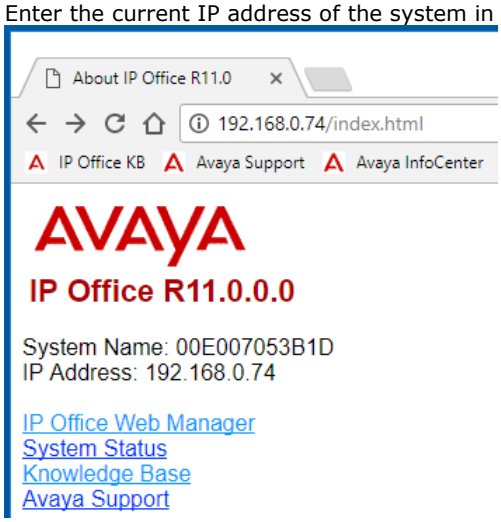
Depending on the conditions that applied when the IP Office control unit was first started, a PC can be connected as follows:

- **If the IP Office is not connected to a network:**
  Connect the PC directly to the IP Office. The PC must be set to an address valid on the same network as the IP Office defaults above.
- **If the IP Office is connected to a network with no DHCP server:**
  Connect the PC directly to the IP Office. The PC must be set to an address valid on the same network as the IP Office defaults above.
- **If the IP Office is connected to a network with a DHCP server:**
  Connect the PC to the network. The PC must be set to be a DHCP client or to an address that is valid for the network. The address being used by the IP Office system will have to be determined from the DHCP server. Most servers list the IP addresses of the clients registered to them.
- **If the IP Office used a pre-built configuration:**
  Use the IP addresses as set in that config. Ensure that the PC is on the same subnet or on a network able to route to that subnet.

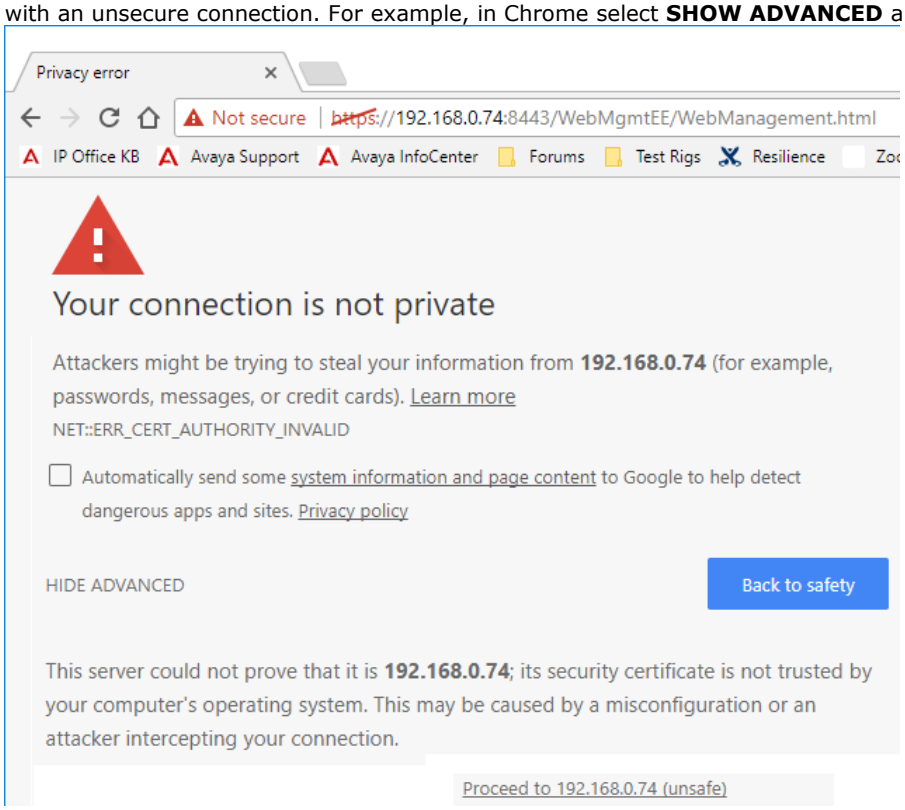
8.2 New System Install

Having determined the new systems IP address and configured your PC to be able to connect to addresses in that range:

1. Enter the current IP address of the system in your browser's address bar.

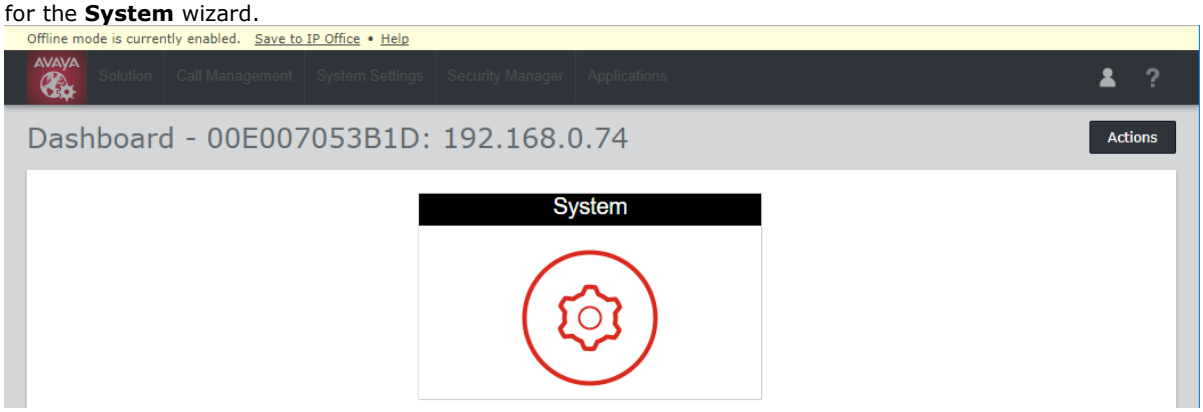


2. Click **IP Office Web Manager**.
   - The address shown is now similar to *https://192.168.0.42:8443/WebMgmtEE/WebManagement.html*. This is the web manager address for non-IP Office Basic Edition mode systems.
3. The connection as this stage is not seen as secure. Follow whichever steps your browser provides for continuing with an unsecure connection. For example, in Chrome select **SHOW ADVANCED** and then **Proceed**.

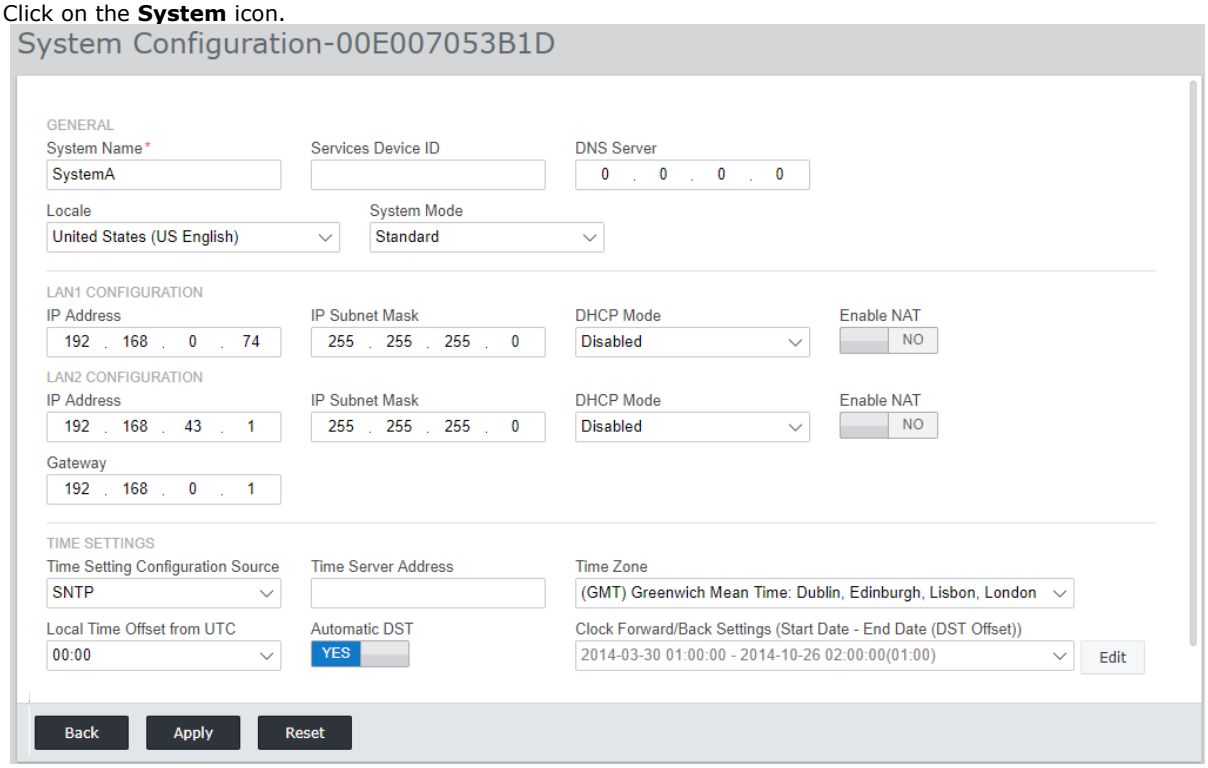


4. At the login menu, login using the default name and password ***Administrator***.

5. IP Office Web Manager is started and displays the system dashboard. For a new system this only contains the icon for the **System** wizard.



6. Click on the **System** icon.

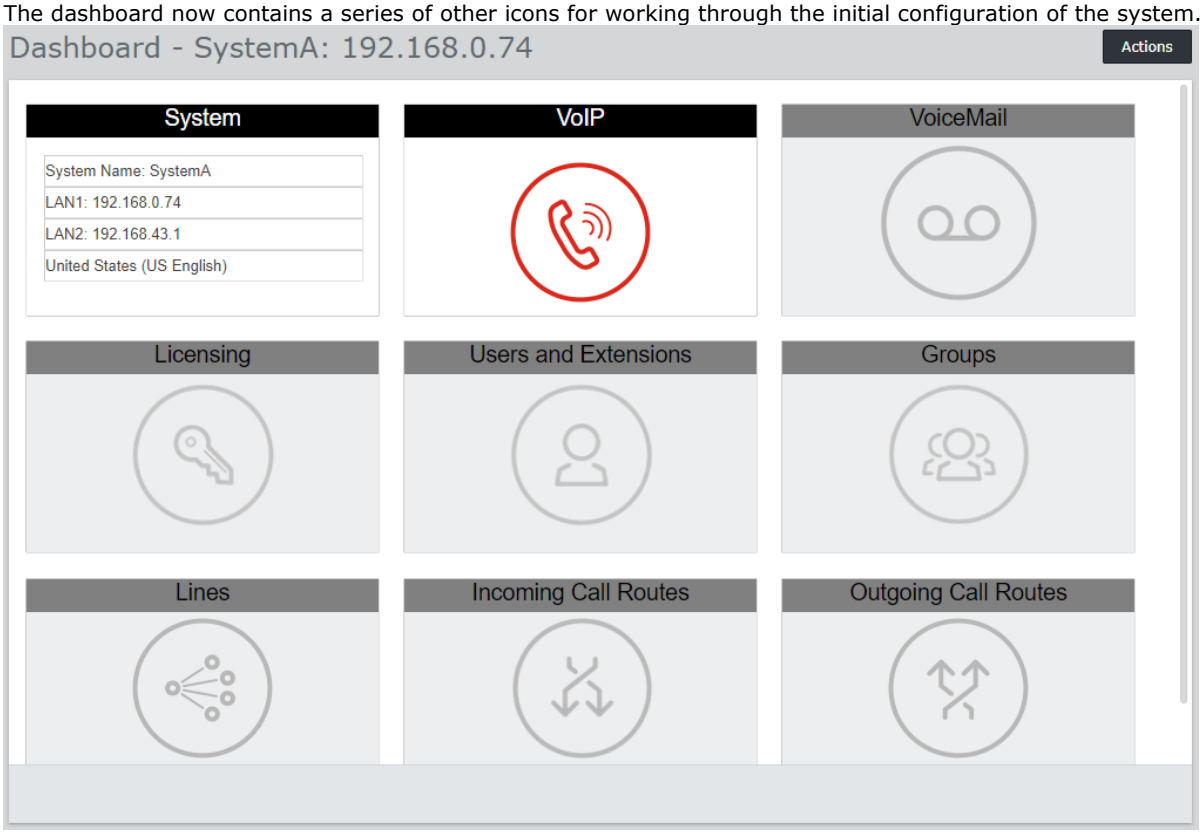


7. Enter the details that you want the system to use. At this stage the key values are a System Name, the Locale, the System Mode (set this to Standard) and the IP address. For full details of the **System** options see System Settings 120.

8. Click **Apply**.

Página2777 de 3226.

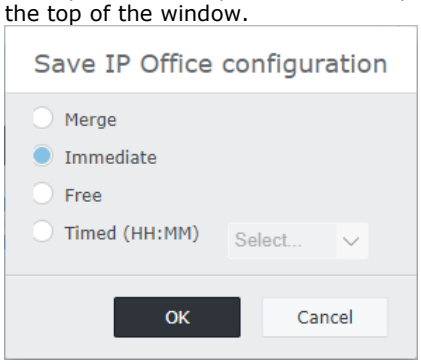
9. The dashboard now contains a series of other icons for working through the initial configuration of the system.



10. The next icon to click is highlighted in red. After you complete each set of settings, the icon in the panel is replaced with a summary of the key settings and the next icon is highlighted. You can return to previous panels if you want to make further changes to their settings. For details of the individual panels use the following links:

- System 120
- Licensing 124
- Lines 127
- VoIP 122
- Users and Extensions 125
- Incoming Call Routes 128
- Voicemail 123
- Groups 126
- Outgoing Call Routes 129 *(United States/Canada only)*

11. Once you have completed all the steps of the wizard, click the **Save to IP Office** link shown in the yellow bar at the top of the window.



12. The save configuration menu is displayed with a recommended save setting based on the changes you have made. For a new install this is likely to be a save using an immediate reboot of the new system. Accept the recommended setting and click **OK**.
13. After the reboot, continue the system configuration using the system's new IP address.

Página2778 de 3226.

8.3 Existing System

You can return to the Dashboard menus at any time after a system has been installed. Simply click on **Solution**. However, most of the panels of the dashboard can only be used to change system settings if accessed whilst IP Office Web Manager is in offline mode.

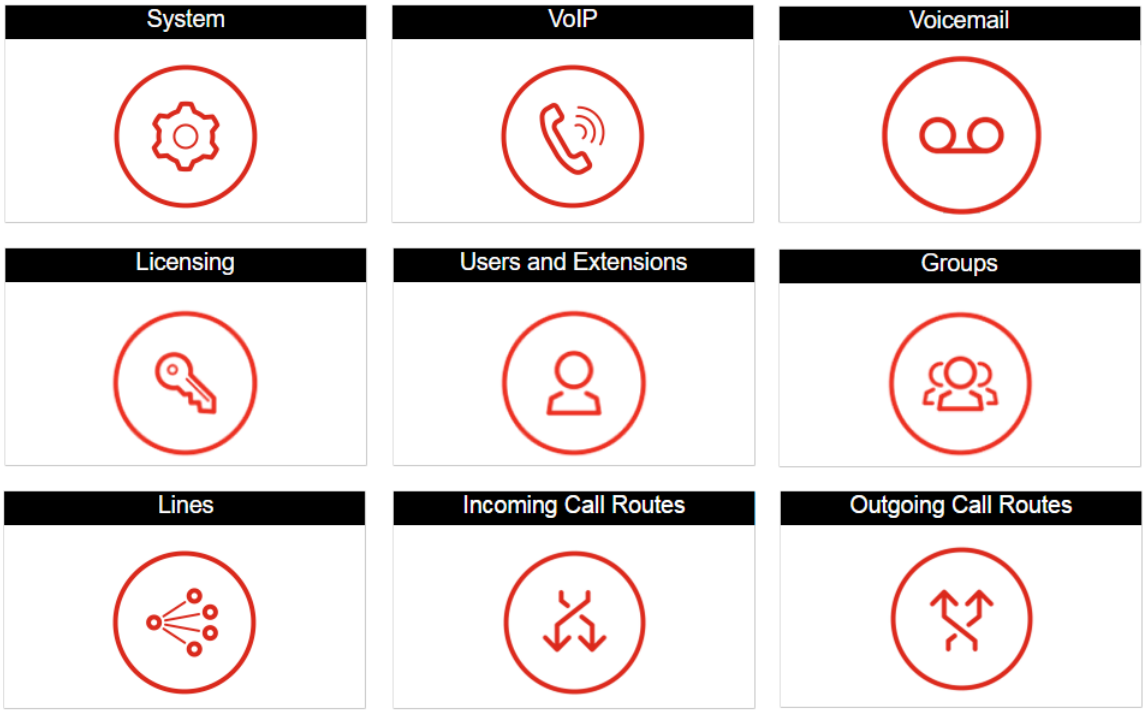
To access the active dashboard on a configured system:

1. Click on **Solution**. The dashboard is displayed.
2. Hover over the icon and click **Offline Mode**.
3. Click **OK**.
   - If the dashboard has previously been used but without saving all the data, it may display an option to either **Resume** or **Discard** the settings from the previous session.
4. You can now use the dashboard menus 119 to change key configuration settings.

Página2779 de 3226.

8.4 Dashboard Wizard Menus

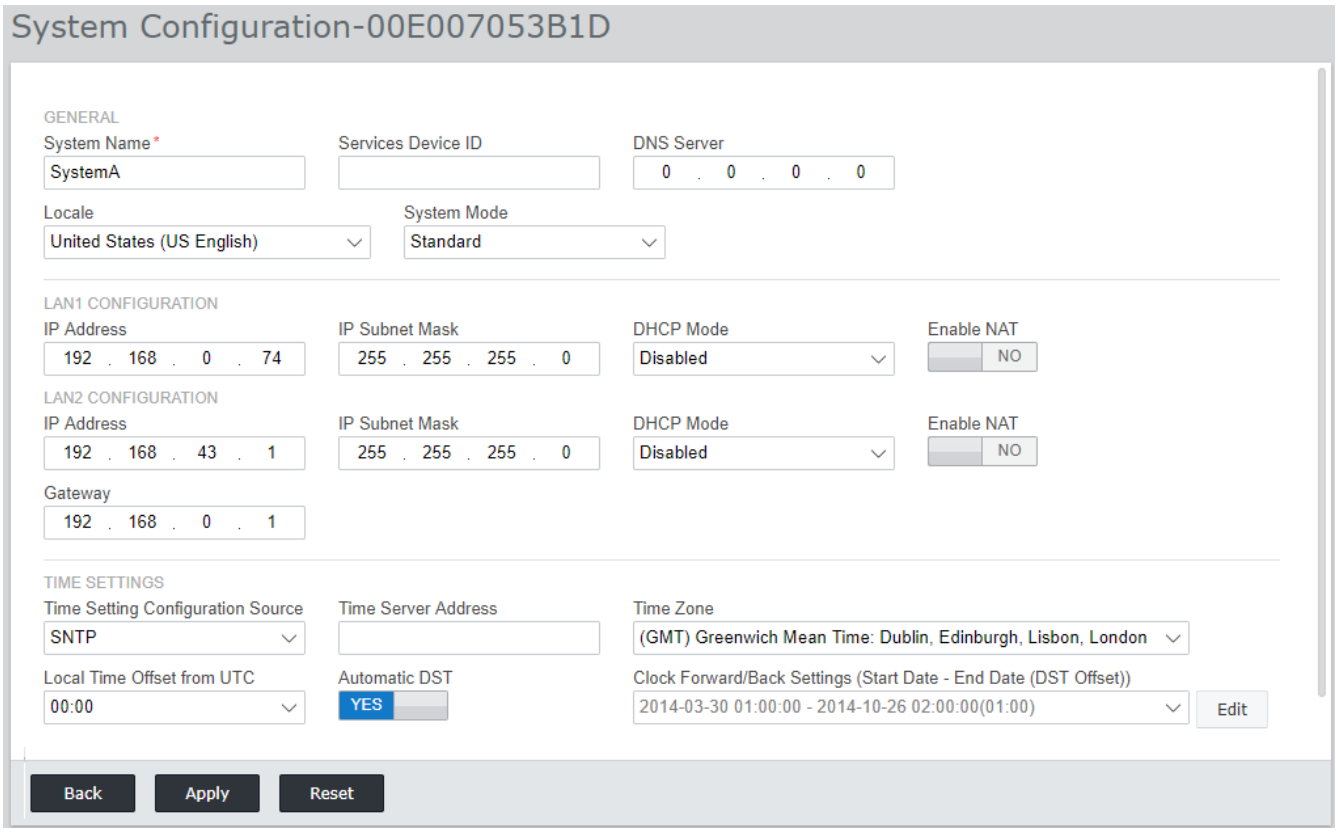
This section provides a summary of the dashboard wizard menus only. For full details refer to the *"Administering IP Office System Using Web Manager"* help and manual.



- System 120
- VoIP 122
- Voicemail 123
- Licensing 124
- Users and Extensions 125
- Groups 126
- Lines 127
- Incoming Call Routes 128
- Outgoing Call Routes 129
  (United States/Canada only)

8.4.1 System Settings

This panel allows the setting of a number of key settings (location, mode, IP address and time/date settings).



- **System name**
  This name is used to identify the system in other tools and menus.
- **Retain Configuration**
  This option is only shown when the dashboard is being used to reconfigure an existing system rather than a new or defaulted system. If selected, this option will retain as much of the existing configuration as possible except those settings changed through the dashboard. If disabled, all other configuration settings other than those set through the dashboard are returned to their defaults.
- **Services Device ID**
  Set this field if a value has been supplied. Normally a value is automatically set when the system is registered through the on-boarding process[138] following installation.
- **DNS Server**
  Enter the address of the domain name server (DNS) the system should use to resolve server names into IP addresses.
- **Locale**
  This value sets a large number of system defaults that are location specific, especially settings relating to telephony. Therefore it is important to set this value correctly to match the actual system location.
- **System Mode**
  The IP500 V2 can be used in a number of modes:
  - ***Basic***
    This option should be selected for a system that will run in one of the IP Office Basic Edition modes. This option is only available when configuring a new IP500 V2. If selected, the dashboard will only show the System settings. For details refer to the Server Edition documentation.
  - ***Standard***
    This option should be selected for a system that should run in either IP Office Essential Edition or IP Office Preferred Edition mode.
  - ***Expansion***
    This option is used for systems being installed as an expansion unit in a Server Edition or IP Office Select network. For details refer to the Server Edition documentation.
- **LAN Configuration**
  These fields are used to set the IP address settings of the system's LAN1 (LAN) and LAN2 (WAN) ports.
- **Time Settings**
  This section sets the time source for the system. The fields available depend on the time source selected.

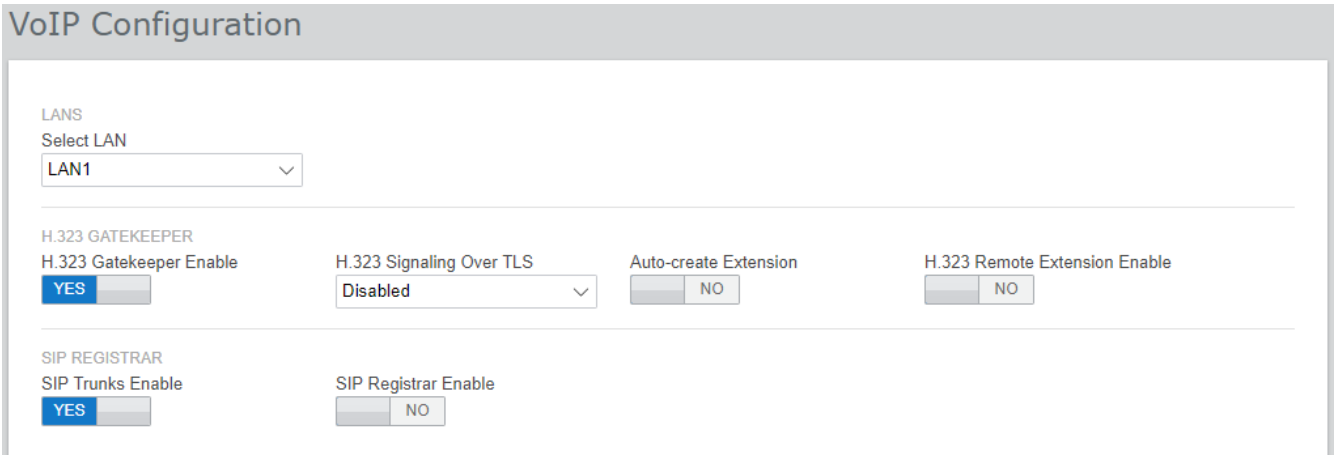
Página2781 de 3226.

- **Time Setting Configuration Source**
  This field is used to set the time source the system should use.
  - ***SNTP***
    If selected, the system will obtain its date and time information from the configured time server address, for example ***0.pool.ntp.org***. The additional settings available are to then apply a time zone, time offset and daylight saving time (DST) options if required.
  - ***Voicemail Pro/Manager***
    If selected, the system will request date and time information from the server running the Voicemail Pro application or IP Office Manager.
  - ***None***
    If selected, the system date and time will need to be set manually. That can be done from an Avaya phone where the user is set as a system phone user. Refer to the IP Office Manager help.

8.4.2 VoIP Settings

This tab is used to enable basic support for IP telephony, trunks and extensions, via H323 and or SIP connections.

- **! Warning:**
  Do not enable any settings unless you are sure that the system will be using H323 or SIP connections. Enabling unnecessary connections introduces additional security requirements which, if not meet, may place the system at risk.

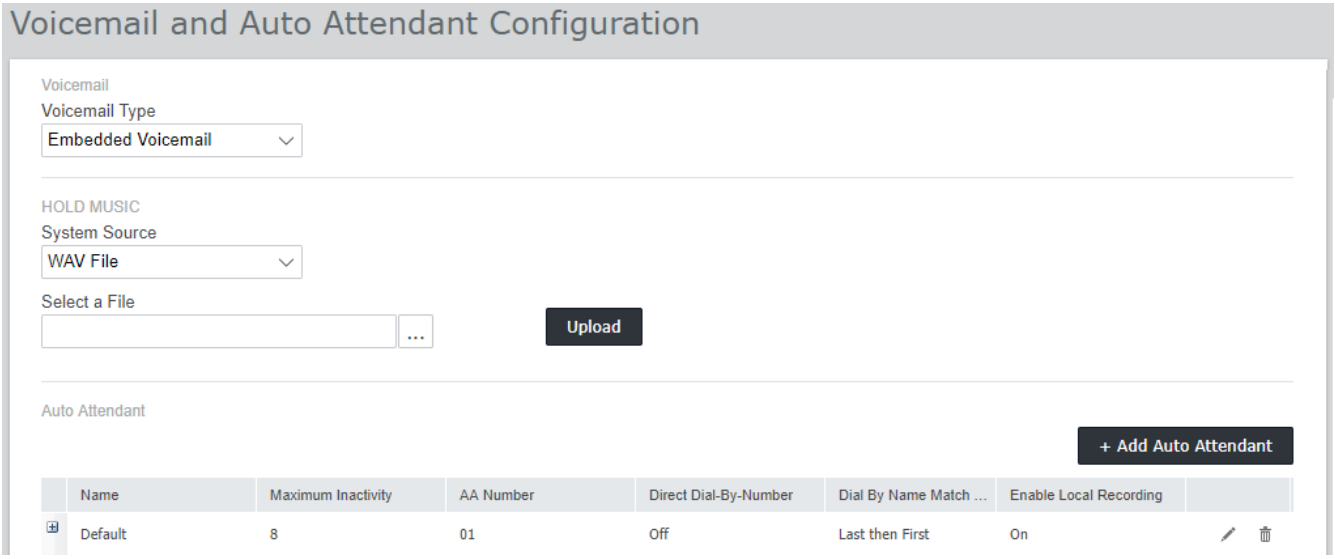


- **Select LAN**
  Select the LAN being configured.
- **H.323 Gatekeeper Enable**
  Only select this option if the system will be installed with H.323 trunks and extensions.
  - **H.323 Signalling Over TLS**
    Support H.323 signalling using TLS. Note that enabling this requires additional configuration and reduces the overall IP phone capacity of the system.
  - **Auto-Create Extension**
    If is selected, the system automatically creates user and SIP extension entries in its configuration based on SIP extension registration. This setting is automatically disabled the settings 24-hours after it is enabled.
  - **H.323. Remote Extension Enable**
    Enable to support Avaya H.323 telephones located at remote locations.
- **SIP Trunks Enable**
  Only select this option if the system will be installed with SIP trunks.
- **SIP Registrar Enable**
  Only select this option if the system will be installed with SIP extensions. When selected, the following additional options are shown:
  - **Auto-create Extn/User:** *Default = Off*
    If is selected, the system automatically creates user and SIP extension entries in its configuration based on SIP extension registration. This setting is automatically disabled the settings 24-hours after it is enabled.
  - **SIP Remote Extn Enable:** *Default = Off*
    Currently remote SIP extension options are only supported for Avaya SIP client applications. Remote connection is not supported for third-party SIP devices.
  - **SIP Domain Name:** *Default = Blank*
    This value is used by SIP endpoints for registration with the system. If left blank, registration uses the LAN IP address. The entry should match the domain suffix part of the **SIP Registrar FQDN** below, for example *acme.com*.
    - Note: For Avaya SIP telephones supported for resilience, the **SIP Domain Name** must be common to all systems in the network.
    - This is the local SIP registrar domain name that needed by SIP devices in order to register with the IP Office. If you are using TLS, this value needs to be included in the security certificates applied to the IP Office and, if used, separate HTTP file server.
  - **SIP Registrar FQDN:** *Default = Blank*
    This is the fully-qualified domain name, for example *example.acme.com*, to which the SIP endpoint should send its registration requests. This address must be resolvable by DNS to the IP address of the IP Office system.

Página2783 de 3226.

8.4.3 Voicemail Settings

This panel displays the voicemail and default music on hold settings of the system. If using embedded voicemail, the form can also be used to configure auto-attendant to answer calls (up to 40).



- **Voicemail Type**
  The main selections options are listed below. For details of the other options refer to the IP Office Web Manager help. Additional fields are displayed depending on the selection.
  - ***Embedded Voicemail***
    This option uses the system's own system SD card as the source for voicemail and storage for messages. This is a simple voicemail solution with only basic features. However, it does provide support for up to 40 auto-attendants.
  - ***Voicemail Pro/Lite***
    Select this option if voicemail will be provided by a server running IP Office Voicemail Pro. Enter the IP address of the server.
- Hold Music
  This option allows you to select the systems default source for music-on-hold. The options are:
  - ***WAV File***
    Use a WAV file uploaded to the system. The file must be called ***holdmusic.wav*** and match the format list below. Use the Select a File option to select and upload the file.

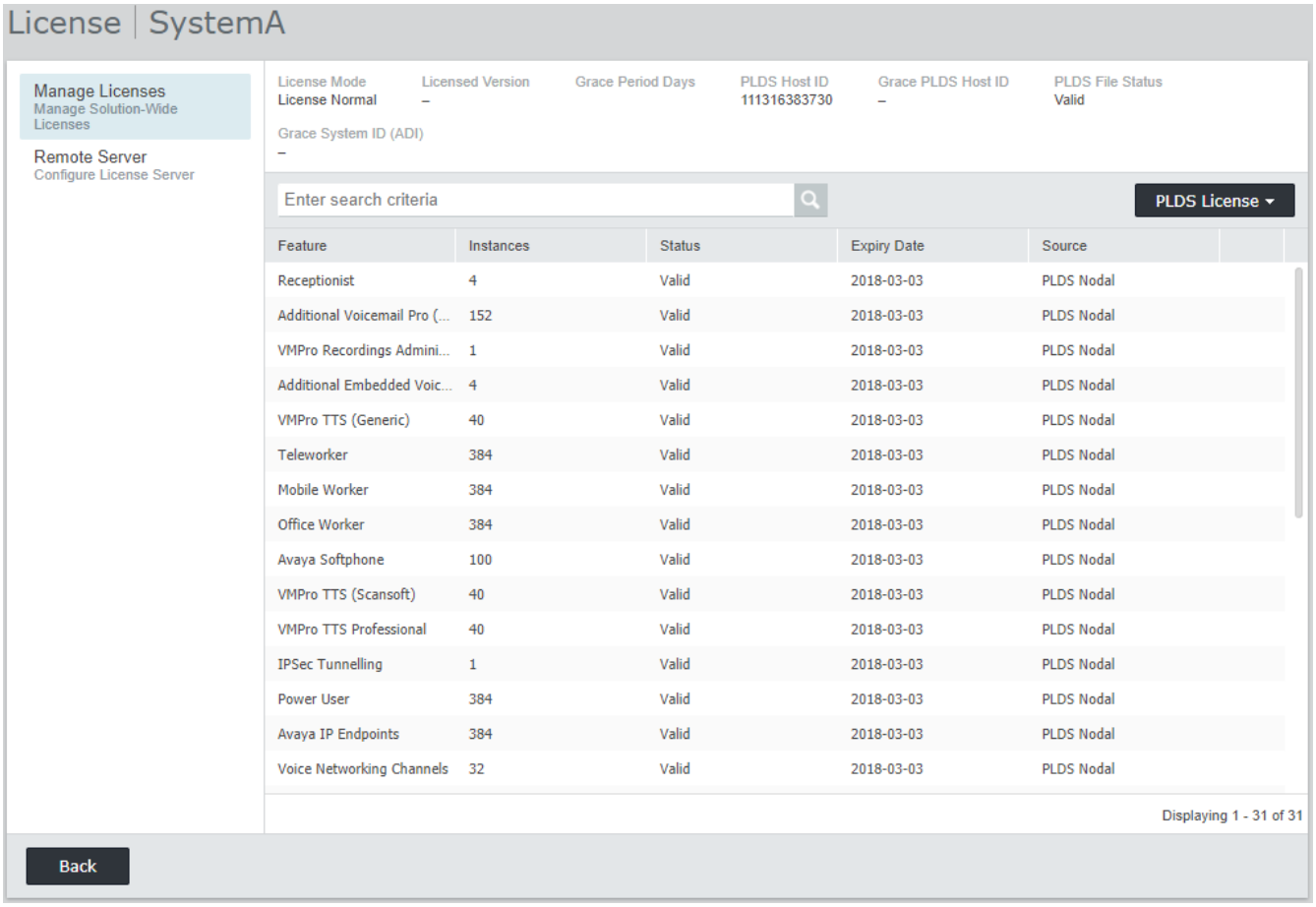
Property	Value	Property	Value
File Type	WAV	**Audio Sample Rate**	8kHz
Bit Rate	128kbps	**Audio Format**	PCM
Audio sample size	16 bit	**Length**	Up to 90 seconds.
Channels	1 (mono)		

  - ***External***
    Use the audio input from the system's Audio port on the rear of the control unit.
  - ***Tone***
    Use a regular repeated tone generated by the system.
- **Auto Attendant**
  If the Voicemail Type is set to Embedded Voicemail, the dashboard allows you to configure auto-attendants. These can be used as destinations for the Incoming Call Routing menu. The wizard automatically creates 3 time profiles call ***Morning***, ***Afternoon*** and ***Evening*** for use by the auto-attendants. These are set to 08:00-11:59, 12:00-16:59 and 00:00-07:59, 7-days a week respectively.

8.4.4 Licensing Settings

This section of the dashboard allows you to add a license file for the system and to see what licenses were included in the file. An unlicensed system will not allow any telephone functions until licenses are added (at minimum for an IP500 V2 an ***Essential Edition*** license is required). The license file must match the PLDS

If the license file was placed on the system SD card[78] before the system was started, the licenses from the file are automatically added.



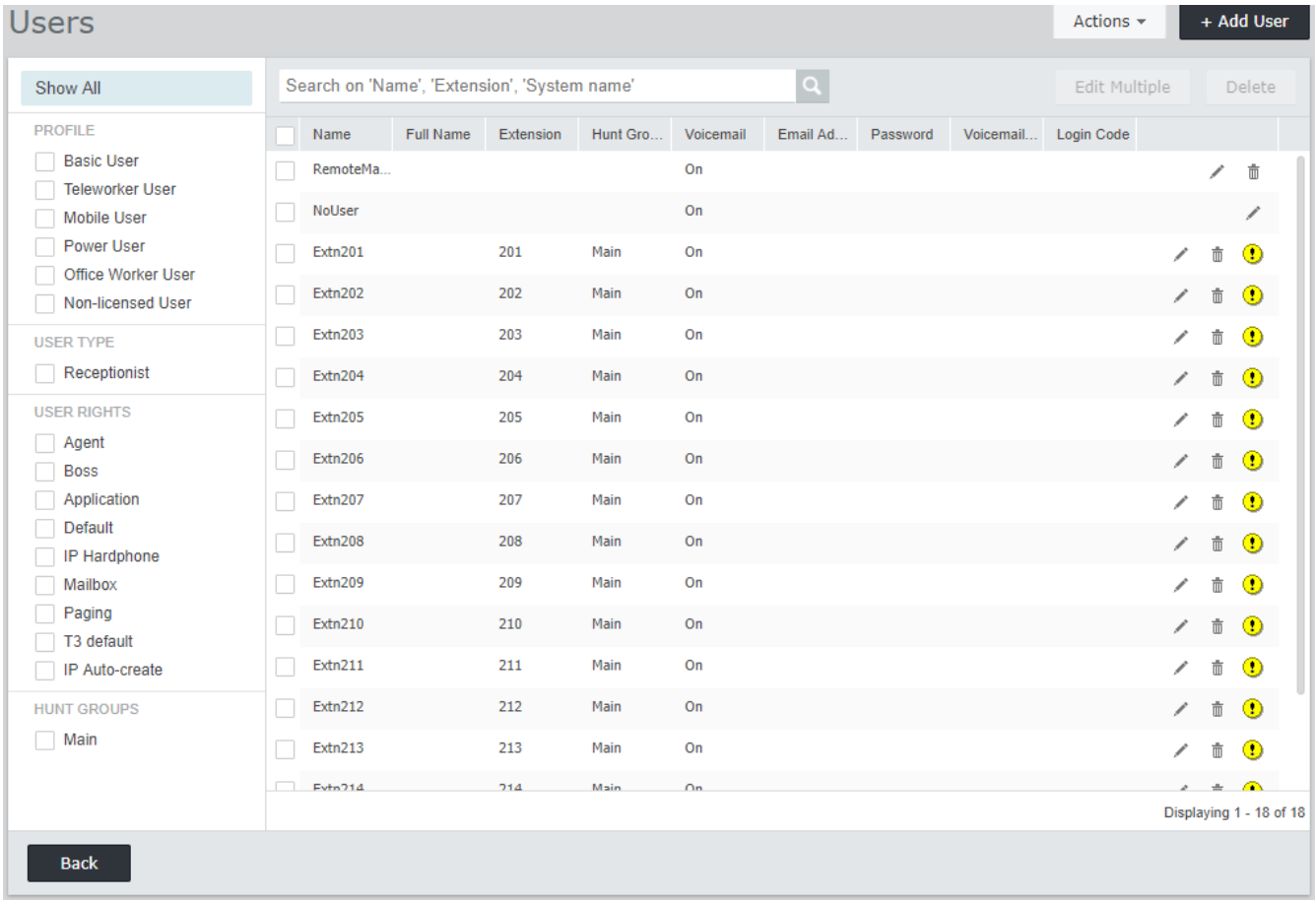
To add a license file:

1. Click **PLDS License** and select **Send To IP Office**.
2. Select the PLDS XML file provided for the system. The file must match the ***PLDS Host ID*** shown on the menu (that host ID is linked to the serial number of the system SD card fitted in the system).
3. Click **OK**. The file is uploaded to the system and replaces any previous license file and the licenses it may have contained.

8.4.5 Users and Extensions

This form displays a list of user in the configuration. For a new IP500 V2 system, a user is automatically created for each physical phone port detected when the system was started.

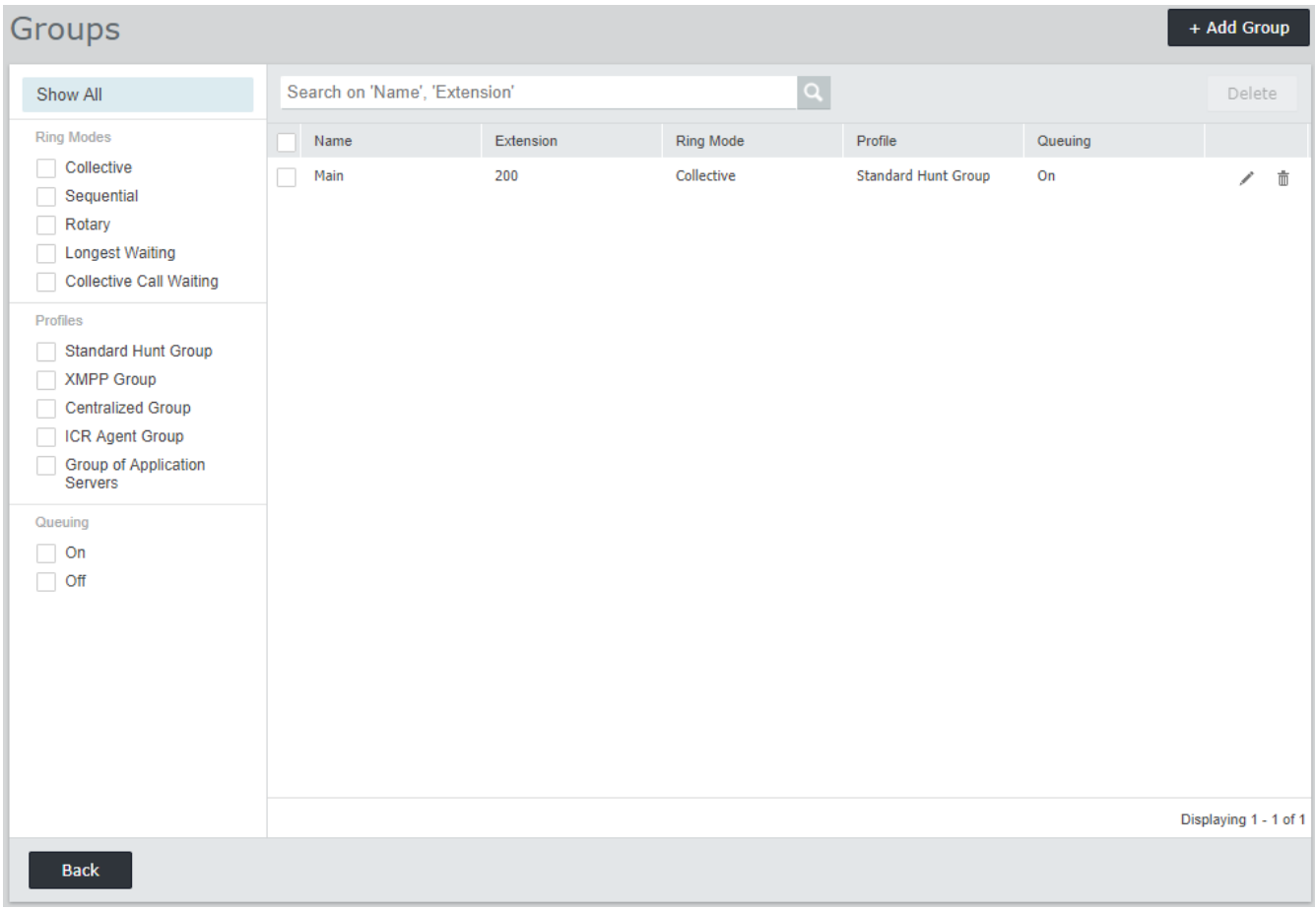
To edit a particular user click on the pencil icon. To add a new user, click **+Add User**. For full details of the user and extension settings refer to the IP Office Web Manager help. As you add users, you can use the panel on the left to filter which users are shown in the list.



8.4.6 Groups

This form displays a list of groups in the configuration. For a new IP500 V2 system, one group, called ***Main*** and with the extension number 200, is automatically added. This group will contain all the phone extensions that were automatically created (one for each physical phone port) when the system was started.

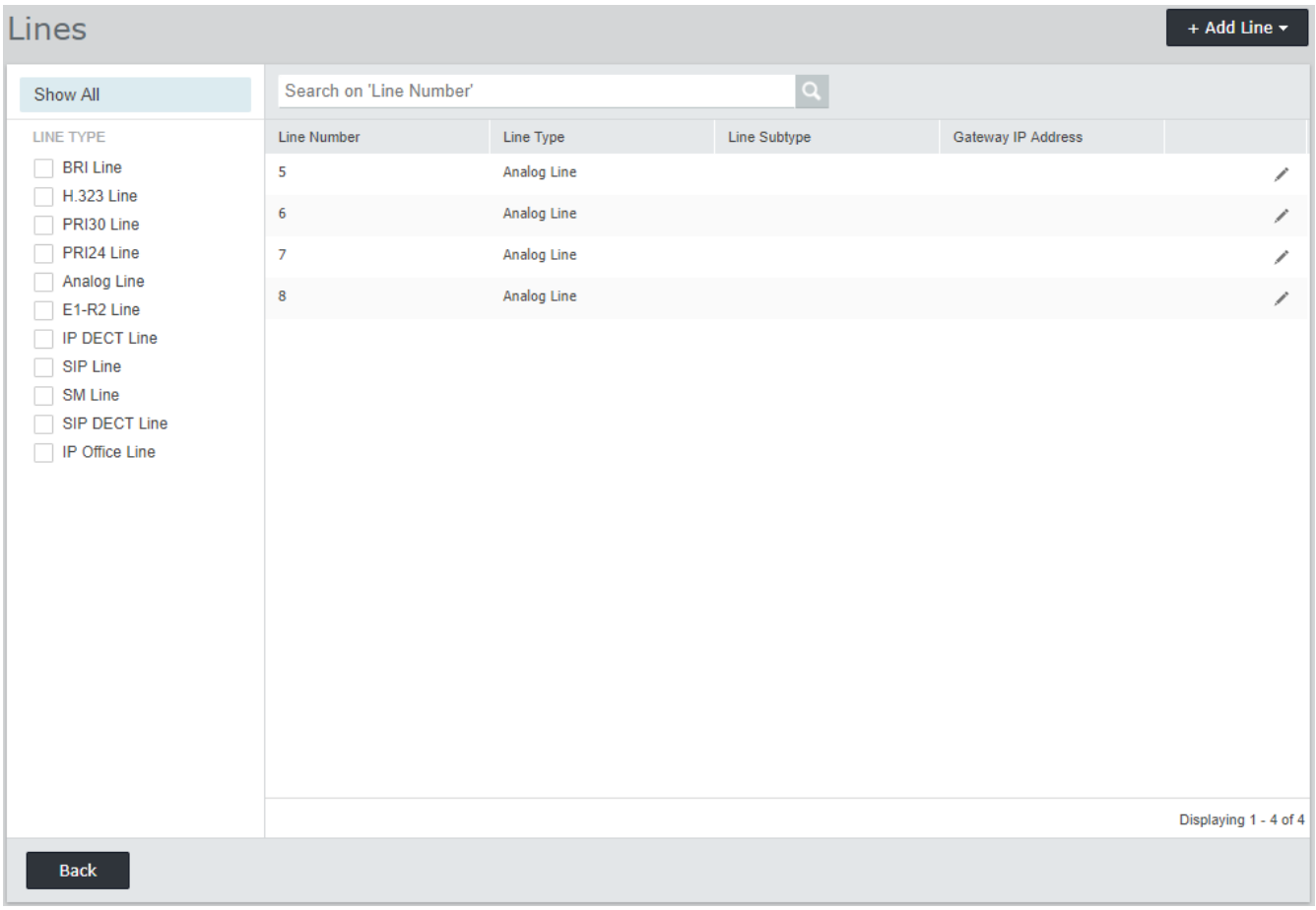
To edit a particular group click on the pencil icon. To add a new group, click **+Add Group**. For full details of the group settings and configuration refer to the IP Office Web Manager help . As you add groups, you can use the panel on the left to filter which groups are shown in the list.



8.4.7 Lines

This form displays a list of all the external lines. For a new IP500 V2 system, the analog, PRI and BRI lines are automatically added with default settings to match the physical line interfaces found in the system when it was started. Other line types need to be added manually.

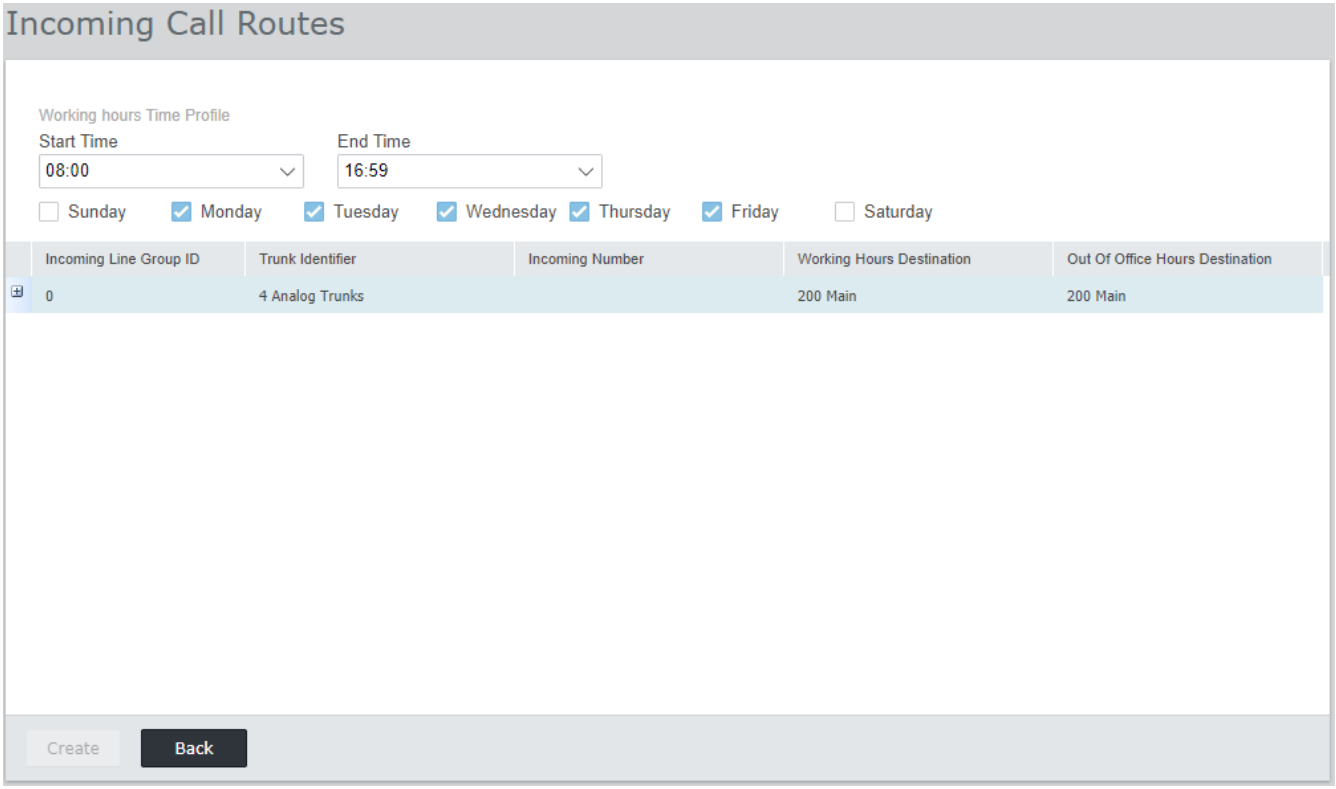
To edit a particular line click on the pencil icon. To add a new line, for example a SIP line, click **+Add Line** and select the line type required. For full details of line settings and configuration refer to the IP Office Web Manager help.



8.4.8 Incoming Call Routes

This part of the dashboard wizard performs two actions:

- Define the days and times for a time profile called **Working Hours**. The default is 08:00 to 16:69 Monday to Friday.
- Select the destinations for the different incoming line group IDs, created through line configuration[127], during and outside the hours defined by the time profile. One entry is shown for each different incoming line group. The destination for each can be set to any user or group extension number or to an auto-attendant name if embedded voicemail auto-attendants have been configured.



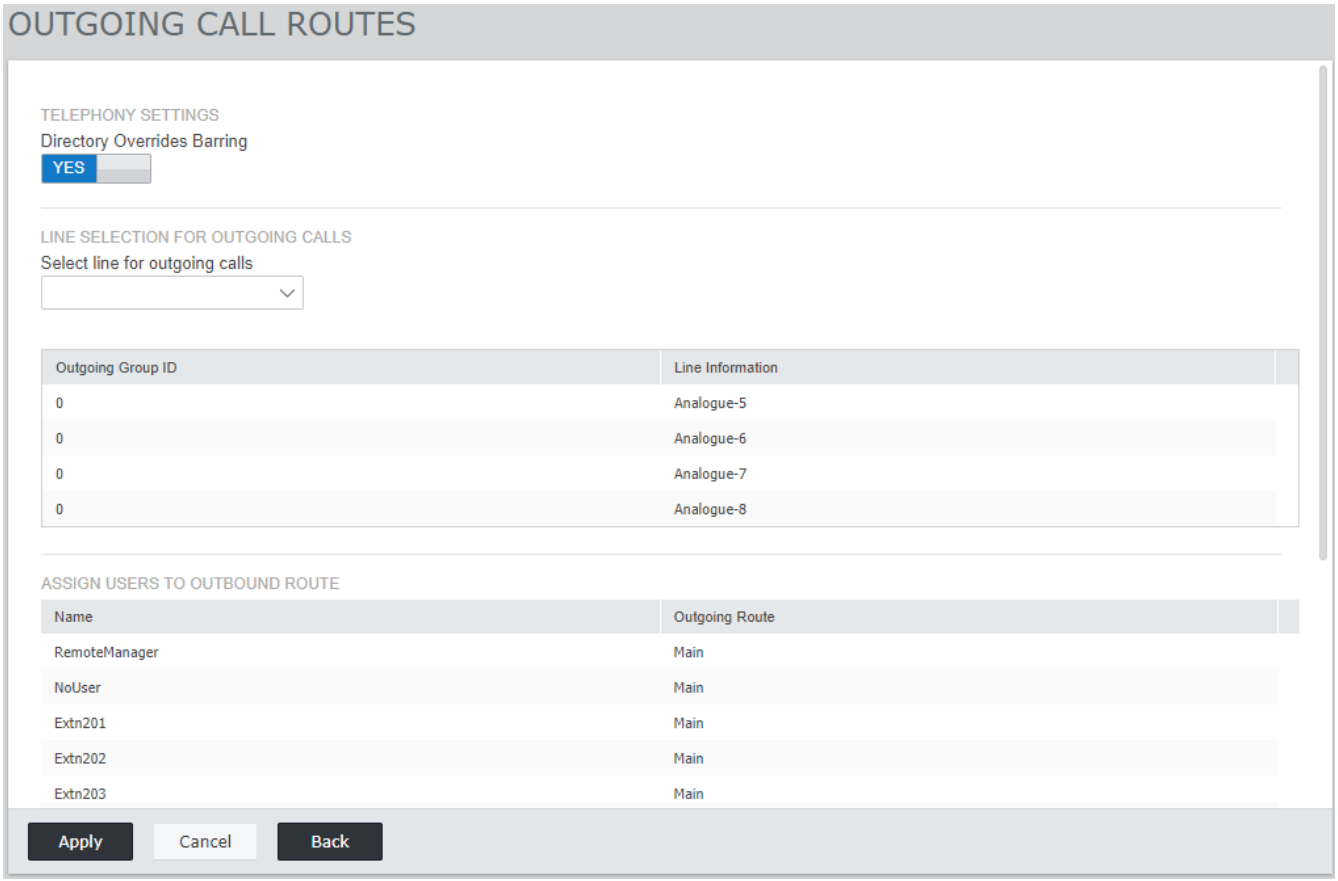
Página2789 de 3226.

8.4.9 Outgoing Call Routes

This dashboard menu is only available on systems where the locale has been set to United States or Canada.

By default the configuration contains one Automatic Route Selection (ARS) entry call ***Main***. All user dialing of external numbers is directed to that ARS entry to determine which lines should carry the outgoing calls (with all lines by default being in line group 0 and that line group used for all calls).

The dashboard wizard add 3 additional ARS entries, called ***Local***, ***National*** and ***International*** respectively.



- **Directory Overrides Barring**
  If enabled, dialing (including speed dials and selection from a directory list) overrides outgoing call barring applied to the user when the number dialed matches a number in the system directory.
- **Select line for outbound calls**
  When click the drop-down lists the available outgoing line group IDs created during line configuration 127. The line group ID selected is applied to all the short codes in the new default ARS entries (***Local***, ***National*** and ***International***) in the configuration.
- **Assign Users to Outbound Route**
  By default each users outgoing calls are routed via the ARS entry Main (this is done by the system short code 9N). This list allows you to select for each users whether their calls should be routed using one of the other default ARS entries (***Local***, ***National*** or ***International***). When a selection is made, a 9N short code with the appropriate ARS destination is added to the user's settings.

Chapter 9.
System Security

9. System Security

The IP Office system and its applications support a range of features for making links between them and users more secure. Full details of the options available are described in the **Avaya IP Office Platform Security Guidelines** 11 manual.

This section covers only some basic changes recommended to help make a new system more secure.

1. **Changing the default security settings** 133
2. **Change the Remote User password** 135
3. **Disabling SIP trunk support** 135
4. **Disabling H.323 telephone support** 135

Additional recommendations:

- If the network to which the IP Office is attached has external public Internet access, that access must be controlled by some additional security devices such as a Firewall and, for VoIP, a Session Border Controller (SBC).
- If LAN2 (the WAN port) is not being used, ensure that it is not connected to the network.

9.1 Changing the Default Security Settings

This process covers the minimal security changes required for the IP Office service run by the server. For full details of all the IP Office security settings, refer to the IP Office Manager help.

To set the initial security configuration:

1. Start IP Office Manager.
2. Select **File | Advanced | Security Settings**.
   - If the **Select IP Office Menu** does not appear, click .
3. Select the server and click **OK**.
4. Enter the administrator user name and password.
5. For a system with default security settings a number of warnings are displayed. Note each warning and click **OK**.
6. Select and change the following passwords:
   a. **System Password**
   This password is used by IP Office Manager for system software upgrades. Click on the **Change** button and enter a new password. Click **OK**.
   b. **Voicemail Password**
   This password is used by the Voicemail Pro server to connect to the IP Office system. When set, the same password also needs to be set in the voicemail server's preferences using the Voicemail Pro client.
   c. **Monitor Password**
   This password is used by the System Monitor application to connect to the IP Office system using UDP or TCP. If not set, the **System Password** set above is used instead.
7. Select **General**.
   a. Enable **Block IP Phone Passcodes**. This stops H.323 and SIP IP phones being registered using passcodes such as 0000 or the same as the extension number.
   b. Check the **IP Office User Details** section. This section defines what security rules are applied to the setting and use of user passwords (other than the voicemail password).
8. The **Application Controls** section indicates a number of unsecure interfaces used by the system. Deselect those that are not required by the planned customer applications. As you select or deselect the controls, the **Application Support** section below changes to show the effect of the change.

Application Control	Used by	Notes
TFTP Server	System Monitor	If disabled, in addition to disabling the other TFTP options below, the system cannot support the network viewer component in the System Monitor application.
TFTP Directory Read	IP DECT	If disabled, DECT operates without the system directory feature.
TFTP Voicemail	Voicemail Pro	Enable only when the system is using a pre-IP Office Release 9.1 voicemail server.
Program Code	IP Office Manager	Used for upgrades from IP Office Manager, recommend disabling when not required.
DevLink	DevLink	
TAPI	TAPI/DevLink	Disable unless the customer site will use TAPI applications with the IP Office.
HTTP Directory Read	one-X Portal for IP Office	Enable only when one-X Portal for IP Office is used. If disabled, one-X Portal for IP Office operates without the personal directory feature.
HTTP Directory Write	one-X Portal for IP Office	Enable only when one-X Portal for IP Office is used. If disabled, one-X Portal for IP Office operates without the personal directory update feature.

9. Click **OK**.
10. Click **Service Users**. By default only the ***Administrator*** and ***EnhTcpaServer*** users are enabled.
    a. Select ***EnhTcpaService***. This service is used by one-X Portal for IP Office. If one-X Portal for IP Office is being installed, we recommend that the password is only changed after that installation is completed. If one-X Portal for IP Office is not being installed:
       - Click on the **Change** button and enter a new password for the service.
       - Click on **Account Status** and selected ***Disabled***.

Página2794 de 3226.

- Click **OK**.

11. Click on the icon to save the security changes.

9.2 Changing the Remote User Password

The IP Office configuration contains a user whose password is used as the default for remote dial in access to the IP Office network. The password of this user should be changed.

To change the remote user password:

1. Start IP Office Manager 68 and connect to the IP Office system.
2. Click on **Users** and in the list of users click on **Remote Manager**.
3. On the **User** tab, enter a new password for the user and click **OK**.
4. Click on the icon and save the updated configuration back to the IP Office system.

9.3 Disabling SIP Trunk Support

The IP Office system supports SIP trunks. If these are not required for the customer installation, we recommend that the system's SIP trunk support is disabled.

To disable SIP trunk support:

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

1. Start IP Office Manager 68 and receive the configuration from the IP Office system.
2. Select **System**.
3. Select **LAN1** and select the **VoIP** tab.
4. Check that **SIP Trunks Enable** is not selected.
5. Repeat the process for **LAN2**.
6. Click on the save icon and save the updated configuration back to the IP Office system.

9.4 Disabling H.323 Telephone Support

The IP Office supports H.323 IP telephones by default. If these are not required for the customer installation, we recommend that the system's H.323 telephone support is disabled.

To disable H.323.telephone support:

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

1. Start IP Office Manager 68 and receive the configuration from the IP Office system.
2. Select **System**.
3. Select **LAN1** and select the **VoIP** tab.
4. Check that **H323 Gatekeeper Enable** is not selected.
5. Check that **H323 Remote Extn Enable** is not selected.
6. Repeat the process for **LAN2**.
7. Click on the save icon and save the updated configuration back to the IP Office system.

Chapter 10.
On-Boarding

10. On-Boarding

On-boarding is a process through which you can register an IP500 V2 system for remote support and maintenance from Avaya. The process of on-boarding is done using the IP Office Web Manager interface.

This section is a short summary of on-boarding. For full details on configure and administer SSL VPN services, see the Avaya IP Office SSL VPN Solutions Guide. You can download the guide from http://support.avaya.com.

Summary Steps

1. Login to IP Office Web Manager
2. **On-Board the System**
   This process has 3 main steps:
   a. **Obtain an Inventory File**
      From the system export a file that contains an inventory of the equipment within the system. This file is required in order to register the system for support.
   b. **Register the System**
      Register the system on the Avaya Global Registration Tool website and upload the system's inventory file. Once the system is registered, an on-boarding file is provided for the system. This file contains configuration settings for the SSL VPN service link.
   c. **Upload an On-Boarding File**
      Upload the on-boarding file to the system. The information within the file is used to update the system's configuration.

Configuration Changes Caused by On-Boarding

When an on-boarding file is uploaded to the IP Office Essential Edition system, it can make a number of changes to the system configuration. It is important to be aware of these potential changes and to ensure that they are not subsequently overwritten or removed.

The changes are as follows. Those marked * are optional and depend on the settings included in the on-boarding file by the service provider.

- **SSL VPN Service**
  A new SSL VPN service is added to the Services section of the configuration.
- **SNMP Alarms***
  SNMP can be configured and two SNMP alarm traps added to the configuration. Note that this will overwrite any existing SNMP settings if SNMP has already been configured.
- **Short Codes***
  Short codes can be added using the ***Set Hunt Group Night Service*** and ***Clear Hunt Group Night Service*** actions. These can be used to enable and disable the SSL VPN service.
- **IP Route***
  A static IP route to the SSL VPN service can be added to the IP routes in the configuration.
- **Security Certificate**
  A security certificate for the SSL VPN service is added to the system's security settings.

Página2799 de 3226.

10.1 On-Boarding

1. Login to IP Office Web Manager[71].
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions** and select **On-boarding**. The On-boarding menu is displayed.
   - **Are you using TAA series hardware?**
     Systems purchased under US Federal Acquisition Regulations (FAR) must comply with the requirements of the Trade America Act (TAA). For various items of IP Office hardware there are TAA compatible variants. Select this option if the IP Office system includes TAA hardware[296]. This is usually indicated by TAA appearing on the label on the back of the system control unit.
3. Click **Get Inventory File** to to download an inventory.xml file for the system. When you register the IP Office system for remote support, the inventory file is required as part of the registration and is uploaded to the Avaya Global Registration Tool (GRT) where the inventory data is populated in the Avaya Customer Support (ACS) database.
4. Click **Register IP Office** to register the system with the the Avaya Global Registration Tool (GRT) website.
5. Once the system is registered, you can download an on-boarding file for the system from the Avaya Global Registration Tool website. This file contains the settings required to establish an SSL VPN connection between the IP Office system and an Avaya VPN Gateway (AVG) server.
6. Use the **On-boarding File Upload** section to upload the on-boarding file to the system.

Página2800 de 3226.

Chapter 11.
SD Card Management

11. SD Card Management

The IP500 V2 control unit has two SD card slots, labeled **System SD** and **Optional SD** respectively. These are used as follows:

- **System SD Card**
  An Avaya System SD card must be present in this slot at all times. This card holds copies of the IP Office firmware and configuration and is used as the IP500 V2 control units non-volatile memory.
  - Each Avaya System SD card has a unique serial number which is used for generating and validating licenses.
  - The card stores the prompts for Embedded Voicemail operation and acts as the message store for Embedded Voicemail messages.
  - Prior to any planned shutdown or restart of the IP Office system, the current configuration running in the IP Office system's RAM memory is copied to the **/primary** folder on the System SD card and to the systems non-volatile memory.
  - Following a restart, the software in the **/primary** folder is loaded by the IP500 V2 control unit. If the required software is not present or valid a sequence of fallback options is used, see Booting from the SD Cards 144 for full details.
  - Following a restart, if present, the configuration file in the **/primary** folder is loaded by the IP500 V2 control unit. If no file is present the system will check for a file in its internal non-volatile memory. If no copy is found it will generate a default configuration file. See Booting from the SD Cards 144 for full details.
  - Once each day (approximately between 00:00 and 00:30) the IP Office will copy the current configuration running in its RAM memory to the **/primary** folder on the card.
  - Configuration changes made using IP Office Manager are first written to the copy of the configuration file on the card and then merged with the configuration running in the IP Office system's RAM memory.
  - The write lock setting on cards in the System SD card slot is ignored.
- **Optional SD Card**
  A card does not have to be present in this slot for normal IP Office operation. The slot can be used for various maintenance actions.
  - A card with an updated IP Office software or configuration can be inserted and those files then transferred to the System SD card in order to upgrade the IP Office system.
  - The full contents of the System SD card can be copied to the Optional SD card while the IP Office system is running.
  - The write lock setting on cards in the Optional SD card slot is honored.

Card Removal	Memory cards should always be shutdown 157 before being removed when the system is running. Though the card slot LEDs indicate when data is being written to an card, lack of flashing LED is not a sufficient safeguard. Shutting down the card disables Embedded Voicemail and IP Office Web Manager. If the **System SD** card is removed, features licensed by the card's serial number continue operating for up to 2 hours.

Card Specification

Non-Avaya cards can be used in the **Optional SD** slot as long as they match or exceed the standard below:

- SDHC 4GB minimum Class 2+. Single partition FAT32 format. (Avaya IP Office SD cards are 8GB, older cards were 4GB.)

SD Card Folders

The **System SD** card **/system** folder contains the following sub-folders:

- **/primary**
  Contains the firmware files for the IP Office control unit, external expansion modules and supported phones. The folder can also contain music on hold files and license key files. This is the main set of files used by the IP Office system when booting up. Also contains the stored copy of the IP Office configuration.
- **/backup**
  Contains a copy of the primary folder at some previous point. A backup copy of the primary contents to this folder can be invoked manually (using IP Office Manager or SSA) or as part of the IP Office software upgrade using IP Office Manager.
- **/backup_apl**
- **/lvmail**
  Contains the system prompts used by Embedded Voicemail. Note that the mailbox messages and greetings are stored in a sub-folder of the **/dynamic** folder.
    - The sub-folder **/AAG** is used to store Embedded Voicemail auto-attendant greetings.
- **/doc**
  Contains initial installation documentation for the system.
- **/dynamic**
  Contains files used by the IP Office and retained through a reboot of the IP Office system.
    - The sub-folder **/lvmail** is used to store individual user and group mailbox messages, name recordings and announcements. The storage capacity for Embedded Voicemail is limited to 25 hours regardless of the capacity of the card.
- **/temp**
  Contains temporary files used by the IP Office and not retained through a reboot of the IP Office system.
- **/ws**

The **Optional SD** card can contain a similar set of folders. These are used as an additional backup or they can be used as the source for upgrading the contents of the System SD card.

Página2804 de 3226.

11.1 Booting from the SD Cards

When being powered up, the IP500 V2 control unit looks for a valid ip500v2.bin binary file to load. It does this using the possible source below in the order shown, skipping to the next source if the file is not present or is not valid.

1. System SD card ***/primary*** folder.
2. The control unit's own internal non-volatile memory. Once a system has been installed, it uses its non-volatile memory to keep copies of the configuration and system binary files it is using. These can be used to restore operation during a system reboot. Note that though a system can boot from non-volatile memory, a System SD card must still be present for correct system operation.
3. System SD card ***/backup*** folder.
4. Optional SD card ***/primary*** folder.
5. Optional SD card ***/backup*** folder.
6. If no file is found, the control unit will fallback to making BOOTP requests to the network. IP Office Manager can respond the BOOTP request. See Erasing the Operational Firmware 199.

Once a valid ip500v2.bin file is found, the IP Office control unit will load that firmware. The source from which the control unit binary file was loaded is then used to load further files.

Configuration File Loading

Having installed the necessary system firmware files as above, the IP500 V2 control unit requires a configuration file:

- If the IP500 V2 booted using binary files from an SD card location, it looks for a valid configuration file in the same location.
  - If a configuration file is present and valid, it is loaded.
  - If a configuration file is present but is not valid, load the configuration copy in its non-volatile memory if present, else it assumes a default configuration.
  - If a configuration file is not present, use the non-volatile memory copy as above unless the reboot is as a result of a default system command.
- If the IP500 V2 booted using binary files from its non-volatile memory, it will also load the configuration copy from that location.
  - It will indicate a boot alarm (see below).
  - It will attempt to restore the firmware file in the System SD card's **/primary** folder using the copy in its non-volatile memory.
  - The normal boot up process of upgrading expansion module firmware does not occur. If the **File | Advanced | Upgrade** command is used, only external expansion modules actually present in the system are listed for upgrade.

Post Boot Operation

During normal operation, configuration and binary files sent to the System SD card **/primary** folder using IP Office Manager are also written to the non-volatile memory.

If the system has booted from its non-volatile memory due to an SD card problem, it is still possible to upgrade the ip500v2.bin file using the IP Office upgrade wizard.

Boot Alarms

The following apply if the IP500 V2 boots using software other than that in its System SD **/primary** folder:

- An alarm will be shown in the System Status Application. It will also generate an alarm if the card in any slot is not compatible. These alarms are also output as SNMP, Syslog or email alarms.
- The IP Office Manager **Select IP Office** menu will display an ⚠ icon indicating that the IP Office system is running using software other than from the System SD card's primary folder.
- The configuration can be read but will be read only. Attempting to send a configuration to the system will cause the error message ***Failed to save configuration data. (Internal error)***.

Bypassing the System SD Card Primary Folder

The control unit can be forced to bypass the System SD card's ***/primary*** folder and non-volatile memory when starting. This is done by pressing the **Aux** button while applying power to the control unit.

This action may be necessary if, following an upgrade of the IP Office system, it is determined that a roll back to the previously backed up firmware and configuration is required. Using the **Aux** button should restore system operation using the ***/backup*** folder files while the installer then restores the contents of the ***/primary*** folder to a previous release.

11.2 Creating an IP Office SD Card

The processes below can be applied to Avaya IP Office SD cards. They can also be applied to non-Avaya SD cards for use in a system's Optional SD card slot. For the System SD slot, only Avaya System SD cards should be used.

The card must be the following format.

- SDHC 4GB minimum Class 2+. Single partition FAT32 format. (Avaya IP Office SD cards are 8GB, older cards were 4GB.)
- ⚠ **WARNING**
  Avaya supplied SD cards should not be formatted using any other method than the format commands within IP Office Manager and System Status Application. Formatting the cards using any other method removes the serial number used for IP Office licensing from the card.
- **! Warning: IP Office Manager Version**
  This process uses software files provided by the installed version of IP Office Manager being used. You must ensure that the version of IP Office Manager used matches the version of software required.
    - **Admin Lite Not Supported**
      Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).

Creating a Card on a Local PC

These processes can be run on an SD card inserted in a card reader on the IP Office Manager PC. That card can then be used in the System SD card slot of a new system or in the Optional SD card slot of an existing system to upgrade that system.

Formatting an SD Card

Avaya SD cards should only be formatted using the format options provided within IP Office applications. This process is not normally necessary with Avaya SD cards unless you suspect that the card has been incorrectly formatted elsewhere.

- ⚠ **WARNING: All File Will Be Erased**
  Note that this action will erase any existing files and folders on the card. Once a card has been formatted, the folders and files required for IP Office operation can be loaded onto the card from the IP Office Manager PC using the Recreate IP Office SD Card command.

1. Insert the SD card into a reader slot on the IP Office Manager computer.
2. Using IP Office Manager, select **File | Advanced | Format IP Office SD Card**.
3. Select **IP Office A-Law** or **IP Office U-Law**. This selection just sets the card label shown when viewing the card details. It does not affect the actual formatting. Select the label that matches the files set you will be placing on the card.
4. Browse to the card location and click **OK**.
5. The status bar at the bottom of IP Office Manager will display the progress of the formatting process.
6. When the formatting is complete, you can use the **Recreate IP Office SD Card** command to load the IP Office folders and files onto the card from the IP Office Manager PC.

Recreating an IP Office SD Card

You can use IP Office Manager to update the set of files on an System SD card to match those expected for the particular IP Office release. This can be used to upgrade the card from an existing system or to prepare the card for a new system.

IP Office Manager updates the card with the binary firmware files for the control unit, external expansion modules and phones. It also includes the prompt files for embedded voicemail operation and an option for the web manager application files.

Existing files such as the system configuration, PLDS license file and embedded voicemail messages and greetings are retained.

- For the card to be used in an control unit's **System SD** card slot it must be Avaya System SD card. The card must be correctly formatted (that can be done using IP Office Manager), however a reformat of an existing working card is not necessary before using recreate to update the card contents.
- The source for the files copied to the SD card are the sub-folders of the ***\Memory Cards*** folder under Manager's applications **Working Directory** (normally ***C:\Program Files(x86)\Avaya\IP Office\Manager***). However, if the **Working Directory** is changed to a location without an appropriate set of ***\Memory Cards*** sub-folders, the required set of files will not be copied onto the SD card.
    - **! WARNING: Installing PCS14 and earlier control units**
      PCS 296 14 or lower units must first install Release 8.1(65) (or higher 8.1) or any Release 9.0 and then upgrade to Release 9.1. Care should be taken to ensure that no calls are made before the upgrade to Release 10.0, otherwise the system will require an 10.0 upgrade license despite being "new". The PCS of the control unit is printed on the label on the back of the control unit.

Setting the Initial System Software Level

When the control unit makes its first call, the version of software it is running is written to a permanent record on the control unit. This becomes the base level of the control unit when considering the future requirements for upgrade licenses, etc. Therefore, for a new system it is important that you upgrade the System SD card to the required software version before starting the system.

Determining the System SD card software level

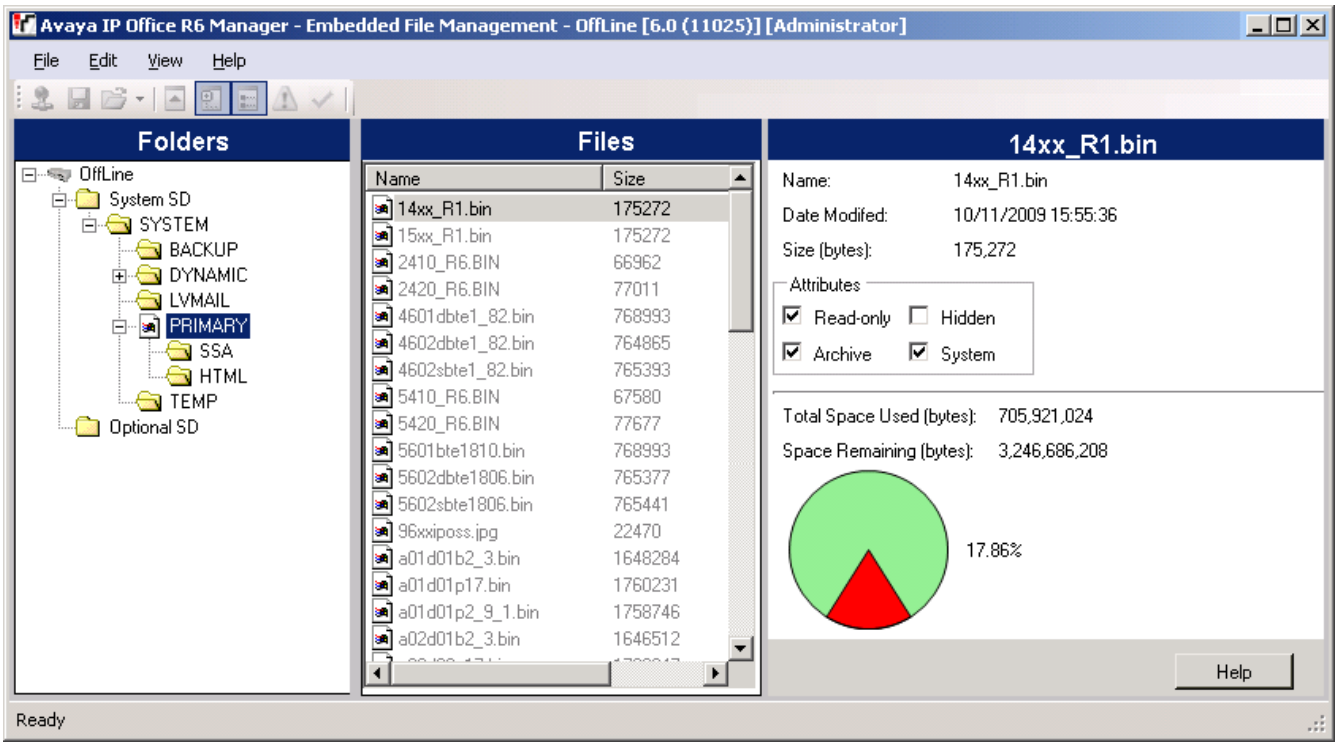
On the SD card, in the ***system/primary*** folder, locate and open the ***filelist.txt*** file. The header section at the start of the file ends with the version of the set of files previously copied onto the card. The remainder of the file lists the actual files.

To upgrade/recreate a System SD card

1. Once started do not interrupt this process, for example by removing the SD card. This process takes approximately 20 minutes.
2. Insert the SD card into a card reader on the IP Office Manager PC.
3. Using IP Office Manager, select **File | Advanced | Recreate IP Office SD Card**.
4. Select **IP Office A-Law** or **IP Office U-Law**. This selection affects how the IP Office systems operates when defaulted with this card present in its **System SD** card slot.
5. Browse to the card location and click **OK**.
6. IP Office Manager will prompt whether you want to include Avaya IP Office Web Manager files as part of the recreate process. Those files are necessary if you want to run IP Office Web Manager 71 to manage the IP Office system into which the card is loaded or if you want to use on-boarding 138.
7. IP Office Manager will start creating folders on the SD card and copying the required files into those folders. This process will take approximately 20 minutes.
8. Do not remove the SD card during the process. Wait until the IP Office Manager displays a message.

11.3 Viewing the Card Contents

Using IP Office Manager you can view the folders and files on the System SD card and the Optional SD card. You can then use various commands to upload and download files to and from the cards.



1. Using IP Office Manager, select **File | Advanced | Embedded File Management**.
2. Using the **Select IP Office** menu, select the IP Office system.
3. The file contents of the memory cards are displayed.

11.4 Backing Up to the Backup Folder

This process copies the contents of the **/primary** folder on the System SD card over the **/backup** folder on the same card. Any files with matching file names are replaced. This takes approximately 6 minutes. For methods to restore from the **/backup** folder see Restore from the Backup Folder 150.

These processes do not backup the prompts, messages and greetings used by the system's voicemail mailboxes and auto attendants. They are stored in the card's **/lvmail** and **/dynamic/lvmail** folders.

11.4.1 Backup to the Backup Folder Using IP Office Manager

To backup to the /backup folder using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | Embedded File Management**.
2. Using the **Select IP Office** menu, select the IP Office system.
3. The file contents of the memory cards are displayed.
4. Select **File | Backup System Files**.
   - The contents of the **/primary** folder on the System SD card will be copied to the **/backup** folder. This process takes approximately 6 minutes.

11.4.2 Backup to the Backup Folder Using System Status Application

To backup to the /backup folder using the System Status Application

1. Start System Status 69 and access the IP Office's status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Backup System Files**.
   - The contents of the **/primary** folder on the System SD card will be copied to the **/backup** folder. This process takes approximately 6 minutes.

11.4.3 Backup to the Backup Folder Using a System Phone

This process can be used by a user configured as a System Phone user and using a 1400, 1600, 9500 or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's **Login Code** is used to restrict access to the system administration functions on the phone.

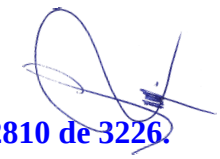
To backup to the /backup folder using a System Phone

1. Select **Features | Phone User | System Admin**.
2. Enter your IP Office user login code.
3. From the menu select **Memory Card**.
4. Select **System Backup**.
   - The contents of the **/primary** folder on the System SD card will be copied to the **/backup** folder. This process takes approximately 6 minutes.

11.4.4 Backup to the Backup Folder Using a IP Office Web Manager

To backup to the /backup folder using IP Office Web Manager

1. Login to IP Office Web Manager 71.
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions** and select **Backup**.
2. For the destination select ***On Device***.
3. Click **Backup**.



Página2810 de 3226.

11.5 Restoring from the Backup Folder

The contents of the **/backup** folder on the System SD card can be copied to the **/primary** folder on the same card. Any files with matching file names are replaced. The system then restarts using the files in the **/primary** folder.

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

11.5.1 Restoring from the Backup Folder Using IP Office Manager

To restore from the /backup folder using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | Embedded File Management**.
2. Using the **Select IP Office** menu, select the IP Office system.
3. The file contents of the memory cards are displayed.
4. Select **File | Restore System Files**.
   - The contents of the **/backup** folder on the System SD card are copied to the **/primary** folder. The process takes approximately 6 minutes.
   - When the process has been completed, the system restarts.

11.5.2 Restoring from the Backup Folder Using System Status Application

To restore from the /backup folder using System Status Application

1. Start System Status 69 and access the IP Office's status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Restore System Files**.
   - The contents of the **/backup** folder on the System SD card are copied to the **/primary** folder. The process takes approximately 6 minutes.
   - When the process has been completed, the system restarts.

11.5.3 Restoring from the Backup Folder Using a System Phone

This process can be used by a user configured as a System Phone user and using a 1400, 1600, 9500 or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's **Login Code** is used to restrict access to the system administration functions on the phone.

To restore from the /backup folder using a System Phone

1. Select **Features | Phone User | System Admin**.
2. Enter your IP Office user login code.
3. From the menu select **Memory Card**.
4. Select **System Restore**.
   - The contents of the **/backup** folder on the System SD card are copied to the **/primary** folder. The process takes approximately 6 minutes.
   - When the process has been completed, the system restarts.

11.5.4 Restoring from the Backup Folder Using IP Office Web Manager

To restore from the /backup folder using IP Office Web Manager

1. Login to IP Office Web Manager 71 .
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions** and select **Restore**.
2. For the destination select ***On Device***.
3. Click **Restore**.

Página2811 de 3226.

11.6 Backing Up to the Optional SD Card

This process copies all files on the System SD card to the Optional SD card. It includes the **/primary** and **/backup** folders and the Embedded Voicemail files including message files. Any matching files and folders on the Optional SD card are overwritten.

The process is a simple copy. Any files already copied that change while the process are not recopied. Any new files addedwhile the process is running, for example voicemail messages, may not be copied.

This process takes at least 90 minutes and may take much longer depending on the amount of data to be copied, for example it will be longer if Embedded Voicemail is being used by the IP Office system to take messages.

11.6.1 Backing Up to the Optional SD Using IP Office Manager

To backup the System SD card to the Optional SD card using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | Embedded File Management**.
2. Using the **Select IP Office** menu, select the IP Office system.
3. The file contents of the memory cards are displayed.
4. Select **File | Copy System Card**.
   - The contents of the System SD card will be copied to the Optional SD card. This process at least 90 minutes and can take much longer.

11.6.2 Backing Up to the Optional SD Using System Status Application

To backup the System SD card to the Optional SD card using System Status Application

1. Start System Status 69 and access the IP Office's status output.
2. In the navigation panel select **System**.
3. Select **Memory Cards**.
4. Select **System Card**.
5. At the bottom of the screen select **Copy System Card**.
   - The contents of the System SD card will be copied to the Optional SD card. This process at least 90 minutes and can take much longer.

11.6.3 Backing Up to the Optional SD Using IP Office Web Manager

To backup the System SD card to the Optional SD card using IP Office Web Manager

1. Login to IP Office Web Manager 71.
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions**. Select **Service Commands** and select **Copy to Optional SD**.
3. Click **OK**.

11.6.4 Backing Up to the Optional SD Using a System Phone

This process can be used by a user configured as a System Phone user and using a 1400, 1600, 9500 or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's **Login Code** is used to restrict access to the system administration functions on the phone.

To backup the System SD card to the Optional SD card using a System Phone

1. Select **Features | Phone User | System Admin**.
2. Enter your IP Office user login code.
3. From the menu select **Memory Card**.
4. Select **Copy**.
   - The contents of the System SD card will be copied to the Optional SD card. This process at least 90 minutes and can take much longer.

Página2813 de 3226.

11.7 Restoring a Configuration from an Optional Card

The following processes copy the configuration file (***config.cfg***) and licenses file (***keys.txt***). The processes take a few seconds.

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

11.7.1 Restoring from the Optional SD Using IP Office Manager

To copy a configuration file from the Optional SD card using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | Embedded File Management**.
2. Using the **Select IP Office** menu, select the IP Office system.
3. The file contents of the memory cards are displayed.
4. Select **File | Upgrade Configuration**.
   - The configuration file (***config.cfg***) and licenses file (***keys.txt***) in the ***/primary*** folder on the Optional SD card are copied to the ***/primary*** folder on the System SD card. This process takes approximately a few seconds.
   - When the process has been completed, the IP Office system will be restarted.

11.7.2 Restoring from the Optional SD Using a System Phone

This process can be used by a user configured as a System Phone user and using a 1400, 1600, 9500 or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's **Login Code** is used to restrict access to the system administration functions on the phone.

To copy a configuration file from the Optional SD card using a System Phone

1. Select **Features | Phone User | System Admin**.
2. Enter your IP Office user login code.
3. From the menu select **Memory Card**.
4. Select **Upgrade Config...**.
   - The configuration file (***config.cfg***) and licenses file (***keys.txt***) in the ***/primary*** folder on the Optional SD card are copied to the ***/primary*** folder on the System SD card. This process takes approximately a few seconds.
   - When the process has been completed, the IP Office system will be restarted.

Página2814 de 3226.

11.8 Loading Software from an Optional SD Card

These processes copy all files in the folder except the configuration file (***config.cfg***) and licenses file (***keys.txt***). The processes take approximately 5 minutes. These process do not restore Embedded Voicemail prompts (see Upgrading Card Software 156).

- **! IP Office Technical Bulletins**
  You must obtain and read the IP Office Technical Bulletin relating to the IP Office software release which intend to install. The bulletin contains important information that may not have been included in this manual. IP Office Technical Bulletins are available from the Avaya support website *(http://support.avaya.com)*.

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

11.8.1 Loading Software from the Optional SD Using IP Office Manager

To copy software files from the Optional SD card using IP Office Manager

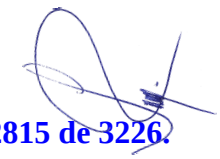
1. Using IP Office Manager, select **File | Advanced | Embedded File Management**.
2. Using the **Select IP Office** menu, select the IP Office system.
3. The file contents of the memory cards are displayed.
4. Select **File | Upgrade Binaries**.
   - The software files (all files in the folder except the configuration file (***config.cfg***) and licenses file (***keys.txt***)) in the ***/primary*** folder on the Optional SD card are copied to the ***/primary*** folder on the System SD card. This process takes approximately 5 minutes.
   - When the process has been completed, the IP Office system will be restarted.

11.8.2 Loading Software from the Optional SD Using a System Phone

This process can be used by a user configured as a System Phone user and using a 1400, 1600, 9500 or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's **Login Code** is used to restrict access to the system administration functions on the phone.

To copy software files from the Optional SD card using a System Phone

1. Select **Features | Phone User | System Admin**.
2. Enter your IP Office user login code.
3. From the menu select **Memory Card**.
4. Select **Upgrade Binaries...**.
   - The software files (all files in the folder except the configuration file (***config.cfg***) and licenses file (***keys.txt***)) in the ***/primary*** folder on the Optional SD card are copied to the ***/primary*** folder on the System SD card. This process takes approximately 5 minutes.
   - When the process has been completed, the IP Office system will be restarted.



11.9 Backing Up to a PC

This process copies the **/backup** folder on the System SD card to a folder specified on the PC running IP Office Web Manager. This process takes approximately 25 minutes.

Before using this process, the contents of the /Backup folder can be updated with the files from the /primary folder on the same card. See Backing Up to the Backup Folder 149.

To backup to a PC using IP Office Web Manager

1. Login to IP Office Web Manager 71.
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions** and select **Backup**.
3. For the destination select ***Client Machine***.
4. Click **Configure Path**.
5. Select the location for the backup and click **Open**. We recommend that you create a new folder and then select that folder.
6. Click **Start Backup**.
7. Wait until a backup completed message is displayed. Click **Cancel** to close the menu.

11.10 Restoring from a PC

This process restores a previous backup, overwriting the /primary folder on the System SD card.

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

To restore from a PC backup using IP Office Web Manager

1. Login to IP Office Web Manager 71.
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions** and select **Restore**.
3. Click **Restore from** and select ***Client Machine***.
4. Click **OK**.
5. Click **Configure Path**.
6. Select the folder containing the previous backup and click **Open**.
7. Click **Start Restore**.
8. Wait until a restore completed message is displayed. Click **Cancel** to close the menu. The system reboots.

Página2816 de 3226.

11.11 Upgrading Card Software

In addition to using the traditional IP Office Upgrade Wizard[181], IP500 V2 control units can be upgraded by loading the required set of firmware files onto the System SD card and rebooting the system.

- **! IP Office Technical Bulletins**
  You must obtain and read the IP Office Technical Bulletin relating to the IP Office software release which intend to install. The bulletin contains important information that may not have been included in this manual. IP Office Technical Bulletins are available from the Avaya support website *(http://support.avaya.com)*.

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

There are a number of ways in which this can be done.

Method	Description	Location	Software Files	Embedded Voicemail Prompts
System SD Card Upgrade[183]	In this method, the System SD card is shut down and removed from the control unit. The card's contents are upgraded using IP Office Manager.	**Local**	✓	✓
Upgrade from Optional SD Card[184]	This method uses an SD card loaded with the required version of IP Office software. The card is inserted into the control unit's Option SD card slot and its contents copied to the System SD card.	**Local**	✓	–

11.12 Memory Card Shutdown/Removal

Before a memory card is removed from an IP Office system that is running, the card must be shutdown. Removing a memory card while the system is running may cause file corruption. Card services can be restarted by either reinserting the card or using a Start Up command[158].

11.12.1 Shutdown a Card Using IP Office Manager

To shutdown a memory card using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | Memory Card Commands | Shutdown**.
2. Using the **Select IP Office** menu, select the IP Office system containing the memory card.
3. Click **OK**.
   - At the back of the control unit, confirm that the appropriate memory card LED is off.
   - The card can now be removed in order to perform the necessary maintenance actions.

11.12.2 Shutdown a Card Using System Status Application

To shutdown a memory card using System Status Application

1. Start System Status[69] and access the IP Office's status output.
2. In the navigation panel select **System**.
3. Select **Memory Cards**.
4. Select either **System Card** or **Optional Card**.
5. At the bottom of the screen select **Shutdown**.
   - At the back of the control unit, confirm that the appropriate memory card LED is off.
   - The card can now be removed in order to perform the necessary maintenance actions.

11.12.3 Shutdown a Card Using IP Office Web Manager

To shutdown a card using IP Office Web Manager

1. Login to IP Office Web Manager[71].
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions**. Select **Service Commands** and select **Memory Card Stop**.
3. Select the card to stop and click **OK**.

11.12.4 Shutdown a Card Using a System Phone

This process can be used by a user configured as a System Phone user and using a 1400, 1600, 9500 or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's **Login Code** is used to restrict access to the system administration functions on the phone.

To shutdown a card using a System Phone

1. Select **Features | Phone User | System Admin**.
2. Enter your IP Office user login code.
3. From the menu select **Memory Card**.
4. Select **System** for the System SD card or **Option** for the Optional SD card.
5. Select **Shutdown**.
   - At the back of the control unit, confirm that the appropriate memory card LED is off.
   - The card can now be removed in order to perform the necessary maintenance actions.

Página2818 de 3226.

11.13 Memory Card Startup

Reinserting a memory card into a system that is already switched on automatically restarts card operation. However, if the card has been shutdown[157] but not removed, it can be restarted using IP Office Manager without requiring a reboot.

11.13.1 Startup a Card Using IP Office Manager

To startup a card using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | Memory Card Commands | Startup**.
2. Using the **Select IP Office** menu, select the IP Office system containing the memory card.
3. Click **OK**.

11.13.2 Startup a Card Using System Status Application

To startup a card using System Status Application

1. Start System Status[69] and access the IP Office's status output.
2. In the navigation panel select **System**.
3. Select **Memory Cards**.
4. Select either **System Card** or **Optional Card**.
5. At the bottom of the screen select **Start Up**.

11.13.3 Startup a Card Using IP Office Web Manager

To startup a card using IP Office Web Manager

1. Login to IP Office Web Manager[71].
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions**. Select **Service Commands** and select **Memory Card Start**.
3. Select the card to start and click **OK**.

11.13.4 Startup a Card Using a System Phone

This process can be used by a user configured as a System Phone user and using a 1400, 1600, 9500 or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's **Login Code** is used to restrict access to the system administration functions on the phone.

To startup a card using a System Phone

1. Select **Features | Phone User | System Admin**.
2. Enter your IP Office user login code.
3. From the menu select **Memory Card**.
4. Select **System** for the System SD card or **Option** for the Optional SD card.
5. Select **Startup**.

Chapter 12.
Additional Processes

12. Additional Processes

This section covers a range of maintenance processes.

Processes

- Changing an IP Office Basic Edition system to standard mode 161
- Switching off a system/System shutdown 163
- Rebooting a system 165
- Changing components 167
- Defaulting the configuration 170
- Default the security settings 173
- Loading a new configuration file 177
- Swapping extension users 186
- Upgrading systems 180
- Out of building telephone installation 36
- Using the external output port 191
- SNMP configuration 192
- Reset button 197
- AUX button 197
- RS232 port maintenance 198
- Erasing the core software 199
- Enabling IP Office Web Manager 202

Other Processes

The following additional maintenance processes are covered in other sections of this document:

- Creating an IP Office SD card 146
- Viewing card contents 148
- Backing up the configuration 149
- Restoring the configuration 150
- Copying to the Optional SD card 152
- Restoring from the Optional SD card 153
- Memory card shutdown/removal 157
- Memory card startup 158
- On-boarding 138
- Installing the administration applications 64

Página2821 de 3226.

12.1 Changing an IP Office Basic Edition System to Standard Mode

The process below will change the mode of the system and default its configuration.

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

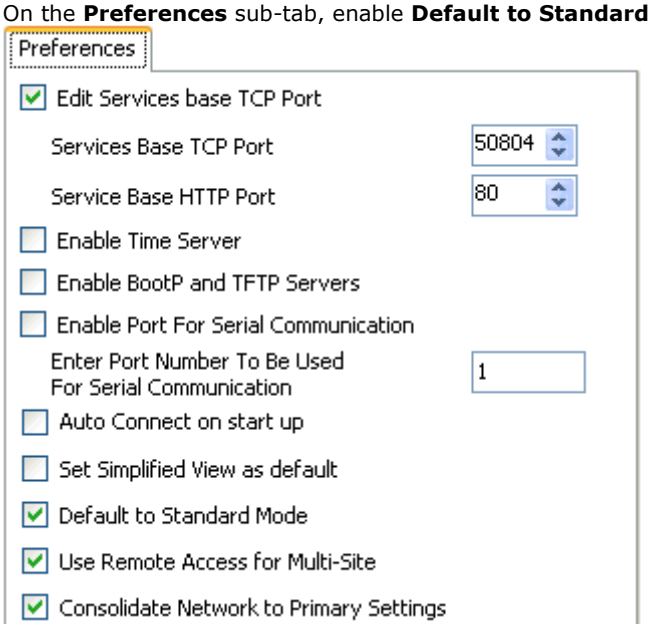
1. Using IP Office Manager, receive the configuration from the system 68 .
2. When requested, enter the service user name and password.
3. The IP Office Manager application automatically switches to its simplified view as the configuration is from a system running in IP Office Basic Edition mode.
4. Select **File | Advanced | Switch to Standard Mode (Default)**.
5. The configuration changes to a default one for a IP Office Essential Edition system and IP Office Manager switches to its advanced view mode.
6. This is a suitable time to begin initial configuration 100 before sending the configuration back to the IP Office system to restart in IP Office Essential Edition.
   - For a system to run in IP Office Essential Edition or IP Office Preferred Edition mode, its configuration must include an **Essential Edition** license. A system without this license will not allow any telephony functions until the license is added.
7. Once the system has rebooted, use IP Office Manager to again receive the configuration from the system. The user name and password for configuration should be the IP Office Standard Version mode defaults **Administrator** and **Administrator**.

12.2 Automating the Change to Standard Mode

If the only systems that you install are ones using IP Office standard modes, IP Office Manager can be set to automatically default the system to IP Office standard mode.

- **! WARNING**
  The processes below require the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

1. In IP Office Manager, select **File | Preferences**.
2. On the **Preferences** sub-tab, enable **Default to Standard Mode**.



3. With this option enabled, when a configuration for a new or defaulted system running in IP Office Basic Edition is received by IP Office Manager, it will automatically be converted to a IP Office Essential Edition configuration.
4. **! Important: IP Address Settings Default to Server**
   The conversion will set the DHCP mode to ***Server*** and the LAN addresses to their defaults of 192.168.42.1 and 192.168.43.1. Using IP Office Manager to change these settings to the required values.
5. This is a suitable time to begin initial configuration[100] before sending the configuration back to the IP Office system to restart in IP Office Essential Edition.
   - For a system to run in IP Office Essential Edition or IP Office Preferred Edition mode, its configuration must include an **Essential Edition** license. A system without this license will not allow any telephony functions until the license is added.
6. Sending the configuration back to the system restarts the system in IP Office Essential Edition mode.

12.3 Switching Off a System

Systems running IP Office Release 6.0 must be shut down in order to perform maintenance rather than just switched off. The shut down can be either indefinite or for a set period of time after which the IP Office will automatically reboot. Note that the control unit memory cards can be shutdown[157] and restarted[158] separately from the system.

During the shut down process, the current configuration in the control unit's RAM memory is copied to the control units non-volatile memory. For IP500 V2 systems that location is the System SD card.

- **! WARNING**
  A shutdown must always be used to switch off the system. Simply removing the power cord or switching off the power input may cause the loss of configuration data.
  - This is not a polite shutdown, any user calls and services in operation will be stopped. Once shutdown, the system cannot be used to make or receive any calls until restarted.
  - The shutdown process takes up to a minute to complete. When shutting down a system with a Unified Communications Module installed, the shutdown can take up to 3 minutes while the card safely closes all open files and closes down its operating system.
- **Shutdown LED Indication**
  When shutdown, the LEDs shown on the system are as follows. Do not remove power from the system or remove any of the memory cards until the system is in this state:
  - LED1 on each IP500 base card installed will also flash red rapidly plus LED 9 if a trunk daughter card is fitted to the base card.
  - The CPU LED on the rear of the system will flash red rapidly.
  - The System SD and Optional SD memory card LEDs on the rear of the system are extinguished.
- **Restarting a System**
  To restart a system when shutdown indefinitely, or to restart a system before the timed restart expires, switch power to the system off and on again.

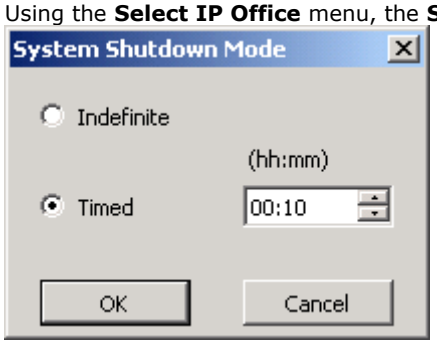
Process Options

1. **Shutting down a system using IP Office Manager**[163]
2. **Shutting down a system using System Status Application**[164]
3. **Shutting down a system using a System Phone**[164]
4. **Shutting down a system using the AUX button**[164]
5. **Shutting down a system using IP Office Web Manager**[164]

12.3.1 Shutdown a System Using IP Office Manager

To shutdown a system using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | System Shutdown**.
2. Using the **Select IP Office** menu, the **System Shutdown Mode** menu is displayed.



3. Select the type of shutdown required. If **Indefinite** is used, the system can only be restarted by having its power switched off and then on again. If a **Timed** shutdown is selected, the IP Office will reboot after the set time has elapsed.
4. Click **OK**.
5. Wait until the LEDs on the front of the system are all fast flashing red before performing any other actions.

Página2824 de 3226.

12.3.2 Shutdown a System Using System Status Application

To shutdown a system using System Status Application

1. Start System Status[69] and access the IP Office's status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Shutdown System**.
4. Select the time duration for the shutdown or indefinite.
5. Click **OK**.
6. Wait until the LEDs on the front of the system are all fast flashing red before performing any other actions.

12.3.3 Shutdown a System Using a System Phone

This process can be used by a user configured as a System Phone user and using a 1400, 1600, 9500 or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's **Login Code** is used to restrict access to the system administration functions on the phone.

Unlike IP Office Manager, a system phone user cannot select an indefinite shutdown. They can set a timed shut down of between 5 minutes and 24 hours.

To shutdown a system using a system phone

1. Select **Features | Phone User | System Admin**.
2. Enter your IP Office user login code.
3. From the menu select **System Shutdown**.
4. Select a time period for the shutdown. It must be in between 5 minutes and 24 hours.
5. Press **Done** and then **Confirm** to begin the shutdown.
6. Wait until the LEDs on the front of the system are all fast flashing red before performing any other actions.

12.3.4 Shutdown a System Using the AUX Button

This method is supported by IP500 V2 control units.

To shutdown a system using the IP500 V2 AUX Button

1. On the rear of the control unit, press and hold the **AUX** button for more than 5 seconds.
2. The control unit will shutdown with the restart timer set to 10 minutes.
3. Wait until the LEDs on the front of the system are all fast flashing red before performing any other actions.

12.3.5 Shutdown a System Using IP Office Web Manager

To shutdown a system using IP Office Web Manager

1. Login to IP Office Web Manager[71].
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions**. Select **Service Commands** and then **System Shutdown**.
3. Click **OK**.
4. Wait until the LEDs on the front of the system are all fast flashing red before performing any other actions.

Página2825 de 3226.

12.4 Rebooting a System

It may occasionally be necessary to reboot the system. For example, after reinserting a System SD card with upgraded system software. That can be done using any of the following processes.

- **! WARNING**
  One of the following methods should always be used to restart a system. Simply removing and then reapplying power to the system may cause the loss of data and unexpected system operation.

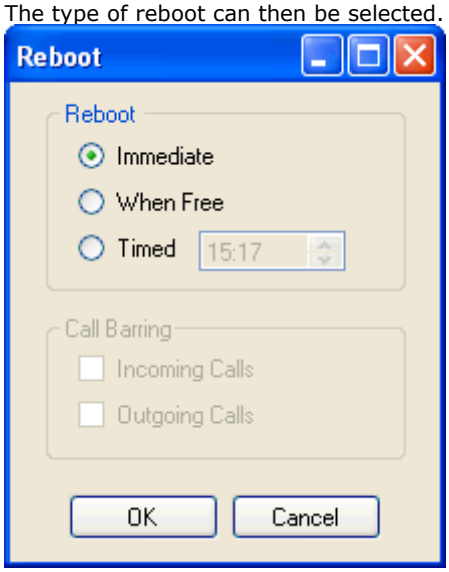
Process Options

1. **Reboot a system using IP Office Manager** 165
2. **Reboot a system using IP Office Web Manager** 166
3. **Reboot a system using the Reset button** 166
4. **Reboot a system using a system phone** 166

12.4.1 Reboot a System Using IP Office Manager

To reboot a system using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | Reboot**.
2. Use the **Select IP Office** menu to locate and select the IP Office system. Enter a valid user name and password.
3. The type of reboot can then be selected.



- **Reboot**
  Select when the reboot should occur.
  - **Immediate**
    Reboot the system immediately.
  - **When Free**
    Reboot the system when there are no calls in progress. This mode can be combined with the **Call Barring** options.
  - **Timed**
    The same as When Free but waits for a specific time after which it then wait for there to be no calls in progress. The time is specified by the **Reboot Time**. This mode can be combined with the **Call Barring** options.
- **Reboot Time**
  This setting is used when the reboot mode **Timed** is selected. It sets the time for the IP Office reboot. If the time is after midnight, the IP Office's normal daily backup is canceled.
- **Call Barring**
  These settings can be used when the reboot mode When Free is selected. They bar the sending or receiving of any new calls.

4. Click **OK**.

12.4.2 Reboot a System Using IP Office Web Manager

To reboot a system using IP Office Web Manager

1. Login to IP Office Web Manager[71].
    a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
    b. Enter an administrator user name and password and click **Login**.
2. Click **Actions**. Select **Service Commands** and then **Reboot**.
3. Select when the reboot should occur.
    - **Immediate**
      Reboot the system immediately.
    - **Free**
      Reboot the system when there are no calls in progress.
    - **Timed**
      Reboot the system at the set time.
4. Click **OK**.

12.4.3 Reboot a System Using the Reset Button

To reboot a system using the Reset button

Use this process to reboot the system when free. Once invoked, the system bars any new incoming or outgoing calls until after the reboot.

1. On the rear of the control unit, press and hold the **Reset** button for between 5 to 10 seconds until the **CPU** led changes to steady orange.
2. When the **CPU** LED changes to steady orange, release the button.
    - If the **CPU** LED changed to flashing orange or red, keep the button held until the **CPU** LED changes to flashing green. Then release the button and reattempt the process once the CPU LED has returned to steady green.
3. Wait for the reboot to complete before performing any other actions.

12.4.4 Rebooting a System Using a System Phone

This function is not supported from system phones on system's running in IP Office standard mode.

12.5 Changing Components

In the sections below, the term component can refer to a card fitted into the IP Office or an external expansion module.

- **! IMPORTANT:**
  You Must Switch Off the Control Unit Before Adding, Removing or Swapping Components
  Base cards, trunk cards and external expansions modules must only be removed and added to an IP Office system when that system is switched off [163]. Failure to do so will result in the new component not loading the correct firmware and not operating or not operating correctly. This applies even when swapping like for like components.

Note that for existing extension ports, by default both an extension entry and a user entry will exist in the IP Office configuration. Extension entries can be deleted without deleting the corresponding user entry. This allows retention of the user settings and association of the user with a different extension by changing that extensions **Base Extension** number to match the user's **Extension ID**.

Processes

- **Like for like replacement** [168]
- **Higher capacity component replacement** [168]
- **Lower capacity component replacement** [168]
- **Adding a new component** [168]
- **Permanent removal of a component** [169]
- **Replacement with a different type of component** [169]

12.5.1 Like for Like Replacement

If replacing with a component of the same type, no configuration changes are necessary.

To do a like for like replacement

1. Shutdown the system[163].
2. Switch off power to the system.
3. Remove the card or external expansion module. Note the card slot or expansion port used as the replacement must be installed in the same position.
4. Install the replacement using the appropriate process for the type of component (Fitting IP500 cards[82], Adding External Expansion Modules[91]).
5. Restart the IP Office system.

12.5.2 Higher Capacity Replacement

If replacing with a component of the same type but higher capacity, when restarted the IP Office will automatically create configuration entries for the new trunks or extensions/users.

To replace a component with one of the same type but higher capacity

1. Shutdown the system[163].
2. Switch off power to the system.
3. Remove the card or external expansion module. Note the card slot or expansion port used as the replacement must be installed in the same position.
4. Install the replacement using the appropriate process for the type of component (Fitting IP500 cards[82], Adding External Expansion Modules[91]).
5. Restart the IP Office system.
6. Use IP Office Manager to configure the new trunks or extensions/users.

12.5.3 Lower Capacity Replacement

If replacing with a component of the same type but lower capacity, after restarting the IP Office the configuration will need to be edited to remove redundant entries.

To replace a component with one of the same type but lower capacity

1. Shutdown the system[163].
2. Switch off power to the system.
3. Remove the card or external expansion module. Note the card slot or expansion port used as the replacement must be installed in the same position.
4. Install the replacement using the appropriate process for the type of component (Fitting IP500 cards[82], Adding External Expansion Modules[91]).
5. Restart the IP Office system.
6. Use IP Office Manager to delete the trunks or extensions/users that are no longer supported by the component installed.

12.5.4 Adding a New Component

If adding a new component to an available slot or port, when restarted the IP Office will automatically create configuration entries for the new trunks or extensions/users.

To add a new component

1. Shutdown the system[163].
2. Switch off power to the system.
3. Install the replacement using the appropriate process for the type of component (Fitting IP500 cards[82], Adding External Expansion Modules[91]).
4. Restart the IP Office system.
5. Use IP Office Manager to configure the new trunks or extensions/users.

Página2829 de 3226.

12.5.5 Permanent Removal

If permanently removing the component, the configuration will need to be edited to remove redundant trunk or extension/user entries.

To permanently remove a component

1. Shutdown the system[163] .
2. Switch off power to the system.
3. Remove the card or external expansion module.
4. Restart the IP Office system.
5. Use IP Office Manager to delete the trunks or extensions/users in the configuration that relate to the component removed.
6. In the **Control Unit** section of the configuration, delete the entry for the component that is no longer present in the system.

12.5.6 Replacemnt with a Different Type

If replacing a component with one of a different type, the process should be divided into two stages.

1. First remove the existing component using the Permanent Removal[169] process and adjust the configuration and reboot.
2. Then install the new component using the Adding a New Component[168] process.

12.6 Defaulting the Configuration

The following processes erases the configuration held in the control unit's memory. That include both the current configuration being used in RAM memory and the backup configuration stored in non-volatile memory. Following this, the system restarts with a default configuration.

This process should be performed from a PC with a fixed IP address, directly connected to the control unit and with the system disconnected from any network. Following this process, the control unit's IP address defaults to 192.168.42.1.

- **Standard Mode systems**
  For IP Office Release 7.0 and higher, IP500 V2 systems using **IP Office A-Law** or **IP Office U-Law** System SD cards default to IP Office Basic Edition mode. Loading the configuration switches IP Office Manager to simplified view. To change the system back to operating in IP Office standard mode, see Changing the System to Standard Mode 103.

Process Options

1. **Defaulting the configuration using IP Office Manager** 170
2. **Defaulting the configuration using IP Office Web Manager** 170
3. **Defaulting the configuration using the Reset button** 170
4. **Defaulting the configuration using a system phone** 172
5. **Defaulting the configuration using Debug** 171
6. **Defaulting the configuration using the Boot Loader** 172

12.6.1 Defaulting the Configuration Using IP Office Manager

Read and note the warnings regarding defaulting the configuration 170 before using this process.

To erase the configuration using IP Office Manager

1. Start IP Office Manager.
2. Select **File | Advanced | Erase Configuration (Default)**.
3. Select the system to be defaulted and click **OK**.
4. Enter an administration name and password and click **OK**.

12.6.2 Defaulting the Configuration Using IP Office Web Manager

Read and note the warnings regarding defaulting the configuration 170 before using this process.

To default the configuration using IP Office Web Manager

1. Login to IP Office Web Manager 71.
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions**. Select **Service Commands** and then **Erase Configuration**.
3. Click **OK**.
4. Wait until the system has rebooted before logging in again.

12.6.3 Defaulting the Configuration Using the Reset Button

Read and note the warnings regarding defaulting the configuration 170 before using this process.

To default the configuration using the Reset button

1. On the rear of the control unit, press and hold the **Reset** button for between 10 to 30 seconds until the **CPU** led changes to flashing orange.
2. When the **CPU** LED changes to flashing orange, release the button.
   - If the **CPU** LED changed to red, keep the button held until the **CPU** LED changes to flashing green. Then release the button and reattempt the process once the CPU LED has returned to steady green.
3. Wait for the reboot to complete before performing any other actions.

Página2831 de 3226.

12.6.4 Defaulting the Configuration Using Debug

Read and note the warnings regarding defaulting the configuration 170 before using this process.

- **WARNING**
  Use of the RS232 port should only be performed if absolutely necessary and only if the actions cannot be completed using IP Office Manager or IP Office Web Manager. In all cases, you must make every effort to ensure that you have a backup copy of the system configuration.

To erase the configuration using debug:

This process erases the IP Office's configuration settings but does not alter its security settings. It is easier to use than the boot loader method.

1. Ensure that you have a backup copy of the IP Office's configuration before performing this action. If a copy of the configuration cannot be downloaded using IP Office Manager, check the IP Office Manager application directory for previously downloaded configurations.
   a. Use IP Office Manager to download an up to date copy of the configuration. If that is not possible, check in the IP Office Manager application folder for a previous copy of the configuration.
   b. Using IP Office Manager, select **File | Open Configuration**.
   c. Using the **Select IP Office Menu**, locate and select the IP Office system. Click **OK**.
   d. Enter the name and password for a service user account on that IP Office. Click **OK**. IP Office Manager will receive and display the configuration from the IP Office.
      - If not already done, this action creates a BOOTP entry in IP Office Manager for the IP Office system.
      - This action also confirms communication between the IP Office Manager PC and the IP Office prior to any following process.
   e. Select **File | Save Configuration As...** and save a copy of the configuration file onto the PC.
2. Attach the serial cable between the PC and the RS232 DTE port on the IP Office control unit.
   a. Start the terminal program on your PC. Ensure that it has been setup as listed in RS232 DTE Port Settings 278 . Within a HyperTerminal session, the current settings are summarized across the base of the screen.
   b. Enter **AT** (note upper case). The control unit should respond ***OK***.
   c. Enter **AT-DEBUG**. The control unit should response with the time and date and then ***Hello>*** to show it is ready to accept commands.
3. To erase the current configuration in RAM memory, enter **eraseconfig**. The ***Hello>*** command prompt reappears when the action is completed.
4. To erase the backup configuration stored in non-volatile Flash memory, enter **erasenvconfig**. The ***Hello>*** command prompt reappears when the action is completed.
5. To reboot the IP Office enter **reboot**. The IP Office will reboot and restart with a defaulted configuration.
6. Close the terminal program session.
7. IP Office Manager can now be used to alter and then upload an old configuration file or receive and edit the control unit's now defaulted configuration.

12.6.5 Default the Configuration Using a System Phone

This process is not supported by system phones for a system running in IP Office standard mode.

12.6.6 Defaulting the Configuration Using Boot Loader

Read and note the warnings regarding defaulting the configuration 170 before using this process.

- **WARNING**
  Use of the RS232 port should only be performed if absolutely necessary and only if the actions cannot be completed using IP Office Manager or IP Office Web Manager. In all cases, you must make every effort to ensure that you have a backup copy of the system configuration.

To erase the configuration and security settings using the Boot Loader

This process also defaults the IP Office security settings.

1. Ensure that you have a backup copy of the IP Office's configuration before performing this action. If a copy of the configuration cannot be downloaded using IP Office Manager, check the IP Office Manager application directory for previously downloaded configurations.
   a. Use IP Office Manager to download an up to date copy of the configuration. If that is not possible, check in the IP Office Manager application folder for a previous copy of the configuration.
   b. Using IP Office Manager, select **File | Open Configuration**.
   c. Using the **Select IP Office Menu**, locate and select the IP Office system. Click **OK**.
   d. Enter the name and password for a service user account on that IP Office. Click **OK**. IP Office Manager will receive and display the configuration from the IP Office.
      - If not already done, this action creates a BOOTP entry in IP Office Manager for the IP Office system.
      - This action also confirms communication between the IP Office Manager PC and the IP Office prior to any following process.
   e. Select **File | Save Configuration As...** and save a copy of the configuration file onto the PC.
2. Attach the serial cable between the PC and the RS232 DTE port on the IP Office control unit.
   a. Start the terminal program on your PC. Ensure that it has been setup as listed in RS232 DTE Port Settings 278 . Within a HyperTerminal session, the current settings are summarized across the base of the screen.
   b. Arrange the program windows so that the Terminal program and IP Office Manager TFTP Log are visible at the same time.
   c. Switch off power to the IP Office control unit.
   d. Power on the control unit and press the escape key every second until you get a Loader message. Below is an example.

      ```
      P12 Loader 2.4
      CPU Revision 0x0900
      ```

   e. Enter **AT** (note upper case). The control unit should respond ***OK***.
   f. If an OK response is not received, check the settings of your terminal program and repeat the process above.
3. Proceed with the erasure process.
   - To erase the alarm log enter ***AT-X1***.
   - To erase the current configuration, enter ***AT-X2***. A typical response if ***Sector 2 Erase (NV Config)*** followed by ***OK***. Enter ***AT-X3***. A typical response is ***Sector Erases (Config)*** followed by a series of ***OK*** responses.
4. Switch power to the control unit off and then back on. Within the terminal program you should see various messages as the control unit performs various start up tasks.
5. Close the terminal program session.
6. IP Office Manager can now be used to alter and then upload an old configuration file or receive and edit the control unit's now defaulted configuration.

12.7 Defaulting Security Settings

If necessary, the security settings for access to the system can be defaulted. This includes resetting all the security service user accounts including those that are used by IP Office applications. Therefore, those application may need to be reconfigured to use the new service user accounts or account passwords.

Defaulting the system security settings does not affect user passwords, voicemail codes and login codes. However, the security settings includes rules for acceptable user passwords. Therefore, following a security default existing user passwords may be flagged as being in error.

Following the security default, the advice in the Securing the System 132 chapter should be followed. For details of the default security settings for a system refer to the IP Office Manager documentation.

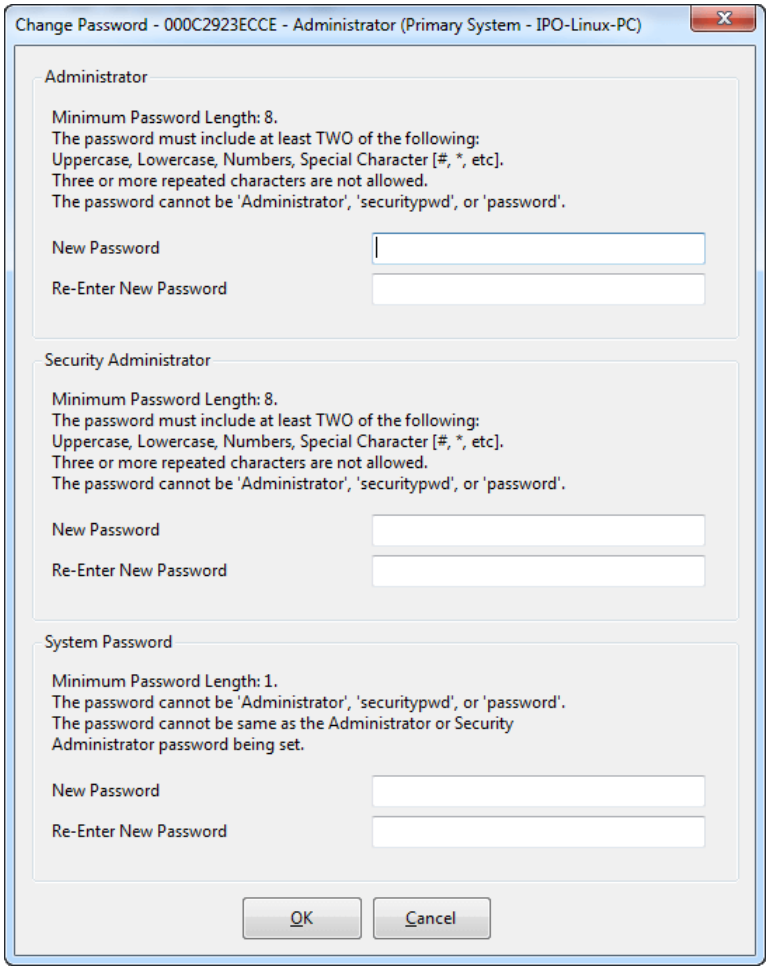
- **! Warning - Service Disruption**
  Whilst defaulting the security settings does not require a system reboot, it may cause service disruption for several minutes while the system generates a new default security certificate.

Process Options

1. **Defaulting the security settings using IP Office Manager** 174
2. **Defaulting the security settings using IP Office Web Manager** 174
3. **Defaulting the security settings using the RS232 port** 175
4. **Defaulting the security settings using the Boot Loader** 176

Logging in after defaulting the security settings:

When IP Office Manager connects to a system with default security settings, you are prompted to change the default passwords. This also applies if any one of the passwords is returned to the default value.



Página2834 de 3226.

12.7.1 Defaulting Security Using IP Office Manager

Read and note the warnings regarding defaulting the security settings 173 before using this process.

- **! Warning - Service Disruption**
  Whilst defaulting the security settings does not require a system reboot, it may cause service disruption for several minutes while the system generates a new default security certificate.

To default a system's security settings using IP Office Manager

1. Start IP Office Manager.
2. Select **File | Advanced | Erase Security Settings (Default)**.
3. Select the system from the menu and click **OK**.
4. Enter a name and password for security configuration access.
5. IP Office Manager indicates when the security settings have been reset.

12.7.2 Defaulting Security Using IP Office Web Manager

Read and note the warnings regarding defaulting the security settings 173 before using this process.

- **! Warning - Service Disruption**
  Whilst defaulting the security settings does not require a system reboot, it may cause service disruption for several minutes while the system generates a new default security certificate.

To default a system's security settings using IP Office Web Manager

1. Login to IP Office Web Manager 71.
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions**. Select **Service Commands** and then **Erase Security Settings**.
3. Click **OK**.

12.7.3 Defaulting Security using the RS232 Port

Read and note the warnings regarding defaulting the security settings 173 before using this process.

- **! Warning - Service Disruption**
  Whilst defaulting the security settings does not require a system reboot, it may cause service disruption for several minutes while the system generates a new default security certificate.
- **⚠ WARNING**
  Use of the RS232 port should only be performed if absolutely necessary and only if the actions cannot be completed using IP Office Manager or IP Office Web Manager. In all cases, you must make every effort to ensure that you have a backup copy of the system configuration.

To default a system' security settings via DTE

This process defaults the IP Office's security settings but does not alter its configuration settings.

1. Attach the serial cable between the PC and the DTE port on the IP Office control unit.
2. Start the terminal program on your PC. Ensure that it has been setup as listed in DTE Port Settings 278. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
3. Enter **AT** (note upper case). The control unit should respond ***OK***.
4. Enter **AT-SECURITYRESETALL**.
5. You will be prompted to confirm the control unit's MAC address before continuing. Enter the address.
6. After approximately a minute, the control unit will respond ***OK*** when the action has been completed.
7. Close the terminal program session.
8. IP Office Manager can now be used to receive and edit the control unit's now defaulted security settings.

12.7.4 Defaulting Security Using the Boot Loader

Read and note the warnings regarding defaulting the security settings 173 before using this process.

- **! Warning - Service Disruption**
  Whilst defaulting the security settings does not require a system reboot, it may cause service disruption for several minutes while the system generates a new default security certificate.
- **⚠ WARNING**
  Use of the RS232 port should only be performed if absolutely necessary and only if the actions cannot be completed using IP Office Manager or IP Office Web Manager. In all cases, you must make every effort to ensure that you have a backup copy of the system configuration.

To default a system's security settings via Boot Loader

This process defaults the IP Office security settings and its configurations settings.

1. Ensure that you have a backup copy of the IP Office's configuration before performing this action. If a copy of the configuration cannot be downloaded using IP Office Manager, check the IP Office Manager application directory for previously downloaded configurations.
   a. Use IP Office Manager to download an up to date copy of the configuration. If that is not possible, check in the IP Office Manager application folder for a previous copy of the configuration.
   b. Using IP Office Manager, select **File | Open Configuration**.
   c. Using the **Select IP Office Menu**, locate and select the IP Office system. Click **OK**.
   d. Enter the name and password for a service user account on that IP Office. Click **OK**. IP Office Manager will receive and display the configuration from the IP Office.
      - If not already done, this action creates a BOOTP entry in IP Office Manager for the IP Office system.
      - This action also confirms communication between the IP Office Manager PC and the IP Office prior to any following process.
   e. Select **File | Save Configuration As...** and save a copy of the configuration file onto the PC.
2. Attach the serial cable between the PC and the RS232 DTE port on the IP Office control unit.
   a. Start the terminal program on your PC. Ensure that it has been setup as listed in RS232 DTE Port Settings 278 . Within a HyperTerminal session, the current settings are summarized across the base of the screen.
   b. Arrange the program windows so that the Terminal program and IP Office Manager TFTP Log are visible at the same time.
   c. Switch off power to the IP Office control unit.
   d. Power on the control unit and press the escape key every second until you get a Loader message. Below is an example.

      ```
      P12 Loader 2.4
      CPU Revision 0x0900
      ```

   e. Enter **AT** (note upper case). The control unit should respond ***OK***.
   f. If an OK response is not received, check the settings of your terminal program and repeat the process above.
3. To erase the current configuration in RAM memory enter **AT-X3**. A typical response is ***Sector Erases (Config)*** followed by a series of ***OK*** responses.
4. To erase the backup configuration stored in non-volatile memory enter **AT-X2**. A typical response if ***Sector 2 Erase (NV Config)*** followed by ***OK***. IP Office 403 only: If running an IP Office 403 control unit, also enter **AT-X4**.
5. Switch power to the control unit off and then back on. Within the terminal program you should see various messages as the control unit performs various start up tasks.
6. Close the terminal program session.
7. IP Office Manager can now be used to alter and then upload an old configuration file or receive and edit the control unit's now defaulted configuration.

Página2837 de 3226.

12.8 Loading a Configuration

The existing configuration of a system can be replaced with a new configuration that has been prepared separately.

- The configuration created must match the physical equipment in the IP Office system onto which it is loaded. Doing otherwise may cause the IP Office system to reset and experience other problems.

Process Options

1. **Creating an offline configuration file** 178
2. **Loading a configuration file using IP Office Manager** 179
3. **Loading a configuration file using IP Office Web Manager** 179
4. **Loading a configuration file onto a System SD card** 179

Página2838 de 3226.

12.8.1 Creating an Offline Configuration File

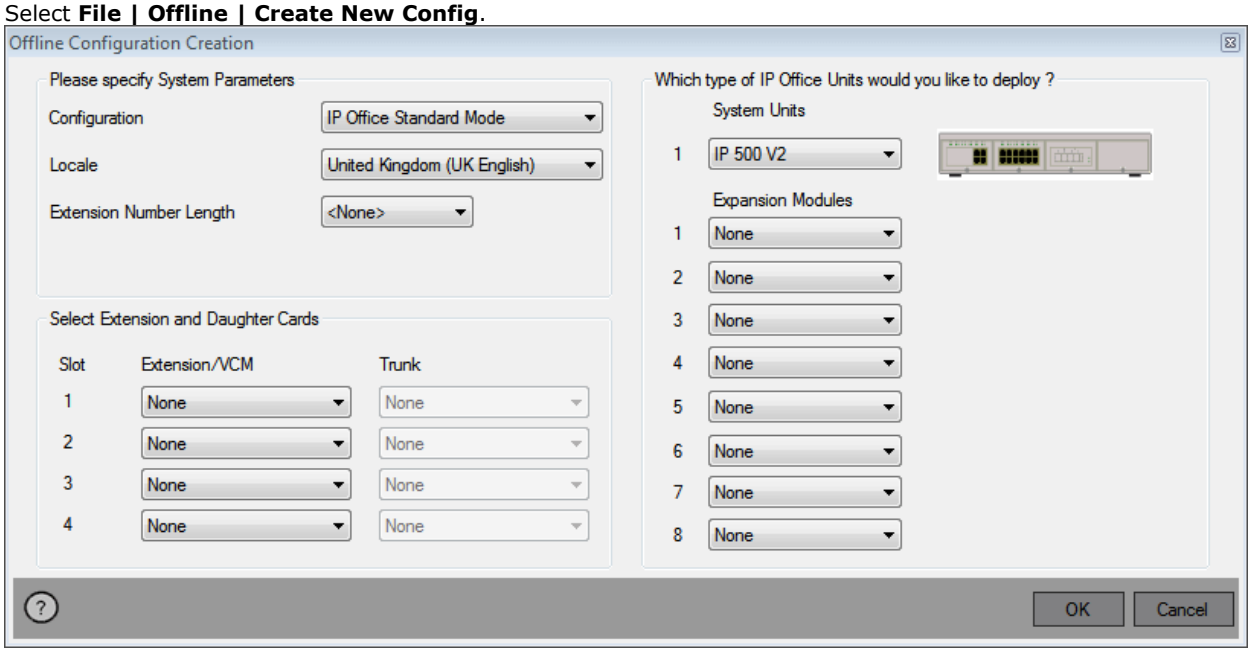
IP Office Manager can be used to create a new configuration without connecting to an IP Office system. During the process, you can specify the locale of the system, what type of trunk cards it uses and what type of control unit and expansion modules to include.

This allows the creation of a configuration prior to installation of system. The configuration file can then be placed onto the System SD card before it is installed into the system. Otherwise the configuration can be uploaded to the system after initial installation of the system.

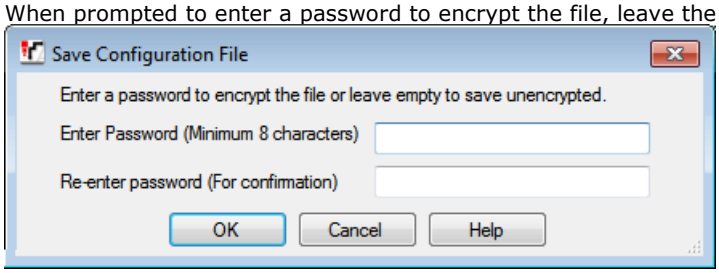
- The configuration created must match the physical equipment in the IP Office system onto which it is loaded. Doing otherwise may cause the IP Office system to reset and experience other problems.

To create an offline configuration file

1. Start IP Office Manager with no configuration loaded into IP Office Manager
2. Select **File | Offline | Create New Config**.



3. Select the type of configuration that you want to create. The equipment and settings are restricted to those supported in the selected mode.
4. When completed click **OK**.
5. IP Office Manager creates and loads the configuration.
6. Edit the configuration to match the customer requirements. This can include importing information from preprepared CSV files 77.
   - Note that since this configuration is being done offline and without licensing, you can configure features that may become unsupported once the configuration is loaded into the live system.
7. When completed, select **File | Save Configuration As**.
8. When prompted to enter a password to encrypt the file, leave the fields blank and click **OK**.



Página2839 de 3226.

12.8.2 Loading a Configuration Using IP Office Manager

This process will replace the existing configuration.

- The configuration created must match the physical equipment in the IP Office system onto which it is loaded. Doing otherwise may cause the IP Office system to reset and experience other problems.

To load an offline configuration using IP Office Manager

1. Start IP Office Manager.
2. Select **File | Offline | Open File...**.
3. Select the configuration file and click **Open**.
4. Check that the configuration settings are as expected and make any adjustments necessary.
5. Select **File | Offline | Send Config...**.
6. Select the system and click **OK**.
7. Enter an administrator name and password and click **OK**.
8. Select when the new configuration should be loaded. Do not select the **Merge** option.
9. Click **OK**.

12.8.3 Loading a Configuration Using IP Office Web Manager

This process will replace the existing configuration.

- The configuration created must match the physical equipment in the IP Office system onto which it is loaded. Doing otherwise may cause the IP Office system to reset and experience other problems.

To load an offline configuration using IP Office Web Manager

1. Login to IP Office Web Manager 71.
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Click **Actions**. Select **Service Commands** and then **Upload Configuration**. Click **Monitoring** and select **Upload Configuration**.
3. Click **Browse** and select the configuration file.
4. Click **Upload**.
5. Click **OK**.
6. Reboot the system for the new configuration to be applied fully. See Rebooting a System 165.

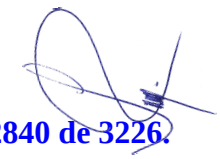
12.8.4 Loading a Configuration onto a System SD Card

This process will replace the existing configuration.

- The configuration created must match the physical equipment in the IP Office system onto which it is loaded. Doing otherwise may cause the IP Office system to reset and experience other problems.

To load a configuration directly onto a System SD card

1. Rename the offline configuration file as *config.cfg*.
2. Shutdown and remove the System SD card. See Memory Card Shutdown/Removal 157.
3. Insert the SD card into the PC and display the card contents.
4. Open the /system/primary folder and replace the existing config.cfg file with the new file.
5. Reinsert the System SD card into the system.
6. Reboot the system. See Rebooting a System 165.



12.9 Upgrading systems

There are several methods by which the system can be upgraded to a new release of IP Office core software.

⚠ WARNINGS

- **! WARNING: Upgrading pre-Release 9.1 Systems:**
  Existing systems running a release lower than 8.1(65) must first upgrade to IP Office Release 8.1(65) (or higher 8.1) or any IP Office Release 9.0 before being upgraded to IP Office Release 9.1 or higher. For the lower releases intermediate upgrade license are not required if the system is being further upgraded.

- **! WARNING: Upgrading pre-Release 10.0 Systems:**
  IP Office Release 10 and higher only support PLDS licenses. To upgrade a system that is using ADI licenses, those licenses must first be migrated to PLDS.

  - License migration is done by obtaining a license migration file using IP Office Manager (**Tools | License Migration**) and then submitting that file to Avaya. Note that this process also migrates any virtual licenses entitlements the system has to equivalent PLDS licenses but now associated with the feature key. Only upgrade the system once the replacement PLDS license file for the system has been obtained. Note that following license migration, Avaya will delete all records of any ADI license entitlements it holds for that feature key.

- **! Warning: Upgrade License Requirements**
  On a new system, when the first call is made, the software level being run is written into the control unit's permanent memory. Any subsequent upgrade to a higher release requires the addition of the **Essential Edition** license for the target release. Systems upgraded without that license display *"No license available"* on some phones and will not allow any telephony functions.

- **! Note: Server Edition Systems**
  IP500 V2 control units configured as IP500 V2 Expansion System systems are licensed and upgraded through the Server Edition web management menus. Refer to the Server Edition documentation.

- **Check IP Office Technical Bulletins**
  Check the latest IP Office Technical Bulletin for the IP Office software release before proceeding any further. It may contain information relating to changes that occurred after this document was completed. Bulletins are available from http://support.avaya.com.

  - **! IP Office Web Manager**
    The addition of IP Office Web Manager requires changes to the security settings of systems. For new systems those changes are made automatically. However, for system being upgraded, the changes can only be made if the system's security settings are defaulted. See Enabling IP Office Web Manager 202 for additional steps that should be performed before upgrading to IP Office Release 8.0 or higher.

- **Other IP Office Applications**
  Upgrading the core software of the IP Office control unit will require upgrades to associated software. The levels of application software supported with the IP Office core are detailed in the IP Office Technical bulletin for the release.

- **DS16B/DS30B Upgrade Behavior:**
  For DS16B/DS30B modules the process of loading the appropriate firmware for the selected mode or upgrading takes up to 10 minutes during which time the module is not available.

- **DS16B2/DS30B2 Upgrade Behavior:**
  The behavior of DS16/30B2 during firmware upgrade or switching modes differs from other external expansion units:

  - During the firmware upgrade, the unit remains operational and can make and receive calls.
  - Once the upgrade is completed (approximately 9 minutes) the unit reboots and takes about 45 seconds to return to normal operation.

Process Options

1. **Upgrading using the IP Office Manager Upgrade Wizard** 181
   This process upgrades the system or systems using the firmware files installed with the IP Office Manager application.
2. **Upgrading a System SD Card using the IP Office Manager PC** 183
   A PC running IP Office Manager can be used to directly update the files on an SD card. That card can then be inserted into the system and the system restarted.
3. **Upgrading using an optional SD card** 184
   This process upgrades the system by using IP Office Manager to create an SD card loaded with the files installed with the IP Office Manager application.
4. **Upgrading using IP Office Web Manager** 185
   This process upgrades the system using a set of firmware files provided for the purpose. It does not require IP Office Manager.

12.9.1 Upgrade Using the Upgrade Wizard

The Upgrade Wizard is part of IP Office Manager. It can be used to upgrade multiple system's at the same time.

- **! Warning: IP Office Manager Version**
  This process uses software files provided by the installed version of IP Office Manager being used. You must ensure that the version of IP Office Manager used matches the version of software required.
    - **Admin Lite Not Supported**
      Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).
- **Multiple Managers**
  If more than one copy of IP Office Manager is running, it is possible for the IP Office to request BIN files from a different IP Office Manager than the one that started the upgrade process. Ensure that only one copy of IP Office Manager is running when upgrading an IP Office system.
- **! WARNING: Upgrading pre-Release 9.1 Systems:**
  Existing systems running a release lower than 8.1(65) must first upgrade to IP Office Release 8.1(65) (or higher 8.1) or any IP Office Release 9.0 before being upgraded to IP Office Release 9.1 or higher. For the lower releases intermediate upgrade license are not required if the system is being further upgraded.
- **! WARNING: Upgrading pre-Release 10.0 Systems:**
  IP Office Release 10 and higher only support PLDS licenses. To upgrade a system that is using ADI licenses, those licenses must first be migrated to PLDS.
    - License migration is done by obtaining a license migration file using IP Office Manager (**Tools | License Migration**) and then submitting that file to Avaya. Note that this process also migrates any virtual licenses entitlements the system has to equivalent PLDS licenses but now associated with the feature key. Only upgrade the system once the replacement PLDS license file for the system has been obtained. Note that following license migration, Avaya will delete all records of any ADI license entitlements it holds for that feature key.

To upgrade systems using the upgrade wizard

1. Ensure that you have a backup copy of the IP Office's configuration before performing this action. If a copy of the configuration cannot be downloaded using IP Office Manager, check the IP Office Manager application directory for previously downloaded configurations.
    a. Use IP Office Manager to download an up to date copy of the configuration. If that is not possible, check in the IP Office Manager application folder for a previous copy of the configuration.
    b. Using IP Office Manager, select **File | Open Configuration**.
    c. Using the **Select IP Office Menu**, locate and select the IP Office system. Click **OK**.
    d. Enter the name and password for a service user account on that IP Office. Click **OK**. IP Office Manager will receive and display the configuration from the IP Office.
        - If not already done, this action creates a BOOTP entry in IP Office Manager for the IP Office system.
        - This action also confirms communication between the IP Office Manager PC and the IP Office prior to any following process.
    e. Select **File | Save Configuration As...** and save a copy of the configuration file onto the PC.
2. Select **File | Advanced | Upgrade**. The UpgradeWiz is started and scans for IP Office modules using the **Unit/Broadcast** address. Adjust this address and click **Refresh** if the expected control units are not shown. The current version of each IP Office BIN file held in the control units memory is shown. That is regardless of whether that .bin file is currently being used by any module in the system.
3. The **Version** column indicates the current version of software installed. The **Available** column indicates the version of software IP Office Manager has available. If the available version is higher, the check box next to that row is automatically selected.
    - If any of the modules have pre-version 2.1 software installed, an upgrade with **Validate** unticked is required. If this is the case, only continue with the upgrade process using a PC with a fixed IP address on the same LAN domain and physical LAN segment as the IP Office control unit and only upgrade the pre-2.1 system.
    - If a multi-stage upgrade is necessary, use the following additional steps to select the appropriate interim software:
        - Right-click on the upgrade wizard and click **Select Directory**. Locate and select the directory containing the bin file for the intermediate software level.
        - The upgrade wizard should now list just the control unit as having upgrade software available.

- Upgrading to particular levels of IP Office 10.0 or higher software requires the appropriate Essential Edition license for the release. The **Licensed** and **Required License** columns indicate the current license entitlement and the required license entitlement for the software the system is currently running.

4. For those modules which you want to upgrade, tick the check box.
5. The following additional options are available:

   - **Backup System Files**
     If selected, before upgrading to the new software, the current files in the System SD cards **/primary** folder are be copied to its **/backup** folder. If there is insufficient space on the SD card for this action, IP Office Manager displays an *"Insufficient space available on SD Card"* warning.

   - **Upload System Files**
     If selected, the full set of software files that IP Office Manager has is copied to the **/primary** folder on the System SD card. In addition to control unit and module software this includes phone software files and the files used for IP Office Web Manager. The firmware files for Avaya IP phones are uploaded first and when this is completed, if **Restart IP Phones** below is also selected, the Avaya IP phones are rebooted. The system then continues to upload any other files. If there is insufficient space on the SD card for this action, IP Office Manager displays an *"Insufficient space available on SD Card"* warning.

   - **Restart IP Phones**
     This option is available if **Upload System Files** above is also selected. If selected, once the system has rebooted and uploaded the phone firmware files, it reboots the IP phones. This causes them to reload the settings files and to recheck whether the firmware they currently have loaded matches that now available from their configured file server (by default the IP Office system). When selected, after the system reboot, the phones display *"Upgrading from system"* until restarted by the system once it has uploaded the phone firmware files.

6. Select **Upgrade**. The system password for each system will be requested. Enter it and click **OK**. The next steps depend on the upgrade options selected. Do not cancel or close the upgrade wizard while these processes are running.

   - **Insufficient space available on SD card**
     This message appears if the System SD card has insufficient space. To proceed with a reliable upgrade the SD card should upgraded locally[183].

   - **Validated Upgrade**
     If using the **Validated** option, a number of actions take place as follows;

     a. The upgrade wizard checks the amount of free RAM memory available in the control unit to temporarily store the new BIN files. If insufficient memory is available, you will be prompted whether to continue with an off-line upgrade or cancel upgrading.

        - If offline is selected, the IP Office is rebooted into offline mode. It may be necessary to use the **Refresh** option within the Upgrade Wizard to reconnect following the reboot. Validate upgrade can then be attempted to again check the amount of available RAM memory for transfer of BIN files. If the memory is still insufficient, the option is offered to either do an unvalidated upgrade or cancel.

     b. The bin files required are transferred to the system and stored in temporary memory.

     c. The backup system files and upload system files actions are performed if they were selected.

     d. Once all file transfers are completed, the upgrade wizard will prompt whether it okay to proceed with the upgrade process. Select **Yes** to continue. The control unit reboots and upgrades itself first. It then proceeds with upgrading the external expansion modules.

   - **Unvalidated Upgrade**
     This method of upgrading should be avoided unless absolutely necessary. It is only required for IP Office systems with pre-2.1 software and should only be done from a IP Office Manager PC with a fixed IP address running on the same LAN segment and subnet as the IP Office system. During the upgrade, the units and modules erases their current software and then request the new software file from IP Office Manager.

7. Following the upgrade, check that the upgrade wizard now shows that the selected units and modules have upgraded. It may be necessary to select **Refresh** to update the information in the upgrade wizard display.
8. Repeat the process as required.

12.9.2 Locally Upgrade the SD System Card Using Manager

The following process can be used if you have physical access to the IP500 V2 control unit. This method can be used with a timed reboot, allowing the card upgrade to be done during normal operation hours followed by a reboot outside of normal operation hours.

If the card is being used for Embedded Voicemail, that service is not available while the card is shutdown. Licensed features will continue running for up to 2 hours whilst the card is shutdown.

- **! Warning: IP Office Manager Version**
  This process uses software files provided by the installed version of IP Office Manager being used. You must ensure that the version of IP Office Manager used matches the version of software required.
    - **Admin Lite Not Supported**
      Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).
- **! WARNING: Upgrading pre-Release 9.1 Systems:**
  Existing systems running a release lower than 8.1(65) must first upgrade to IP Office Release 8.1(65) (or higher 8.1) or any IP Office Release 9.0 before being upgraded to IP Office Release 9.1 or higher. For the lower releases intermediate upgrade license are not required if the system is being further upgraded.
- **! WARNING: Upgrading pre-Release 10.0 Systems:**
  IP Office Release 10 and higher only support PLDS licenses. To upgrade a system that is using ADI licenses, those licenses must first be migrated to PLDS.
    - License migration is done by obtaining a license migration file using IP Office Manager (**Tools | License Migration**) and then submitting that file to Avaya. Note that this process also migrates any virtual licenses entitlements the system has to equivalent PLDS licenses but now associated with the feature key. Only upgrade the system once the replacement PLDS license file for the system has been obtained. Note that following license migration, Avaya will delete all records of any ADI license entitlements it holds for that feature key.

To upgrade a System SD Card using a PC

1. Shutdown the System SD memory card[157] and remove it from the control unit.
2. Follow the process for recreating the SD card[146]. This process will overwrite the software files on the card with the files available to IP Office Manager. This process takes approximately 20 minutes.
    - The process does not affect any current configuration file, Embedded Voicemail announcements and messages, or temporary SMDR data files.
    - The process deletes any current PLDS license file. The file needs to be restored after the SD card is recreated.
3. When the recreate process has completed, reinsert the card into the control unit's **System SD** card slot.
4. Using IP Office Manager select **File | Advanced | Reboot**.
5. In the **Select IP Office** menu, select the IP500 V2 system and click **OK**.
6. Select the type of reboot that you want performed and click **OK**.
7. When the system is rebooted, as it restarts it will load the software files in the primary folder of the System SD card.

12.9.3 Upgrading Using an Optional SD Card

The PC running IP Office Manager can be used to load the full set of operation files onto an SD card. This includes the firmware for the core system, phone firmware files and files for embedded voicemail. If the card contains configuration, message and prompt files, those files are not deleted by this process.

- **! Warning: IP Office Manager Version**
  This process uses software files provided by the installed version of IP Office Manager being used. You must ensure that the version of IP Office Manager used matches the version of software required.
    - **Admin Lite Not Supported**
      Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).
- **! WARNING: Upgrading pre-Release 9.1 Systems:**
  Existing systems running a release lower than 8.1(65) must first upgrade to IP Office Release 8.1(65) (or higher 8.1) or any IP Office Release 9.0 before being upgraded to IP Office Release 9.1 or higher. For the lower releases intermediate upgrade license are not required if the system is being further upgraded.
- **! WARNING: Upgrading pre-Release 10.0 Systems:**
  IP Office Release 10 and higher only support PLDS licenses. To upgrade a system that is using ADI licenses, those licenses must first be migrated to PLDS.
    - License migration is done by obtaining a license migration file using IP Office Manager (**Tools | License Migration**) and then submitting that file to Avaya. Note that this process also migrates any virtual licenses entitlements the system has to equivalent PLDS licenses but now associated with the feature key. Only upgrade the system once the replacement PLDS license file for the system has been obtained. Note that following license migration, Avaya will delete all records of any ADI license entitlements it holds for that feature key.

Upgrade by Updating an Optional SD Card

1. Shutdown the Optional SD card and remove the card from the system. See Memory Card Shutdown/Removal 157.
2. Follow the process for recreating the SD card 146. This process will overwrite the software files on the card with the files available to IP Office Manager. This process takes approximately 20 minutes.
3. Reinsert the card into the Optional SD card slot on the system.
4. Copy the files from the Optional SD card to the System SD card. See Loading Software from an Optional SD Card 154.
5. Reboot the system. See Rebooting a System 165.

12.9.4 Upgrading Using IP Office Web Manager

Avaya may make upgrade packages available for use with IP Office Web Manager. Once unpacked onto a local PC, the process below can be used to upgrade the system.

- **! WARNING: Upgrading pre-Release 9.1 Systems:**
  Existing systems running a release lower than 8.1(65) must first upgrade to IP Office Release 8.1(65) (or higher 8.1) or any IP Office Release 9.0 before being upgraded to IP Office Release 9.1 or higher. For the lower releases intermediate upgrade license are not required if the system is being further upgraded.

- **! WARNING: Upgrading pre-Release 10.0 Systems:**
  IP Office Release 10 and higher only support PLDS licenses. To upgrade a system that is using ADI licenses, those licenses must first be migrated to PLDS.

  - License migration is done by obtaining a license migration file using IP Office Manager (**Tools | License Migration**) and then submitting that file to Avaya. Note that this process also migrates any virtual licenses entitlements the system has to equivalent PLDS licenses but now associated with the feature key. Only upgrade the system once the replacement PLDS license file for the system has been obtained. Note that following license migration, Avaya will delete all records of any ADI license entitlements it holds for that feature key.

To upgrade a system using IP Office Web Manager

1. Login to IP Office Web Manager 71.
   a. Enter the system's IP address in the browser. Select **IP Office Web Manager**. Alternatively, enter *https://<IP_Address>:8443/WebMgmtEE/WebManagement.html*.
   b. Enter an administrator user name and password and click **Login**.
2. Unpack the upgrade files to a location on your client PC.
3. Click **Actions** and select **Upgrade**.
4. Click **Configure Path**.
5. Select the folder containing the unpacked upgrade files and click **Open**.
6. Click **Start Upgrade**.

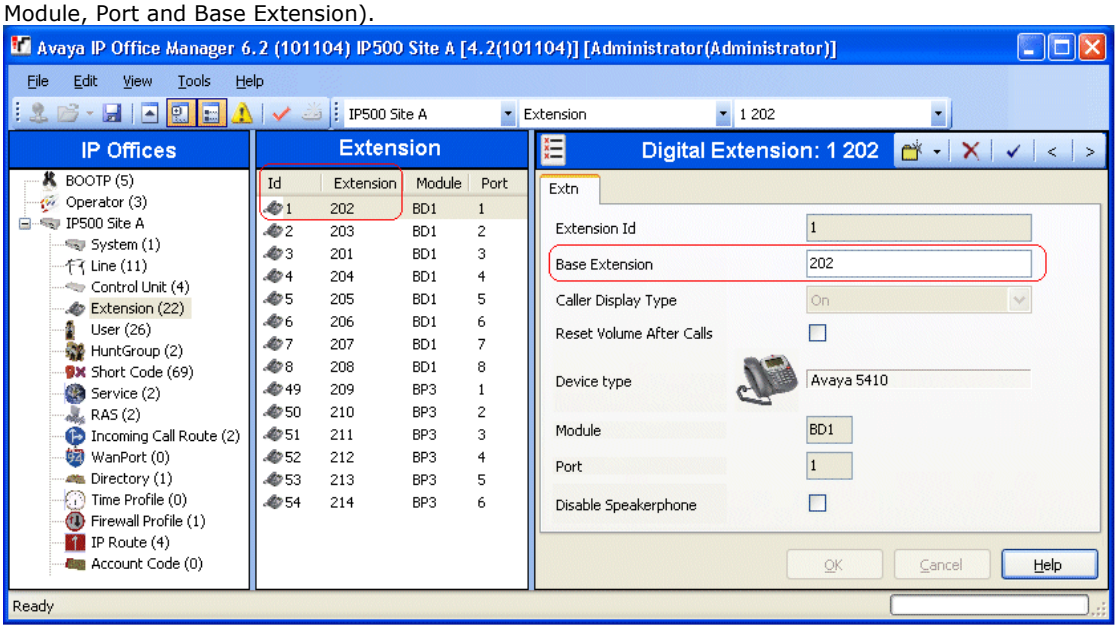
12.10 Swapping Extension Users

Whilst the example below shows 2 users swapping extensions the method can be used to swap multiple users within the configuration and effecting the swaps after a single merge of the configuration changes.

Swapping Extension Users

For this example User A (202) and User B (203) want to swap extensions.

1. Load the IP Office configuration and select **Extension**.
2. Locate the extension with the **Base Extension** set to ***202***, ie. matching User A's extension number.
   - If the group pane is visible (**View | Group Pane**) in IP Office Manager, it shows the extension details (ID, Module, Port and Base Extension).

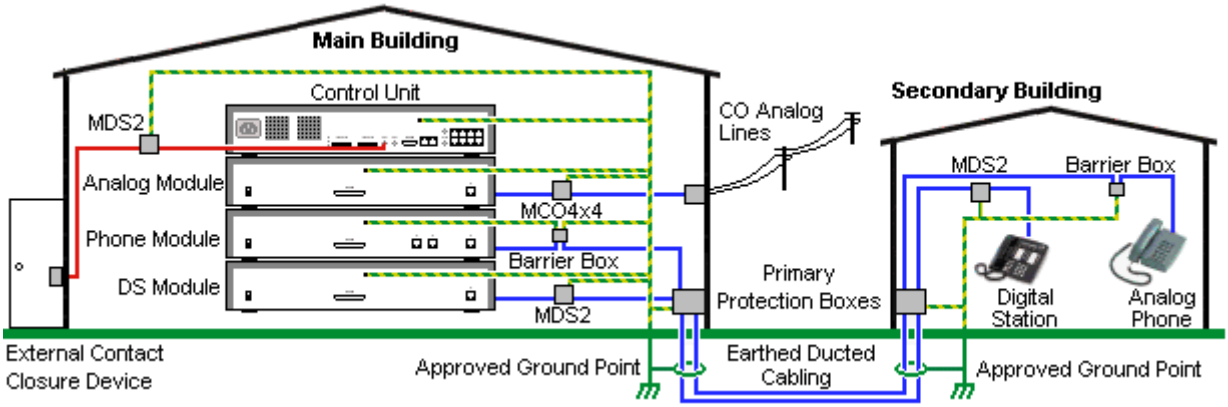


3. Select that extension and change its **Base Extension** setting to ***203***, ie. to now match User B's extension number. If IP Office Manager is set to validate edits, it will warn that this change conflicts with the existing Base Extension setting of another extension. Ignore the warning at this stage. Click **OK**.
4. Locate the other extension with the **Base Extension** set to ***203***, ie. matching User B's extension number.
5. Select that extension and change its **Base Extension** setting to ***202***, ie. to now match User A's extension number. If the error pane is visible (**View | Error Pane**), the warnings about extension conflicts should now disappear. Click **OK**.
6. Save the configuration back to the IP Office system.
7. At each of the extensions dial the log out short code set on the IP Office system. By default this is ****36***.
   - If any of the users is set to **Forced Login**, they will have to complete the login process at their new extension using their Login Code.

12.11 Out of Building Telephone Installations

The following are the only supported scenarios in which wired extensions and devices outside the main building can be connected to the IP Office system. In these scenarios, additional protection, in the form of protective grounding and surge protectors, must be fitted.

- **WARNING**
  The fitting of additional protection does not remove the risk of damage. It merely reduces the chances of damage.



- Only ports on IP Office external expansion modules are supported. Out-of-building connection to ports on base cards in the control unit is not supported.
- Cables of different types, for example trunk lines, phone extensions, ground and power connections, should be kept separate.
- All cabling between buildings should be enclosed in grounded ducting. Ideally this ducting should be buried.
- A Primary Protection Box must be provided at the point where the cables enter the building. This should be three point protection (tip, ring and ground). Typically this would be gas tube protection provided by the local telephone company. The ground wire must be thick enough to handle all the lines being affected by indirect strike at the same time.

Connection Type	Protection Device Type	Requirement
Analog Phone Extensions Phones External expansion module (POT[276] or PHONE[276]) ports only.	**IP Office Barrier Box**[189] Supports a single connection. Maximum of 16 on any expansion module.	• Connection from the expansion module to the phone must be via a surge protector at each end and via the primary protection point in each building. • The IP Office external expansion modules, control unit and IROB devices must be connected to the protective ground point in their building. • The between building connection must be via earthed ducting, preferable underground. The cable must not be exposed externally at any point.
DS Phone Extensions	**ITW Linx MDS2**[188] Supports up to 4 connections. This device was previously referred to as the Avaya 146E.	
BST Phone Extensions	None	Currently not supported.
Analog Trunks	**ITW Linx MCO4x4**[188] Supports up to 4 two-wire lines. This device was previously referred to as the Avaya 146C.	For installations in the Republic of South Africa, the fitting of surge protection on analog trunks is a requirement. For other locations where the risk of lightning strikes is felt to be high, additional protection of incoming analog trunks is recommended.
External Output Switch	**ITW Linx MDS2**[188] Supports up to 4 connections. This device was previously referred to as the Avaya 146E.	Connections from an IP Office Ext O/P port to an external relay device must be via a surge protector. When using the MDS2 on the Ext O/P port, use only the Line 1 and Equipment 1 jacks, do not use the Line 2 or Equipment 2 jacks.

The towerMAX range of devices are supplied by ITWLinx (http://www.itwlinx.com).

Página2848 de 3226.

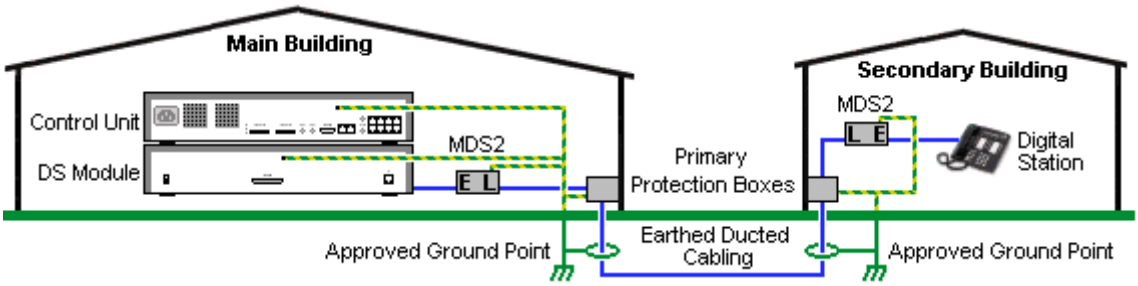
12.11.1 DS Phones

When digital phone extensions are required in another building, additional In-Range Out-Of-Building (IROB) protective equipment must be used. For phones connected to IP Office DS[271] ports, the supported device supplied by ITWLinx is a towerMAX DS/2 module. This IROB device was previous badged by Avaya as the 146E IROB.

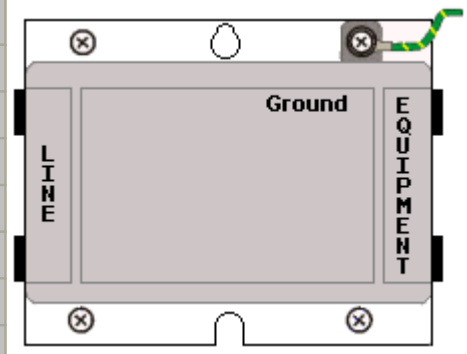
- **! WARNING**
  This device is not supported for BST port connections, ie. 4100 Series, T-Series, 7400 Series and M-Series phones.

The protection device should be installed as per the instructions supplied with the device. The ground points on the IP Office control unit and any external expansion modules must be connected to a protective ground using 18AWG wire with a green and yellow sleeve.

Typically the IROBs 2 RJ45 EQUIPMENT ports are straight through connected to the 2 RJ45 LINE ports. This allows existing RJ45 structured cabling, using pins 4 and 5, to be used without rewiring for up to two DS connection. However, each of these ports can be used to connect a second extension using pins 3 and 6.



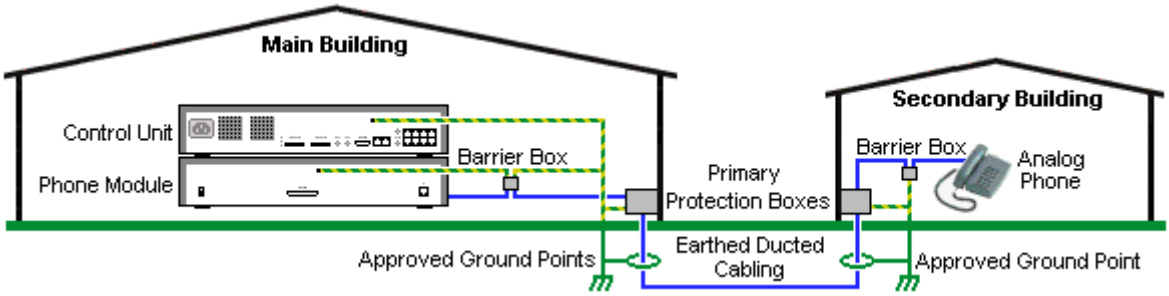
LINE		Signal		EQUIPMENT	
RJ45	1	Not used.		1	RJ45
	2	Not used.		2	
8 1	3	Ring II (Optional)		3	8 1
	4	Ring I		4	
	5	Tip I		5	
	6	Tip II (Optional)		6	
	7	Not used.		7	
	8	Not used.		8	

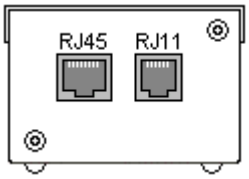
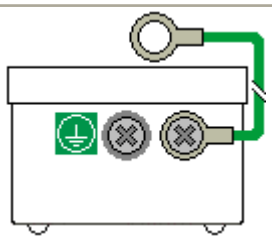


12.11.2 Analog Phone Barrier Box

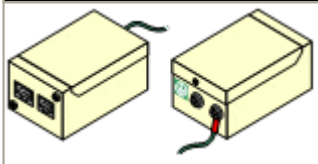
Where analog phone extensions are required in another building, additional protective equipment must be used, in the form of IP Office Phone Barrier Boxes and protective earth connections.

- **CAUTION**
  PHONE (POT) ports on the front of control units must not be used for extensions that are external to the main building.
- The correct IP Office specific barrier boxes must be used. These modules have been designed specifically for the signalling voltages used by the IP Office system:
  - Only the IP Office Phone Barrier Box should be used with Phone V1 modules.
  - Only the IP Office Phone Barrier Box V2 should be used with Phone V2 modules.
  - No other type of analog phone barrier box should be used.
- Where more than 3 barrier boxes are required in a building, they must be rack mounted using a Barrier Box rack mounting kit[190].
- A maximum of 16 barrier boxes can be used with any Phone module.
- The Phone Barrier Box does not connect the ringing capacitor in Phone V1 modules.



Main Building	Barrier Box	Secondary Building
• **RJ11** Connect to PHONE (POT) port on the Phone module using cable supplied with the barrier box. • **RJ45** Connect to the secondary building barrier box via primary protection in both buildings.		• **RJ11** Connect to analog phone. Cable not supplied. • **RJ45** From main building via primary protection in both buildings.
• **Center Screw** Connect to main building protective ground (or ground terminal of Barrier Box Rack Mounting Kit). Use 18AWG (minimum) wire with a green and yellow sleeve. • **Right-Hand Screw** Connect to ground point on Phone module using ground cable supplied with barrier box.		• **Center Screw** Connect to main building protective ground. Use 18AWG (minimum) wire with a green and yellow sleeve. • **Right-Hand Screw** Not used.

1. The following wires must be kept apart, that is not routed in the same bundle:
   - Earth leads from the barrier box to the Phone modules.
   - Internal wires, for example extension leads going directly to the Phone modules.
   - Wires from external telephone going directly to the barrier boxes.

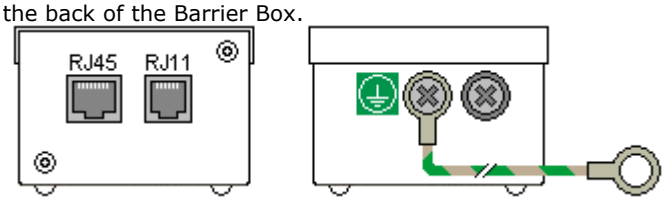
IP Office Barrier Boxes		SAP Code
	**Phone Barrier Box (81V)** Use with Phone V1 module. Includes an RJ45 to RJ11 cable and a functional earth lead.	700293897
	Phone Barrier Box V2 (101V) Use with Phone V2 module. Includes an RJ45 to RJ11 cable and a functional earth lead.	700385495
	Barrier Box Rack Mounting Kit	700293905

Página2850 de 3226.

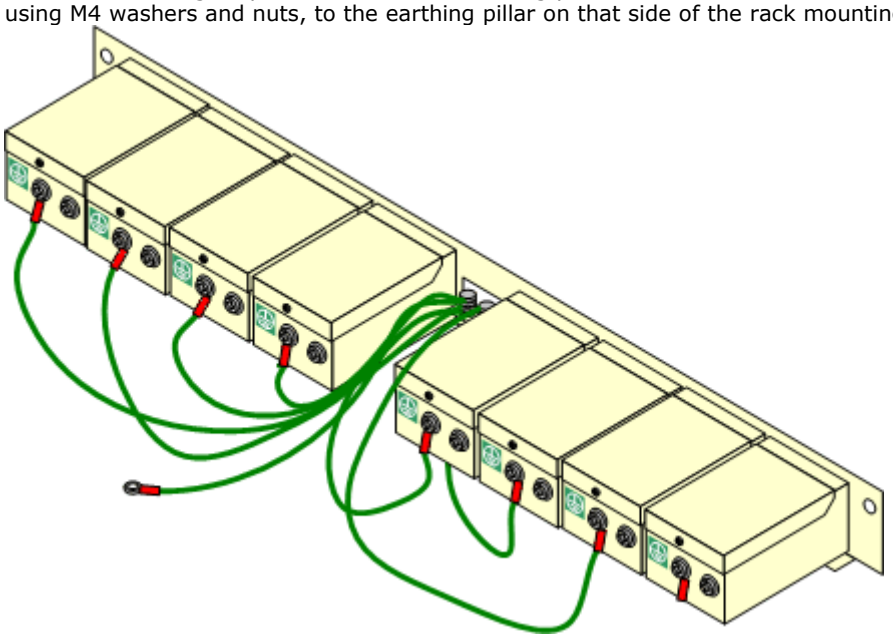
12.11.3 Rack Mounting Barrier Boxes

Where more than 3 Phone Barrier Boxes are used they must be rack mounted. The Barrier Box Rack Mounting Kit (SAP Code 700293905) supports up to 8 Phone Barrier Boxes.

1. Unscrew the two screws arranged diagonally at the front of each barrier box and use these same screws to reattach the barrier box to the rack mounting strip.
2. Each barrier box is supplied with a solid green ground wire connected to its functional ground screw. Remove and discard this wire. Connect a green/yellow ground wire to the protective earth screw in the center of the Point on the back of the Barrier Box.



3. The rack mounting strip has threaded M4 earthing pillars. Connect the other end of the barrier box ground wire, using M4 washers and nuts, to the earthing pillar on that side of the rack mounting strip.



4. Using 14AWG wire with green and yellow sleeve, connect one of the earthing pillars to the buildings protective earth.
5. Using 14AWG wire with green and yellow sleeve, connect the other earthing pillar to the Phone module.
6. Ensure that the following wires are not routed together in the same bundle:
   - Earth lead from the barrier box to the Phone module.
   - Internal wires, e.g. wires going directly to the Phone module.
   - Wires from external telephone going directly to the barrier boxes.

12.12 Using the External Output Port

All the IP Office control units are equipped with a EXT O/P port. The port is marked as EXT O/P and is located on the back of the control unit adjacent to the power supply input socket.

The port can be used to control up to two external devices such as door entry relay switches. The usual application for these switches is to activate relays on door entry systems. However, as long as the criteria for maximum current, voltage and if necessary protection are met, the switches can be used for other applications.

The switches can be switched closed, open or pulsed (closed for 5 seconds and then open). This can be done in a number of ways:

- Using IP Office short codes.
- Through the **Door Release** option in IP Office SoftConsole.
- Via the **Open Door** action in Voicemail Pro.

Default Short Codes

The following are the default short codes in the IP Office configuration for external output switch operation. They use the short code features Relay On (closed), Relay Off (open) and Relay Pulse.

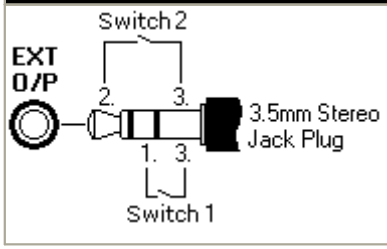
State	Switch 1	Switch 2
Closed	*39	*42
Open	*40	*43
Pulse	*41	*44

12.12.1 Port Connection

These ports are found on the rear of all IP Office control units. They are used for connection to external switching relays. The port uses a standard 3.5mm stereo jack plug for connection.

The IP Office is able to open (high resistance), close (low resistance) or pulse (close for 5 seconds and then open) two switches within the port. Either switch can be operated separately. These switches are intended for activation of external relays in systems such as door opening systems.

- **CAUTION:**
  In installations where this port is connected to a device external to the building, connection must be via a MDS2 Surge Protector and a protective ground connection must be provided on the IP Office control unit. When using the MDS2 on the Ext O/P port, use only the Line 1 and Equipment 1 jacks, do not use the Line 2 or Equipment 2 jacks.

EXT O/P	Pin	Description
	1	Switch 1.
	2	Switch 2.
	3	0 Volts (Ground/Chassis)

- Switching Capacity: 0.7A.
- Maximum Voltage: 55V d.c.
- On state resistance: 0.7 ohms.
- Short circuit current: 1A.
- Reverse circuit current capacity: 1.4A.
- Ensure that pins 1 and 2 are always at a positive voltage with respect to pin 3.

3.5mm stereo audio jack plugs are frequently sold as pre-wired sealed modules. It may be necessary to use a multi-meter to determine the wiring connections from an available plug. Typically 3 (common to both relays) is the cable screen.

Página2852 de 3226.

12.13 SNMP

SNMP (Simple Network Management Protocol) is a standard network protocol that allows the monitoring and management of data devices across a network. An SNMP agent can be built into network devices such as routers and hubs. An SNMP manager application, for example CastleRock or HP OpenView, can then communicate with those devices.

IP Office 2.0 and above supports SNMP communication. This communication can be:

- **Polling:**
  Some SNMP applications (called "managers") send out polling messages to the network. They then record the responds of any SNMP enabled devices (called "agents"). This allows the application to create a network map and to raise an alarm when devices previously present do not respond.
  - Most SNMP manager applications can also do simple IP address polling to locate non-SNMP enabled devices. However this method of polling does not identify the device type or other information.
  - SNMP polling including details about the responding device. For example an IP Office control unit's response includes the control unit type, level of software, routing table information, up time, etc.
- **Traps:**
  When certain events occur, a devices SNMP agent can send details of the event to the SNMP manager. This is called an SNMP 'trap'. These appear in the event log of the SNMP manager. Most SNMP managers can be configured to give additional alerts in response to particular traps.
- **Management:**
  Some SNMP agents support device management and configuration changes through the SNMP manager interface. This is not supported by IP Office.

IP Office SNMP operation has been tested against Castle Rock SNMPc-EE 5.1.6c and HP OpenView Network Node Manager 6.41.

What Information is Available Via SNMP

As described above, SNMP information can either be polled by the SNMP application or received as the result of the IP Office sending SNMP trap information.

While the ***.mib*** files should not be edited, they can be read using a text editor and contain descriptions of all the various information objects that can be polled or sent and the information tha each object will include. For a list of the ***.mib*** files, see Installing the IP Office MIB Files 193. The ***NOTIFICATION-TYPE*** objects are those used for SNMP traps 195, the other types of objects are those that can be polled 195.

Página2853 de 3226.

12.13.1 Installing the IP Office MIB Files

To allow full communication between an SNMP agent and an SNMP manager, the SNMP manager must load MIB files (Management Information Base) specific to the SNMP agent device and the features it supports. These MIB files contain details of the information the agent can provide and the traps that it can send. Full details of the structure of the IP Office MIB files, MIB groups within those files and event traps can be found in the "IP Office Installation Manual".

The MIB files for IP Office operation are included on the IP Office DVD in the folder ***\AdminCD\smnp_mibs***. The actual files required and the method of loading depend on the SNMP manager application being used. The details below cover the two SNMP manager applications tested.

HP Open View Network Node Manager

1. Copy the following MIB files to the applications MIBs folder.

	MIB File	Source
a.	rfc2737-entity-mib.mib	snmp_mibs\standard folder on OpenView Install CD.
b.	avayagen-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on IP Office Admin DVD.
c.	ipo-prod-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on IP Office Admin DVD.
d.	ipo-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on IP Office Admin DVD.
e.	inet-address-mib.mib	\AdminCD\snmp_mibs\Standard folder on IP Office Admin DVD.
f.	rfc2213-integrated-services-mib.mib	\AdminCD\snmp_mibs\standard folder on OpenView Install CD.
g.	diffserv-dscp-tc.mib	\AdminCD\snmp_mibs\Standard folder on IP Office Admin DVD.
h.	diffserv-mib-hpov.mib	\AdminCD\snmp_mibs\Standard folder on IP Office Admin DVD.
i.	ipo-phones-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on IP Office Admin DVD.

2. Start the OpenView Network Node Manager console.
3. Select Options and then Load/Unload MIBs: SNMP.
4. Select Load and select all the MIB files listed above.
5. Select Compile.

CastleRock SNMPc 5.1.6c and earlier

1. Copy the following MIB files to the applications MIBs folder, normally C:\Program Files\SNMPc Network Manager\mibfiles.

	MIB file	Source
a.	ENTITY-MIB	\AdminCD\snmp_mibs\Standard on IP Office Admin DVD.
b.	AVAYAGEN-MIB.mib	\AdminCD\snmp_mibs\IPOffice on IP Office Admin DVD.
c.	IPO-PROD-MIB.mib	\AdminCD\snmp_mibs\IPOffice on IP Office Admin DVD.
d.	IPO-MIB.mib	\AdminCD\snmp_mibs\IPOffice on IP Office Admin DVD.
e.	INET-ADDRESS-MIB.mib	\AdminCD\snmp_mibs\Standard on IP Office Admin DVD.
f.	INTEGRATED-SERVICES-MIB	\AdminCD\snmp_mibs\Standard on IP Office Admin DVD.
g.	DIFFSERV-DSCP-TC.mib	\AdminCD\snmp_mibs\Standard on IP Office Admin DVD.
h.	DIFFSERV-MIB.mib	\AdminCD\snmp_mibs\Standard on IP Office Admin DVD.
i.	IPO-PHONES-MIB.mib	\AdminCD\snmp_mibs\IPOffice on IP Office Admin DVD.

2. In SMNPc select Config | MIB Database.
3. Select Add and select the MIB files listed above in the order listed.

CastleRock SNMPc V5.0.1

The MIB installation instructions provided above are correct for CastleRock SNMPc V5.0.8 and later. For V5.0.1 of CastleRock SNMPc the following must be carried out:

1. Copy all of the IP Office MIBs and standard MIBs from the IP Office Administrator Applications DVD to the SNMPc mibfiles directory.
2. In the SNMPc mibfiles directory open the files STANDARD.mib and SNMPv2-SMI.mib in Notepad.
3. In the SNMPv2-SMI.mib file find the definition of zeroDotZero and copy this to the clipboard.
4. In the STANDARD.MIB file find the SNMPv2-SMI section and paste in the definition of zeroDotZero from the clipboard before the end of this section (just before the END statement).
5. Save the modified STANDARD.MIB file.
6. Add the MIB file SNMP-FRAMEWORK-MIB.mib to the MIB database using the instructions provided in the IP Office installation guide.
7. Add all the MIB files listed in the instructions provided in the IP Office installation guide in the order given.
8. Compile the MIBs ready for use.

The reason for this is: The IPO-PHONES-MIB.mib relies upon the DIFFSERV-MIB.mib for the definition of the textual convention of IndexInteger. The DIFFSERV-MIB needs the definition of the textual convention zeroDotZero which is normally defined in SNMPv2-SMI.mib. However including SNMPv2-SMI.mib in the MIB file compilation list results in errors due to conflicts with what appear to be internal definitions within SNMPc and the SNMPv2-SMI section in its STANDARD.mib file. Therefore to resolve the issue the required definition of zeroDotZero must be placed in the SNMPv2-SMI section in SNMPc's STANDARD.mib file.

12.13.2 Enabling SNMP and Polling Support

In order for the IP Office control unit to be discovered and polled by an SNMP manager, its SNMP agent must be enabled and placed in the same read community as the SNMP manager.

1. In IP Office Manager, receive the control unit's configuration.
2. Double-click **System** from the Configuration Tree panel and select the SNMP tab.
3. Tick **SNMP Enabled**.
4. In SNMP Port, enter the UDP port number used by the IP Office SNMP agent to listen for and respond to SNMP traffic. The normal default is 161.
5. In **Community (Read-only)**, enter the community to which the device belongs for read access. This community name must match that used by the SNMP manager application when sending requests to the device. The community public is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
6. Click **OK**.
7. Send the configuration back to the IP Office and select reboot.
8. Following the IP Office reboot, the SNMP manager should be able to discover the control unit.
9. The control unit's response will include details of the control unit type and the current level of core software.

12.13.3 Enabling SNMP Trap Sending

In IP Office Manager, receive the control unit's configuration.

1. Double-click **System** from the configuration tree panel and select the **System Events** tab.
2. Ensure that **SNMP Enabled** is ticked and set the other settings required for the SNMP Agent Configuration section.
3. Click the Alarms tab.
4. Click **Add...** and select **Trap** as the type of new alarm. You can add up to 2 SNMP traps, each with different destination and alarm settings.
   - **Server Address**
     Enter the IP address or fully-qualified domain name of the PC running the SNMP manager application.
   - **Port**
     Enter the Port on which the traps messages should be sent. This is the UDP port on which the IP Office sends SNMP trap messages. The default is 162.
   - **Community**
     Set the Community that will be used by the agent and the SNMP manager. The community public is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
   - **Format**
     The default to use is IP Office. SMGR is only used for system being managed through Avaya SMGR.
   - **Minimum Severity Level**
     Set the alarm severity or higher for alarms that should be sent.
5. Select the **Events** which should be sent.
6. Click on **OK**.
7. Send the configuration back to the IP Office and select reboot.

12.14 Refreshing the System Files from Manager

This process will copy all system files not present on the System SD card and those files which have a different version to those already present on the card. This process can be used to refresh the card contents if it is suspected some files may be missing.

This process is not supported as a method of upgrading. It should only be used with the version of IP Office Manager that matches the software already being run by the system.

- **Admin Lite Not Supported**
  Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).

To upgrade a system using the embedded file manager

1. Using IP Office Manager, select **File | Advanced | Embedded File Management**.
2. Using the **Select IP Office** menu, select the IP Office system.
3. The file contents of the memory cards are displayed.
4. Select **File | Backup System Files**. The contents of the **/primary** folder on the System SD card will be copied to the **/backup** folder. This process takes approximately 6 minutes.
5. Select **File | Upload System Files**. The system files that IP Office Manager has will be uploaded to the **/primary** folder on the System SD card. This includes IP Office software files and Embedded Voicemail prompt files. It does not include phone firmware and bin files. Depending on the files that need to be updated, this process can take up to 40 minutes.

12.15 Reset Button

IP500 V2 control units have a **Reset** button. Pressing the button while the control unit is starting up will pause the start up until the button is released. The effect of pressing the button during normal operation will depend on how long the button is pressed and is indicated by the CPU LED.

Press Duration (seconds)	CPU LED	Action	Summary
0 to 5.	**Off**	**None**	None.
5 to 10.	**Orange**	**Reboot When Free**	Reboot when free with new incoming/outgoing call barring. A reboot using the reset button is recorded in the Audit Trail.
10 to 30.	**Flashing orange**	**Erase Configuration**	Erase the configuration, alarm log and audit trail. Immediate reboot without waiting for active calls to end. See Erasing the configuration 170 for full details.
30 to 40.	**Red**	**Erase All.**	Erase configuration, alarm log and core software. See Erasing the Operational Software 199 for full details.
Over 40.	**Flashing green**	**None**	None.

12.16 AUX Button

IP500 V2 control units have an AUX button. This button can be used as follows.

- If pressed during a restart of the control unit, the control unit skips booting 144 from the ***/primary*** folder on the System SD card.
- If pressed for more than 5 seconds when a system is running, the control unit shuts down for 10 minutes.

12.17 RS232 Port Maintenance

The RS232 port on the back of system control unit is not normally used when configuring an IP Office system. However, the port can be used for a number of maintenance processes.

- **WARNING**
  Use of the RS232 port should only be performed if absolutely necessary and only if the actions cannot be completed using IP Office Manager or IP Office Web Manager. In all cases, you must make every effort to ensure that you have a backup copy of the system configuration.

RS232 Port Maintenance Processes

1. **RS232 port cable connection and configuration** 278
2. **Defaulting the configuration using debug** 171
3. **Defaulting the configuration using the Boot Loader** 172
4. **Defaulting the security using the RS232 port** 175
5. **Defaulting the security using the Boot Loader** 176
6. **Erasing the core software using debug** 200
7. **Erasing the core software using the Boot Loader** 201

12.18 Erasing the Core Software

When the firmware loaded by the control unit is erased, the control unit begins making BOOTP requests for replacement firmware files. IP Office Manager can act as a BOOTP server and respond to the control units request with the appropriate file from those installed with IP Office Manager.

Unlike other control units, when the firmware loaded by an IP500 V2 control unit is erased, the IP500 V2 control unit will first look for replacement firmware on its SD cards before falling back to using a BOOTP request to IP Office Manager.

- ⚠ Do not perform any of the following processes unless absolutely necessary. The IP Office software can normally be upgraded using IP Office Manager[180] .
- ⚠ This process erases the operational software. Before attempting this process you must know the MAC and IP addresses of the system, plus have a backup copy of its configuration and the correct .bin file for the control unit type and level of software.
- ⚠ The presence of any firewall blocking TFTP and or BOOTP causes this process to fail.

The processes below should be performed from a PC with a fixed IP address, directly connected to the IP Office control unit and with the IP Office system disconnected from any network. During the process, the control unit's IP address may default to a value in the 192.168.42.1 to 192.168.42.10 range. If this occurs, it may be necessary to amend the BOOTP entry in IP Office Manager to match the address the system is using.

Process Options

1. **Erasing core software using the Reset button**[199]
   Note that this method also defaults the configuration.
2. **Erasing core software using Debug**[200]
3. **Erasing core software using the Boot Loader**[201]

12.18.1 Erasing Core Software Using the Reset Button

Read the note and the warnings regarding erasing the core software[199] before using this process. Also read and note the warnings regarding defaulting the configuration[170] before using this process.

To erase the core software and configuration using the Reset button

Use this process to reboot the system when free. Once invoked, the system bars any new incoming or outgoing calls until after the reboot.

1. Run IP Office Manager.
   - In the **BOOTP** entries, check that there is an entry that matches the MAC Address, IP Address and .bin file used by the system. An entry is normally automatically created when a configuration has been loaded from that IP Office. .
     - If an entry is not present, create a new entry manually. The first two details can be found in the Control Unit settings in the configuration file. Then close and restart IP Office Manager.
   - Under **File | Preferences** ensure that IP Office Manager is set to 255.255.255.255. Also check that **Enable BootP Server** is checked.
   - Select **View | TFTPLog**.
   - Check that the required .bin file is present in Manager's working directory.
2. On the rear of the control unit, press and hold the **Reset** button for between 30 to 40 seconds until the **CPU** led changes to red.
3. When the **CPU** LED changes to red, release the button.
4. The system erases its current software and sends out a BootP request on the network for new software.

12.18.2 Erasing Core Software Using Debug

Read the note and the warnings regarding erasing the core software 199 before using this process.

- **WARNING**
  Use of the RS232 port should only be performed if absolutely necessary and only if the actions cannot be completed using IP Office Manager or IP Office Web Manager. In all cases, you must make every effort to ensure that you have a backup copy of the system configuration.

To erase the core software using Debug

1. Run IP Office Manager.
   - In the **BOOTP** entries, check that there is an entry that matches the MAC Address, IP Address and .bin file used by the system. An entry is normally automatically created when a configuration has been loaded from that IP Office. .
     - If an entry is not present, create a new entry manually. The first two details can be found in the Control Unit settings in the configuration file. Then close and restart IP Office Manager.
   - Under **File | Preferences** ensure that IP Office Manager is set to 255.255.255.255. Also check that **Enable BootP Server** is checked.
   - Select **View | TFTPLog**.
   - Check that the required .bin file is present in Manager's working directory.
2. Attach the serial cable between the PC and the RS232 DTE port on the IP Office control unit.
   a. Start the terminal program on your PC. Ensure that it has been setup as listed in RS232 DTE Port Settings 278 . Within a HyperTerminal session, the current settings are summarized across the base of the screen.
   b. Enter **AT** (note upper case). The control unit should respond ***OK***.
   c. Enter **AT-DEBUG**. The control unit should response with the time and date and then ***Hello>*** to show it is ready to accept commands.
3. To erase the current configuration in RAM memory enter **upgrade**.
4. The IP Office will erase its current software and then send out a BootP request on the network for new software. IP Office Manager will respond and start transferring the software using TFTP.

12.18.3 Erasing Core Software Using the Boot Loader

Read the note and warnings regarding erasing the core software 199 before using this process.

- **WARNING**
  Use of the RS232 port should only be performed if absolutely necessary and only if the actions cannot be completed using IP Office Manager or IP Office Web Manager. In all cases, you must make every effort to ensure that you have a backup copy of the system configuration.

To erase the core software using the Boot Loader

1. Run IP Office Manager.
   - In the **BOOTP** entries, check that there is an entry that matches the MAC Address, IP Address and .bin file used by the system. An entry is normally automatically created when a configuration has been loaded from that IP Office. .
     - If an entry is not present, create a new entry manually. The first two details can be found in the Control Unit settings in the configuration file. Then close and restart IP Office Manager.
   - Under **File | Preferences** ensure that IP Office Manager is set to 255.255.255.255. Also check that **Enable BootP Server** is checked.
   - Select **View | TFTPLog**.
   - Check that the required .bin file is present in Manager's working directory.
2. Attach the serial cable between the PC and the RS232 DTE port on the IP Office control unit.
   a. Start the terminal program on your PC. Ensure that it has been setup as listed in RS232 DTE Port Settings 278 . Within a HyperTerminal session, the current settings are summarized across the base of the screen.
   b. Arrange the program windows so that the Terminal program and IP Office Manager TFTP Log are visible at the same time.
   c. Switch off power to the IP Office control unit.
   d. Power on the control unit and press the escape key every second until you get a Loader message. Below is an example.

      ```
      P12 Loader 2.4
      CPU Revision 0x0900
      ```

   e. Enter **AT** (note upper case). The control unit should respond ***OK***.
   f. If an OK response is not received, check the settings of your terminal program and repeat the process above.
3. Enter **AT-X**. The control unit should respond **Multi-Sector Erase**.
4. The control unit will now request the .bin file it requires. For IP500 V2 control units this will be from files on the System SD card. For other control units it will be from IP Office Manager and appears in the TFTP Log.
5. If the file transfers does not appear to be taking place, check that the IP address shown in the TFTP Log matches the BOOTP entry. Adjust the BOOTP entry if necessary.
6. When completed the system will reboot.

12.19 Enabling IP Office Web Manager

Access to IP Office Web Manager is via the system's IP address and then selecting the ***IP Office Web Management*** link. In order to use IP Office Web Manager, a number of criteria as listed below must be met. Most of these are applied automatic to a new system installed with IP Office Release 8.0 or higher. However, for systems being upgraded to IP Office Release 8.0 or higher, additional upgrade steps may be required.

Enabling IP Office Web Manager

1. The IP Office Web Manager files must be present on the System SD card. This can be done in a number of way:
   - By selecting to include those files when prompted to do so while recreating the IP Office SD card 146 using IP Office Manager.
   - By selecting **Upload System Files** when upgrading the system using IP Office Manager.
2. The IP Office system security must allow IP Office Web Manager operation:
   - This is done automatically for any new system installed with IP Office Release 8.0 or higher software.
   - This is done automatically for any existing pre-IP Office Release 8.0 system during the upgrade if the system is set to use the pre-IP Office Release 8.0 default password.
   - For any system upgraded to IP Office Release 8.0 without first being set back to the default password, either:
     - Using IP Office Manager:
       1. If not already done, select **View | Advanced View**.
       2. Select **File | Advanced | Erase Security Settings (Default)**.
       3. From the **Select IP Office** dialog, select the required system and click **OK**.
       4. Enter the user name **Administrator** and the password for that account.
       5. IP Office Manager will confirm if the action was successful or not.
     - Default the system security settings using an RS232 DTE cable 173.

Chapter 13.
System Components

13. System Components

This section covers the individual components that can comprise an IP Office installation.

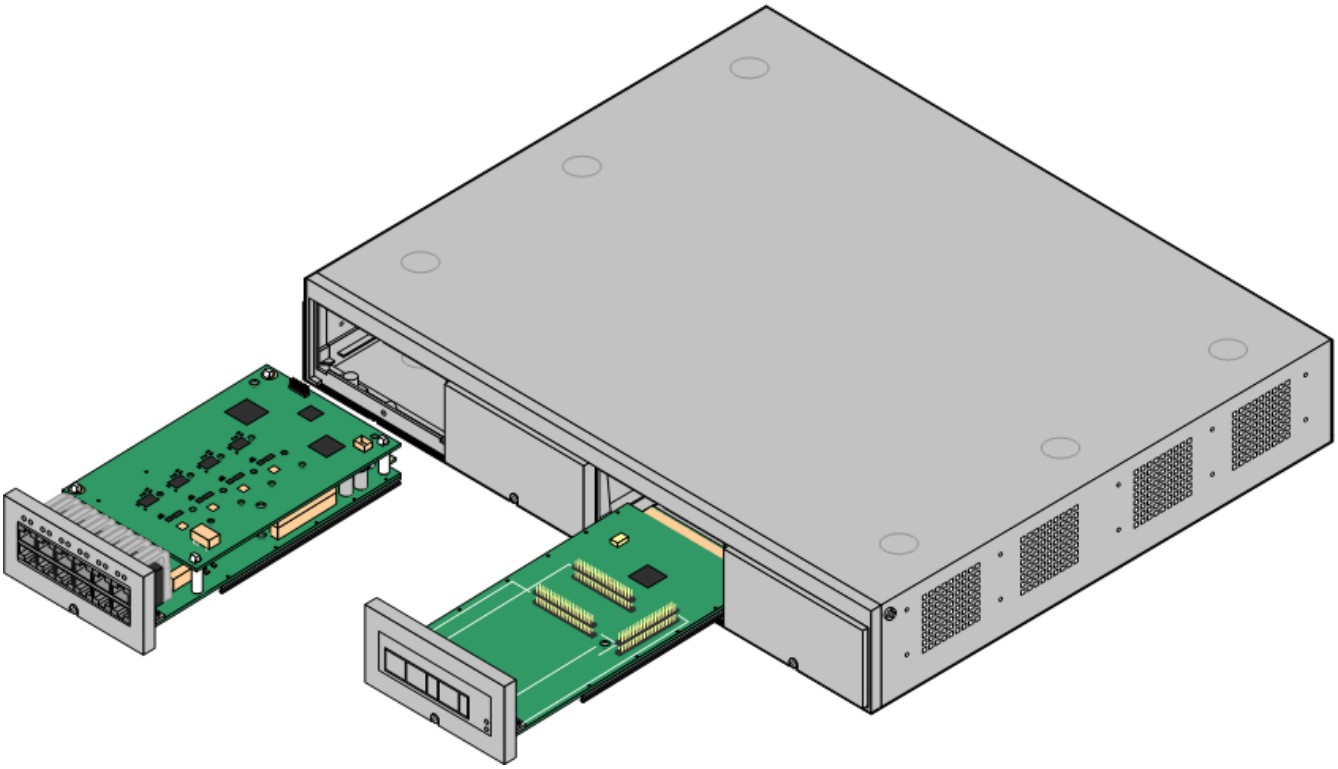
- **IP500 V2 Control Unit** 205
- **System SD Cards** 208
- **IP500 Base Cards** 209
- **IP500 Trunk Daughter Cards** 223
- **IP500 External Expansion Modules** 228
- **Mounting Kits** 247
- **Phones** 249
- **Phone Add-Ons** 250
- **Applications** 251
- **Physical Ports** 264
- **Licenses** 279

Additional information is included for:

- **Hardware Software Compatibility** 286
- **Hardware PCS Levels** 296
- **TAA Hardware** 296

13.1 IP500 V2 Control Unit

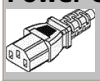
The slots are numbered 1 to 4 from left to right. They can be used in any order. However if the capacity for a particular type of card is exceeded, the card in the rightmost slot will be disabled. The unit must not be used with uncovered slots.

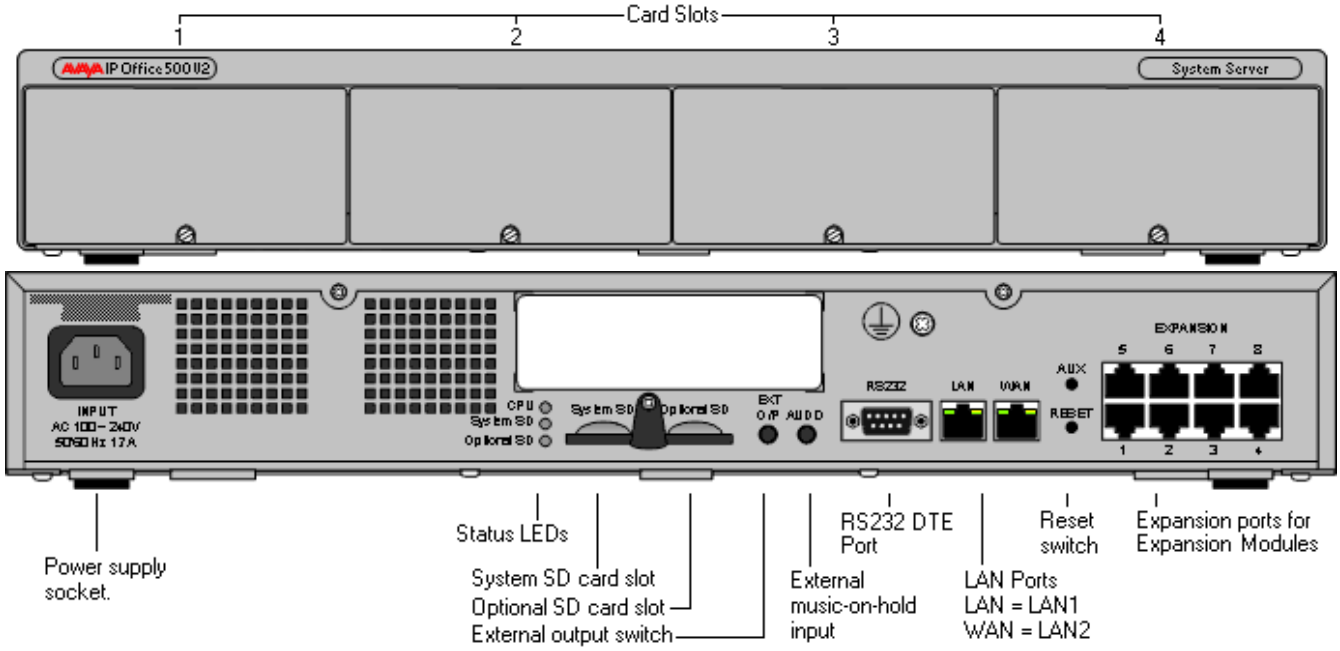


- The Avaya IP Office IP500 V2 is also known as "IPO IP500 V2 Cntrl Unit", "IP Office IP 500 v2", "IPO IP500 v2", "IP 500 V2", "IP500 V2", "IPO 500v2 System Unit Assembly" or "IP Office 500 v2". Throughout this documentation the term IP500 V2 is used.

Feature	Capacity
Maximum Extensions	Up to 384 extensions in IP Office standard modes.
Conference Parties	128 as standard but maximum 64 in any individual conference. Silence suppression is applied to conferences with more than 10 parties.
Trunks Cards	4 IP500 trunk daughter cards.
Voice Compression Channels	Up to 148 channels using IP500 VCM and IP500 Combination cards.
Voicemail Channels	Maximum 40 usable for Voicemail Pro/TAPI WAV connection sessions subject to available licenses. For Embedded Voicemail, up to 6 (2 by default, additional channels require licenses).
Locales	Supported in all IP Office locales[42].
Minimum Software Level	IP Office Essential Edition: 6.0 minimum. IP Office Basic Edition - PARTNER® Mode: 6.0 minimum. IP Office Basic Edition - Norstar Mode: 6.1 minimum. IP Office Basic Edition: 7.0 minimum. Bin file = ip500v2.bin.
Power Supply	Internal power supply unit.
Mounting	Free-standing, rack mounted (requires IPO IP500 RACK MNTG KIT) or wall mounted (requires IPO IP500 WALL MNTG KIT).
Dimensions	Width: 445mm/17.5". Depth: 365mm/14.4". Height: 73mm/2.9"/2U. Clearance: 90mm minimum all sides, 220m at front.
Memory	Maximum configuration file size: 2048KB.

Página2866 de 3226.

Name		Description	Country	SAP Code
IP500 V2 Control Units	**IPO IP500 V2 Cntrl Unit**	IP Office 500 V2 Control Unit		700476005
	IPO IP500 V2 Cntrl Unit TAA	" Trade Agreements Act[296] compliant variant.		700501510
Avaya SD Memory Card	**IPO IP500 V2 SYS SD CARD AL**	IP500 V2 A-Law SD Card		700479702
	IPO IP500 V2 SYS SD CARD MUL	IP500 V2 U-Law SD Card		700479710
IEC60320 C13 Earthed Power Cord 	**IPO - PWR LEAD (EARTHED) EU CEE7/7**	CEE7/7	Europe	700289762
	IPO - PWR LEAD (EARTHED) UK	BS1363	United Kingdom	700289747
	IPO - PWR LEAD (EARTHER) US	NEMA5-15P	America	700289770
Mounting Kits	**IPO IP500 WALL MNTG KIT V3**	IPO IP500 WALL MNTG KIT V3		700503160
Miscellaneous	**IP500 Blanking Plate Kit**	IP500 Blanking Plate Kit		700429194



Ports	Description
AUDIO 267	3.5mm Stereo jack socket. Used for external music on hold source input.
AUX 144	• If pressed during a restart of the control unit, the control unit skips booting 144 from the ***/primary*** folder on the System SD card. • If pressed for more than 5 seconds when a system is running, the control unit shuts down for 10 minutes.
CPU	Indicates the status of the control unit. • **Alternate red/green** = Starting up. • **Green on** = Okay. • **Red on** = No software. • **Flashing Red** = Error/Shutdown.
EXPANSION 273	RJ45 socket. Used for direct connection to external expansion modules using the Expansion Interconnect cable supplied with the expansion module.
EXT O/P 191	3.5mm Stereo jack socket. Used for switching external relay systems such as door entry controls. The port contains two independent switches controlled by the IP Office.
INPUT 31	AC power input port.
LAN 274	RJ45 socket. The port is a full-duplex 10/100Mbps auto-sensing, MDI crossover port. With the WAN port forms a managed layer 3 Ethernet switch.
Optional SD 142	Used for the Optional SD card. The LED is used in the same way as for the System SD *(see below)*.
RESET 197	This switch is used to restart the IP Office, optionally erasing the configuration and or the core software in the process. See Reset Button 197.
RS232 278	9-Way D-Type socket. Used for system maintenance.
System SD 142	Used for the System SD card,. The LED is used as follows. • **Off** = Card shutdown. • **Green on** = Card present. • **Green flashing** = Card in use. • **Orange steady** = Reset imminent. • **Red flashing** = Card initializing or shutting down. • **Red fast flashing** = card full • **Red steady** = Card failure/wrong type.
WAN 274	RJ45 socket. The port is a full-duplex 10/100Mbps auto-sensing, MDI crossover port. With the WAN port forms a managed layer 3 Ethernet switch. This port is not supported on systems running in IP Office Basic Edition - PARTNER® Mode, IP Office Basic Edition - Norstar Mode or IP Office Basic Editions.
⏚	Used for connection of a functional or protective ground 93. Use of a ground for all systems is recommended and for some locales may be a regulatory requirement.

Página2868 de 3226.

13.2 IP500 V2 System SD Cards

This type of card is used with IP500 V2 control units and is a mandatory item. The card is used for system licensing and also for Embedded Voicemail if required. It also holds the firmware files loaded by the system and telephones when the system is installed.

The control unit must be fitted with one of these feature keys even if no licenses are being used.

- The PLDS host ID used for the license file must match that shown by the 12 digit **PLDS ID** printed on the SD card label. Older cards have an 10 digit feature key serial number shown by **FK** or **FK SN**. For those cards add the prefix ***11*** to obtain the card's PLDS ID.

- By default the card can be used for 2 ports of Embedded Voicemail. Additional ports up to a maximum of 6 can be enabled by the addition of licenses[279]. The voicemail mailbox message and prompt capacity supports 2 simultaneous connections and 15 hours of storage. This can be expanded up to 6 channels by the addition of licenses, each of which enables an additional two channels and an additional 5 hours of storage.

- ⚠ **WARNING**
  These cards should only be formatted using IP Office Manager or System Status Application. The cards should only be removed from a system after either a card shut down[157] or a system shut down[163].

Feature Key Dongle	SAP Code
IPO IP500 V2 SYS SD CARD A-LAW	700479702
IPO IP500 V2 SYS SD CARD MU-LAW	700479710

  - **IP Office U-Law SD Card**
    A system fitted with this type of card defaults to U-Law telephony and IP Office Basic Edition ***Key System*** operation. Intended for North American locales.

  - **IP Office A-Law SD Card**
    A system fitted with this type of card defaults to A-Law telephony and IP Office Basic Edition ***PBX System*** operation. Intended for locales outside North America.

Embedded Voicemail

The System SD card can be used to provide Embedded Voicemail for the system. Unlicensed, the Embedded Voicemail provided by the system supports 2 simultaneous connections and 15 hours of storage. This can be expanded up to 6 channels by the addition of licenses[279], each of which enables an additional two channels and an additional 5 hours of storage.

For full details of Embedded Voicemail setup and configuration, refer to the Embedded Voicemail Installation manual. The cards are preloaded with the following languages:

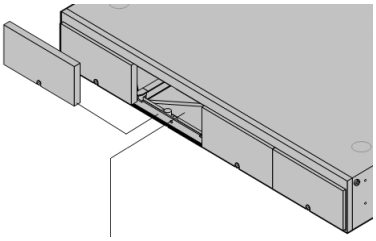
- **Arabic**, **Cantonese**, **Danish**, **Dutch**, **English (UK)**, **English (US)**, **Finnish**, **French**, **French (Canada)**, **German**, **Hebrew**, **Italian**, **Japanese**, **Korean**, **Mandarin**, **Norwegian**, **Polish**, **Portuguese**, **Portuguese (Brazil)**, **Russian**, **Spanish**, **Spanish (Argentina)**, **Spanish (Latin)**, **Spanish (Mexico)**, **Swedish**, **Turkish**.

PCM Encoding

- **A-Law or Mu-Law**
  PCM (Pulse Code Modulation) is a method for encoding voice as data. In telephony, two methods PCM encoding are widely used, A-law and Mu-law (also called U-law). Typically Mu-law is used in North America and a few other locations while A-law by the rest of the world. As well as setting the correct PCM encoding for the region, the A-Law or Mu-Law setting of an IP Office system when it is first started affects a wide range of regional defaults relating to line settings and other values.

  - For IP500 V2 systems, the encoding default is set by the type of System SD card installed when the system is first started.

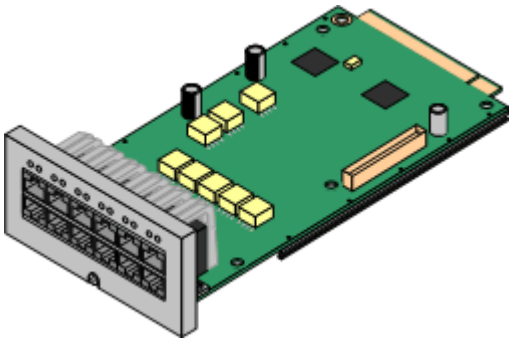
13.3 IP500 Base Cards



The IP500 V2 control unit has 4 slots for the insertion of IP500 base cards. The slots are numbered 1 to 4 from left to right. Normally they can be used in any order, however if the capacity for a particular type of card is exceeded, the card in the rightmost slot will be disabled.

Each base card includes an integral front panel with ports for cable connections. Typically the first 8 ports on the left are for connection of extension devices. The 4 ports on the left are used for connection of trunks if a trunk daughter card[25] is added to the base card.

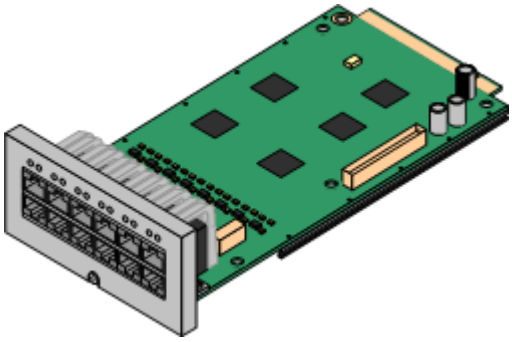
IP500 Digital Station Base Card[218]



This card provides 8 DS (digital station) ports for the connection of Avaya digital phones.

- The card can be fitted with an IP500 trunk daughter card[25] which uses the base card ports for trunk connection.
- **Maximum:** 3 per control unit.
  - Connections for 4100, 7400, M-Series and T-Series phones use the IP500 TCM8 Digital Station card.

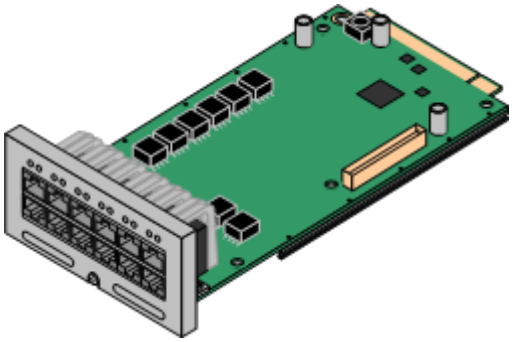
IP500 Analog Phone Base Card[213]



The card is available in two variants, supporting either 2 or 8 analog phone ports.

- The card can be fitted with an IP500 trunk daughter card[25] which uses the base card ports for trunk connection.
- **Maximum:** 4 per control unit.
  - The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors.
  - If fitted with an IP500 Analog Trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12.

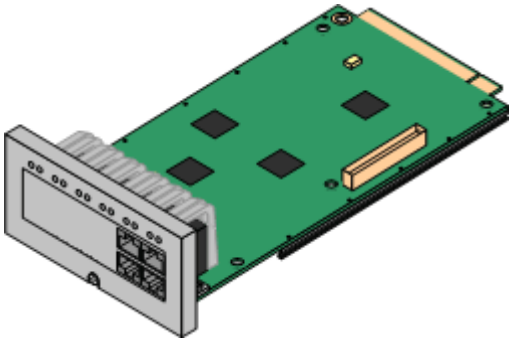
IP500 TCM8 Digital Station Card[220]



This card provides 8 BST (digital station) ports for the connection of Avaya 4100, 7400, M-Series and T-Series phones.

- The card can be fitted with an IP500 trunk daughter card[25] which uses the base card ports for trunk connection.
- **Maximum:** 4 per control unit per IP500 V2 control unit.

IP500 VCM Base Card[221]

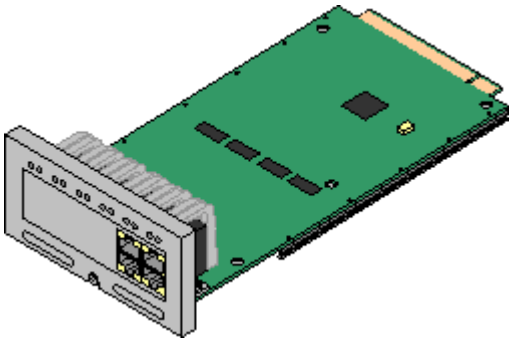


This card is available in variants supporting either 32 or 64 voice compression channels for use with VoIP calls.

- The card can be fitted with an IP500 trunk daughter card[25] which uses the base card ports for trunk connection.
- **Maximum:** 2 per control unit.

Página2870 de 3226.

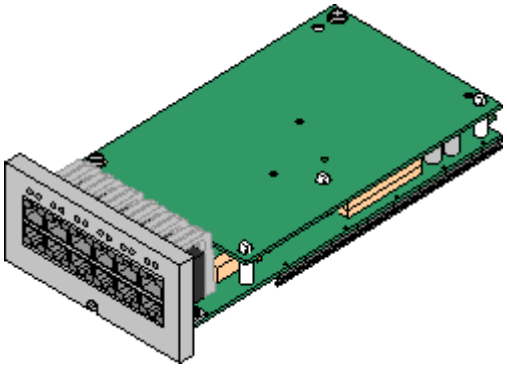
IP500 4-Port Expansion Base Card [212]



This card adds an additional 4 expansion ports for external expansion modules. The card is supplied with four 2m yellow interconnect cables.

- This card does not accept any IP500 trunk daughter card.
- **Maximum:** 1 per control unit (Right-hand slot 4 only).
- **Supported Expansion Modules:** The following external expansion modules are supported:
  - IP500 Analogue Trunk Module
  - IP500 BRI So Module
  - IP500 Digital Station Module
  - IP500 Digital Station Module
  - IP500 Digital Station Module
  - IP500 Phone Module

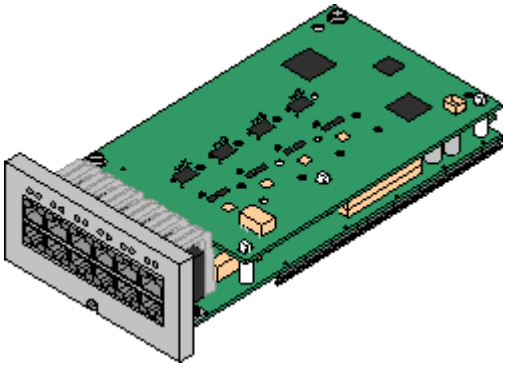
IP500 BRI Combination Card [216]



This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 2 BRI trunk ports (9-10, 4 channels). The card also includes 10 voice compression channels.

- **Maximum:** 2 combination cards per IP500 V2 control unit, regardless of type.
  - IP500 Combination cards are pre-fitted with a trunk daughter card which cannot be removed or changed for another type/capacity trunk daughter card.
  - IP Office Basic Edition - Norstar Mode and IP Office Basic Edition systems are limited to a maximum of 12 BRI channels using BRI Combination and or BRI trunk daughter cards.

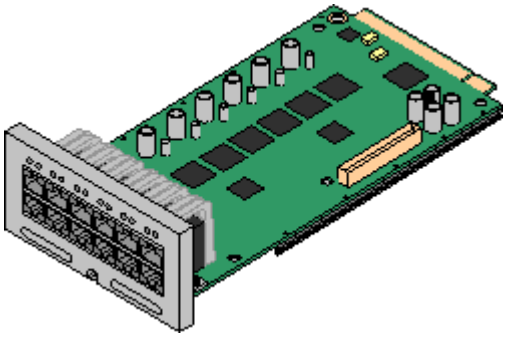
IP500 ATM Combination Card/IP500 ATM Combination Card V2 [214]



This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 4 analog trunk ports (9-12). The card also includes 10 voice compression channels.

- **Maximum:** 2 combination cards per IP500 V2 control unit, regardless of type.
  - IP500 Combination cards are pre-fitted with a trunk daughter card which cannot be removed or changed for another type/capacity trunk daughter card.
  - The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors.
  - During power failure phone port 8 is connected to analog trunk port 12.

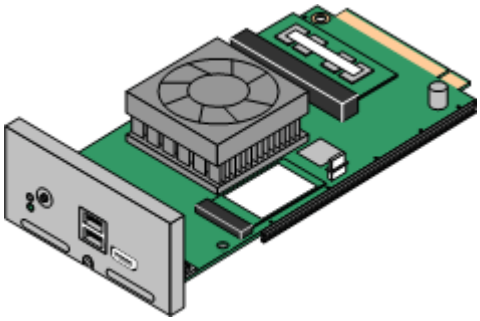
IP500 ETR6 Base Card [219]



This card is only supported in an IP500 V2 control unit running in IP Office Basic Edition - PARTNER® Mode or IP Office Basic Edition. It provides 6 ETR ports for connection of ETR phones. 2 Analog extension ports are also provided for emergency use only with an analog trunk card.

- The card can be fitted with an IP500 trunk daughter card which uses the base card ports for trunk connection.
- **Maximum:** 3 per IP500 V2 control unit.
- The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors.
- If fitted with an IP500 Analog Trunk daughter card, during power failure phone ports 7 and 8 are connected to analog trunk port 12. However during normal operation analog phone ports 7 and 8 are not useable.

Unified Communications Module [217]

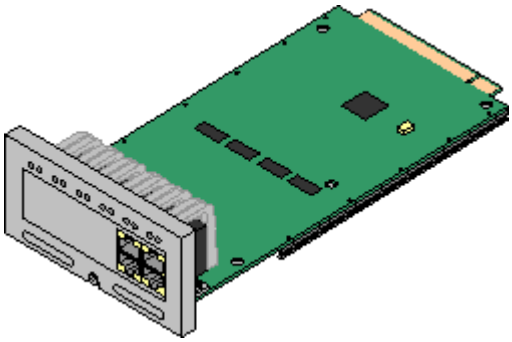


This card acts as an embedded Linux server for the one-X Portal for IP Office and/or Voicemail Pro applications.

13.3.1 4-Port Expansion Card

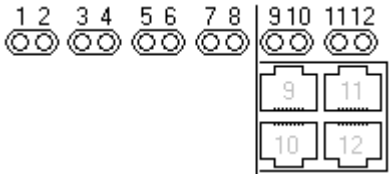
This card is used to add 4 additional expansion ports to the control unit.

- Systems running in IP Office standard modes support 8 external expansion modules as standard. If fitted with an IP500 4-Port Expansion Base Card, up to 12 external expansion modules are supported.



- **Supports**
  Provides 4 additional expansion ports[273] for connection of external expansion modules.
- **Supported Expansion Modules:** The following external expansion modules are supported:
  - IP500 Analogue Trunk Module
  - IP500 BRI So Module
  - IP500 Digital Station Module
  - IP500 Digital Station Module
  - IP500 Digital Station Module
  - IP500 Phone Module
- **Maximum per Control Unit:** 1 - Right-hand slot 4 only.
- **IP500 Trunk Card Support:** ✗.
- **IP Office Modes:** Not supported in IP Office Basic Edition modes.

- Each external expansion module is supplied with a blue 1 meter (3'3'') expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on an IP500 4-Port Expansion card, a yellow 2 meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. 4 Yellow cables are supplied with the IP500 4-Port Expansion card.



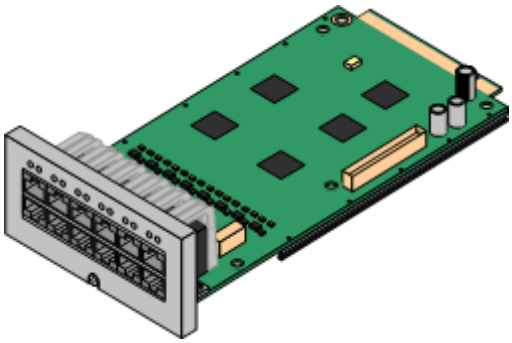
- LEDs 1 to 8 are used for the expansion ports on the rear of the control unit. LEDs 9 to 12 are used for the card's own expansion ports.

Green	**On**	Expansion module present.
Red	**Flashing**	Initializing.
Red	**On**	Error.
Orange	**Regular Flash**	Base card okay.

Name	Description	SAP Code
IPO IP500 EXP CARD 4PT	Includes 4 yellow 2 metre interconnect cables.	700472889
IPO EXP CABLE RJ45/RJ45 2M YELLOW	Only for use with the 4-Port Expansion card.	700472871

13.3.2 Analog Phone

This card is used to add analog phone ports to the control unit. It is available in two variants, providing either 2 or 8 analog extension ports.



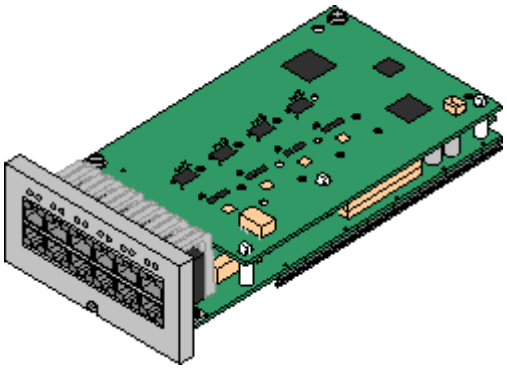
- **Supports**
  Provides either 8 or 2 analog[267] phone ports depending on card variant.
- **Maximum per Control Unit:** 4.
- **IP500 Trunk Card Support:** ✓ 1.
- **IP Office Modes:** Supported in all modes.

Port Type	Ports	Features
Analog Phone	**1 to 8**	• Supports ICLID modes DTMFA, DTMFC, DTMFD, FSK and UK20. • REN 2 (1 for external bell device). • Off-Hook current: 25mA • Ring Voltage: 40V. • Intended for connection to two-wire analog phones, the ports do not include a ringing capacitor. For connection to 4-wire analog phones, connection should be via a master socket with ringing capacitors. • If fitted with an analog trunk card, for the Phone 8, during power failure extension port 8 is connected to the analog trunk port 12. **Port LEDs** • No status LEDs are used for analog phone extensions. • LED1 is also used for base card status: • **Red On** = Error/Not supported. • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.
Optional Trunk Card Ports	**9 to 12**	The card can be fitted with one trunk daughter card of any type. The trunk daughter card then uses ports 9 to 12 on the base card for its trunk connections. **Port LEDs** LED use depends on the type of daughter card installed on the base card: • LED 9 is also used for daughter card status. • **Red On** = Error • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown. **Analog Card** • **Green on** = V1: Card installed. V2: Line connected to the port but idle. • **Green flashing** = Line in use. **PRI Card** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use. • **Red/Green Fast Flash** (port 9) or **Green Fast Flash** (port 10) = Alarm indication signal (AIS) from the trunk remote end. • **Red with Green Blink** (port 9) or **Green Blink** (port 10) = Port in loopback mode (set through IP Office System Monitor). **BRI Card** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use.

Name	Description	SAP Code
IPO 500 Extn Card Phone 2	IP Office 500 Extension Card Phone 2	700431778
IPO 500 Extn Card Phone 8	IP Office 500 Extension Card Phone 8	700417231

13.3.3 ATM Combination Card

These cards are used to add a combination of ports to an IP500 V2 control unit. Not supported by IP500 control units. The newer IP500 ATM Combination Card V2 version is supported by IP Office Release 8.1 Feature Pack 1 and higher only.



- **Supports**
  - 10 voice compression channels. Codec support is G.711, G729a and G.723 with 64ms echo cancellation. G.722 is supported by IP Office Release 8.0 and higher.
  - 6 Digital Station ports for supported Avaya DS digital telephones 39 (except 3800 Series).
  - 2 Analog Extension ports.
  - 4 Analog Trunk ports:
    Depending on the version of combination card, V1 or V2, the analog trunk daughter card is equivalent to an IP500 Analog Trunk Card 4 224 V1 or V2 respectively.
- During power failure phone port 8 is connected to analog trunk port 12.
- **Maximum per Control Unit:** 2 combination cards of any type per IP500 V2 control unit.
- **IP500 Trunk Card Support:** ✓ 1.
  - IP500 Combination cards are pre-fitted with a trunk daughter card which cannot be removed or changed for another type/capacity trunk daughter card.
- **IP Office Modes:** Supported in all modes.
- **Minimum Software Level:** 6.0+.
  This depends on the version of the card as follow:
  - **V1:** 6.0+. New build PCS04 cards are only supported in systems running IP Office Release 6.1(20), 7.0(12) or 8.0 and higher. Refer to IP Office Technical Tip 237.
  - **V2:** IP Office Release 8.1 Feature Pack 1 or higher.

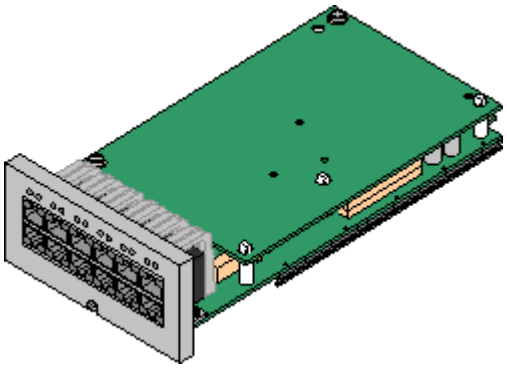
Port Type	Ports	Features
Digit Station	**1 to 6**	Provides DS 271 ports for supported Avaya DS digital telephones 39 (except 3800 Series). **LEDs** • **Green Flashing** = Phone detected. • **Green On** = Phone active. • LED1 is also used for base card status: • **Red On** = Error/Not supported. • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.
Analog Phone	**7 to 8**	• Supports ICLID modes DTMFA, DTMFC, DTMFD, FSK and UK20. • REN 2 (1 for external bell device). • Off-Hook current: 25mA • Ring Voltage: 40V. • Intended for connection to two-wire analog phones, the ports do not include a ringing capacitor. For connection to 4-wire analog phones, connection should be via a master socket with ringing capacitors. • During power failure extension port 8 is connected to the analog trunk port 12. • No status LEDs are used for analog phone extensions.
Analog Trunk	**9 to 12**	• DTMF, ICLID and busy tone detection. • Over-voltage/lightning protection (may still require additional protection equipment 36). • DTMF and LD (loop disconnect) dialing. • Echo cancellation. **LEDs** • **Green on** = V1: Card installed. V2: Line connected to the port but idle. • **Green flashing** = Line in use. • LED 9 is also used for daughter card status. • **Red On** = Error • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.

Página2875 de 3226.

Name	Description	SAP Code
IPO IP500 V2 COMB CARD ATM4	IPO IP500 V2 COMBINATION CARD ATM4	700476013
IPO IP500 V2 COMB CARD ATM4 TAA	" Trade Agreements Act[296] compliant variant.	700501513
IPO IP500 V2 COMB CARD ATM4 V2	IPO IP500 V2 COMBINATION CARD ATM4 V2	700504556

13.3.4 BRI Combination Card

This card is used to add a combination of ports to an IP500 V2 control unit.



- **Supports**
  - 10 voice compression channels. Codec support is G.711, G729a and G.723 with 64ms echo cancellation. G.722 is supported by IP Office Release 8.0 and higher.
  - 6 Digital Station ports for supported Avaya DS digital telephones[39] (except 3800 Series).
  - 2 Analog Extension ports.
  - 2 BRI Trunk ports (4 BRI channels).
- **Maximum per Control Unit:** 2 combination cards of any type.
  - IP Office Basic Edition - Norstar Mode and IP Office Basic Edition systems are limited to a maximum of 12 BRI channels using BRI Combination and or BRI trunk daughter cards.
- **IP500 Trunk Card Support:** ✓ 1.
  - IP500 Combination cards are pre-fitted with a trunk daughter card which cannot be removed or changed for another type/capacity trunk daughter card.
- **IP Office Modes:** Not supported in IP Office Basic Edition - PARTNER® Mode mode.

Port Type	Ports	Features
Digit Station	**1 to 6**	Provides DS[271] ports for supported Avaya DS digital telephones[39] (except 3800 Series). **LEDs** • **Green Flashing** = Phone detected. • **Green On** = Phone active. • LED1 is also used for base card status: • **Red On** = Error/Not supported. • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.
Analog Phone	**7 to 8**	• Supports ICLID modes DTMFA, DTMFC, DTMFD, FSK and UK20. • REN 2 (1 for external bell device). • Off-Hook current: 25mA • Ring Voltage: 40V. • Intended for connection to two-wire analog phones, the ports do not include a ringing capacitor. For connection to 4-wire analog phones, connection should be via a master socket with ringing capacitors. • No status LEDs are used for analog phone extensions.
BRI Trunk	**9 to 10**	• Each trunk port supports 2B+D channels. • ETSI or AusTS013 basic rate protocol set through the IP Office configuration. **LEDs** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use. • LED 9 is also used for daughter card status. • **Red On** = Error • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.
Not Used	**11 to 12**	–

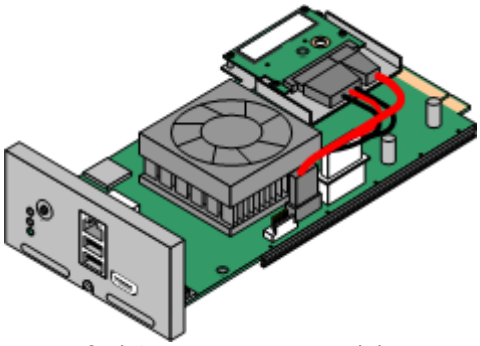
Name	Description	SAP Code
IPO IP500 V2 COMB CARD BRI	IPO IP500 V2 COMBINATION CARD BRI	700476021

Página2877 de 3226.

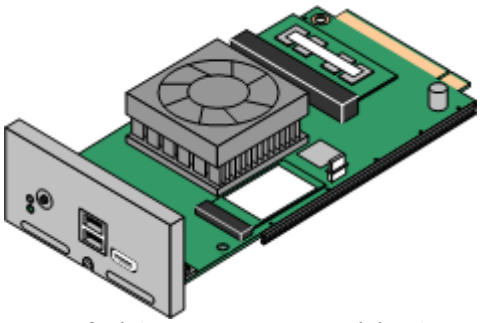
13.3.5 Unified Communications Module

This card is an embedded server that allows Linux based IP Office applications to be run within the IP Office control unit rather than requiring separate PCs. The IP address of the server is set during its initial configuration and can then be changed through web browser access to the server.

There are two type of card. The Unified Communications Module v2 is supported by IP Office Release 9.1 and higher. The Unified Communications Module v1 is supported for IP Office Release 8.0 Q1 2012 Service Pack or higher. Though physically different, the two types of card current support the same applications and application capacities. However, the v2 does not provide an implied Preferred Edition license and is not supplied with pre-installed software.



Unified Communications Module v1



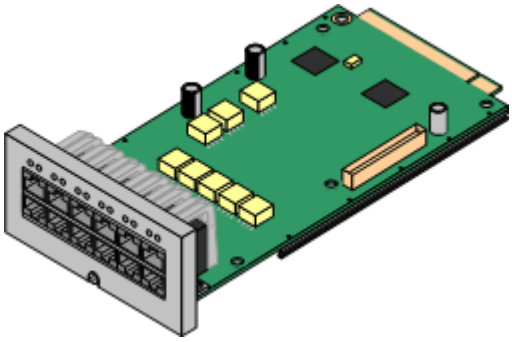
Unified Communications Module v2

- **Supports**
  Voicemail Pro and or one-X Portal for IP Office applications.
  - **IP Office Users:** Up to 200 users when running Voicemail Pro and one-X Portal for IP Office. More than 200 users when running just Voicemail Pro.
  - **Simultaneous one-X Portal for IP Office Users:** 50.
  - **Maximum voicemail ports:** Up to 20 ports when running Voicemail Pro and one-X Portal for IP Office. Up to 40 ports when running just Voicemail Pro.
  - **Small Community Network:** Maximum 6 systems.
- **Licenses**
  For both card types, an **Essential Edition** license is required as a pre-requisite. The voicemail server on the card also requires the system to have a **Preferred Edition** license.
  - On pre-IP Office Release 10 systems the Unified Communications Module v1 grants the host system the virtual Preferred Edition license it needs for Voicemail Pro. This no longer applies for IP Office Release 10 and higher. Existing IP Office systems being upgraded to IP Office Release 10 must use the IP Office license migration process to retain the existing license.
- **Maximum per Control Unit:** 1 per control unit.
- **IP500 Trunk Card Support:** ✗
- **IP Office Modes:** Not supported in IP Office Basic Edition modes.
- **! WARNING:**
  The Unified Communications Module v1 card is supplied with a removable plastic cover that locates over the external ports (LAN, USB and HDMI) on the faceplate of the card. This cover should always be in place during normal operation of the card. The cover should only be temporarily removed during maintenance actions that require access to the ports and should be replaced when the maintenance is completed.
- **! WARNING: Card Remains Hot After System Shutdown**
  When removing an Unified Communications Module from a system, care should be taken not to touch the heat sink on the module. The heat sink remains hot for a long period after system shutdown.

Name	Description	SAP Code
IPO UC MODULE	IP Office Unified Communications Module v1	700501442
IPO UC MODULE V2	IP Office Unified Communications Module v2	700507449

13.3.6 Digital Station

This card is used to add digital station (DS) extension ports to an IP500 and IP500 V2 control unit. It provides 8 RJ45 DS extension ports for use with supported Avaya DS digital telephones[39]. A further 4 RJ45 ports are provided for trunk connections when an IP500 trunk card is fitted to this card.



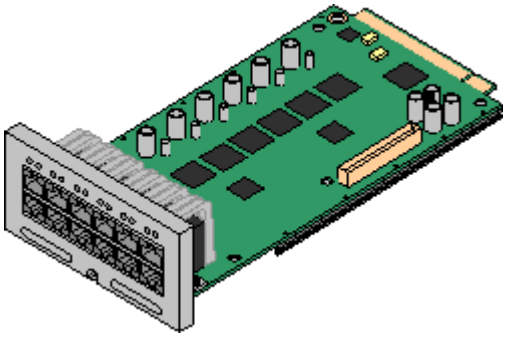
- **Supports**
  Provides 8 DS[271] ports for Avaya DS digital telephones[39].
- **Maximum per Control Unit:** 3 per control unit.
- **IP500 Trunk Card Support:** ✓ 1.
- **IP Office Modes:** Supported in all modes.

Port Type	Ports	Features
Digit Station	**1 to 8**	Provides DS[271] ports for supported Avaya DS digital telephones[39] (except 3800 Series). **LEDs** • **Green Flashing** = Phone detected. • **Green On** = Phone active. • LED1 is also used for base card status: • **Red On** = Error/Not supported. • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.
Optional Trunk Card Ports	**9 to 12**	The card can be fitted with one trunk daughter card of any type. The trunk daughter card then uses ports 9 to 12 on the base card for its trunk connections. **Port LEDs** LED use depends on the type of daughter card installed on the base card: • LED 9 is also used for daughter card status. • **Red On** = Error • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown. **Analog Card** • **Green on** = V1: Card installed. V2: Line connected to the port but idle. • **Green flashing** = Line in use. **PRI Card** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use. • **Red/Green Fast Flash** (port 9) or **Green Fast Flash** (port 10) = Alarm indication signal (AIS) from the trunk remote end. • **Red with Green Blink** (port 9) or **Green Blink** (port 10) = Port in loopback mode (set through IP Office System Monitor). **BRI Card** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use.

Name	Description	SAP Code
IPO 500 Extn Card Dgtl Sta 8	IP Office 500 Extension Card Digital Station 8	700417330
IPO IP500 Extn Card Dgtl Sta 8 TAA	" Trade Agreements Act[296] compliant variant.	700501512

13.3.7 ETR6 Card

This card is used to add 6 ETR[39] phone extension ports to an IP500 V2 control unit. It also includes 2 analog extension ports which are for emergency use only when the card is fitted with an analog trunk daughter card. A further 4 RJ45 ports (9 to 12) are provided for trunk connections when an IP500 trunk daughter card is fitted to this card.



- **Supports** ETR[39] and analog phones. Each ETR phone can be used for an ETR or analog phone. Support for ETR 34D phone is limited to a maximum of 2 per ETR6 card and 4 in total.
  - Paging to external paging equipment is not supported via ETR6 ports. It is supported via POT ports.
  - The only analog phones tested by Avaya for IP Office Essential Edition are the Avaya 6200 Series. If other analog phones are used, it is the customer's own responsibility to ensure that those phones work as required.
- **Maximum per Control Unit:** 3.
- **IP500 Trunk Card Support:** ✓ 1. The IP500 BRI trunk daughter card is not supported.
- **IP Office Modes:** Only supported in IP Office Basic Edition - PARTNER® Mode or IP Office Basic Edition (U-Law) modes using a North-American locale.

Port Type	Ports	Features

ETR	**1 to 6**	• REN 1.
		• DTMF dialing only.
		• Message waiting indication 51V stepped.
		• ICLID mode Bellcore 202.
		LEDs
		• No status LED are used for ETR ports.
		• LED1 is also used for base card status:
		  • **Red On** = Error/Not supported.
		  • **Red Slow Flash** = Initializing.
		  • **Red Flash every 5 seconds** = Card okay.
		  • **Red Fast Flash** = System shutdown.

EF	**7 to 8**	• If fitted with an IP500 Trunk Daughter card, during power failure both these ports are connected to analog trunk port 12. • Supports ICLID modes DTMFA, DTMFC, DTMFD, FSK and UK20. • REN 2 (1 for external bell device). • Off-Hook current: 25mA • Ring Voltage: 40V. • Intended for connection to two-wire analog phones, the ports do not include a ringing capacitor. For connection to 4-wire analog phones, connection should be via a master socket with ringing capacitors. • No status LEDs are used for analog phone extensions.

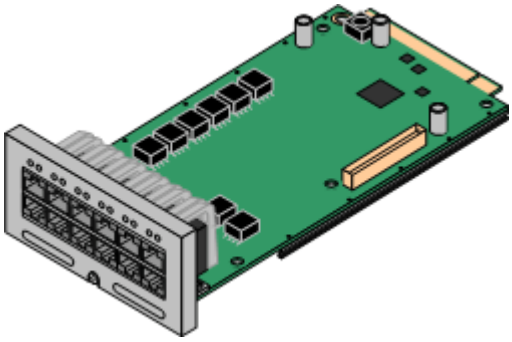
Optional Trunk Ports	**9 to 12**	Depends on the type of trunk daughter card fitted. The ETR6 can be fitted with either a Analog Trunk[224] card or PRI Trunk[227] card.
		LEDs
		LED use depends on the type of daughter card installed on the base card:
		• LED 9 is also used for daughter card status.
		  • **Red On** = Error
		  • **Red Slow Flash** = Initializing.
		  • **Red Flash every 5 seconds** = Card okay.
		  • **Red Fast Flash** = System shutdown.
		Analog Card
		  • **Green on** = V1: Card installed. V2: Line connected to the port but idle.
		  • **Green flashing** = Line in use.
		PRI Card
		  • **Off** = No trunk present.
		  • **Green on** = Trunk present.
		  • **Green flashing** = Trunk in use.
		  • **Red/Green Fast Flash** (port 9) or **Green Fast Flash** (port 10) = Alarm indication signal (AIS) from the trunk remote end.
		  • **Red with Green Blink** (port 9) or **Green Blink** (port 10) = Port in loopback mode (set through IP Office System Monitor).

Name	Description	SAP Code
IPO IP500 V2 EXTN CARD ETR6	IPO IP500 V2 EXTN CARD ETR6	700504202

Página 2880 de 3226.

13.3.8 TCM8 Digital Station

This card is used to add BST RJ45 extension ports to an IP500 V2 control unit. It provides 8 RJ45 extension ports for supported Avaya BST digital telephones[39]. A further 4 RJ45 ports are provided for trunk connections when an IP500 trunk card is fitted to this card.



- **Supports**
  Provides 8 BST ports for supported 4100, 7400, M and T-Series digital stations.
- **Maximum per Control Unit:** 4.
- **IP500 Trunk Card Support:** ✓ 1.
- **IP Office Modes:** Supported in all modes.

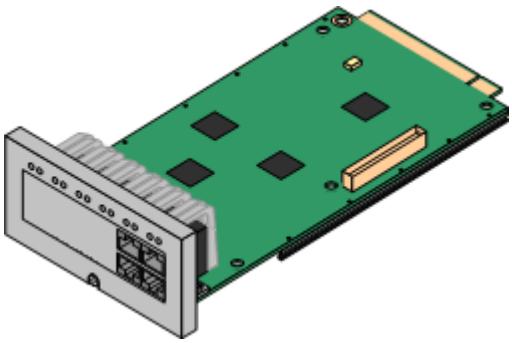
Port Type	Ports	Features
BST	**1 to 8**	**LEDs** • **Green On** = Phone detected. • LED1 is also used for base card status: • **Red On** = Error/Not supported. • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.
Optional Trunk Card Ports	**9 to 12**	The card can be fitted with one trunk daughter card of any type. The trunk daughter card then uses ports 9 to 12 on the base card for its trunk connections. **LEDs** LED use depends on the type of daughter card installed on the base card: • LED 9 is also used for daughter card status. • **Red On** = Error • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown. **Analog Card** • **Green on** = V1: Card installed. V2: Line connected to the port but idle. • **Green flashing** = Line in use. **PRI Card** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use. • **Red/Green Fast Flash** (port 9) or **Green Fast Flash** (port 10) = Alarm indication signal (AIS) from the trunk remote end. • **Red with Green Blink** (port 9) or **Green Blink** (port 10) = Port in loopback mode (set through IP Office System Monitor). **BRI Card** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use.

Name	Description	SAP Code
IPO 500 TCM 8 Extn Card Assy	IP Office 500 TCM 8	700500758

13.3.9 VCM

This type of card is used to add voice compression channels to the control unit. Those channels are used for VoIP calls including IP extensions and or IP trunks. IP500 V2 control units support up to 148 voice compression channels, using IP500 VCM cards and IP500 Combination Cards 214.

The cards are available in 32 channel and 64 channel variants. All the card variants have 4 RJ45 ports which are used for trunk connections when an IP500 trunk daughter card 223 is fitted.



- **Supports**
  Codecs G.711, G.729ab and G.723 with 64ms echo cancellation. The maximum number of simultaneous channels useable on an IP500 VCM base card is affected by the codec being used. The following table assumes that all calls using the VCM use the same codec. Note: Whilst IP500 VCM cards support G729b, it is not supported by other IP Office systems such as Linux based systems.
  - G.722 is supported by IP Office Release 8.0 and higher in systems with an IP500 VCM card or an IP500 Combination card.

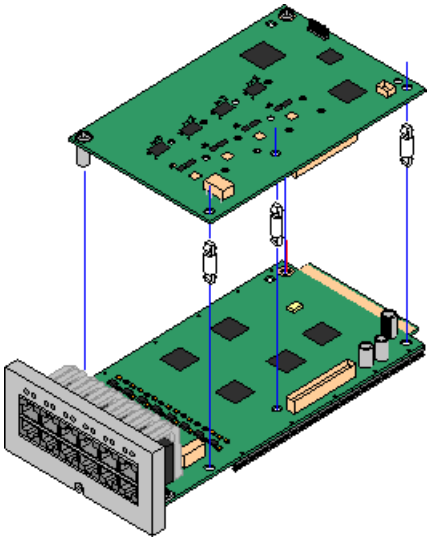
Codec	IP500 VCM 32 IP500 VCM 32 V2	IP500 VCM 64 IP500 VCM 64 V2
G.711	32	64
G.729ab	30	60
G.723	22	44
G.722	30	60

- **Maximum per Control Unit:** 2.
- **IP500 Trunk Card Support:** ✓ 1.
- **IP Office Modes:** Not supported in IP Office Basic Edition modes.

Port Type	Ports	Features
Not present	**1 to 8**	Not present. **LEDs** • LEDs 1 to 8 are unlabelled. They are used to indicate voice compression channel usage. Each LED lit represents 12.5% of the available voice compression channel capacity in use (total card capacity rather than licensed capacity). • LED1 is also used for base card status: • **Red On** = Error/Not supported. • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown.
Optional Trunk Card Ports	**9 to 12**	The card can be fitted with one trunk daughter card of any type. The trunk daughter card then uses ports 9 to 12 on the base card for its trunk connections. **LEDs** LED use depends on the type of daughter card installed on the base card: • LED 9 is also used for daughter card status. • **Red On** = Error • **Red Slow Flash** = Initializing. • **Red Flash every 5 seconds** = Card okay. • **Red Fast Flash** = System shutdown. **Analog Card** • **Green on** = V1: Card installed. V2: Line connected to the port but idle. • **Green flashing** = Line in use. **PRI Card** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use. • **Red/Green Fast Flash** (port 9) or **Green Fast Flash** (port 10) = Alarm indication signal (AIS) from the trunk remote end. • **Red with Green Blink** (port 9) or **Green Blink** (port 10) = Port in loopback mode (set through IP Office System Monitor). **BRI Card** • **Off** = No trunk present. • **Green on** = Trunk present. • **Green flashing** = Trunk in use.

	Name	Description	SAP Code
IP500 Voice Compression Modules	**IPO IP500 MC VCM 32**	IP Office 500 Media Card Voice Coding Module 32	700417389
	IPO IP500 VCM 32 TAA	" Trade Agreements Act[296] compliant variant.	700501518
	IPO IP500 MC VCM 64	IP Office 500 Media Card Voice Coding Module 64	700417397
IP500 Voice Compression Modules V2	**IPO IP500 MC VCM 32 V2**	IP500 Media Card Voice Coding Module 32 V2	700504031
	IPO IP500 VCM 32 TAA V2	" Trade Agreements Act[296] compliant variant.	700504033
	IPO IP500 MC VCM 64 V2	IP500 Media Card Voice Coding Module 64 V2	700504032

13.4 IP500 Trunk Daughter Cards

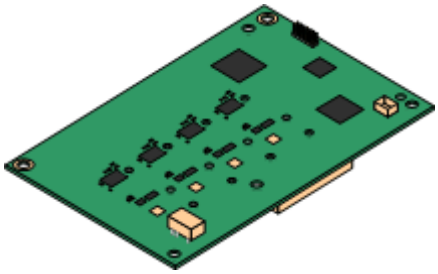


Many IP500 base cards[22] can be fitted with an IP500 trunk daughter cards to support the connection of trunks to the base card.

Each daughter card is supplied with the stand off pillars required for installation and a label to identify the daughter cards presence on the front of the base card after installation.

- IP500 Combination cards are pre-fitted with a trunk daughter card which cannot be removed or changed for another type of trunk daughter card.

IP500 Analog Trunk Card/IP500 Analog Trunk Card V2[224]

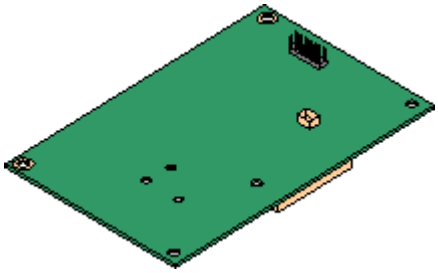


These cards allow the base card to support 4 analog loop-start trunks.

  - The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors.
  - If fitted base card with analog phone ports, during power failure phone port 8 is connected to analog trunk port 12.

- **Maximum:** 4 per control unit. The IP500 Analog Trunk Card V2 is only supported in the IP500 V2.

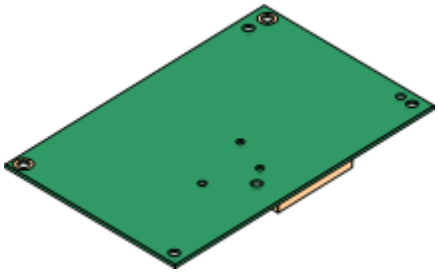
IP500 PRI-U Trunk Card[227]



This card allows the base card to support up to 2 PRI trunk connections. The card is available in single and dual port variants. The card can be configured for E1 PRI, T1 robbed bit, T1 PRI or E1R2 PRI trunks. A T1(J) variant for use in Japan is also available.

- **Maximum:** 4 per control unit.
- The IP Office system supports 8 unlicensed B-channels on each IP500 PRI-U port fitted. Additional B-channels, up to the capacity of ports installed and PRI mode selected require **IP500 Universal PRI (Additional Channels)**[280] licenses added to the configuration. These additional channels consume the licenses based on which additional channels are configured as in-service from port 9 of slot 1 upwards. D-channels are not affected by licensing.

IP500 BRI Trunk Card[226]



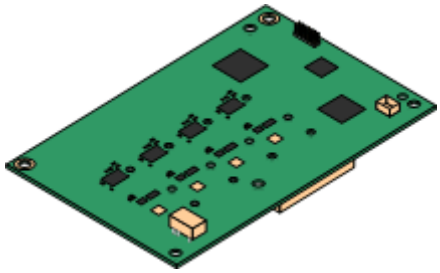
This card allows the base card to support up to 4 BRI trunk connections, each trunk providing 2B+D digital channels. The card is available in 2 port (4 channels) and 4 port (8 channels) variants.

- **Maximum:** 4 per control unit.
- **S-Bus Connection**: The card can be switched from To trunk mode to So mode. This mode requires additional terminating resistors and an ISDN crossover cable connection, see BRI Port (So)[268].
  - IP Office Basic Edition - Norstar Mode and IP Office Basic Edition systems are limited to a maximum of 12 BRI channels using BRI Combination and or BRI trunk daughter cards.

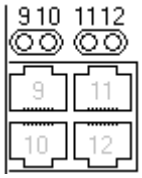
13.4.1 Analog Trunk Card

These cards can be added to an IP500 base card to provide that card with support for 4 loop-start analog trunks. The newer IP500 Analog Trunk Card V2 version is supported by IP500 V2 systems running IP Office Release 8.1 Feature Pack 1 or higher only.

This card can be fitted to any non-combo IP500 base card except the IP500 4-Port Expansion card and Unified Communications Module.



- **Ports/Channels**
  4 Loop-start analog trunk ports. Connections via the host IP500 base card.
  - DTMF, ICLID and busy tone detection.
  - Over-voltage/lightning protection (may still require additional protection equipment[36]).
  - DTMF and LD (loop disconnect) dialing.
  - Echo cancellation.
- **Echo Cancellation**
  The card supported echo cancellation that varies depending on the card type.
  - **V1:** Echo cancellation manually selectable to either ***8***, ***16***, ***32***, ***64*** or ***128*** milliseconds or ***Off***. The default is 16 milliseconds.
  - **V2:** Echo cancellation manually selectable to either ***On*** or ***Off***. The default is ***On***. The IP500 Analog Trunk Card V2 also supports echo reduction which is set to ***On*** by default.
- **Service Status/Line Status Indication**
  - **V1:** Detection of individual line status for idle lines is not supported. Therefore, the card LEDs and System Status Application simply indicate that the card is installed and when the line is in use.
  - **V2:** Automatic detection of line status for idle lines is supported. The card LEDs and System Status Application indicate that the individual line is connected and idle or is in use.
- **Impedance Matching**
  - **V1:** For this card only manual impedance matching is useable and only in selected locales.
  - **V2:** This card supports automatic impedance matching at system startup and this mode is enabled by default. Manual or no impedance matching can be used if required. Impedance matching is supported in all locales.
- **Voice Activity Detection (VAD)**
  Support for ATM4U-V2 cards on IP Office Release 9.1 and higher only. When enabled, allows the support on analog trunks of functions that require call progress indication, for example the use of mobile twinning. This function does not enable support for mobile call control. The function is not enabled by default.
- **Power Failure Port**
  Regardless of the IP500 card hosting it, during power failure pins 4 and 5 of port 12 are connected to pins 7 and 8. In addition, when fitted to an IP500 Analog Phone 8 base card, during power failure extension port 8 is connected to the analog trunk port 12.
- **License:** No license required.
- **Maximum per Control Unit:** 4.
- **Minimum Software Level:**
  This depends on the version of the card as follow:
  - **V1:** 4.0+.
    New build PCS10 and higher cards are only supported in systems running IP Office Release 6.1(20), 7.0(12) or 8.0 and higher. Refer to IP Office Technical Tip 237.
  - **V2:** 8.1 Feature Pack 1+



Daughter Card Ports (9-12)
The LEDs for ports 9 to 12 of the IP500 base card are used as follows:

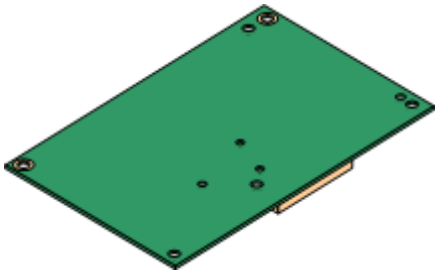
- **Green on** = V1: Card installed. V2: Line connected to the port but idle.
- **Green flashing** = Line in use.
- LED 9 is also used for daughter card status.
  - **Red On** = Error
  - **Red Slow Flash** = Initializing.
  - **Red Flash every 5 seconds** = Card okay.
  - **Red Fast Flash** = System shutdown.

Name	Description	SAP Code
IPO 500 Trnk Anlg 4 Uni	IP Office 500 Trunk Card Analog 4 Universal	700417405
IPO IP500 Trunk Card Anlg 4 V2	IP Office 500 Trunk Card Analog 4 Universal V2	700503164

13.4.2 BRI Trunk Cards

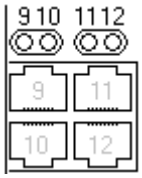
This card can be added to an IP500 base card to provide that card with support for BRI-To[269] trunks. The card is available in 8 channel (4 physical trunks) or 4 channel (2 physical trunks) variants.

This card can be fitted to any non-combo IP500 base card except the IP500 4-Port Expansion card and Unified Communications Module.



- **Ports/Channels**
  2 or 4 BRI trunk ports. Connections via ports 9 to 12 of the host IP500 base card.
  - Each trunk port supports 2B+D channels.
  - ETSI or AusTS013 basic rate protocol set through the IP Office configuration.
- **License:** No license required.
- **Maximum per Control Unit:** 4.
- **Minimum Software Level:** 4.0+.
- **S-Bus Connection:** On IP Office 4.2+ systems, the card can be switched from To[269] trunk mode to So[268] mode. This mode requires additional terminating resistors and an ISDN crossover cable connection, see BRI Port (So)[268].
- This card is approved for use in the following countries:

Brazil.	New Zealand.
China.	Russia.
India.	South Africa.
Argentina.	United Arab Emirates (UAE).
Australia.	European Union (EU).



Daughter Card Ports (9-12)
The LEDs for ports 9 to 12 of the IP500 base card are used as follows:

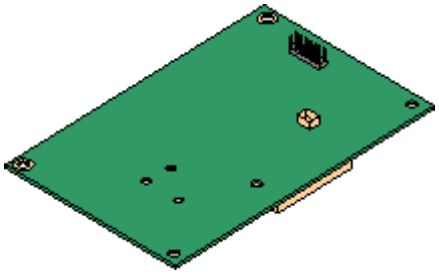
- **Off** = No trunk present.
- **Green on** = Trunk present.
- **Green flashing** = Trunk in use.
- LED 9 is also used for daughter card status.
  - **Red On** = Error
  - **Red Slow Flash** = Initializing.
  - **Red Flash every 5 seconds** = Card okay.
  - **Red Fast Flash** = System shutdown.

Name	Description	SAP Code
IPO 500 Trnk BRI 4 Uni	IP Office 500 Trunk Card Basic Rate 4 Universal	700417413
IPO IP500 TRNK BRI 4 UNI TAA	" Trade Agreements Act[296] compliant variant.	700501515
IPO 500 Trnk BRI 8 Uni	IP Office 500 Trunk Card Basic Rate 8 Universal	700417421
IP0 IP500 BRI S0 CONVTR CBL	IP500 BRI So Converter Cable	700458649

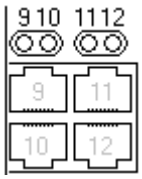
13.4.3 PRI Trunk Cards

This card can be added to an IP500 base card to provide that card with support for PRI trunks. The card is available in single port or dual port variants.

This card can be fitted to any non-combo IP500 base card except the IP500 4-Port Expansion card and Unified Communications Module.



- **Ports/Channels**
  1 or 2 PRI trunk ports[277]. Each port supports the following PRI line types. On dual port cards, both ports will be the same line type. The line type selection can be changed using IP Office Manager. The options available depend on the IP Office operation mode and locale.
    - E1 PRI (30B+D channels per port).
    - E1R2 PRI (30B channels per port).
    - T1 robbed bit (24B channels per port) or T1 PRI (23B+D channels per port).
    - A T1(J) variant for use in Japan is also available (9.1 Feature Pack and higher).
  - The required mode can be selected within IP Office Manager by right-clicking on the line icon and selecting **Change Universal PRI Card Line Type** and then selecting the required line type.
  - Physical trunk connection is via ports 9 and 10 of the host IP500 base card.
  - Port 11 and 12 can be used as test points for connection of test and monitoring equipment for the adjacent port.
- **Licenses**
  The IP Office system supports 8 unlicensed B-channels on each IP500 PRI-U port fitted. Additional B-channels, up to the capacity of ports installed and PRI mode selected require **IP500 Universal PRI (Additional Channels)** licenses added to the configuration. These additional channels consume the licenses based on which additional channels are configured as in-service from port 9 of slot 1 upwards. D-channels are not affected by licensing.
- **Maximum per Control Unit:** 4 per control unit in IP Office standard modes. 1 single port card only in other modes.
- **Minimum Software Level:** 4.1+.



Daughter Card Ports (9-12)
The LEDs for ports 9 to 12 of the IP500 base card are used as follows:

- **Off** = No trunk present.
- **Green on** = Trunk present.
- **Green flashing** = Trunk in use.
- **Red/Green Fast Flash** (port 9) or **Green Fast Flash** (port 10) = Alarm indication signal (AIS) from the trunk remote end.
- **Red with Green Blink** (port 9) or **Green Blink** (port 10) = Port in loopback mode (set through IP Office System Monitor).
- LED 9 is also used for daughter card status.
  - **Red On** = Error
  - **Red Slow Flash** = Initializing.
  - **Red Flash every 5 seconds** = Card okay.
  - **Red Fast Flash** = System shutdown.

Name	Description	SAP Code
IPO 500 TRNK PRI UNVRSL SNGL	IP Office 500 Trunk Card Primary Rate 1 Universal	700417439
IPO IP500 TRNK PRI UNVRSL SNGL TAA	" Trade Agreements Act[296] compliant variant.	700501514
IPO 500 TRNK PRI UNIVRSL DUAL	IP Office 500 Trunk Card Primary Rate 2 Universal	700417462
IPO IP500 TRNK PRI UNVSL DUAL TAA	" Trade Agreements Act[296] compliant variant.	700501517
IPO IP500 Trunk CARD T1(J) PRI DUAL JAPAN	Dual T1(J) Interface Card	700509377

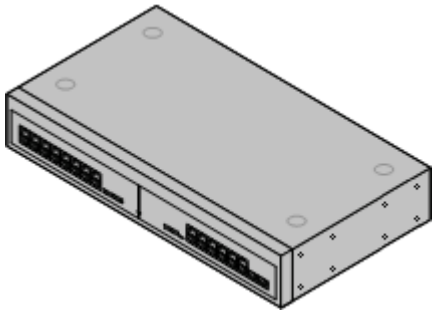
13.5 IP500 External Expansion Modules

The following IP500 external expansion modules are supported by IP Office Release 11.0. Each module uses an external power supply unit[30] supplied with the module. A locale specific power cord[31] for the PSU must be ordered separately.

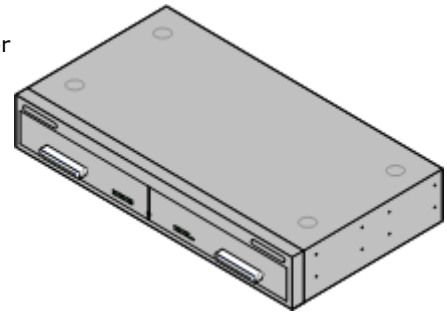
The external module can be stacked on top of the control unit. They can also be wall or rack mounted using one of the IP Office mounting kits[247].

- Systems running in IP Office standard modes support 8 external expansion modules as standard. If fitted with an IP500 4-Port Expansion Base Card, up to 12 external expansion modules are supported.

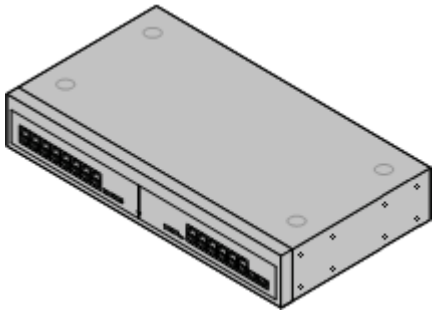
- **IP500 Digital Station Modules**[231]
  Provides, depending on variant, an additional 16 or 30 RJ45 DS[271] ports for supported Avaya DS digital phones[39].



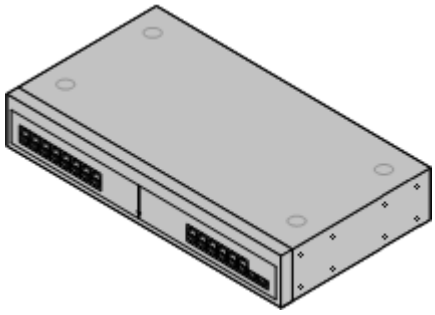
- **IP500 Digital Station A Modules**[233]
  Provides, depending on variant, RJ21 ports for connection of an additional 16 or 30 Avaya BST digital phones[39]. Supported by IP500 V2 only.



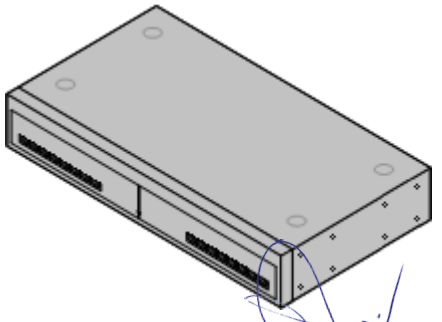
- **IP500 Digital Station B/B2 Modules**[236]
  Provides, depending on variant, an additional 16 or 30 RJ45 ports. These can be used as either DS[271] ports for supported Avaya DS digital phones[39] or BST[270] ports for supported Avaya BST digital phones[39]. However, the module can only support one port type at any time. For IP Office Release 10.1 the DS16B/DS30B modules have been superseded by the DS16B2/DS30B2 modesl.



- **IP500 Phone Modules**[238]
  Provides, depending on variant, an additional 16 or 30 PHONE[276] ports for connecting analog phones.



- **IP500 Analog Trunk Module**[229]
  Provides an additional 16 ANALOG[267] ports for connection of analog trunks. Supports both loop-start and ground-start trunks.
  - Use with ground start trunks requires that the trunk module and the IP Office control unit are grounded.
  - In IP Office Basic Edition - PARTNER® Mode, IP Office Basic Edition - Norstar Mode and IP Office Basic Editions, only 1 Analog Trunk module is supported.

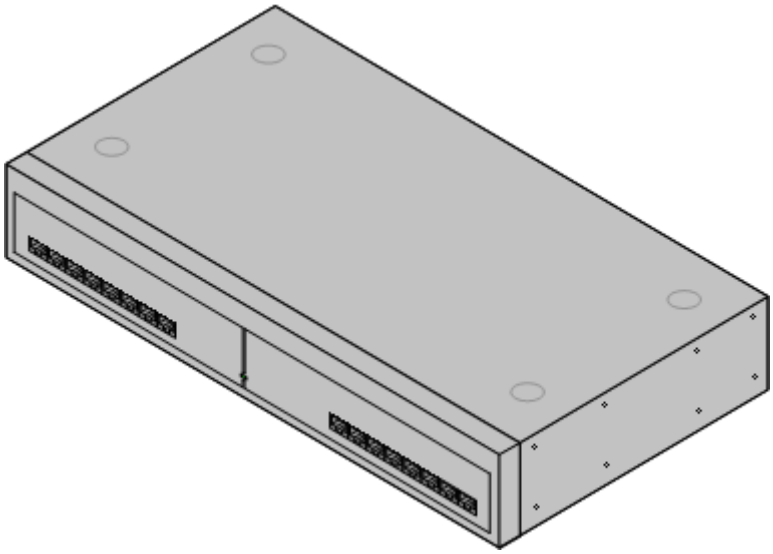


Página2889 de 3226.

13.5.1 Analog Trunk 16

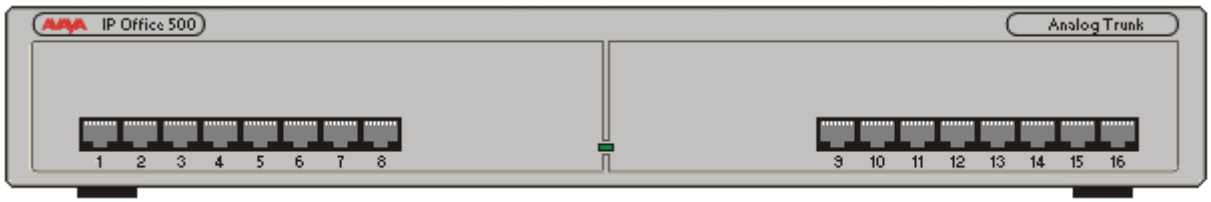
The IP500 Analog Trunk module can be used to add 16 additional analog trunks to an IP Office system. The module supports both loop-start and, with suitable grounding, ground-start trunks.

- In IP Office Basic Edition - PARTNER® Mode, IP Office Basic Edition - Norstar Mode and IP Office Basic Editions, only 1 Analog Trunk module is supported.
  - **WARNING**
    In all IP Office installations, any module being used for analog trunk connections must be connected to a functional earth[35].
  - **WARNING**
    Within areas of high lightning risk, any module using analog trunk connections must be connected to a protective ground[35] and to surge protection equipment[36].



Feature	Details
Locales	This module is currently only supported in North American locales.
Minimum Software Level	IP Office core software level 1.0 minimum. Bin file = naatm16.bin.
Included	Power supply unit (see below) and Expansion Interconnect cable.
Power Supply	The module is supplied with a 2-pin, 40W external power supply unit. The PSU has an integral power cord for connection to the module's DC I/P socket. A locale specific IEC60320 C13 power cord[30] for the external PSU is required but is not supplied with the module.
Mounting	The module is designed as a free-standing module that can be stacked on or under other IP Office modules. The module can be wall or rack mounted using the IPO IP500 RACK MNTG KIT V3[247].
Dimensions	Width: 445mm/17.5". Depth: 245mm/9.7". Height: 71mm/2.8"/2U.
Weight	Unboxed: 2.9Kg/6.6lbs. Boxed: 4.2Kg/9.4lbs.

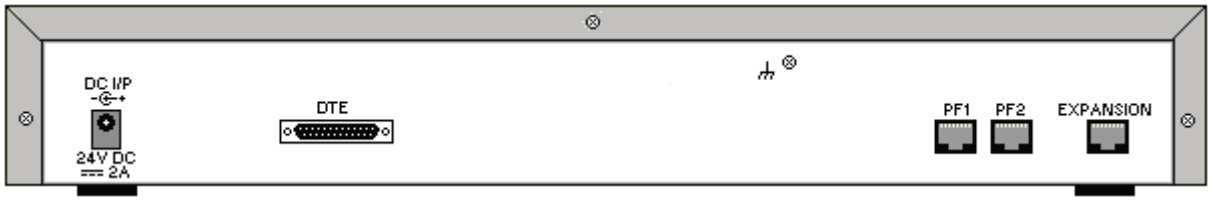
Module Front



Port LEDs	None
Module Center LED	The center LED on all external expansion modules is used to indicate the overall state of the module as follows: • **Red flashing** = Module starting up/Loading firmware. • **Red on** = Error. • **Green on** = Module okay.

Página2890 de 3226.

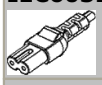
Module Rear



Ports	Description
ANALOG 267	RJ45 socket. Used for connection to analog trunks. Ports can be configured as either loop-start or ground-start trunks through the IP Office configuration. In the event of power failure, Analog ports 1 and 2 are directly connected to analog extension ports PF1 and PF2 respectively. If used the connected phones must be clearly labeled as power failure devices. This is only supported for loop-start analog trunks.
DC I/P 271	DC power input port. Used for connection of the power lead from an Avaya 40W external power supply unit supplied with the expansion module. A locale specific IEC60320 C7 power cord 30 for the external PSU is required but is not supplied with the module.
DTE 278	25-Way D-Type socket. For Avaya use only.
EXPANSION 273	RJ45 Socket. Used for direct connection to an Expansion port on an IP Office control unit using the Expansion Interconnect cable supplied with the module.
PF 275	RJ45 socket. Power failure analog extension ports. See Analog section above.
⏚	Ground point. Used for connection of a functional earth 35 if required. On older modules where this screw is not present, the top-center cover screw should be used instead. • IMPORTANT In all IP Office installations, any module being used for analog trunk connections must be connected to a functional earth 35. • ⚠ WARNING Within areas of high lightning risk, any module using analog trunk connections must be connected to a protective ground 35 and to surge protection equipment 36.

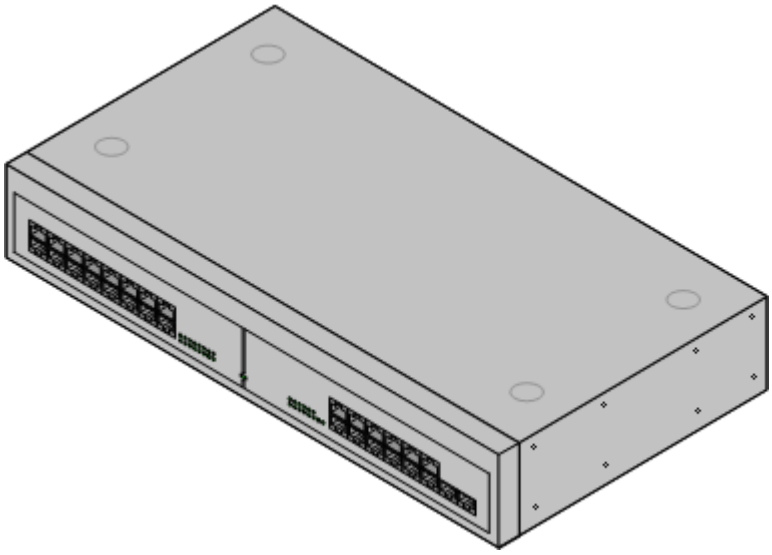
Part Codes and Related Equipment

All expansion modules are supplied with a base software level and should be upgraded to match the core software of the control unit in the IP Office system. Expansion modules include an external power supply unit (PSU) and an appropriate interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

Item	Variant	Country	SAP Code
IPO IP500 EXP MOD ANLG TRNK 16	**America**	America	700449473
IPO IP500 EXP MOD ANLG TRNK 16 TAA	" Trade Agreements Act 296 compliant variant.	America	700501511
IEC60320 C7 Power Cord 	**NEMA1-15**	America	700213390
Mounting Kit	**IPO IP500 WALL MNTG KIT V3**	All	700503160

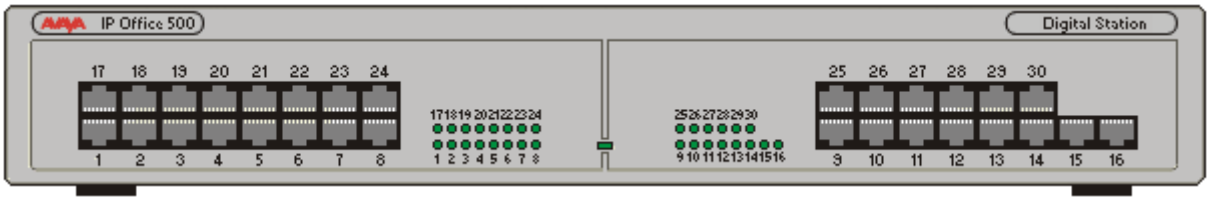
13.5.2 DS16/30

IP Office 500 Digital Station modules can be used to add additional DS ports[271] to an IP Office system for support Avaya DS digital telephones[39]. The module is available in 16 and 30 port variants, referred to as the IP500 DS16 and IP500 DS30 respectively. These modules are also known as IP500 DS V2 modules. These modules have been superseded by the IP500 DS16B/30B[236].



Feature	Details
Locales	Supported in all IP Office locales[42].
Minimum Software Level	IP Office core software level 2.1(31) minimum. Bin file = nadcpV2.bin.
Included	Power supply unit (see below) and Expansion Interconnect cable.
Power Supply	The module is supplied with a Earthed 3-Pin, 60W external power supply module. The PSU has an integral power cord for connection to the module's DC I/P socket. A locale specific IEC60320 C13 power cord[30] for the external PSU is required but is not supplied with the module.
Mounting	The module is designed as a free-standing module that can be stacked on or under other IP Office modules. The module can be wall or rack mounted using the IPO IP500 RACK MNTG KIT V3[247].
Dimensions	Width: 445mm/17.5". Depth: 245mm/9.7". Height: 71mm/2.8".
Weight	Unboxed: 3.5Kg/7.8lbs. Boxed: 4.8Kg/10.8lbs. (Based on DS30)

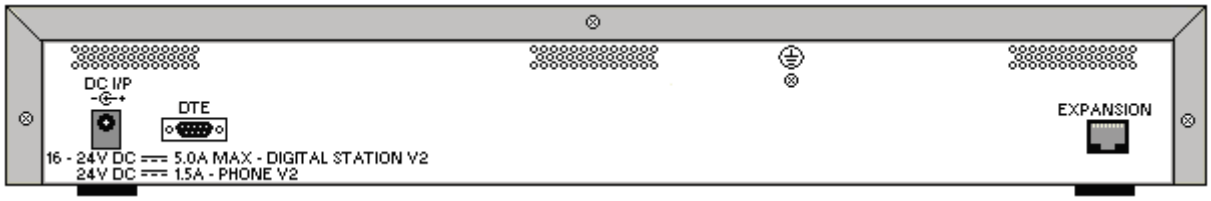
Module Front



Port LEDs	• **Green Flashing** = Phone detected. • **Green On** = Phone active.
Module Center LED	The center LED on all external expansion modules is used to indicate the overall state of the module as follows: • **Red flashing** = Module starting up/Loading firmware. • **Red on** = Error. • **Green on** = Module okay.

Página2892 de 3226.

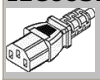
Module Rear



Port	Description
DC I/P 271	DC power input port. Used for connection of the power lead from an Avaya earthed 60W external power supply unit supplied with the expansion module. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
DS 271	RJ45 socket. Digital Station port. Used for connection of IP Office supported DS phones 39. If connected to an out-of-building extension 36, the connection must be made via additional IROB barrier devices in addition to the buildings primary protection. The module must also be connected to a protective ground.
DTE 278	9-Way D-Type socket. For Avaya use only.
EXPANSION 273	RJ45 Socket. Used for direct connection to an Expansion port on an IP Office control unit using the Expansion Interconnect cable supplied with the module.
⏚	Protective Ground point. Use of a protective ground is required for all installations, see Grounding (Earthing) 93. Where the module is connected to analog extensions in another building, an IP Office Phone Barrier Box V2 (101V) is required at both ends, see Lightning Protection/Out-of-Building Connections 36.

Part Codes and Related Equipment

All expansion modules are supplied with a base software level and should be upgraded to match the core software of the control unit in the IP Office system. Expansion modules include an external power supply unit (PSU) and an appropriate interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

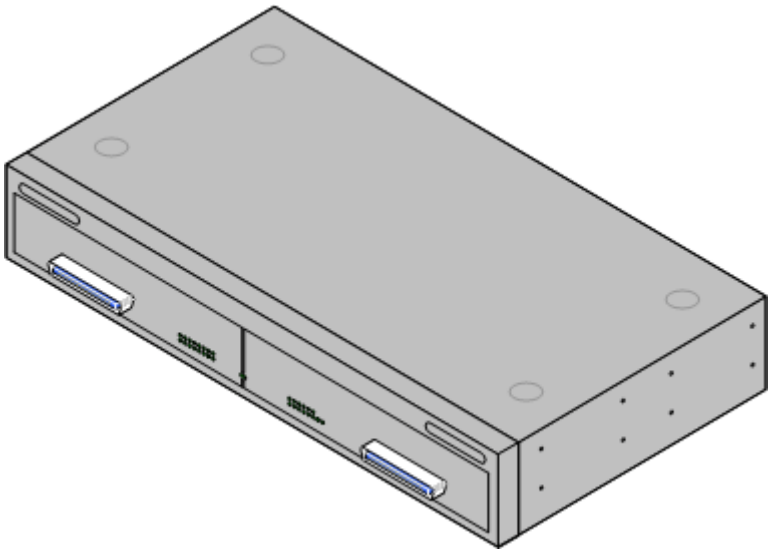
Item	Variant	Country	SAP Code
IPO IP500 EXP MOD DGTL STA 16	**16 Ports**	All	700449499
IPO IP500 EXP MOD DGTL STA 16 TAA	" Trade Agreements Act 296 compliant variant.		–
IPO IP500 EXP MOD DGTL STA 30	**30 Ports**		700426216
IEC60320 C13 Power Cord 	**CEE7/7**	Europe	700289762
	BS1363	United Kingdom	700289747
	NEMA5-15P	America	700289770
Mounting Kit	**IPO IP500 WALL MNTG KIT V3**	All	700503160

Página2893 de 3226.

13.5.3 DS16A/30A

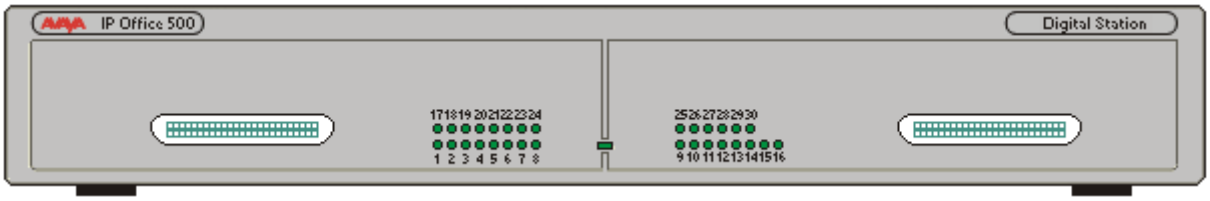
These modules can be used to add additional BST ports[270] for supported Avaya BST digital telephones[39]. The module is available in 16 and 30 port variants, referred to as the IP500 DS16A and IP500 DS30A respectively.

The modules use RJ21 connectors; 1 on the 16 port version, 2 on the 30 port version. For BST connections using RJ45 port, use the IP500 DS16B/30B modules[236].



Feature	Details
Locales	Supported in all IP Office locales[42].
Minimum Software Level	IP Office Release 7.0 minimum (BST only). Bin file = nadcpaV1.bin.
Included	Power supply unit (see below) and Expansion Interconnect cable.
Power Supply	The module is supplied with a Earthed 3-Pin, 60W external power supply module. The PSU has an integral power cord for connection to the module's DC I/P socket. A locale specific IEC60320 C13 power cord[30] for the external PSU is required but is not supplied with the module.
Mounting	The module is designed as a free-standing module that can be stacked on or under other IP Office modules. The module can be wall or rack mounted using the IPO IP500 RACK MNTG KIT V3[247].
Dimensions	Width: 445mm/17.5". Depth: 245mm/9.7". Height: 71mm/2.8".
Weight	Unboxed: 3.5Kg/7.8lbs. Boxed: 4.8Kg/10.8lbs. (Based on DS30A RJ21)

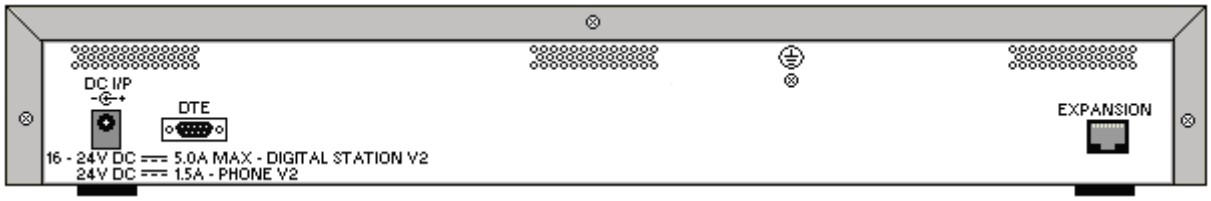
Module Front



Port LEDs	• **Green On** = Phone detected.
Module Center LED	The center LED on all external expansion modules is used to indicate the overall state of the module as follows: • **Red flashing** = Module starting up/Loading firmware. • **Red on** = Error. • **Green on** = Module okay. • **Green flashing** = Module starting up/Loading firmware (IP500 DS16A/30A module only).

Página2894 de 3226.

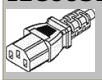
Module Rear



Ports	Description
DC I/P 271	DC power input port. Used for connection of the power lead from an Avaya earthed 60W external power supply unit supplied with the expansion module. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
RJ21 270	For IP Office Release 7.0, the modules support just phones requiring BST ports 270 .
DTE 278	9-Way D-Type socket. For Avaya use only.
EXPANSION 273	RJ45 Socket. Used for direct connection to an Expansion port on an IP Office control unit using the Expansion Interconnect cable supplied with the module.
⏚	Protective Ground point. Use of a protective ground is required for all installations, see Grounding (Earthing) 93 . Where the module is connected to analog extensions in another building, an IP Office Phone Barrier Box V2 (101V) is required at both ends, see Lightning Protection/Out-of-Building Connections 36 .

Part Codes and Related Equipment

All expansion modules are supplied with a base software level and should be upgraded to match the core software of the control unit in the IP Office system. Expansion modules include an external power supply unit (PSU) and an appropriate interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

Item	Variant	Country	SAP Code
IPO 500 Digital Station 16A RJ21 UNIT ASSY	**RJ21**	All	700500699
IPO 500 Digital Station 30A RJ21 UNIT ASSY	**RJ21**		700500698
IEC60320 C13 Power Cord 	**CEE7/7**	Europe	700289762
	BS1363	United Kingdom	700289747
	NEMA5-15P	North America	700289770
Mounting Kit	**IPO IP500 WALL MNTG KIT V3**	All	700503160

RJ21 Cable Pin Out

The following pin-out is used for the RJ21 ports.

1st RJ21 Connector

Port		Pin	Wire
1	Tip	26	White/Blue
	Ring	1	Blue/White
2	Tip	27	White/Orange
	Ring	2	Orange/White
3	Tip	28	White/Green
	Ring	3	Green/White
4	Tip	29	White/Brown
	Ring	4	Brown/White
5	Tip	30	White/Slate
	Ring	5	Slate/White
6	Tip	31	Red/Blue
	Ring	6	Blue/Red
7	Tip	32	Red/Orange
	Ring	7	Orange/Red
8	Tip	33	Red/Green
	Ring	8	Green/Red
9	Tip	34	Red/Brown
	Ring	9	Brown/Red
10	Tip	35	Red/Slate
	Ring	10	Slate/Red
11	Tip	36	Black/Blue
	Ring	11	Blue/Black
12	Tip	37	Black/Orange
	Ring	12	Orange/Black
13	Tip	38	Black/Green
	Ring	13	Green/Black
14	Tip	39	Black/Brown
	Ring	14	Brown/Black
15	Tip	40	Black/Slate
	Ring	15	Slate/Black
16	Tip	41	Yellow/Blue
	Ring	16	Blue/Yellow
Not Used		42	Yellow/Orange
		17	Orange/Yellow
		43	Violet/Slate
		08	Slate/Violet

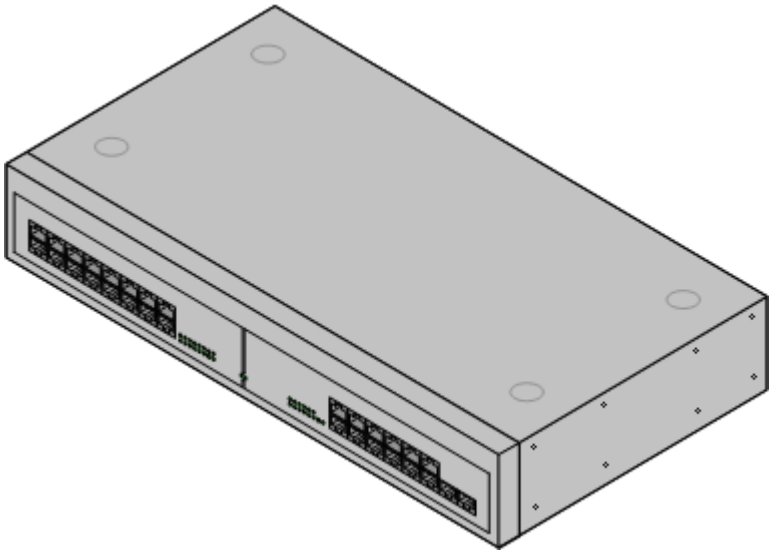
2nd RJ21 Connector

Port		Pin	Wire
17	Tip	26	White/Blue
	Ring	1	Blue/White
18	Tip	27	White/Orange
	Ring	2	Orange/White
19	Tip	28	White/Green
	Ring	3	Green/White
20	Tip	29	White/Brown
	Ring	4	Brown/White
21	Tip	30	White/Slate
	Ring	5	Slate/White
22	Tip	31	Red/Blue
	Ring	6	Blue/Red
23	Tip	32	Red/Orange
	Ring	7	Orange/Red
24	Tip	33	Red/Green
	Ring	8	Green/Red
25	Tip	34	Red/Brown
	Ring	9	Brown/Red
26	Tip	35	Red/Slate
	Ring	10	Slate/Red
27	Tip	36	Black/Blue
	Ring	11	Blue/Black
28	Tip	37	Black/Orange
	Ring	12	Orange/Black
29	Tip	38	Black/Green
	Ring	13	Green/Black
30	Tip	39	Black/Brown
	Ring	14	Brown/Black
Not Used		40	Black/Slate
		15	Slate/Black
		41	Yellow/Blue
		16	Blue/Yellow
		42	Yellow/Orange
		17	Orange/Yellow
		43	Violet/Slate
		08	Slate/Violet

13.5.4 DS16B/30B, DS16B2/30B2

This type of module can be used to add additional RJ45 ports for digital telephones. Through the system configuration, each module is set to either DS[271] mode for support Avaya DS digital telephones[39] or BST[270] mode ports for supported Avaya BST digital telephones[39] (DS ports only on IP500 control units). See DS16B2/30B2 Port Mode Selection[110].

The modules are available in 16 and 30 port variants, referred to as the IP500 DS16B and IP500 DS30B respectively. The DS16B and DS30B have now been superseded by the DS16B2 and DS30B2 models which provide the same functionality.

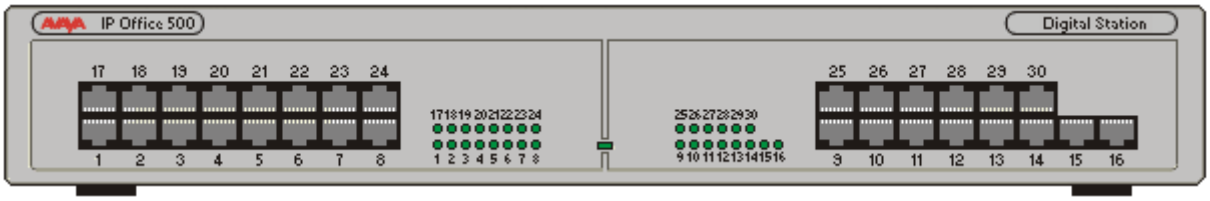


Feature	Details
Locales	Supported in all IP Office locales[42].
Minimum Software Level	• **DS16B/DS30B:** IP Office Release 9.0. IP500 (DS only) and IP500 V2 (DS or TCM). For IP Office Release 8.1 (Service Pack 9+) these modules only support DS ports. • **DS16B2/DS30B2:** IP Office Release 10.1. Also IP Office Release 9.1 SP12 and IP Office Release 10.0 SP5.
Included	Power supply unit (see below) and Expansion Interconnect cable.
Power Supply	The module is supplied with a Earthed 3-Pin, 60W external power supply module. The PSU has an integral power cord for connection to the module's DC I/P socket. A locale specific IEC60320 C13 power cord[30] for the external PSU is required but is not supplied with the module.
Mounting	The module is designed as a free-standing module that can be stacked on or under other IP Office modules. The module can be wall or rack mounted using the IPO IP500 RACK MNTG KIT V3[247].
Dimensions	Width: 445mm/17.5". Depth: 245mm/9.7". Height: 71mm/2.8".
Weight	Unboxed: 3.5Kg/7.8lbs. Boxed: 4.8Kg/10.8lbs. (Based on DS30)

- **DS16B/DS30B Upgrade Behavior:**
  For DS16B/DS30B modules the process of loading the appropriate firmware for the selected mode or upgrading takes up to 10 minutes during which time the module is not available.
- **DS16B2/DS30B2 Upgrade Behavior:**
  The behavior of DS16/30B2 during firmware upgrade or switching modes differs from other external expansion units:
  - During the firmware upgrade, the unit remains operational and can make and receive calls.
  - Once the upgrade is completed (approximately 9 minutes) the unit reboots and takes about 45 seconds to return to normal operation.

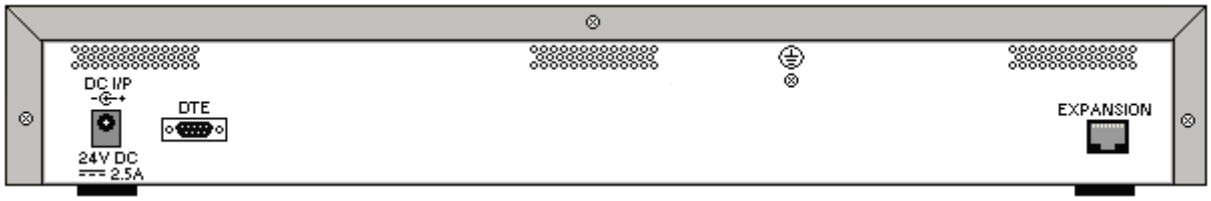
Página2897 de 3226.

Module Front



Port LEDs	• **Green Flashing** = Phone detected. • **Green On** = Phone active.
Module Center LED	The center LED on all external expansion modules is used to indicate the overall state of the module as follows: • **Red flashing** = Module starting up/Loading firmware. • **Red on** = Error. • **Green on** = Module okay.

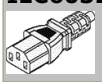
Module Rear



Port	Description
DC I/P 271	DC power input port. Used for connection of the power lead from an Avaya earthed 60W external power supply unit supplied with the expansion module. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
DS 271	RJ45 socket. Digital Station port. Used for connection of IP Office supported DS phones 39. If connected to an out-of-building extension 36, the connection must be made via additional IROB barrier devices in addition to the buildings primary protection. The module must also be connected to a protective ground.
DTE 278	9-Way D-Type socket. For Avaya use only.
EXPANSION 273	RJ45 Socket. Used for direct connection to an Expansion port on an IP Office control unit using the Expansion Interconnect cable supplied with the module.
⏚	Protective Ground point. Use of a protective ground is required for all installations, see Grounding (Earthing) 93 . Where the module is connected to analog extensions in another building, an IP Office Phone Barrier Box V2 (101V) is required at both ends, see Lightning Protection/Out-of-Building Connections 36 .

Part Codes and Related Equipment

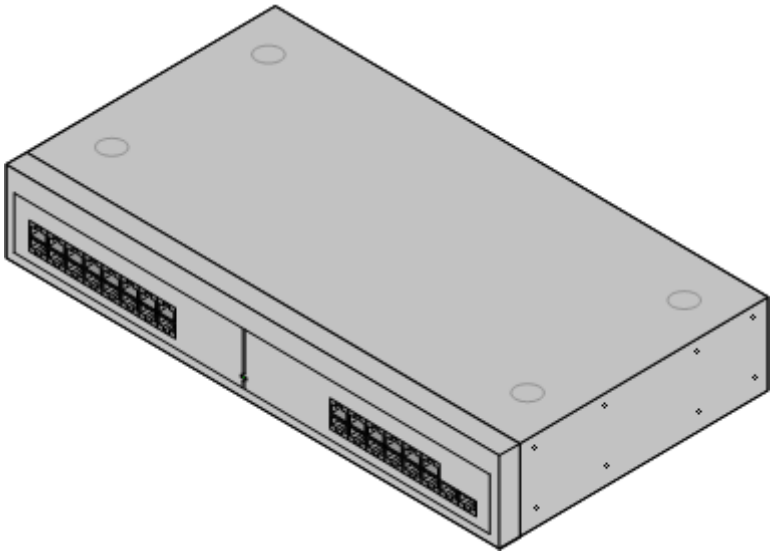
All expansion modules are supplied with a base software level and should be upgraded to match the core software of the control unit in the IP Office system. Expansion modules include an external power supply unit (PSU) and an appropriate interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

Item	Variant	Country	SAP Code
IPO IP500 EXP MOD DS16B DGTL ST	**16 Ports**	All	700501585
IPO IP500 EXP MOD DS30B DGTL ST	**30 Ports**	All	700501586
IPO IP500 EXP MOD DS16B2 DGTL ST	**16 Ports**	All	700511093
IPO IP500 EXP MOD DS30B2 DGTL ST	**30 Ports**	All	700511094
IEC60320 C13 Power Cord	**CEE7/7**	Europe	700289762
	**BS1363**	United Kingdom	700289747
	NEMA5-15P	America	700289770
Mounting Kit	**IPO IP500 WALL MNTG KIT V3**	All	700503160

Página2898 de 3226.

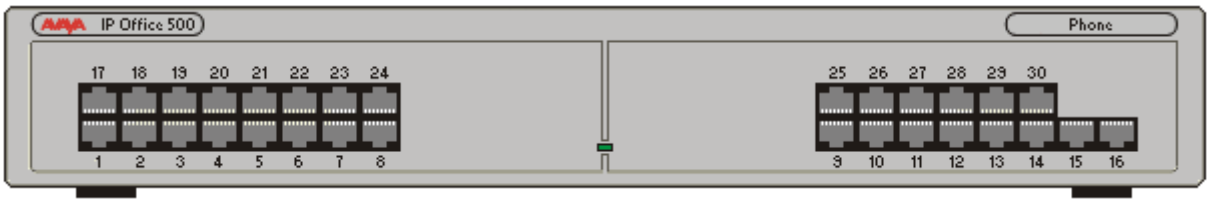
13.5.5 Phone 16/30

IP500 Phone modules can be used to add additional PHONE ports to an IP Office system. The module is available in 16 and 30 port variants, referred to as the IP500 Phone 16 and IP500 Phone 30 respectively.



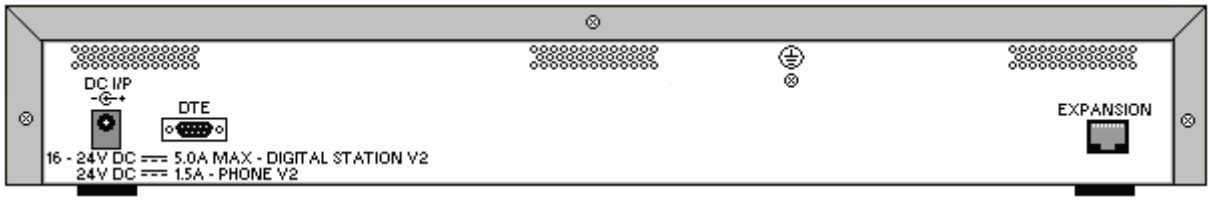
Feature	Details
Locales	Supported in all IP Office locales 42.
Minimum Software Level	IP Office core software level 2.1(36) minimum. Bin file = dvpots.bin.
Included	Power supply unit (see below) and Expansion Interconnect cable.
Power Supply	The module is supplied with a Earthed 3-Pin, 60W external power supply unit. The PSU has an integral power cord for connection to the module's DC I/P socket. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
Mounting	The module is designed as a free-standing module that can be stacked on or under other IP Office modules. The module can be wall or rack mounted using the IPO IP500 RACK MNTG KIT V3 247.
Dimensions	Width: 445mm/17.5". Depth: 245mm/9.7". Height: 71mm/2.8".
Weight	Unboxed: 3.1Kg/6.94lbs. Boxed: 4.4Kg/9.7lbs. (Based on Phone 30 V2)

Module Front



Module Center LED	The center LED on all external expansion modules is used to indicate the overall state of the module as follows: • **Red flashing** = Module starting up/Loading firmware. • **Red on** = Error. • **Green on** = Module okay. • **Green flashing** = Module starting up/Loading firmware (IP500 DS16A/30A module only).

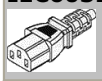
Module Rear



Ports	Description
DC I/P 271	DC power input port. Used for connection of the power lead from an Avaya earthed 60W external power supply unit supplied with the expansion module. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
DTE 278	9-Way D-Type socket. For Avaya use only.
EXPANSION 273	RJ45 Socket. Used for direct connection to an Expansion port on an IP Office control unit using the Expansion Interconnect cable supplied with the module.
PHONE 276	RJ45 socket. Used for connection of analog phones. Intended for two-wire analog phones. For connection to 4-wire analog phones connection should be via a master socket with ringing capacitors. If connected to an out-of-building extension 36, the connection must be made via additional IP Office Barrier Boxes 189 in addition to the buildings primary protection. The module must also be connected to a protective ground.
⏚	Protective Ground point. Use of a protective ground is required for all installations, see Grounding (Earthing) 35. Where the module is connected to analog extensions in another building, an IP Office Phone Barrier Box V2 (101V) is required at both ends, see Lightning Protection/Out-of-Building Connections 36 .

Part Codes and Related Equipment

All expansion modules are supplied with a base software level and should be upgraded to match the core software of the control unit in the IP Office system. Expansion modules include an external power supply unit (PSU) and an appropriate interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

Item	Variant	Country	SAP Code
IPO IP500 EXP MOD PHONE 16	**16 Ports**	All	700449507
IPO IP500 EXP MOD PHONE 30	**30 Ports**	All	700426224
IEC60320 C13 Power Cord 	**CEE7/7**	Europe	700289762
	BS1363	United Kingdom	700289747
	NEMA5-15P	America	700289770
Mounting Kit	**IPO IP500 WALL MNTG KIT V3**	All	700503160
IPO PHONE BARRIER BOX (101V) RHS		All	700385495

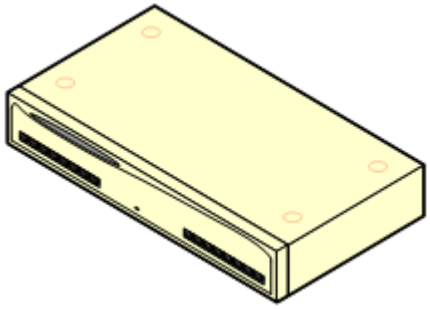
Página2900 de 3226.

13.6 IP400 Expansion Modules

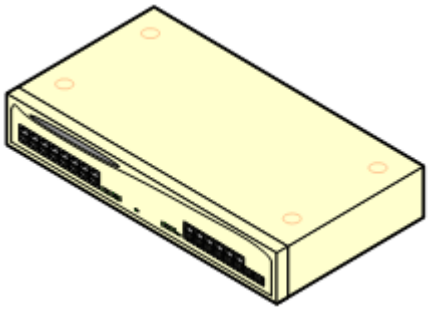
The following IP400 external expansion modules are supported by IP Office Release 11.0 and can be used with IP500 V2 control units. Each module uses an external power supply unit[30] supplied with the module. A locale specific power cord[31] for the PSU must be ordered separately.

If being rack mounted these units use the IP400 rack mounting kit. If being rack mounted, these units use the IPO IP500 RACK MNTG KIT. They cannot be wall mounted.

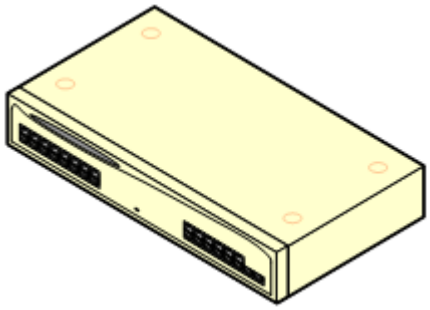
- **IP400 Analog Trunk Module (ATM16)**[241]
  Provides an additional 16 ANALOG[267] ports for connection of analog trunks. Supports both loop-start and ground-start trunks.
  - Available in a number of variants for different locales.
  - Use with ground start trunks requires that the trunk module and the IP Office control unit are grounded.



- **IP400 Digital Station Module V2**[243]
  Provides, depending on variant, an additional 16 or 30 DS[271] ports for supported Avaya digital phones[39]. Supersedes the previous Digital Station module.



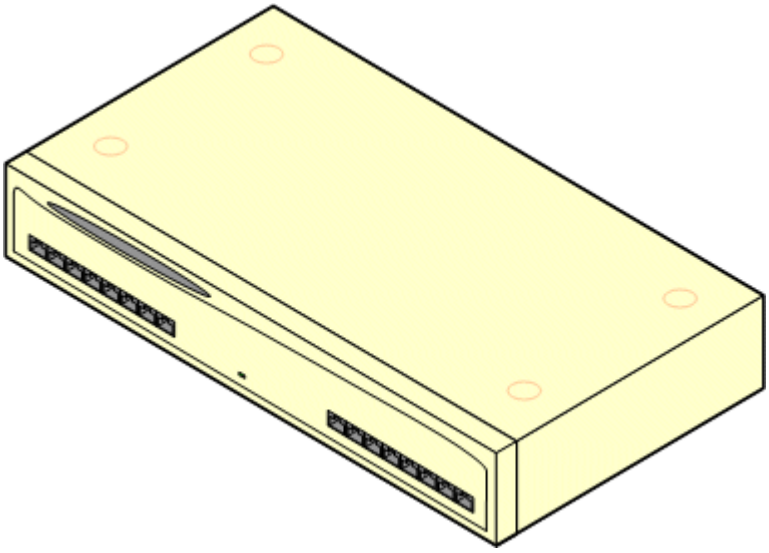
- **IP400 Phone Module V2**[245]
  Provides, depending on variant, an additional 16 or 30 PHONE[276] ports for analog phones. Supersedes the previous Phone module. With IP Office 3.1, the Phone V2 supports a wider range of message waiting indication (MWI) options than Phone V1 modules.



13.6.1 Analog Trunk 16

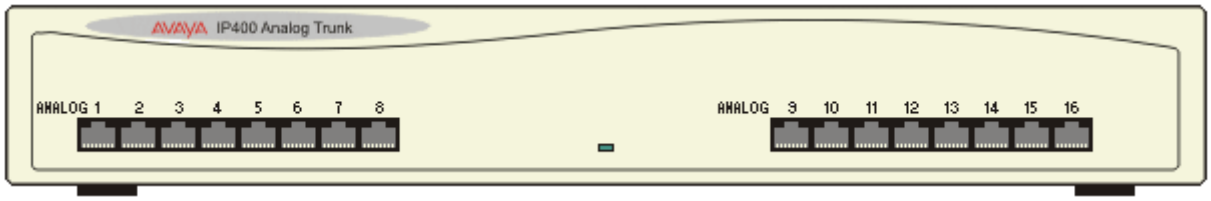
The IP400 Analog Trunk module (also known as the ATM16) is used to add 16 additional analog trunks to an IP Office system. The module supports both loop-start and, with suitable grounding, ground-start trunks.

- **WARNING**
  In all IP Office installations, any module being used for analog trunk connections must be connected to a functional earth 35.
- **WARNING**
  Within the Republic of South Africa and in areas of high lightning risk, any module using analog trunk connections must be connected to a protective ground 35 and to surge protection equipment 36.

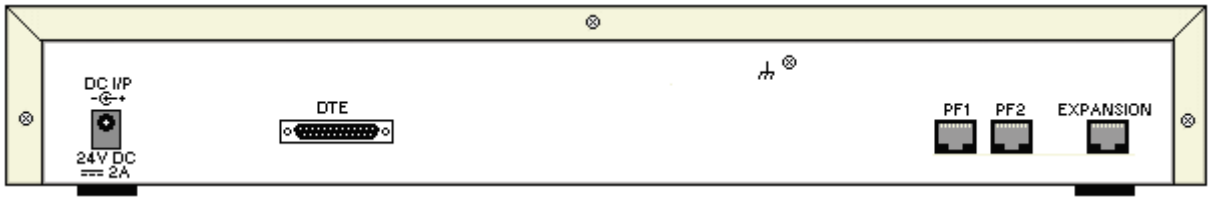


Feature	Details
Locales	Specific variants are provided for different IP Office locales, see below.
Minimum Software Level	IP Office core software level 1.0 minimum. Bin file = naatm16.bin.
Included	Power supply unit (see below) and Expansion Interconnect cable.
Power Supply	The module is supplied with a 2-pin, 40W external power supply unit. The PSU has an integral power cord for connection to the module's DC I/P socket. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
Mounting	The module is designed as a free-standing module that can be stacked on or under other IP Office modules. The module can be rack mounted in a 19" rack system using the optional IP400 Rack Mounting Kit.
Dimensions	Width: 445mm/17.5". Depth: 245mm/9.7". Height: 71mm/2.8"/2U.
Weight	Unboxed: 2.9Kg/6.6lbs. Boxed: 4.2Kg/9.4lbs.

Module Front



Module Rear



Ports	Description
ANALOG 267	RJ45 socket. Used for connection to analog trunks. Ports can be configured as either loop-start or ground-start trunks through the IP Office configuration. In the event of power failure, Analog ports 1 and 2 are directly connected to analog extension ports PF1 and PF2 respectively. If used the connected phones must be clearly labeled as power failure devices. This is only supported for loop-start analog trunks.
DC I/P 271	DC power input port. Used for connection of the power lead from an Avaya 40W external power supply unit supplied with the expansion module. A locale specific IEC60320 C7 power cord 30 for the external PSU is required but is not supplied with the module.
DTE 278	25-Way D-Type socket. For Avaya use only.
EXPANSION 273	RJ45 Socket. Used for direct connection to an Expansion port on an IP Office control unit using the Expansion Interconnect cable supplied with the module.
PF 275	RJ45 socket. Power failure analog extension ports. See Analog section above.
⏚	Ground point. Used for connection of a functional earth 35 if required. On older modules where this screw is not present, the top-center cover screw should be used instead. • IMPORTANT In all IP Office installations, any module being used for analog trunk connections must be connected to a functional earth 35 . • ⚠ WARNING Within the Republic of South Africa and in areas of high lightning risk, any module using analog trunk connections must be connected to a protective ground 35 and to surge protection equipment 36.

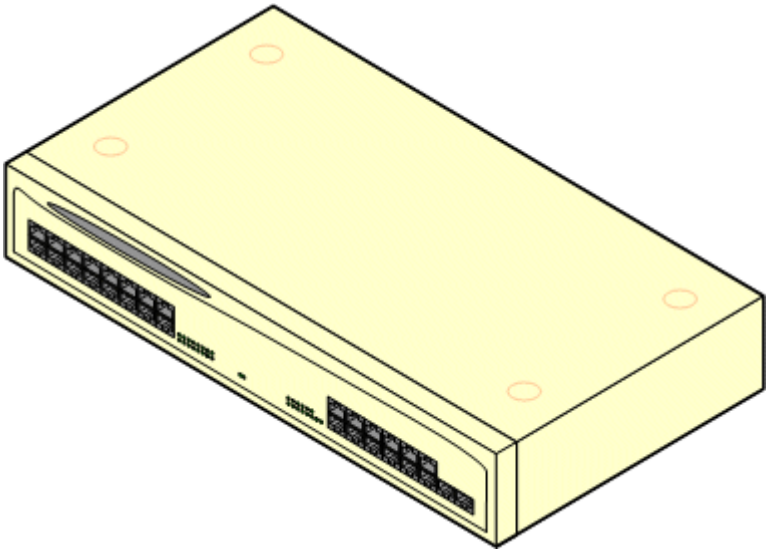
Part Codes and Related Equipment

All expansion modules are supplied with a base software level and should be upgraded to match the core software of the control unit in the IP Office system. Expansion modules include an external power supply unit (PSU) and an appropriate interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

Item	Variant	Country	SAP Code
IP400 Analog Trunk 16	America	America	700211360
	Europe	Europe	700241680
	New Zealand	New Zealand	700241698
IEC60320 C7 Power Cord	CEE7/16	Europe	700213382
	BS1363	United Kingdom	700213374
	NEMA1-15	America	700213390
	Korea	Korea	700254519
IP400 Rack Mounting Kit		All	700210800

13.6.2 Digital Station V2

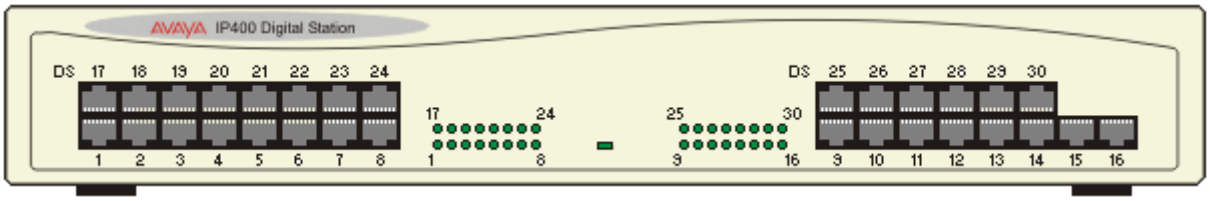
The IP400 Digital Station V2 (also known as DS V2) is used to add additional DS ports to an IP Office system. The DS V2 is available in 16 and 30 port variants, referred to as DS16 V2 and DS30 V2 respectively.



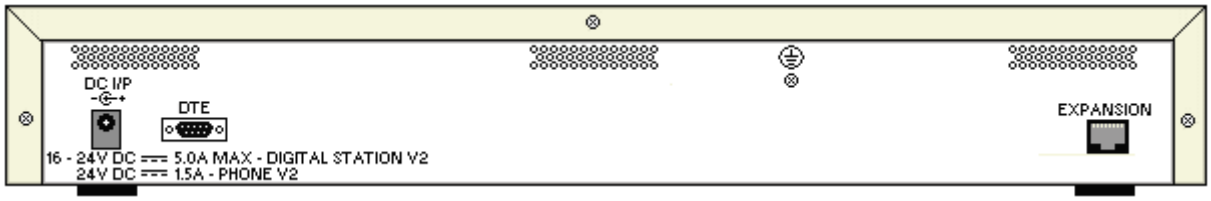
The DS V2 supersedes the original IP400 Digital Station, now referred to as a DS V1. The module version is indicated by labels both the base and the rear of the module.

Feature	Details
Locales	Supported in all IP Office locales 42.
Minimum Software Level	IP Office core software level 2.1(31) minimum. Bin file = nadcpV2.bin.
Included	Power supply unit (see below) and Expansion Interconnect cable.
Power Supply	The module is supplied with a Earthed 3-Pin, 60W external power supply module. The PSU has an integral power cord for connection to the module's DC I/P socket. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
Mounting	The module is designed as a free-standing module that can be stacked on or under other IP Office modules. The module can be rack mounted in a 19" rack system using the optional IP400 Rack Mounting Kit.
Dimensions	Width: 445mm/17.5". Depth: 245mm/9.7". Height: 71mm/2.8"/2U.
Weight	Unboxed: 3.5Kg/7.8lbs. Boxed: 4.8Kg/10.8lbs. (Based on DS30 V2)

Module Front



Module Rear



Ports	Description
DC I/P 271	DC power input port. Used for connection of the power lead from an Avaya earthed 60W external power supply unit supplied with the expansion module. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
DS 271	RJ45 socket. Digital Station port. Used for connection of IP Office supported DS phones 39. If connected to an out-of-building extension 36, the connection must be made via additional IROB barrier devices in addition to the buildings primary protection. The module must also be connected to a protective ground.
DTE 278	9-Way D-Type socket. For Avaya use only.
EXPANSION 273	RJ45 Socket. Used for direct connection to an Expansion port on an IP Office control unit using the Expansion Interconnect cable supplied with the module.
⏚	Protective Ground point. Use of a protective ground is required for all installations, see Grounding (Earthing) 35. Where the module is connected to analog extensions in another building, an IP Office Phone Barrier Box V2 (101V) is required at both ends, see Lightning Protection/Out-of-Building Connections 36.

Part Codes and Related Equipment

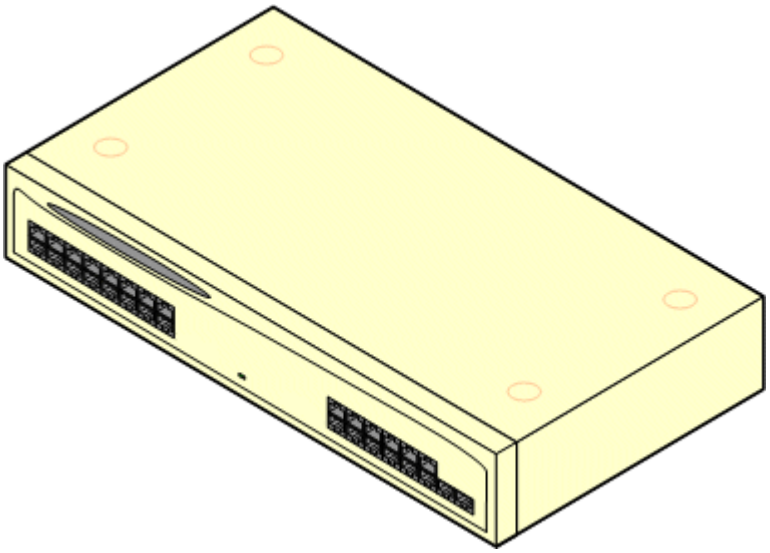
All expansion modules are supplied with a base software level and should be upgraded to match the core software of the control unit in the IP Office system. Expansion modules include an external power supply unit (PSU) and an appropriate interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

Item	Variant	Country	SAP Code
IP400 Digital Station V2	16 Ports	All	700359839
	30 Ports		700359847
IEC60320 C13 Power Cord	CEE7/7	Europe	700289762
	BS1363	United Kingdom	700289747
	NEMA5-15P	America	700289770
IP400 Rack Mounting Kit		All	700210800

Página2905 de 3226.

13.6.3 Phone V2

The IP400 Phone V2 module (also known as the Phone V2 module) is used to add additional analog PHONE ports to an IP Office system. The Phone V2 module is available in 16 and 30 port variants, referred to as the Phone 16 and Phone 30 respectively.

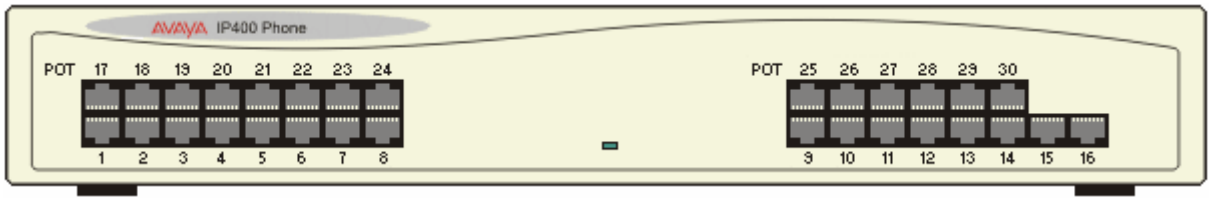


The Phone V2 module supersedes the original IP400 Phone module, now referred to as the Phone V1. The module version is indicated by labels on both the base and the rear of the module. Key changes are:

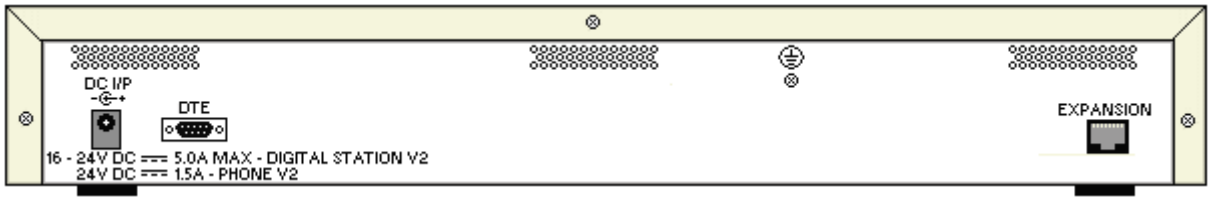
- The Phone V2 uses an earthed 3-pin 60W external power supply unit.
- With IP Office 3.1, the message waiting indication (MWI) on each port can be configured for ***None***, ***On***, ***51V Stepped***, ***81V***, ***Line Reversal A*** or ***Line Reversal B***. ***On*** uses the default determined by the system locale. Ports on a Phone V2 module can additionally be configured for ***101V*** operation.
- These ports do not include a ringing capacitor. Therefore for connection to 4-wire analog phones, where this is a requirement (typically the United Kingdom and New Zealand), connection should be via a Master socket containing ringing capacitors.
- The DTE serial port on the rear of the module has been changed to a 9-pin D-type socket.

Feature	Details
Locales	Supported in all IP Office locales.
Minimum Software Level	IP Office core software level 2.1(36) minimum. Bin file = dvpots.bin.
Included	Power supply unit (see below) and Expansion Interconnect cable.
Power Supply	The module is supplied with a Earthed 3-Pin, 60W external power supply unit. The PSU has an integral power cord for connection to the module's DC I/P socket. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
Mounting	The module is designed as a free-standing module that can be stacked on or under other IP Office modules. The module can be rack mounted in a 19" rack system using the optional IP400 Rack Mounting Kit.
Dimensions	Width: 445mm/17.5". Depth: 245mm/9.7". Height: 71mm/2.8"/2U.
Weight	Unboxed: 3.1Kg/6.94lbs. Boxed: 4.4Kg/9.7lbs. (Based on Phone 30 V2)

Module Front



Module Rear



Ports	Description
DC I/P 271	DC power input port. Used for connection of the power lead from an Avaya earthed 60W external power supply unit supplied with the expansion module. A locale specific IEC60320 C13 power cord 30 for the external PSU is required but is not supplied with the module.
DTE 278	9-Way D-Type socket. For Avaya use only.
EXPANSION 273	RJ45 Socket. Used for direct connection to an Expansion port on an IP Office control unit using the Expansion Interconnect cable supplied with the module.
PHONE 276	RJ45 socket. Used for connection of analog phones. Intended for two-wire analog phones. For connection to 4-wire analog phones connection should be via a master socket with ringing capacitors. If connected to an out-of-building extension 36, the connection must be made via additional IP Office Barrier Boxes 189 in addition to the buildings primary protection. The module must also be connected to a protective ground.
⏚	Protective Ground point. Use of a protective ground is required for all installations, see Grounding (Earthing) 93. Where the module is connected to analog extensions in another building, an IP Office Phone Barrier Box V2 (101V) is required at both ends, see Lightning Protection/Out-of-Building Connections 36.

Part Codes and Related Equipment

All expansion modules are supplied with a base software level and should be upgraded to match the core software of the control unit in the IP Office system. Expansion modules include an external power supply unit (PSU) and an appropriate interconnect cable. They do not include a locale specific power cord for the external PSU or any phone extension cables.

Item	Variant	Country	SAP Code
IP400 Phone V2	16 Ports	All	700359904
	30 Ports		700359912
IEC60320 C13 Power Cord	CEE7/7	Europe	700289762
	BS1363	United Kingdom	700289747
	NEMA5-15P	America	700289770
IP400 Rack Mounting Kit		All	700210800

13.7 Mounting Kits

The following mounting kits are available for use with IP Office systems.

13.7.1 IP500 Wall Mounting Kits

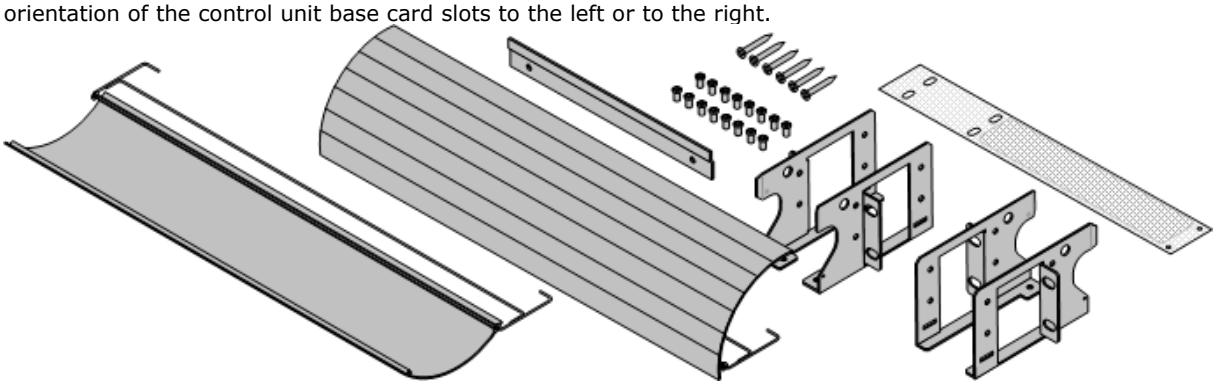
IP500 V2 control units and IP500 external expansion modules can be wall or rack mounted. To do this, a wall mounting kit is required in addition to suitable wall fixings.

In addition to the existing environmental requirements[51] for an IP Office system, the following additional requirements apply when wall mounting a unit:

- The wall surface must be vertical, flat and vibration free. Attachment to temporary walls is not supported.
- Only the screws provided with the mounting kit should be used to attach the brackets to the control unit or expansion modules.
- The installation must be done by a service person.
- Ensure that the system has been shut down and power has been removed from all the units. Shut down the system using a shutdown command and then remove the power. Do not simply remove the power.
- A suitable plywood mounting surface of at least 1m x 1m x 19mm (39" x 39" x 0.75") is required. If an expansion box is being mounted as well a plywood mounting surface of at least 1.2m x 1.2m x 19mm (48" x 48" x 0.75") is required.
- A minimum of 6 x 45mm long 5mm/6mm (1.75" #10/#12) pan head screws must be used to secure the plywood to the wall studs.
- The supplied 20mm long 4mm (#8 ¾") wood screws must be used to secure the brackets to the plywood mounting surface

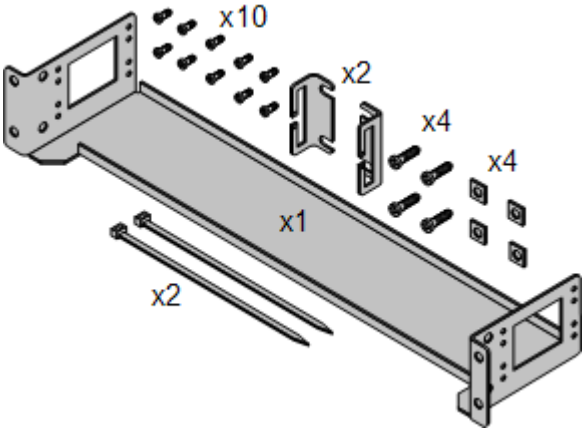
The following kit is currently available:

- **IPO IP500 WALL MNTG KIT V3** *(SAP Code 700503160)*
  This kit can be used for wall and rack mounting of IP500 V2 control units and IP500 external expansion modules. The kit incorporates cable routing at the front and rear of the unit. For wall mounted control units, it allows orientation of the control unit base card slots to the left or to the right.



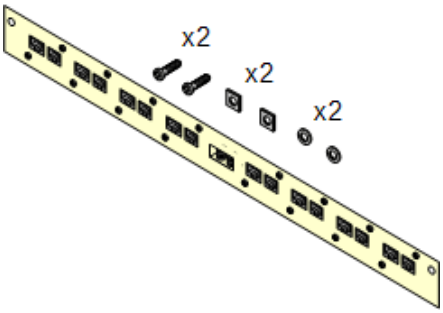
13.7.2 Rack Mounting Kit

- **IPO IP500 RACK MNTG KIT** *(SAP Code 700429202)*
  This kit contains all the components required for the rack mounting of a single IP500 V2 control unit or IP500 external expansion module. This includes screws for fixing of the brackets to the module, bolts for securing the module in the rack and cable tidy brackets..



Página2908 de 3226.

13.7.3 Barrier Box Rack Mounting Kit



- **Barrier Box Rack Mounting Kit** *(SAP 700293905)*
  Barrier boxes must be used for out-of-building analog phone extensions[36]. This bracket allows up to 8 IP Office barrier boxes to be rack mounted and simplifies the number of connections to the protective ground point in the rack. This kit must be used when more than 3 barrier boxes are in use and supports a maximum of 16 barrier boxes for a single external expansion module.

Página2909 de 3226.

13.8 Phones

IP Office Release 11.0 supports the following phones and phone add-ons. Availability may depend on location and may be subject to local restrictions. For historic phone support, see Hardware/Software Compatibility[290].

Enhanced Tip and Ring (ETR Ports)

These phones are only supported on an ETR6 card in a IP500 V2 systems. They are only supported in IP Office Basic Edition - PARTNER® Mode and IP Office Basic Edition systems running a North American locale and U-Law companding.

- **ETR Series:** ETR6, ETR6D, ETR18, ETR18D, ETR34D *(ETR 34D phones are limited to a maximum of 2 per card and 4 in total)*

Avaya DS Digital Telephones (DS Ports)

These digital stations connect to the IP Office via DS[271] ports. They are supported by all IP Office modes.

- **1400 Series:** 1403, 1408, 1416
- **9500 Series:** 9504, 9508

The following additional DS port phones are only supported in IP Office standard modes:

- **2400 Series:** 2402, 2410, 2420.

Avaya BST Digital Telephones (BST Ports)

These digital stations connect to the IP500 V2 IP Office system via BST ports.

- **4100 Series:** 4135, 4136, 4145, 4145EX, 4146, 4146EX - Connection to IP Office BST ports via a Digital Mobility Solution system.
- **7400 Series:** 7420, 7430, 7434, 7439, 7440, 7444, 7449 - Connection to IP Office BST ports via a Digital Mobility Solution system.
- **ACU:** Audio Conferencing Unit
- **M-Series:** M7100, M7100N, M7208, M7208N, M7310, M7310N, M7324, M7324N.
- **T-Series:** T7000, T7100, T7208, T7316, T7316E, T7406, T7406E

Analog Telephones

Analog phones and devices connect to PHONE[276] ports with the IP Office system. However due to the variety of analog phones and device available no guarantee of operation is given. It is the responsibility of the IP Office installer and maintainer to test and verify the operation of proposed analog equipment.

- **6200 Series:** 6211, 6219, 6221 *(North America)*.
- **B100 Series:** B149, B159, B169*.
- **Interquartz Gemini:** 9330-AV, 9335-AV, 9281-AV *(Europe, Middle East, Africa, Asia-Pacific)*.

IP Telephones

IP Phones (SIP and H323) connect to the IP Office system via the RJ45 LAN or WAN. These device require an Avaya IP Endpoint license and voice compression resources.

H323:

- **1600 Series:** 1603IP/SW, 1608, 1608-I, 1616, 1616-I
- **3600 Series:** 3641, 3645
- **3700 Series:** 3701, 3711 - Connection via DECT base stations. 3720, 3725, 3730, 3735, 3740, 3745, 3749 - Connection via DECT R4 base stations.
- **9600 Series:** 9608, 9608G, 9611G, 9620L, 9620C, 9621G, 9630G, 9640, 9640G, 9641G, 9641GS, 9650, 9650C.

SIP:

- **1000 Series:** 1010, 1040
- **1100 Series:** 1120E, 1140E
- **1200 Series:** 1220, 1230
- **B100 Series:** B169*, B179, B199.
- **D100 Series:** These DECT handsets (up to 8) use a base station that connects to the IP Office system using a SIP trunk and appear on the IP Office as SIP extensions.
- **E129:** A simple SIP telephone, the E129 support auto-answer, handsfree and headset operation.
- **H175:** SIP video telephone.
- **H200:** H229, H239, H249.
- **J100 Series:** J129, J139, J159, J169, J179.
- **K100 Series:** K155*, K165, K175.

*The B169 is a DECT phone that connects to a DECT base station. The base station connects to the IP Office. Analog and SIP base stations exist.

Página2910 de 3226.

13.9 Phone Button Modules

The maximum combined number of buttons on button modules per system is 1024.

- **1100 KEM:** *+18 (Max 3 per phone, 56 per system)*
  Add-on for 1120E and 1140E phones. Each module provides 18 additional programmable buttons.
- **1200 KEM:** *+12 (Max 7 per phone, 85 per system)*
  Add-on for 1220 and 1230 phones. Each module provides 12 additional programmable buttons.
- **BM12:** *+24 (Max 3 per phone, 42 per system)*
  Add-on for 9508, 9608, 9611 and 9641 phones. Provides 12 physical buttons assignable in 2 pages for 24 programmable buttons in total. When used with a 9508, power must be supplied to the phone using an inline power module.
- **BM32:** *+32 (Max 3 per phone, 32 per system)*
  Add-on for the 1616 phones that provides two columns of 16 buttons. Up to 3 BM32 modules are supported with any 1616. However, when used with more than one module the telephone must be powered from a power supply unit rather than PoE.
- **JEM24:** *+24 (Max 3 per phone, 14/42 per system*)*
  Add-on for the J169 and J179 phones. Each module provides 24* dual-LED programmable buttons with information display adjacent to each button.
  - *A single JEM24 connected to a phone supports 72 programmable button slots arranged in 3-pages, accessed using the page scroll button on the module. When multiple CBM24 modules are connected to a phone, each only supports 24 programmable button slot (i.e. a single page). This must be kept in mind when considering capacity, a single module attached to a phone uses the same button capacity as 3 modules on the same phone.
  - To support more than 2 button modules, the phone must use the J100 5V mains power supply unit rather than PoE.
  - JEM24 and JBM24 button modules cannot be combined on the same phone.
- **DBM32:** *+32 (Max 3 per phone, 32 per system)*
  Add-on for the 1416 phones that provides two columns of 16 buttons. Up to 3 BM32 modules are supported with any 1416. When used with a DBM32 button module, the telephone must be powered from a power supply unit.
- **EU24:** *+24 (Max 1 per phone, 8 per system)*
  Add-on for the 2420, 4620, 4620SW, 4625, 5620, 5620SW and 5621. Provides an additional 24 programmable buttons. Button display icons are on two switchable pages with 12 icons on each page.
- **EU24BL:** *+24 (Max 1 per phone, 8 per system)*
  As per the EU24 above but with a backlight function to match the 4621. Not supported on the 2420.
- **JBM24:** *+24 (Max 3 per phone, 42 per system)*
  Add-on for the J169 and J179 phones. Each module provides 24 dual-LED programmable buttons with information display adjacent to each button.
  - To support more than 2 button modules, the phone must use the J100 5V mains power supply unit rather than PoE.
  - JEM24 and JBM24 button modules cannot be combined on the same phone.
- **KLM:** *+48 (Max 2 per phone, 21 per system)*
  Used with M7324 phones. Up to 2 buttons modules are supported per phone. Each button module provides 48 programmable buttons.
- **SMB24:** *+24 (Max 3 per phone, 42 per system.)*
  Supported with 9630G, 9640, 9640G, 9650 and 9650C telephones. For IP Office Release 9.0, also supported with 9608, 9608G, 9611G, 9641G and 9641GS.
- **T7316E KEM:** *+24 (Max 9 per phone, 42 per system.)*
  Used with T7316E phones. Each button module provides 24 programmable buttons. Up to 4 buttons modules are supported per phone without additional power supply. From 5 to 9 modules can be supported with additional power. Maximum 9 per phone (4 without additional power).

13.10 Applications

This section outlines the requirements for various IP Office applications. These are just outlines, for full details refer to the specific installation manuals for those applications and to the IP Office Technical Bulletins.

- IP Office Application Server 252
- Avaya IX Workplace Client 254
- one-X Portal for IP Office 255
- Avaya Communicator 256
- IP Office Web Client 254
- SoftConsole 257
- TAPI 258
- Voicemail Pro 259
- Web Collaboration 260
- IP Office Manager 253
- Media Manager 253
- System Monitor 255
- System Status Application (SSA) 257

13.10.1 IP Office Application Server

This is not a single application, the IP Office Application Server is a single server installation package for the applications listed below. The DVD installs a CentOS Linux operating system, the IP Office applications and a set of web pages for server management. Note that the installation overwrites any existing operating system and data on the server PC.

- **one-X Portal for IP Office** 255
  User and configuration access is via web browser in the same way as for a Windows server installation of one-X Portal for IP Office.
  - **IP Office Web Client** 254
    This is a WebRTC client supported in a browser. It allows the user to make, answer and control audio and video calls from their PC. It is useable by users configured for one-X Portal for IP Office. Requires an IP Office Application Server with the WebRTC Gateway service configured.
- **Voicemail Pro** 259
  Configuration access is done using a Windows installation of the Voicemail Pro client software. An installation package for the Voicemail Pro client is included on the IP Office Application Server server.

For Voicemail Pro server running on a Linux based platform, the following features are not supported:

- **VB Scripting**
- **VPNM**
- **UMS Web Voicemail**
  (However, access via IMAP and one-X Portal for IP Office are available as alternatives.)

When logged into the voicemail server using the Voicemail Pro client, those features not supported are grayed out or hidden. If those features are present in an imported call flow, they will not function and calls attempting to use those features will be disconnected.

The Voicemail Pro client's backup and restore functions cannot currently be used to move voicemail data between a Linux based server and a Windows based server or vice versa. The client functions for importing and exporting module and the call flow database can be used.

For Small Community Network scenarios where multiple voicemail servers are present, for example distributed and backup server, a mix of Linux based and Windows based servers are allowed.

- **Media Manager** 253
  Voicemail Pro can be used for manual and automatic call recording. Those recording are placed into mailboxes. Media Manager allows those recordings to be redirected to a separate store where details of each recording are maintained in a searchable database. This allows recordings to be archived, searched and played back separately from mailbox messages. This application requires entry of a additional licenses into the IP Office configuration. This application requires an IP Office Application Server including additional hard disk for storage of recordings.
- **Web Collaboration** 260
  Share documents and messages in a conference. Web Collaboration provides the user with functions to share documents, applications and their desktop in a web collaboration conference. This runs in parallel with an audio conference hosted by the IP Office system. Internal users licensed for web collaboration can use WebRTC to stream audio via the web collaboration conference rather than having to make a parallel telephone call to the audio conference.

Details	
DVD	IP Office Application Server Release 11.0 DVD Set (2)
License	✓ - Depends on the IP Office applications selected during installation. The IP Office Application Server server itself does not require any license.

PC Requirements

Refer to the *"Installing and Maintaining the Avaya IP Office Application Server"* manual.

13.10.2 IP Office Manager

This tool is used to access all parts of the IP Office configuration. Different levels of access can be defined to control which parts of the configuration the IP Office Manager user can view and alter. IP Office Manager is also used to upgrade the software files used by an IP Office system. When running is also acts as a TFTP server from which some Avaya phones can request new software.

- **IP Office Manager Version**
  It is important to download and install the correct version of the IP Office administration suite including IP Office Manager.
  - For system installation, you should use the version of IP Office Manager that matches the IP Office release required on the system. This sets the version of software loaded when recreating the System SD card 75.
  - For system maintenance, the version of IP Office Manager used sets the version of software uploaded to a system when upgrading the system 180.
  - For system configuration IP Office Manager is backward compatible. IP Office Manager Version 11.0 is backwards compatible for configuring systems running software from IP Office Release 6.0 upwards. IP Office Manager cannot load the configuration of an IP Office system running a higher version of software.
  - **Admin Lite Not Supported**
    Note that the IP Office Manager installed from the **AdminLite** installer is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. To support IP500 and IP500 V2 systems, ensure that you download and install the full IP Office Administration suite installer (approximately 1.46GB compared to the 100MB AdminLite installer).

Details	
DVD	IP Office Release 11.0 User/Admin DVD Set (2) (700513659) (Disk 1)
Languages	English, Brazilian, Chinese (Simplified), Dutch, French, German, Italian, Russian, Spanish (Mexican).
License	✗ No license required.

PC Requirements

For PC requirements refer to the appropriate IP Office installation or implementation manual for the application. For operating system and browser support refer to Operating System Summary 261.

13.10.3 Media Manager

Voicemail Pro 259 can be used for manual and automatic call recording. Normally those recordings are placed into the mailbox specified for the user or hunt group whose call is being recorded and are then treated as normal messages. Media Manager allows those recordings to be redirected into a database on the server running Media Manager. This allows recordings to be archived and searched separately from user messages. User access is via web browser.

Media Manager is a service that can be run on an IP Office Application Server which can also host Voicemail Pro and/or one-X Portal for IP Office. However, the server must be configured with a separate disk or partition for the storage of the call recordings.

Details	
License	✓ Media Manager. See Voicemail Pro Licenses 284.

13.10.4 Avaya IX Workplace Client (Equinox)

This is a unified communication application that supports calls, directory contacts, presence, instant messaging and many other features. It is supported as an application on a wide range of operating systems; Windows, Android, macOS and iOS (see Operating System Suppor 261 t for details).

Avaya IX Workplace Client on Vantage phones is supported from 11.0.4.0 onwards using Vantage R2.0.1 firmware.

On IP500 V2 systems Avaya IX Workplace Client is supported for the following users:

User Profile	System Licenses	User Licenses	Mode	OS
Basic User	Essential Edition	Avaya Softphone License	Standalone	macOS, Windows
Mobile User	Essential Edition + Preferred Edition	Mobile Worker + Avaya Softphone License	Standalone	macOS, Windows
Teleworker User	Essential Edition + Preferred Edition	Teleworker	Simultaneous	macOS, Windows
Office Worker User	Essential Edition + Preferred Edition	Office Worker	Simultaneous	macOS, Windows
Power User	Essential Edition + Preferred Edition	Power User	Simultaneous	Android, iOS, macOS, Windows

- **Standalone Mode**
  In this mode, Avaya IX Workplace Client is the users sole telephony device whilst they are logged into Avaya IX Workplace Client. Logging into Avaya IX Workplace Client will log them off any other extension. Similarly logging on at another phone will log them out of Avaya IX Workplace Client.
- **Simultaneous Mode**
  In this mode, the user can be logged in on both a physical desk phone and a softphone client such as Avaya IX Workplace Client at the same time. They can choose to make and answer calls on each extension
  - Softphone clients includes Avaya IX Workplace Client clients, Avaya Communicator clients, one-X Mobile clients, IP Office Web Client and IPOCC Agent Web Client.
  - Simultaneous client usage was previously only supported if the softphone client registered to the same IP Office on which the user was configured. For R11.0, the softphone client can be registered to any IP Office in the network.
- **Shared Control Mode**
  Simultaneous mode Windows and macOS users can put their Avaya IX Workplace Client client into shared control mode. In that mode, the application is used to make and answer calls via their desk phone.
  - Currently only supported for Avaya IX Workplace Client clients and desk phones registered to the same IP Office server.
  - Audio calls only, no video call support.

Additional Notes

- Installation Avaya IX Workplace Client on Windows automatically replaces any installation of Avaya Communicator on the same PC.

13.10.5 IP Office Web Client

This is an Avaya WebRTC client which can be used with IP Office systems. For IP500 V2 installations, it requires the IP500 V2 to be supported by one-X Portal for IP Office 255 running from an IP Office Application Server 252. The IP Office Application Server server is configured with a WebRTC Gateway service.

The application is useable by any user licensed and configured for one-X Portal for IP Office and using the Chrome browser on a Windows or macOS PC.

A thick-client is also available for Windows. The installer can be downloaded from one-X Portal for IP Office or with a IP Office Web Client browser session. The thick-client includes an embedded version of Chrome and so does not require the user's PC to have Chrome installed as a browser.

For details of installation, refer to the *"Installing and Maintaining the IP Office Application Server"* manual.

Página2915 de 3226.

13.10.6 Monitor

Monitor (also known as System Monitor) is a tool that can show all activity on the IP Office system in great detail. As a consequence, interpretation of Monitor traces requires a high-level of data and telephony protocol knowledge. However, all IP Office installers and maintainers must understand how to run Monitor when necessary as Avaya may request copies of Monitor traces to resolve support issues.

For IP Office 4.0 and higher, the System Status Application[257] has been added to provide more easily interpreted information than is provided by Monitor.

Details	
DVD	IP Office Release 11.0 User/Admin DVD Set (2) (700513659) (Disk 1)
Languages	English only.
License	✗ No license required.

PC Requirements

For PC requirements refer to the appropriate IP Office installation or implementation manual for the application. For operating system and browser support refer to Operating System Summary[261].

13.10.7 one-X Portal for IP Office

This application is installed on a server PC connected to the IP Office. Users can access the one-X portal from their own PC using a web browser.

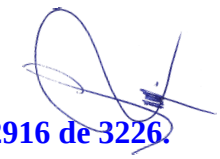
The application allows the user to control their phones, access voicemail messages, call logs and phone directories.

Details	
DVD	IP Office Release 11.0 User/Admin DVD Set (2) (700513659) (Disk 2) or IP Office Application Server Release 11.0 DVD Set (2)
License	✓ See User Licenses[282].
Languages	Brazilian Portuguese, Czech, Dutch, English (UK), English (US), French, German, Italian, Japanese, Korean, Polish, Russian, Swedish, Turkish and Latin Spanish.

The one-X Portal for IP Office server application can be installed on a Windows server or be provided by an IP Office Application Server[252] or Unified Communications Module[217].

PC Requirements

For PC requirements refer to the appropriate IP Office installation or implementation manual for the application. For operating system and browser support refer to Operating System Summary[261].



13.10.8 Avaya Communicator

Avaya Communicator is a user softphone application which allows the user to make and answer their calls from a range of telephone devices. Avaya Communicator client software is available Windows and iPad devices. An addition version, Avaya Communicator for Web supported through Google Chrome, is not covered by this documentation.

Details	
License	✓ See the table below.
Languages	Dutch, English (UK), English (US), French, Italian, Brazilian Portuguese, Russian and Spanish.

The features available to the user depend on how the user is licensed for Avaya Communicator and whether the system also includes one-X Portal for IP Office 255 and Voicemail Pro 259.

		Avaya Communicator Mode	
		Lite Mode	**Advanced Mode**
Basic Features		• Make calls, hold calls, mute and transfer calls. • System directory. • Local application call log.	• Make calls, hold calls, mute and transfer calls. • System directory. • Local application call log.
Advanced Features *(Require one-X Portal for IP Office and Voicemail Pro)*		–	• User directories and call logs via one-X Portal for IP Office • Presence (XMPP). • 2-Party Instant Messaging • 2-Party video calls. • Dual extension support.
Licenses Required	**System License**	• **Essential Edition**	• **Essential Edition + Preferred Edition**
	User Licenses	• **Avaya Softphone**	• **Office Worker** or • **Teleworker** or • **Power User**.
System Mode	**IP Office Essential Edition**	✓ Yes	–
	IP Office Preferred Edition	✓ Yes	✓ Yes
Client Connection		Support for basic mode features is provided directly by the IP Office system.	Support for advanced mode features is provided by the one-X Portal for IP Office and Voicemail Pro applications.

- **Client Software**
  The source for the Avaya Communicator client software depends on the user device. However, since Avaya Communicator is supported on a number of Avaya platforms, in all cases the installer must ensure that they obtain a Avaya Communicator client that specifically states IP Office support.

Windows PC Requirements

For PC requirements refer to the appropriate IP Office installation or implementation manual for the application. For operating system and browser support refer to Operating System Summary 261.

Página2917 de 3226.

13.10.9 SoftConsole

This is a licensed application. It is intended for telephone system operators or receptionists. Its displays details of calls directed to the user and allows them to quickly see the status of the callers required destination and transfer the call. The SoftConsole user is able to access a range of details about the status of users and groups on the IP Office system.

- The IP Office SoftConsole works in conjunction with a physical IP Office extension phone to provide the speech path for calls.
- Up to 4 simultaneous SoftConsole users can be licensed.

Details	
DVD	IP Office Release 11.0 User/Admin DVD Set (2) (700513659) (Disk 1) or Linux server App Center tab.
Languages	Brazilian, Chinese (Simplified), Danish, Dutch, English (UK), English (US), Finnish, French, German, Italian, Korean, Japanese, Latin Spanish, Norwegian, Portuguese, Russian, Spanish and Swedish.
License	✓ Licensed application. See below.

Licenses

License	Description	RFA Name	SAP
Receptionist	Adds one additional SoftConsole user. A maximum of four SoftConsole user can be licensed.	IPO LIC RECEPTIONIST RFA	171987

PC Requirements

For PC requirements refer to the appropriate IP Office installation or implementation manual for the application. For operating system and browser support refer to Operating System Summary 261.

13.10.10 System Status Application

This tool provides a wide range of information about the current status of an IP Office 4.0 or higher system. Its includes available resources and components within the system. This includes details of current call in progress. Details of the number of alarms are recorded and the time date of the most recent alarms.

When required for diagnostics escalation SSA is able to take a snap shot image of the IP Office system's status including a copy of its current configuration. Use of SSA requires an IP Office service user name and password that has been configured for System Status access in the IP Office's security settings.

- For IP500 V2 systems, SSA is pre-installed on the system's Avaya SD memory card and can be run by browsing to the IP Office system's IP address.

Details	
DVD	IP Office Release 11.0 User/Admin DVD Set (2) (700513659) (Disk 1)
License	✗ No license required.

PC Requirements

For PC requirements refer to the appropriate IP Office installation or implementation manual for the application. For operating system and browser support refer to Operating System Summary 261.

13.10.11 TAPI

IP Office TAPI is a client PC application that allows TAPI compliant applications to interact with the IP Office. The IP Office TAPI software can be used in one of two modes, depended on whether it is licensed or not. The same software is installed in either case with the licenses, if any, being entered in the IP Office system configuration.

- **1st Party TAPI**
  In this unlicensed mode the TAPI software supports control of an individual user's associated extension, allowing a TAPI compliant application to answer (requires a phone that supports handsfree answer) and make calls.
- **3rd Party TAPI**
  In this licensed mode, TAPI software can be used to control call function on multiple user extension. This mode is used with CTI Developer applications.

Details	
DVD	IP Office Release 11.0 User/Admin DVD Set (2) (700513659) (Disk 1)
License	✗ Optional. Licenses are required for 3rd party TAPI mode operation. See CTI Licenses 285 .

PC Requirements

For PC requirements refer to the appropriate IP Office installation or implementation manual for the application. For operating system and browser support refer to Operating System Summary 261 .

13.10.12 Voicemail Pro

This application requires various licenses entered into the IP Office configuration to control the features it offers and the number of simultaneous connections (40). The operation of Voicemail Pro can be customized to provide special services. .

The Voicemail Pro software can be installed as separate Voicemail Pro client and server parts. This allows the remote administration of the Voicemail Pro server from a PC with just the Voicemail Pro client installed. A copy of the client is automatically installed locally with the Voicemail Pro server.

Source	
DVD	IP Office Release 11.0 User/Admin DVD Set (2) (700513659) (Disk 1) or IP Office Application Server Release 11.0 DVD Set (2)
Languages	Chinese-Mandarin, Chinese-Cantonese, Danish, Dutch, English-UK, English-US, Finnish, French, French-Canadian, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Portuguese Brazilian, Russian, Spanish, Spanish-Argentinean, Swedish, Turkish.
License	✓ See Voicemail Pro Licenses 284 .

The details below are for a Windows based server installation of Voicemail Pro. Voicemail Pro can also be installed as part of a Linux based server installation using the IP Office Application Server DVD 252 .

The Voicemail Pro server part of the software consists of several components in addition to the core server software, these are:

- **Campaigns**
  The Voicemail Pro can be configured to run a campaign. This consists of a series of questions for which the Voicemail Pro records the callers answer or key presses. The resulting recordings can then be played back by users. The web aspect of campaigns allows user to perform this playback and processing of campaign recordings via their web browser. This requires an IIS web server to be run on the same PC as the Voicemail Pro software.
- **Text to Speech (TTS)**
  Through adding additional licenses, the Voicemail Pro is able to use the TTS functions of Windows to speak text and numbers to callers in addition to recording prompts. This is intended mainly for scenarios where the Voicemail Pro is obtaining text and number values from a customer database.
- **Unified Messaging Service (UMS)**
  Voicemail Pro supports a feature called voicemail email to send messages or message alerts to a user's email mailbox. This however is a one-way process with no link back to the user's voicemail mailbox on whether the email has been read or deleted. UMS allows this to become a two-way process, where users can play voicemail messages through their email mailbox or voicemail mailbox.

PC Requirements

For PC requirements refer to the appropriate IP Office installation or implementation manual for the application. For operating system and browser support refer to Operating System Summary 261 .

13.10.13 Web Collaboration

Web Collaboration is a service supported from an IP Office Application Server. It works in conjunction with one-X Portal for IP Office and Voicemail Pro.

Web Collaboration provides the user with functions to share documents, applications and their desktop in a web collaboration conference. This runs in parallel with an audio conference hosted by the IP Office system.

- Capacity matches the IP Office audio conferencing capacity. Bandwidth requirement 250kbps per user.
- Host users must be licensed for one-X Portal for IP Office as an **Office Worker**, **Teleworker** or **Power User** profile plus also a **Web Collaboration** license.
- Conference scheduling, via one-X Portal for IP Office, requires a **Power User** license.
- Hosts can upload documents in PDF, JPEG and PNG formats.
  - 10 documents per user
  - 6MB per document.
- Application and desktop sharing is not supported for MAC PC users.
- Launch from browser URL 263 or directly from Avaya Communicator, one-X Portal (including Outlook plugin and Call Assistant) and IP Office Web Client.
- Languages: English, French, Spanish, German, Italian, Portuguese, Russian, Swedish, Chinese, Japanese, Korean.
- Video is not supported.
- For IP Office Release 10.0, internal users licensed for web collaboration can use WebRTC to stream audio via the web collaboration conference rather than having to make a parallel telephone call to the audio conference.

13.10.14 IP Office Ports

Details of the range of ports used by IP Office and IP Office applications are found at https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003.

Most PC firewalls requests the user to allow various exceptions when a newly installed application first runs. However this is not always the case, especially if the firewall is located elsewhere than the user's PC.

13.11 Operating System Support

This sections summarizes the support for IP Office applications by IP Office Release 11.0.

Some specific features of applications may have additional requirements. Those requirements will be details in the specific installation manual for the application. Unless otherwise stated, the operating system is the latest supported version from the operating system developer.

13.11.1 Windows Support

The table below list the IP Office applications installable on supported Windows operating system. It does not include browseable applications[263].

Microsoft Windows	7	8.1	10	2012/ 2012 R2	2016
	Professional, Enterprise, Ultimate	Pro, Enterprise	Pro, Enterprise	Standard	Standard, Essentials
Server Applications					
one-X Portal for IP Office	–	–	–	✓	✓
IP Office Contact Center	–	–	–	✓	–
Voicemail Pro Server	✓	✓	✓	✓	✓
... plus UMS	–	–	–	✓	✓
... plus campaigns	–	–	–	✓	✓
... MAPI service for Linux Voicemail Pro	✓	–	–	✓	✓
User Applications					
one-X Portal plug-in for Outlook	✓	✓	✓	–	–
" Call Assistant	✓	✓	✓	–	–
" plug-in for MS Lync 2013	✓	✓	✓	–	–
IP Office Web Client Thick Client	✓	✓	✓	–	–
Avaya Communicator	✓	✓	✓	–	–
Avaya IX Workplace Client	✓	✓	✓	–	–
SoftConsole	✓	✓	✓	–	–
TAPI - 1st Party	✓	✓	✓	✓	✓
TAPI - 3rd Party	✓	✓	✓	✓	✓
TAPI WAV[1]	✓	✓	✓	–	–
Web Conferencing Desktop Sharing	✓	✓	✓	–	–
Maintainer Applications					
IP Office Manager	✓	✓	✓	✓	✓
System Monitor	✓	✓	✓	✓	✓
System Status Application	✓	✓	✓	✓	✓
Voicemail Pro Client	✓	✓	✓	✓	✓

1. TAPI WAV is not supported on 64-bit operating systems.

13.11.1.1 Exchange/Outlook Support

Outlook Support

Application\Outlook Version	2007	2010	2013	2016
Voicemail Pro UMS/IMAP	–	✓	✓	✓
TAPI Dialing	–	✓	✓	✓
one-X Portal for IP Office plug-in for Outlook	–	✓	✓[1]	✓[1]

1. Screen popping of Outlook contacts not supported.

Exchange Support

Application\Exchange Server	2010	2013	2016
Voicemail Pro UMS	✓	✓	✓
one-X Portal for IP Office Presence	✓	✓	✓
one-X Portal for IP Office Calendar	✓	✓	–
Avaya IX Workplace Client Calendar	✓	✓	✓

13.11.2 Android Support

The table below lists the IP Office applications supported Android operating systems. It does not include browseable applications[263].

IP Office Application	4.4	5.x	6.X	7.X	8.0
	Kit Kat	Lollipop	Marshmallow	Nougat	Oreo
Avaya IX Workplace Client[254]	✓[1]	✓[1]	✓	✓	✓

1. Zang services not supported.

13.11.3 Apple Support

macOS PCs

The table below lists the IP Office applications supported macOS operating systems. It does not include browseable applications[263].

Application	10.8	10.9	10.10	10.11	10.12	10.13
	Mountain Lion	Mavericks	Yosemite	El Capitan	Sierra	High Sierra
Web Conferencing Desktop Sharing[260]	✓	✓	✓	✓	✓	✓
Avaya IX Workplace Client[254]	–	–	–	✓	✓	✓

iPad

- Avaya Communicator[256] is supported on iOS 6.1 and higher.
- Avaya IX Workplace Client[254] is supported on iOS 10 and 11.

iPhone

- one-X Mobile is supported on iOS 7.0 and higher.
- Avaya IX Workplace Client is supported on iOS 10 and 11.

13.11.4 Linux Support

The following IP Office server applications are supported with IP500 V2 systems when run on an IP Office Application Server[252]. The IP Office Application Server includes the installation of its own operating system.

- **Voicemail Pro**
- **one-X Portal for IP Office**
- **Media Manager**

Página2923 de 3226.

- **Web Collaboration**
- **WebRTC Gateway** (for support of IP Office Web Client usage)

13.11.5 Browser Support

The table below lists the support for IP Office applications which are accessed using a web browser.

Application\Browser	Internet Explorer		Edge	Firefox	Google Chrome	macOS Safari 8 Safari 9 Safari 10
	10.0[5]	11.0				
Voicemail Pro Campaigns	✓	✓	✓	–	–	–
Voicemail Pro UMS Webmail	✓	✓	✓	–	–	–
one-X Portal for IP Office [1]	✓	✓	✓	✓	✓	✓
IP Office Web Client	–	–	–	–	✓	–
Avaya Communicator for Web	–	✓	–	–	✓	–
IP DECT R4 Admin	✓	✓	✓	✓	✓	✓
D100 DECT Admin	✓	✓	✓	✓	✓	✓
Web Collaboration [4]	✓	✓	✓	✓	✓	✓
IP Office Web Manager [3]						
" on PC	✓	✓	✓	✓	✓	✓
" on iPad tablet (iOS6+)	–	–	–	–	✓	✓
" on Android tablet (KitKat 4.4+)	–	–	–	–	✓	–
Avaya Communicator for Web	–	✓	–	–	✓	–

Notes:

1. one-X Portal for IP Office browsing is not supported from Windows server operating systems.
2. The version of IE must match the operating system. For example 32-bit browser on a 32-bit OS.
3. Some IP Office Web Manager features are only supported on Windows PC operating systems, for example Backup, restore, upgrade, launch System Status Application/Voicemail Pro/IP Office Manager, file uploads.
4. WebRTC audio is only supported using Chrome or Firefox.
5. IE10 is only supported on Windows Server 2012 (not R2).

13.12 Physical Ports

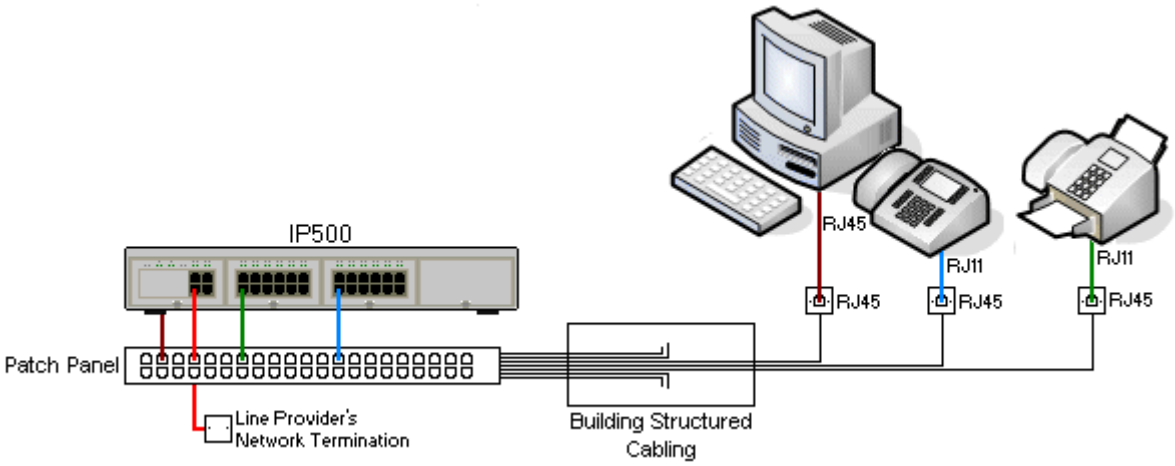
The following port types are found on the IP Office control unit and external expansion modules:

- **ANALOG** 267
  Used for the connection of external analog trunks.
- **AUDIO** 267
  Used for input of an external music on hold source.
- **BRI** 269
  Used for connection of BRI trunks (Quad BRI trunk card). In IP Office standard modes they can also be used for ISDN terminals devices (So8 mode).
- **BST (RJ21)** 270 and **BST (RJ45)** 270
  Connections for M-Series and T-Series phones supported by IP Office. Also for Digital Mobility Solution system supporting 4100 Series and 7400 Series phones. See supported Avaya BST digital phones 39 .
- **DC I/P** 271
  Power input from external power supply unit.
- **DS** 271
  Connection of Avaya digital station phones supported by IP Office.
- **RS232/DTE** 278
  Used for control unit maintenance under Avaya guidance. On expansion modules not used.
- **EF** 272
  Emergency power failure ports found on the ETR6 base card.
- **ETR** 272
  Only supported on IP500 V2 control unit running in IP Office Basic Edition - PARTNER® Mode or IP Office Basic Editions.
- **EXPANSION** 273
  Used for interconnection of external expansions modules and control units.
- **EXT O/P** 191
  Used to control external relay systems. The port provides two switchable (on, off and pulse) controls.
-
  Used for connection of functional or protective ground if required.
- **LAN** 274
  10/100Mbps Ethernet LAN ports.
- **PF** 275
  Analog power fails ports.
- **PHONE** 276 **(POT)** 276
  Analog phone extension ports. On older units these ports are labeled as POT ports.
- **PRI** 277
  PRI trunk ports.

13.12.1 Cables

The IP Office systems are designed primarily for use within an RJ45 structured cabling system using CAT3 unshielded twisted-pair (UTP) cabling and RJ45 sockets.

A structured cabling system is one where cables are run from a central RJ45 patch panel in the communications/data room to individual RJ45 sockets at user locations. All wires in each cable between the patch panel and the desk socket are connected straight through. This arrangement allows devices connected at the patch panel to be swapped to match the type of device that needs to be connected at the user socket. For example, making one user socket a phone port and another user socket a computer LAN port, without requiring any rewiring of the cables between the patch panel and the user location.



- **Traditional IDC Punchdown Wiring Installations**
  Where necessary, the far end RJ45 plug can be stripped from IP Office cables and wired into traditional wiring systems using punch-block connectors. This type of installation should be performed by an experienced wiring technician.
- **Trunk Connections**
  The majority of IP Office trunk ports use RJ45 connectors for acceptance of an RJ45-to-RJ45 cable. However, connection at the line provider's end may require use of a different plug type in order to match the line providers equipment.
- **RJ11 Phone Connectors**
  Many phones use RJ11 sockets and are supplied with RJ11-to-RJ11 cables. RJ11 plugs can be inserted into RJ45 sockets and in many case the connection will work. However this is not recommended or supported as the connection lock is not truly positive and may become disconnected. An RJ45-to-RJ11 cable[271] is available for these connections.

Standard IP Office Cables

The following are Avaya standard cables available for use with IP Office systems. The maximum length is applicable if the standard Avaya cable is replaced with an alternate cable.

Cable	Description	SAP Code	Standard Length	Maximum Length
9-Way DTE Cable 278	Connects to control unit RS232 DTE port. 9-Way D-type plug to 9-way D-type socket.	–	2m/6'6''.	2m/6'6''.
Structured Cabling DS Line Cable 271	Connects from RJ45 sockets to RJ11 socketed DS and analog phones.	TT700047871	4m/13'2''.	See table below.
BRI/PRI Trunk Cable 269	Connects BRI/PRI trunk ports to the line provider's network termination point. RJ45 to RJ45. Red.	700213440	3m/9'10''.	–
Expansion Interconnect Cable 273	Connects the control unit to expansion modules. RJ45 to RJ45. Blue. May be replaced by a yellow interconnect cable (2m (6'6") - 700472871) supplied with the IP500 4-Port Expansion 212 card when using that card.	700213457	1m/3'3''.	1m/3'3''.
LAN Cable 274	Connects from IP Office LAN ports to IP devices. RJ45 to RJ45. Grey.	700213481	3m/9'10''.	100m/328'.

The table below details the maximum total cable distances for DS and analog extensions using different cable thicknesses. Cabling should be Category-1 unshielded twisted pair cable or better.

Telephone	Unshielded Twisted-Pair (UTP) - 50nf/Km		
	AWG22 (0.65mm)	AWG24 (0.5mm)	AWG26 (0.4mm)
1400 Series	1200m/3937'	1000m/3280'.	670m/2200'
9500 Series	1200m/3937'	1000m/3280'	670m/2200'
BST	580m/1900'	365m/1200'	228m/750'
Analog Phones	1000m/3280'	1000m/ 3280'	400m/1312'
ETR Phones	305m/1000'	305m/1000'	122m/400'

13.12.2 ANALOG Port

These ports are analog trunk ports.IP500 analog trunk cards only support loop-start trunks. The ATM16 Analog Trunk[229] module supports both loop-start and ground-start trunks, switchable within the IP Office configuration.

ANALOG	Pin	Description
	1	Not used.
	2	Not used.
	3	Not used.
	4	Ring.
	5	Tip.
	6	Not used.
	7	Not used.
	8	Not used.

- **Off-Hook Current:** 25mA.
- **IMPORTANT**
  In all IP Office installations, any module being used for analog trunk connections must be connected to a functional earth[35].
- **WARNING**
  Within the Republic of South Africa and in areas of high lightning risk, any module using analog trunk connections must be connected to a protective ground[35] and to surge protection equipment[36].

13.12.3 AUDIO Port

This port is found on the rear of all IP Office control units. It is used for the input of an external music-on-hold sound source. Note that if the IP Office has loaded an internal music-on-hold sound file, any input from this socket is ignored.

The port is a 3.5mm stereo jack socket suitable for use with the most standard audio leads and connection to the 'headphone' output socket of most audio systems.

The use of a 'headphone' socket allows simple volume adjustment. Connection via a 'Line Out' socket may require additional equipment in order to adjust the volume level.

Pin No.	Description
Common	Common
Left	Audio In - Left Channel.
Right	Audio In - Right - Channel.

- Input impedance: 10k /channel. Maximum a.c. signal – 200mV rms.

13.12.4 BRI Port (So)

For IP Office 4.2+, IP500 BRI trunk daughter cards can be switched from To to So mode.

IP Office			Wire	ISDN Terminal	
RJ45	Pin	BRI		PIN	RJ45
	1	–	White/Orange	1	
	2	–	Orange/White	2	
	3	⬅ Rx-A	White/Green	3	
	4	➡ Tx-B	Blue/White	4	
	5	➡ Tx-A	White/Blue	5	
	6	⬅ Rx-B	Green/White	6	
	7	–	White/Brown	7	
	8	–	Brown/White	8	

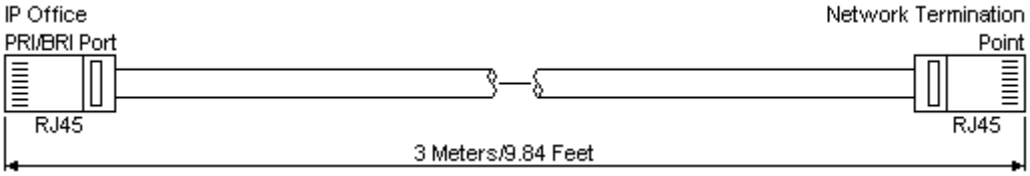
- **Terminating Resistors**
  100ohm Terminating resistors are required across the transmit and receive wire pairs at each end of the S-bus.
  - For IP Office 4.2+, individual ports of an IP500 BRI daughter card can be switched to So mode. This is done by setting the **Line Sub-Type** to ***S-Bus*** in the IP Office configuration. In this case terminating resistors must be added at the IP Office end in addition to those at the other end of the S-bus connection.
    - Addition of the necessary termination at the IP Office end can be done using an IP500 BRI So Converter Cable (700458649). This short (25cm/10") cable includes both the necessary terminating resistors and the cable cross-over.
  - Many ISDN terminal devices includes terminating resistors. If this is not the case, 100ohm (+/-5%) resistors must be connected across the receive wire pair and the transmit wire pair in the junction box immediately before the last ISDN terminal on the S-bus.

13.12.5 BRI Port (To)

These ports are BRI To interface ports for connection to external BRI trunk services.

PRI/BRI Trunk Cable

This cable is used to connect from IP Office BRI/PRI trunk ports to the line providers network termination equipment. If that equipment does not use RJ45 sockets, the cable may need to be stripped and rewired or an alternate cable used. The appropriate signal pin-outs and wire colours are detailed below.



IP Office				Wire	Network Termination	
BRI	RJ45	BRI	PRI		PIN	RJ45
RJ45 8 1	1	–	⬅Rx-A	White/Orange	1	RJ45 8 1
	2	–	⬅Rx-B	Orange/White	2	
	3	➡Tx-A	–	White/Green	3	
	4	⬅Rx-A	➡Tx-A	Blue/White	4	
	5	⬅Rx-B	➡Tx-B	White/Blue	5	
	6	➡Tx-B	–	Green/White	6	
	7	–	–	White/Brown	7	
	8	–	–	Brown/White	8	

- Supply: BRI/PRI trunks cards are not supplied with these cables.
- Cable Color: Red.
- SAP Code: 700213440.
- Standard Length: 3m/9'10".
- Maximum Length: 5m/16'5''.
- Though not used pins 7 and 8 are through connected for ease of construction.

13.12.6 BST Port (RJ21)

These ports are found on IP500 Digital Station 16A/30A[233] external expansion modules. They are supported by IP500 V2 systems running IP Office Release 7.0 and higher. See supported Avaya BST digital telephones[39].

1st RJ21 Connector

Port		Pin	Wire
1	Tip	26	White/Blue
	Ring	1	Blue/White
2	Tip	27	White/Orange
	Ring	2	Orange/White
3	Tip	28	White/Green
	Ring	3	Green/White
4	Tip	29	White/Brown
	Ring	4	Brown/White
5	Tip	30	White/Slate
	Ring	5	Slate/White
6	Tip	31	Red/Blue
	Ring	6	Blue/Red
7	Tip	32	Red/Orange
	Ring	7	Orange/Red
8	Tip	33	Red/Green
	Ring	8	Green/Red
9	Tip	34	Red/Brown
	Ring	9	Brown/Red
10	Tip	35	Red/Slate
	Ring	10	Slate/Red
11	Tip	36	Black/Blue
	Ring	11	Blue/Black
12	Tip	37	Black/Orange
	Ring	12	Orange/Black
13	Tip	38	Black/Green
	Ring	13	Green/Black
14	Tip	39	Black/Brown
	Ring	14	Brown/Black
15	Tip	40	Black/Slate
	Ring	15	Slate/Black
16	Tip	41	Yellow/Blue
	Ring	16	Blue/Yellow
Not Used		42	Yellow/Orange
		17	Orange/Yellow
		43	Violet/Slate
		08	Slate/Violet

2nd RJ21 Connector

Port		Pin	Wire
17	Tip	26	White/Blue
	Ring	1	Blue/White
18	Tip	27	White/Orange
	Ring	2	Orange/White
19	Tip	28	White/Green
	Ring	3	Green/White
20	Tip	29	White/Brown
	Ring	4	Brown/White
21	Tip	30	White/Slate
	Ring	5	Slate/White
22	Tip	31	Red/Blue
	Ring	6	Blue/Red
23	Tip	32	Red/Orange
	Ring	7	Orange/Red
24	Tip	33	Red/Green
	Ring	8	Green/Red
25	Tip	34	Red/Brown
	Ring	9	Brown/Red
26	Tip	35	Red/Slate
	Ring	10	Slate/Red
27	Tip	36	Black/Blue
	Ring	11	Blue/Black
28	Tip	37	Black/Orange
	Ring	12	Orange/Black
29	Tip	38	Black/Green
	Ring	13	Green/Black
30	Tip	39	Black/Brown
	Ring	14	Brown/Black
Not Used		40	Black/Slate
		15	Slate/Black
		41	Yellow/Blue
		16	Blue/Yellow
		42	Yellow/Orange
		17	Orange/Yellow
		43	Violet/Slate
		08	Slate/Violet

13.12.7 BST Port (RJ45)

These ports are found on the IP500 Digital Station 16B/30B expansion modules[236]. They are supported by IP500 V2 systems running IP Office Release 9.0 and higher. See supported Avaya BST digital phones[39].

13.12.8 DC I/P Port

Found on all IP Office control units and expansion modules. Used for connection from the external power supply unit[30] supplied with the control unit or module.

- No other type of power supply unit should be used with the module or module unless specifically indicated by Avaya.
- Power cords must not be attached to the building surface or run through walls, ceilings, floors and similar openings.

13.12.9 DS Ports (RJ45)

These ports are used for connection from an RJ45 structured cabling system to digital station phones supported by the IP Office. DS ports are provided by IP500 Digital Station Cards[218], IP500 ATM Combination Cards[214], IP500 BRI Combination Cards[216] and IP500 Digital Station[231] external expansion modules.

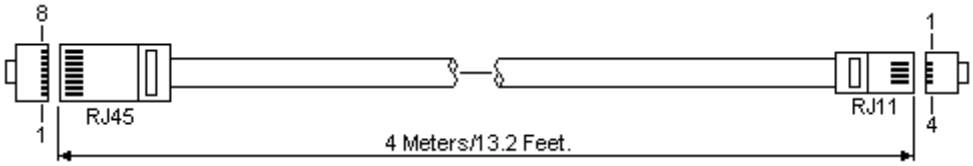
Though the RJ11 to RJ11 cables supplied with some phones can be plugged directly into RJ45 ports including those on IP Office modules, this is not recommend as the connection lock is not positive and may become disconnected.

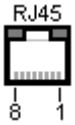
- DS ports on external expansion modules can be connected to out-of-building extensions[36]. If this is the case, connection must be made via suitable protective devices at each end and via each building primary protection. In addition, the Digital Station module must be connected to a protective ground.
- DS ports on base cards within the control unit must not be connected to out-of-building extensions.

Structured Cabling Line Cord

This is an RJ45 to RJ11 cable suitable for connection from a structured cabling system RJ45 port to a DS phone. It can also be used for two-wire analog phone extensions.

This cable is not suitable for connection from an Avaya 1151D1/B2 power supply unit to a DS phone with a EU24 or XM24 add-on module. In those cases the cables supplied with the power supply unit and the add-on module should be used.



IP Office			Phone	
DS Port	Pin	Description	Pin	Port
RJ45  8 1	1	Not used.	–	RJ11 6 1
	2	Not used.	1	
	3	Not used.	2	
	4	Signal 1.	3	
	5	Signal 2.	4	
	6	Not used.	5	
	7	Not used.	6	
	8	Not used.	–	

- SAP Code: T700047871.

Página2932 de 3226.

13.12.10 EF Port

These ports are found on the ETR6 base card. They are analog trunk ports that are only useable when the card is fitted with an IP500 analog trunk daughter card. When in power fail, the EF ports are connected to trunk port 12.

13.12.11 ETR Port

ETR (Enhanced Tip and Ring) ports are provided by the ETR6 base card. They can be used for the connection of DTMF analog phone devices and Avaya ETR phones.

- Paging to external paging equipment is not supported via ETR6 ports. It is supported via POT ports.

13.12.12 EXPANSION Port

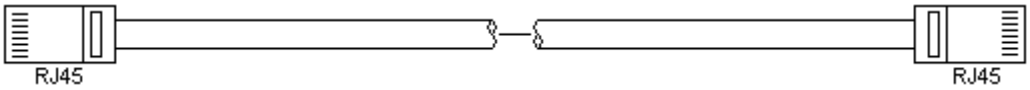
This type of port is found on the rear of IP Office control units and external expansion modules. It is used for connecting the external expansion modules to there parent IP Office control unit.

The connection between these ports should only be done using an Avaya Expansion Interconnect Cable. No other cable type should be used.

- Each external expansion module is supplied with a blue 1 meter (3'3'') expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on an IP500 4-Port Expansion card, a yellow 2 meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. 4 Yellow cables are supplied with the IP500 4-Port Expansion card.

Expansion Interconnect Cable

The Expansion Interconnect cable is used to link expansion ports between the IP Office control unit and external expansion modules.



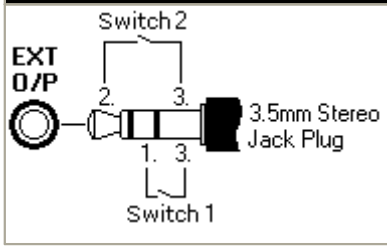
- Supply: One cable is normally supplied with each external expansion module.
- SAP Code: 1m (3'3") Blue cable - 700213457, 2m (6'6") Yellow cable - 700472871.

13.12.13 EXT O/P Port

These ports are found on the rear of all IP Office control units. They are used for connection to external switching relays. The port uses a standard 3.5mm stereo jack plug for connection.

The IP Office is able to open (high resistance), close (low resistance) or pulse (close for 5 seconds and then open) two switches within the port. Either switch can be operated separately. These switches are intended for activation of external relays in systems such as door opening systems.

- **CAUTION:**
  In installations where this port is connected to a device external to the building, connection must be via a MDS2 Surge Protector and a protective ground connection must be provided on the IP Office control unit. When using the MDS2 on the Ext O/P port, use only the Line 1 and Equipment 1 jacks, do not use the Line 2 or Equipment 2 jacks.

EXT O/P	Pin	Description
	1	Switch 1.
	2	Switch 2.
	3	0 Volts (Ground/Chassis)

- Switching Capacity: 0.7A.
- Maximum Voltage: 55V d.c.
- On state resistance: 0.7 ohms.
- Short circuit current: 1A.
- Reverse circuit current capacity: 1.4A.
- Ensure that pins 1 and 2 are always at a positive voltage with respect to pin 3.

3.5mm stereo audio jack plugs are frequently sold as pre-wired sealed modules. It may be necessary to use a multi-meter to determine the wiring connections from an available plug. Typically 3 (common to both relays) is the cable screen.

13.12.14 LAN Port

These ports are found on IP Office control units. They are used for connection to IP LANs and IP devices.

All IP Office LAN ports are 10/100Mbps auto-sensing. The ports are full-duplex 10/100Mbps auto-sensing, MDI crossover ports. They form a managed layer 3 Ethernet switch.

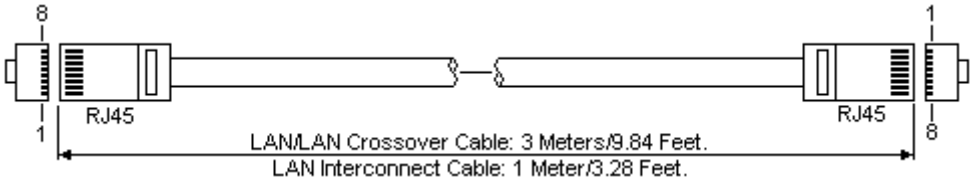
The WAN port is not supported on systems running in IP Office Essential Edition mode.

The LEDs are used as follows:

- Green: On = connected, Flashing = Activity.
- Yellow: On = 100Mbps, Off = 10Mbps.

LAN Cables

These are CAT5 UTP cables for connection of various IP devices within the IP Office system.



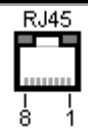
IP Office							
LAN	**Pin**	**MDIX (Normal)**	**MDI (Crossover)**	**Wire**	**Standard/ Interconnect**	**Crossover**	
RJ45 8 1	1	⬅Rx-A.	➡Tx-A.	White/Orange	1	3	RJ45 8 1
	2	⬅Rx-B.	➡Tx-B.	Orange/White	2	6	
	3	➡Tx-A.	⬅Rx-A.	White/Green	3	1	
	4	Not used.	Not used.	Blue/White	4	4	
	5	Not used.	Not used.	White/Blue	5	5	
	6	➡Tx-B.	⬅Rx-B.	Green/White	6	2	
	7	Not used.	Not used.	White/Brown	7	7	
	8	Not used.	Not used.	Brown/White	8	8	

- **SAP Code:**
  - **LAN Cable - GREY: 700213481.**
    Standard straight LAN cable.
  - **LAN Crossover Cable - Black: 700213473.**
    LAN crossover cable.

13.12.15 PF Port

These ports are found on the rear of the Analog Trunk 16 expansion module[229]. They are analog extension ports that can be used in conjunction with analog loop-start trunks during power failure to the IP Office system. See also Emergency and Power Failure Ports[47].

Any phones connected to these ports should be clearly labeled as power fail extensions in accordance with the appropriate national and local regulatory requirements.

PF	Pin	Description
	1	Not used.
	2	Pin 2 is internally connected to pin 5 via a ringer capacitor.
	3	Not used.
	4	Ring.
	5	Tip.
	6	Pin 6 is internally connected to pin 5 via a ringer capacitor.
	7	Not used.
	8	Not used.

- Minimum Wire Size: AWG 26.
- Maximum Cable Length:
  - AWG26: 500m / 1640'.
  - AWG24, AWG22: 1000m / 3280'.

13.12.16 PHONE (POT) Port

These ports are analog extension ports. On older IP Office units these ports were labeled as POT ports rather than PHONE ports.

PHONE ports on Phone V1/V2 expansion modules can be connected to out-of-building extensions[36]. If this is the case, connection must be made via suitable protective devices (IP Office Barrier Box) at each end and via each building primary protection. In addition the Phone module must be connected to a protective ground.

PHONE ports on IP Office control units must not be connected to out-of-building extensions.

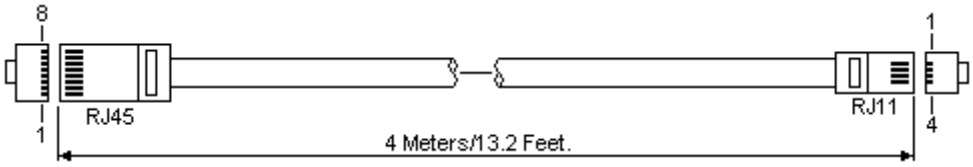
PHONE	Pin	Description
	1	Not used.
	2	Not used.
	3	Not used.
	4	Ring.
	5	Tip.
	6	Not used.
	7	Not used.
	8	Not used.

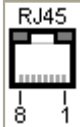
- REN: 2
- Off-Hook Current: 25mA.
- Ring Voltage:
  - IP500 V2 Control Unit, IP500 Phone Modules: 49V rms.
- Minimum Wire Size: AWG 26.
- Maximum Cable Length:
  - AWG26: 0.5km / 1640 feet.
  - AWG24, AWG22: 1km / 3280 feet.

These ports do not include a ringing capacitor. Therefore, for connection to 4-wire analog phones where this is a requirement (typically the United Kingdom and New Zealand), connection should be via a Master socket containing ringing capacitors.

Structured Cabling Line Cord

This is an RJ45 to RJ11 cable suitable for connection from a structured cabling system RJ45 port to a DS phone. It can also be used for two-wire analog phone extensions.



IP Office			Phone	
DS Port	Pin	Description	Pin	Port
	1	Not used.	–	
	2	Not used.	1	
	3	Not used.	2	
	4	Signal 1.	3	
	5	Signal 2.	4	
	6	Not used.	5	
	7	Not used.	6	
	8	Not used.	–	

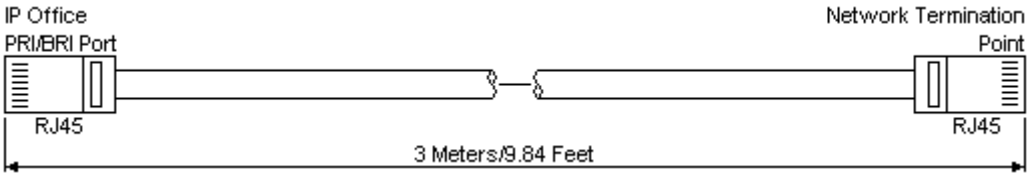
Página2937 de 3226.

13.12.17 PRI Port

These ports are used for connection to PRI trunk services including E1, T1 and E1-R2.

PRI Trunk Cable

This cable is used to connect from IP Office PRI trunk ports to the line providers network termination equipment. If that equipment does not use RJ45 sockets, the cable may need to be stripped and rewired or an alternate cable used. The appropriate signal pin-outs and wire colours are detailed below.



IP Office			Wire	Network Termination	
RJ45		PRI		PIN	RJ45
RJ45 8 1	1	⬅ Rx-A	White/Orange	1	RJ45 8 1
	2	⬅ Rx-B	Orange/White	2	
	3	–	White/Green	3	
	4	➡ Tx-A	Blue/White	4	
	5	➡ Tx-B	White/Blue	5	
	6	–	Green/White	6	
	7	–	White/Brown	7	
	8	–	Brown/White	8	

- Supply: PRI trunks cards are not supplied with these cables.
- Cable Color: Red.
- SAP Code: 700213440.
- Standard Length: 3m/9'10".

13.12.18 RS232 Port (DTE)

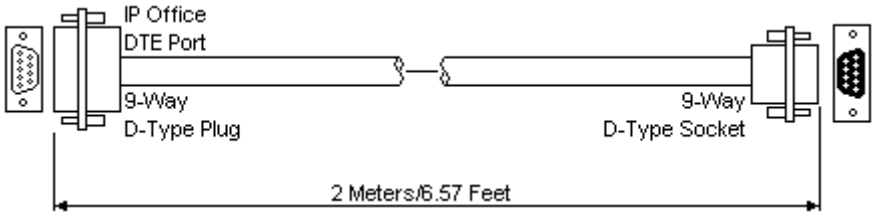
These ports are found on the rear of all IP Office control units and external expansion modules. The similar ports on external expansion modules are only used by Avaya.

The RS232 DTE ports can be used for a number of system maintenance processes[198]. An asynchronous terminal program such as HyperTerminal is also required. Configure this for operation via a PC serial port, as follows:

- **Bits per second:** 38400
- **Data bits:** 8
- **Parity:** None
- **Stop bits:** 1
- **Flow control:** None
- **Settings | Emulation:** TTY

DTE Cables

These cables are used for system maintenance and diagnostics under Avaya guidance. They can also be used for connection of RS232 serial terminal adaptor equipment to the IP Office control unit. The cable required depends on the IP Office control unit. This cable is a "Straight through DB9 female to DB9 male serial cable".



IP Office 9-Way RS232 DTE Port	Signal	PC/Terminal Adaptor
3	⬅ Receive data	3
2	➡ Transmit Data	2
7	⬅ RTS (Request To Send)	7
8	➡ CTS (Clear To Send)	8
6	➡ DSR (Data Set Ready)	6
5	● Ground	5
1	➡ DCD (Data Carrier Detect)	1
4	⬅ DTR (Data Terminal Ready)	4
9	➡ RI (Ring Indicator)	9

13.13 Licences

This section covers licenses used IP500 V2 IP Office systems running IP Office Release 10.0. It does not include details of licenses used for other types of IP Office systems such as Server Edition.

The IP Office system requires licensing for some features, see Licenses[279]. The license file can be either uploaded manually or pre-loaded onto the System SD card[78].

How is the system licensed?

- An XML file containing the full set of PLDS licenses is uploaded to the system. The license file is unique to the feature key serial number of the System SD card installed in the system.
    - The PLDS host ID used for the license file must match that shown by the 12 digit **PLDS ID** printed on the SD card label. Older cards have an 10 digit feature key serial number shown by **FK** or **FK SN**. For those cards add the prefix ***11*** to obtain the card's PLDS ID.

Minimum License Requirements

For IP Office Essential Edition, the system requires an **Essential Edition** system license for the specific IP Office release you want it to run.

Upgrade Licensing

From IP Office Release 10.0 onwards, the PLDS XML license file is release-specific. For a system to be upgraded to a new major release of IP Office software, a new license file specific to the target release is required. This applies even if the file contains the same set of licenses .

13.13.1 System Edition Licenses

These license are used to set what range of features the IP Office system supports.

- **Essential Edition :**
  The system requires this license to run in IP Office Essential Edition mode. Until entered, the system operates as a IP Office Basic Edition system.
    - This license is also a pre-requisite to the **Preferred Edition** license.
    - This license enables embedded voicemail with up to 2 simultaneous connections and 15 hours of storage.
- **Essential Edition Additional Voicemail Ports :**
  This license enables two additional embedded voicemail connections and an additional 5 hours of storage. Multiple licenses can be added for a maximum of up to 6 connections and 25 hours storage.
- **Preferred Edition (Voicemail Pro) :**
  This license enables support for Voicemail Pro as the IP Office's voicemail server with 4 voicemail ports. The **Preferred Edition** license allows the voicemail server to provide the services listed below. For IP Office Release 8.0 and higher, an **Essential Edition** license is a pre-requisite for this license on IP500 V2 systems.
    - Mailboxes for all users and hunt groups.
    - Announcements for users and hunt groups.
    - Customizable call flows.
    - Call recording to mailboxes.
    - Campaigns.
    - TTS email reading for users licensed to **Mobile Worker** or **Power User** profiles. Also requires TTS licenses.
    - Use of **Conference Meet Me** functions.
    - Visual basic scripting *(Windows based Voicemail Pro only)*

    1. A **Preferred Edition**[279] system license is a pre-requisite for any user profile license other than **Basic User**.
        - In a Small Community Network, the **Preferred Edition** license of the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server, for example for distributed voicemail, still requires its own **Preferred Edition** license.
- **Branch System**
  This license enables support for enterprise branch features. These relate to an IP Office system being used as a branch site switch in an Avaya Aura network. Additional **SM Trunk** licenses are required for the SM lines configured between the branch and the Avaya Aura.

13.13.2 Upgrade Licenses

Existing IP Office systems being upgraded to IP Office Release 11.0 require a software upgrade license.

- **! Warning: Upgrade License Requirements**
  On a new system, when the first call is made, the software level being run is written into the control unit's permanent memory. Any subsequent upgrade to a higher release requires the addition of the **Essential Edition** license for the target release. Systems upgraded without that license display *"No license available"* on some phones and will not allow any telephony functions.

- **! Note: Server Edition Systems**
  IP500 V2 control units configured as IP500 V2 Expansion System systems are licensed and upgraded through the Server Edition web management menus. Refer to the Server Edition documentation.

13.13.3 Trunk Licensing

The following trunks licenses can be used by a IP Office Essential Edition system.

- **IP500 Universal PRI (Additional channels)**
  These licenses are used to enable additional B-channels above the basic 8 on an IP500 PRI-U card. The IP500 PRI-U card supports E1, T1 and E1-R2 PRI modes. The IP Office system supports 8 unlicensed B-channels on each IP500 PRI-U port fitted. Additional B-channels, up to the capacity of ports installed and PRI mode selected require licenses. These additional channels consume licenses based on which additional channels are configured as in-service from port 9 of slot 1 upwards. D-channels are not affected by licensing. The license is available in 2, 8 and 22 channel variants which can be combined for the total number of channels required.

- **SIP Trunk Channels**
  These licenses are used to configure the maximum number of simultaneous SIP trunk calls supported. The licenses are consumed by calls in progress on a SIP channel. For SIP support the system also requires VCM resources 221 . The license is available in 1, 5, 10 and 20 channel variants which can be combined for the total number of channels required.

- **IP500 Voice Networking**
  These licenses enable support for SCN, QSIG and H323 IP trunks. For voice networking support, the system also requires VCM resources 221 .

- **SM Trunk Channels**
  These licenses are used to enabled SM lines for connection to an Avaya Aura network. The IP Office system also requires a **Branch System** license.

13.13.4 Telephone/Endpoint Licenses

The use of H323 and SIP phones with IP Office is controlled by the following licenses. Different licenses are used for Avaya IP phones and non-Avaya phones including non-Avaya soft phones.

For IP soft phones, the license requirements vary depending on the particular application and are not covered here. Refer to the specific documentation for the application. However, most Avaya soft phone applications do not require an Avaya IP Endpoint license.

By default, the endpoint licenses are consumed by each IP phone that registers with the system in the order that the phones register. However, it is possible to reserve a license for a particular extension in order to ensure that that phone always obtains a license first if available. This is done through the **Reserve Licence** setting of the extension's settings in the system configuration. Licenses are released if the phone unregisters unless reserved.

- **Warning**
  Avaya IP phones without a license are still able to register but are limited to making emergency calls only (***Dial Emergency*** short code calls). The associated user is treated as if logged off and the phone may display *"No license available"* and *"Emergency Calls Only"*. If a license becomes available, it is assigned to any unlicensed DECT handsets first and then to any other unlicensed Avaya IP phone in the order that the phones registered.

- **Avaya IP Endpoints License**
  These licenses are used to license additional physical Avaya IP phones. This includes all 1600, 9600, DECT R4, Spectralink and VPN phones supported.
- **3rd Party IP Endpoints License**
  These licenses are used for support of non-Avaya IP phones including SIP extensions. The available license are used in order of phone registration. If no licenses are available the phone is not able to register. This license was previously called the **IP End-points** license.
- **Avaya Softphone License**
  This license is used to allow support for Avaya Communicator 256 or Avaya IX Workplace Client 254 by a user whose licensed profile does not normally support those applications as part of the profile license.

13.13.5 User Licenses

The features available to a basic user can be enhanced by the addition of user licenses. Once these licenses are present in the system configuration, the corresponding profiles can be applied to selected users through their **User | User | Profile** setting in the system configuration.

Note that for all profiles other than **Basic User**, a **Preferred Edition** system license is a pre-requisite for the required user licenses.

	Basic User	Office Worker	Teleworker	Mobile Worker	Power User
one-X Portal Services	–	✓	✓	–	✓
" Telecommuter options	–	–	✓	–	✓
UMS Web Services	–	✓	✓	–	✓
Mobility Features	–	–	–	✓	✓
TTS for Email Reading [4]	–	–	–	✓	✓
Remote Worker [2]	–	–	✓	–	✓
Avaya Communicator [3]	✓[7]	✓	✓	–	✓
Avaya IX Workplace Client	✓[5]	✓	✓	✓[5]	✓
Web Collaboration [6]	–	✓	✓	–	✓
" Conference Scheduling	–	–	–	–	✓

1. A **Preferred Edition**[279] system license is a pre-requisite for any user profile license other than **Basic User**.
   - In a Small Community Network, the **Preferred Edition** license of the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server, for example for distributed voicemail, still requires its own **Preferred Edition** license.
2. Release 8.0 supports users using remote H323 extensions. Up to 4 Basic users are supported on remote extensions on system. Additional remote users are supported if licensed and configured for either a ***Teleworker*** or ***Power User*** user profile.
3. Require that the one-X Portal for IP Office and Voicemail Pro applications are also installed for advanced features.
4. TTS for Email Reading also requires the voicemail system to be licensed for the number of simultaneous TTS session required.
5. Supported for Avaya IX Workplace Client[254] standalone mode using a Avaya Softphone License.
6. Also requires a **Web Collaboration** license.
7. Supported for Avaya Communicator[256] basic mode using a Avaya Softphone License.

User Licenses

- **Teleworker License**
  These licenses set the number of users who can have their profile set as ***Teleworker***. For user with this optional, additional settings are enabled in the configuration for the following services: one-X Portal for IP Office with Telecommuter option, Avaya Communicator and UMS Web Services. A **Preferred Edition** system license[279] is a pre-requisite for this license.
- **Mobile Worker License**
  These licenses set the number of users who can have their profile set as ***Mobile Worker***. For user with this optional, additional settings are enabled in the configuration for the following services: Mobility Features and TTS for Email Reading. For IP Office Release 8.0 and higher, all mobility features are enabled for all users by the **Essential Edition** license. A **Preferred Edition** system license[279] is a pre-requisite for this license.
- **Office Worker License**
  These licenses set the number of users who can have their profile set as ***Office Worker***. For user with this optional, additional settings are enabled in the configuration for the following services: one-X Portal for IP Office (no telecommuter features) and UMS Web Services. A **Preferred Edition** system license[279] is a pre-requisite for this license.
- **Power User Profile License**
  These licenses set the number of users who can have their profile set as ***Power User***. For user with this optional, the same additional services as for Teleworker and Mobile Worker are enabled for the user. A **Preferred Edition** system license[279] is a pre-requisite for this license.

Other User Licenses

In addition to the user profile licenses above, the following individual user licenses are available:

Página2943 de 3226.

- **Receptionist:**
  This license is used to enable support for the IP Office SoftConsole application. This license can only be used by users set to **Receptionist** in the IP Office configuration. A maximum of 4 receptionist are supported. This license was previously called **SoftConsole**. An instance of this license is consumed by each user configured as a **Receptionist**.
- **Web Collaboration**
  This license can be used to enable support for the Web Collaboration application 260. One license instance is required for each user configured for web collaboration. Supported with users licensed as **Office Worker**, **Teleworker** or **Power User**.

13.13.6 Voicemail Pro Licenses

Voicemail Pro is enable by the addition of the following licenses.

- **Preferred Edition (Voicemail Pro) :**
  This license enables support for Voicemail Pro as the IP Office's voicemail server with 4 voicemail ports. The **Preferred Edition** license allows the voicemail server to provide the services listed below. For IP Office Release 8.0 and higher, an **Essential Edition** license is a pre-requisite for this license on IP500 V2 systems.
  - Mailboxes for all users and hunt groups.
  - Announcements for users and hunt groups.
  - Customizable call flows.
  - Call recording to mailboxes.
  - Campaigns.
  - TTS email reading for users licensed to **Mobile Worker** or **Power User** profiles. Also requires TTS licenses.
  - Use of **Conference Meet Me** functions.
  - Visual basic scripting *(Windows based Voicemail Pro only)*

  1. A **Preferred Edition**[279] system license is a pre-requisite for any user profile license other than **Basic User**.
     - In a Small Community Network, the **Preferred Edition** license of the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server, for example for distributed voicemail, still requires its own **Preferred Edition** license.
- **Preferred Edition Additional Voicemail Ports**
  The required license for Voicemail Pro server support (Preferred Edition (Voicemail Pro)) also enables 4 voicemail ports. These licenses can be used to add additional voicemail ports up to the maximum capacity of the IP Office system (IP500 V2 = 40). This license was previously called **Additional Voicemail Pro (ports)**. These licenses are available in 2, 4, 8 and 16 port variants which can be combined for the total number of ports required.
- **Media Manager**
  Allows the use of Media Manager on an IP Office Application Server to provide long term archiving of call recordings. In a Small Community Network, each IP Offices requires its own license.
- **VMPro Networked Messaging**
  Enables VPNM (Voicemail Pro Networked Messaging) functionality within Voicemail Pro. This allows message exchange with remote Voicemail Pro systems and Avaya Interchange systems.
- **VMPro TTS (Generic)**
  This legacy license enables the use of text to speech facilities using third party TTS software with Voicemail Pro on a Windows server. One license per simultaneous instance of TTS usage. Note that the IP Office Advance Edition license also enables 8 ports of generic TTS but useable with Speak Text actions only.
- **VMPro TTS (ScanSoft)**
  This legacy license enables the use of text to speech facilities using Avaya supplied TTS software with Voicemail Pro on a Windows server. One license per simultaneous instance of TTS usage.
- **VMPro TTS Professional**
  This license enables the use of text to speech facilities provided by Voicemail Pro on a Linux based server. One license per simultaneous instance of TTS usage.
- **UMS Web Services**
  These licenses are used to enable UMS voicemail services support for users set to the ***Basic User*** profile. Other users are enabled for UMS through their licensed user profile. These licenses are also used to license hunt groups for UMS voicemail services. Each license enables 1 user.

13.13.7 Trial Licenses

Trial licenses can be requested. Each is valid for 60 days from the date of issue and can only be issued once for a particular System SD card serial number. Apart from that restriction, the trial licenses work the same as full licenses.

13.13.8 CTI Licenses

- **CTI Link Pro :**
  Enables CTI Link Pro functionality (TAPI Link Pro and DEVLink Pro).
- **Wave User :**
  Allows streaming of WAV files, using TAPILink Pro, for 3rd party voice applications. This is a per user license. Note that TAPI WAV calls use system data channels taken from the same pools as used for voicemail ports. The maximum number of simultaneous TAPI WAV user calls and voicemail users is determined by the IP Office control unit type; IP500 V2 =40.

13.13.9 Other Licenses

- **Audix Voicemail :**
  Enables IP Office to use a remote Intuity Audix or Modular Messaging system for voicemail rather than requiring a local voicemail server.
- **IPSec Tunneling :**
  Enables the IP Office to initiate and terminate IPSec and L2TP tunnels.
- **Avaya Contact Center Select**
  This license is required for the support of Avaya Contact Center Select.

13.14 Hardware/Software Compatibility

This page summarizes the hardware and software components supported on different releases of IP Office core software. Additional information for other Avaya products including compatible software versions, can be obtained from the **Avaya Product Compatibility Matrix** website (https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml).

- **Controls Units** 287
  - **External Expansion Modules** 287
  - **Base and Trunk Cards** 288
- **Server Platforms** 289
- **Phones** 290
- **Applications** 295

Página2947 de 3226.

13.14.1 Control Units and Control Unit Components

Control Units

Control Unit	Material Code	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
Small Office Edition	–	–	–	–	–	–	–	–	–	–	–	–
IP403	700350382	–	–	–	–	–	–	–	–	–	–	–
IP406 V1	700210776	–	–	–	–	–	–	–	–	–	–	–
IP406 V2	700359946	✓[1]	✓[1]		–	–	–	–	–	–	–	–
IP412	700350408	✓	✓	✓	–	–	–	–	–	–	–	–
IP500	700417207	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP500 V2	700476005	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. For an IP406 V2 control unit to run IP Office Release 4.0 or higher software up to IP Office Release 6.1, the control unit must be PCS 8 or higher.

External Expansion Modules

Module	Material Code	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
IP400 ATM16[3]	700211360	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 DS16	700184807	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP400 DS30	700184880	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP400 DS16 V2[3]	700359839	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 DS30 V2[3]	700359847	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 Phone 8	700184773	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP400 Phone 16	700184781	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP400 Phone 30	700184799	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP400 Phone 8	700359896	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP400 Phone 16 V2[3]	700359904	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 Phone 30 V2[3]	700359912	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP400 So8	700185077	–	–	–	–	–	–	–	–	–	–	–
IP400 WAN3[1]	–	–	–	–	–	–	–	–	–	–	–	–
IP400 WAN3 10/100[1]	700262009	✓	✓	✓	–	–	–	–	–	–	–	–
IP500 ATM16[2]	700449473	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 So8	700449515	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP500 DS16	700449499	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS30	700426216	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS16A (RJ21)	700500699	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS30A (RJ21)	700500698	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
IP500 DS16B	700501585	–	–	–	–	–	✓[5]	✓	✓	✓	✓	✓
IP500 DS30B	700501586	–	–	–	–	–	✓[5]	✓	✓	✓	✓	✓
IP500 DS16B2	700511093	–	–	–	–	–	–	–	✓[4]	✓[4]	✓	✓
IP500 DS30B2	700511094	–	–	–	–	–	–	–	✓[4]	✓[4]	✓	✓
IP500 Phone 16 V2	700449507	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Phone 30 V2	700426224	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. Not supported on IP500 and IP500 V2 systems.
2. North America only, unless accepted in targeted country.
3. These IP400 variants are still supported on IP Office Release 9.1 and higher.
4. Originally only supported in R10.1. Further support added in R9.1 SP12 and R10.0 SP5.
5. Service Pack 9 and higher.

Base and Cards

Base Cards	Material Code	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
IP500 Phone 2	700431778	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Phone 8	700417231	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Digital Station 8	700417330	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Card Carrier[6]	700417215	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
IP500 VCM 32[6]	700417389	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 VCM 64[6]	700417397	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 VCM 32 V2[6]	700504031	–	–	–	–	–	✓	✓	✓	✓	✓	✓
IP500 VCM 64 V2[6]	700504032	–	–	–	–	–	✓	✓	✓	✓	✓	✓
IP500 4-Port Expansion[6]	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 ETR6[1][2]	700476039	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 ATM4 Combo Card[1]	700476013	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
" PCS04 296 and higher[5]	700476013	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 ATM4 Combo Card V2[1]	700504556	–	–	–	–	–	✓	✓	✓	✓	✓	✓
IP500 BRI Combo Card BRI[1]	700476021	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 TCM 8[1]	700500758	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
Unified Communications Module v1[1][6]	700501442	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Unified Communications Module v2[1][6]	700507449	–	–	–	–	–	–	–	✓	✓	✓	✓

Trunk Cards	Material Code	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
IP500 Alog Trunk Card	700417405	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
" PCS10 296 and higher[4]	700417405	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 Alog Trunk Card V2[1][3]	700503164	–	–	–	–	–	✓	✓	✓	✓	✓	✓
IP500 BRI 4 Trunk Card	700417413	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 BRI 8 Trunk Card	700417421	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 PRI-1U	700417439	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 PRI-2U	700417462	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP500 T1(J) PRI Dual	700509377	–	–	–	–	–	–	–	✓	✓	✓	✓

1. IP500 V2 systems only.
2. Only supported in IP Office Basic Edition - PARTNER® Mode or IP Office Basic Edition (U-Law) modes running in a North American locale.
3. Supported for 8.1 Feature Pack 1 and higher.
4. These cards are support by IP Office Release 4.0 and higher. However, PCS10 and higher cards are only supported in systems running IP Office Release 6.1(20), 7.0(12) or 8.0 and higher. Refer to IP Office Technical Tip 237.
5. These cards are supported by IP Office Release 6.0 and higher. However, PCS04 and higher cards are only supported in systems running IP Office Release 6.1(20), 7.0(12) or 8.0 and higher. Refer to IP Office Technical Tip 237.
6. Not supported for IP Office Basic Edition mode systems.

13.14.2 Server Platforms

For R11.0.4.2 and higher, the currently shipped Avaya platforms are the R230 and R640 models.

Server Platform	Material Code	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
DL120G7 SRVR IPO R8+	269810	–	–	–	–	–	✓	✓	✓	✓	✓	✓
DL120G7 SRVR IPO R8+ FRANCE TELECOM	270391	–	–	–	–	–	✓	✓	✓	✓	✓	✓
DL120G7 SRVR IPO R8.1+ SE EXP	270395	–	–	–	–	–	✓	✓	✓	✓	✓	✓
R210 II XL SERVER IP OFFICE UNIFIED COMMUNICATIONS	302786	–	–	–	–	–	✓	✓	✓	✓	✓	✓
R210 II XL SERVER IP OFFICE FRANCE TELECOM	302787	–	–	–	–	–	✓	✓	✓	✓	✓	✓
R210 II XL SERVER IP OFFICE SERVER EDITION EXPANSION	302788	–	–	–	–	–	–	✓	✓	✓	✓	✓
R210 II XL SERVER IP OFFICE CONTACT CENTER SERVER	306626	–	–	–	–	–	–	–	✓	✓	✓	✓
R220 II XL SERVER IP OFFICE UNIFIED COMMUNICATIONS	380223	–	–	–	–	–	–	–	✓	✓	✓	✓
R220 II XL SERVER IP OFFICE FRANCE TELECOM	380224	–	–	–	–	–	–	–	✓	✓	✓	✓
R220 II XL SERVER IP OFFICE SERVER EDITION EXPANSION	380225	–	–	–	–	–	–	–	✓	✓	✓	✓
R220 II XL SERVER IP OFFICE CONTACT CENTER	380226	–	–	–	–	–	–	–	✓	✓	✓	✓
R230 XL SRVR IPO UC	390081	–	–	–	–	–	–	–	–	–	–	✓
R230 XL SRVR IPO FRANCE TELECOM	390082	–	–	–	–	–	–	–	–	–	–	✓
R230 XL SRVR IPOCC	390083	–	–	–	–	–	–	–	–	–	–	✓
DL360G7 SRVR IPO R8.1+ PRIMARY	270393	–	–	–	–	–	✓	✓	✓	✓	✓	✓
R620 SRVR IPO SE PRIMARY	306961	–	–	–	–	–	–	✓	✓	✓	✓	✓
R630 SRVR IPO SE/UC	383542	–	–	–	–	–	–	✓	✓	✓	✓	✓
R630 SRVR IPOCC	383555	–	–	–	–	–	–	✓	✓	✓	✓	✓
R640 SRVVR P3 IPO	700514262	–	–	–	–	–	–	–	–	–	✓	✓

13.14.3 Phones

- 1000 Series 290
- 1100 Series 290
- 1200 Series 290
- 1400 Series 290
- 1600 Series 290
- 2400 Series 290
- 3600 Series 290
- 3700 Series 290
- 3800 Series 291
- 3900 Series 291
- 4100 Series 291
- 4400 Series 291
- 4600 Series 291
- 5400 Series 291
- 5600 Series 291
- 6400 Series 292
- 7400 Series 292
- 9500 Series 292
- 9600 Series 292
- B100 Series 292
- D100 Series 293
- E100 Series 293
- H100 Series 293
- H200 Series 293
- J100 Series 293
- K100 Series 293
- M-Series 293
- T-Series 293
- T3 Series 294
- T3 IP Series 294

1000 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
1010	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1040	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

1100/1200 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
1120E	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1140E	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1220	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
1230	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓

1400 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
1403	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1408	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1416	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1600 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
1603[1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603-I	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603SW	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1603SW-I	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1608[1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1608-I	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1616[1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1616-I	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. 4.2 Q4 '08+.

2400 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
2402D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2410D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2420	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

3600 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
3616	✓	✓	✓	✓	✓	✓	–	–	–	–	–
3620	✓	✓	✓	✓	✓	✓	–	–	–	–	–
3626	✓	✓	✓	✓	✓	✓	–	–	–	–	–
3641	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3645	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

3700 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
3701	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Página2951 de 3226.

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
3711	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
3720	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3725	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3730[1]	–	–	–	–	–	–	–	✓	✓	✓	✓
3735[1]	–	–	–	–	–	–	–	✓	✓	✓	✓
3740	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
3745	–	–	–	–	–	–	–	–	✓	✓	✓
3749	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

1. Supported from 9.1 SP11, 10.0 SP4.

3800/3900 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
3810	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
3910	–	✓	✓	✓	✓	✓	✓	✓	✓	–	–
3920	–	✓	✓	✓	✓	✓	✓	✓	✓	–	–

4100 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
4135	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4136	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4145	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4145EX	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4146	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
4146EX	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

4400 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
4406D	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4412D	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4424D	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

4600 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
4601	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4602IP	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4602SW	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4606	–	–	–	–	–	–	–	–	–	–	–
4610SW	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4612	–	–	–	–	–	–	–	–	–	–	–
4620	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4621	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
4624	–	–	–	–	–	–	–	–	–	–	–
4625	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

5400 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
5402	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5410	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5420	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

5600 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
5601	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5602IP	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5602SW	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Página2952 de 3226.

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
5610SW	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5620	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
5621	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

6400 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
6408D	✓	✓	✓	–	–	–	–	–	–	–	–
6416D	✓	✓	✓	–	–	–	–	–	–	–	–
6424D	✓	✓	✓	–	–	–	–	–	–	–	–

7400 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
7420	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7430	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7434	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7439	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7440	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7444	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
7449	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

9500 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
9504	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
9508	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

9600 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
9608	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9608G	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9611	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9620		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9620L	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9620C	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9621G	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9621GS	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9630		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9630G	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9640	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9640G	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9641G	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9641GS	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
9650	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9650C	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. Release 8.0 2012 Q1 service pack and higher.

B100 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
B149 *(analog)*	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
B159 *(analog)*	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
B169 *(DECT via analog or SIP base station)*	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
B179 *(SIP)*	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
B199 *(SIP)*	–	–	–	–	–	–	–	–	–	–	✓

Página2953 de 3226.

D100 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
D160	–	–	–	–	–	✓[1]	✓	✓	✓	✓	✓

1. Supported for 8.1 Feature Pack 1 and higher.

E100 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
E129	–	–	–	–	–	–	✓	✓	✓	✓	✓
E159	–	–	–	–	–	–	✓	✓	✓	✓	✓
E169	–	–	–	–	–	–	✓	✓	✓	✓	✓

H100 Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
H175	–	–	–	–	–	–	–	–	✓	✓	✓

H200 Series[1]

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
H229	–	–	–	–	–	–	–	–	–	–	✓
H239	–	–	–	–	–	–	–	–	–	–	✓
H249	–	–	–	–	–	–	–	–	–	–	✓

1. Supported from R11.0 SP1.

J100 Series

NB: Support does not include 3PCC Open SIP variants of these phones.

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
J129[1]	–	–	–	–	–	–	–	–	✓	✓	✓
J139[3]	–	–	–	–	–	–	–	–	–	–	✓
J159[4]	–	–	–	–	–	–	–	–	–	–	✓
J169[2]	–	–	–	–	–	–	–	–	–	–	✓
J179[2]	–	–	–	–	–	–	–	–	–	–	✓

1. Supported from R10.0 SP2.
2. Supported on earlier releases using H323 firmware. Refer to the *"IP Office SIP Extension Installation Notes"*.
3. Supported from R11.0 SP1.
4. Supported from R11.0.4.2.

K100 Series (Vantage Phones)

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
K155	–	–	–	–	–	–	–	–	–	–	✓[1]
K165	–	–	–	–	–	–	–	–	–	–	✓
K175	–	–	–	–	–	–	–	–	–	–	✓

1. Supported from R11.0 SP1.

M-Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
M7100	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7100N	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7208	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7208N	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7310	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7310N	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7324	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
M7324N	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

T-Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
T7000	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7100	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7208	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

Página2954 de 3226.

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
T7316	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7316E	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7406	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
T7406E	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓
ACU	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓

T3/T3IP Series

Phone	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
T3 Compact	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
T3 Classic	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
T3 Comfort	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
T3 IP Compact	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
T3 IP Classic	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
T3 IP Comfort	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–

13.14.4 Applications

NB: Particular applications many require additional servers and licenses for operation with the IP Office system. This table simply indicates which applications are supported for IP500 V2 users.

Application	5.0	6.0	6.1	7.0	8.0	8.1	9.0	9.1	10.0	10.1	11.0
Call Detail Records (CDR)	–	–	–	–	–	–	–	–	–	–	–
Conferencing Center	✓	–	–	–	–	–	–	–	–	–	–
Compact Business Center	–	–	–	–	–	–	–	–	–	–	–
Contact Recorder	–	–	–	–	–	✓	✓	✓	✓	✓	–
ContactStore	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Customer Call Reporter	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Compact Contact Center	✓	–	–	–	–	–	–	–	–	–	–
Data Migration Manager	–	–	–	✓	✓	✓	✓	–	–	–	–
Delta Server	✓	–	–	–	–	–	–	–	–	–	–
Avaya Communicator for Windows	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Avaya Communicator for iPad	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Avaya Communicator for Web	–	–	–	–	–	–	–	✓	✓	✓	✓
Avaya IX Workplace Client	–	–	–	–	–	–	–	–	–	–	✓
IP Office Contact Center	–	–	–	–	–	–	✓	✓	✓	✓	✓
Integrated Contact Reporter	–	–	–	–	–	–	–	–	–	✓	–
Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Media Manager	–	–	–	–	–	–	–	–	–	✓	✓
MS-CRM	✓	–	–	–	–	–	–	–	–	–	–
Phone Manager	✓	✓	✓	✓	✓	✓	–	–	–	–	–
" Pro	✓	✓	✓	✓	✓	✓	–	–	–	–	–
" Pro Softphone	✓	✓	✓	✓	✓	✓	–	–	–	–	–
one-X Mobile	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
one-X Mobile Preferred	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
one-X Portal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
" Call Assistant	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
" Lync plug-in	–	–	–	–	–	✓	✓	✓	✓	✓	✓
" Outlook plug-in	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
" Salesforce plug-in	–	–	–	–	✓	✓	✓	✓	–	–	–
IP Office Web Client	–	–	–	–	–	–	–	–	–	–	✓
Outbound Call Express	–	–	–	–	–	✓	✓	✓	–	–	–
SoftConsole	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
System Status Application	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
System Monitor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TAPI Link Lite	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TAPI Link Pro	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integrated Messaging	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Video Softphone (Mac)	–	–	–	–	✓	✓	✓	✓	✓	✓	–
" (Windows)	–	✓	✓	✓	✓	✓	✓	✓	–	–	–
Voicemail Lite	–	–	–	–	–	–	–	–	–	–	–
Voicemail Pro	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web Collaboration	–	–	–	–	–	–	–	✓	✓	✓	✓

13.15 PCS Levels

Each item of IP Office hardware has a Product Change Status (PCS) level. This is usually included on the label on the hardware prefix with **PCS**.

The PCS level is increased each time a significant change is made to the components of that piece of hardware. For example the PCS level may increased when a component is replaced by one from a different supplier.

Normally changes to a PCS level are not important and items of the same hardware but with different PCS levels are still identical in operation and can be interchanged. However, there are some exceptions as listed below.

PCS Level Restrictions

- **IP500 Analog Trunk Card V1**
  These cards are support by IP Office Release 4.0 and higher. However, PCS10 and higher cards are only supported in systems running IP Office Release 6.1(20), 7.0(12) or 8.0 and higher. Refer to IP Office Technical Tip 237.
- **IP500 ATM4 Combination Card V1**
  These cards are supported by IP Office Release 6.0 and higher. However, PCS04 and higher cards are only supported in systems running IP Office Release 6.1(20), 7.0(12) or 8.0 and higher. Refer to IP Office Technical Tip 237.
- **IP500 V2 Control Unit**
  To support IP Office Release 9.1 or higher, PCS 14 or lower units must first install Release 8.1(65) (or higher 8.1) or any Release 9.0 and then upgrade to Release 9.1 or higher. Care should be taken to ensure that no calls are made before the final upgrade, otherwise the system will require upgrade license.

13.16 TAA

Those items labeled as TAA are compliant with the requirements of the Trade Agreements Act which is a pre-requisite for federal purchases in the United States of America. Unless otherwise stated, the TAA variants of equipment are physically and functionally the same as the non-TAA variants.

		SAP Code
Control Unit	**IPO IP500 V2 CNTRL UNIT TAA** [205]	700501510
Base Cards	**IPO IP500 EXTN CARD DGTL STA 8 TAA** [218]	700501512
	IPO IP500 V2 COMB CARD ATM TAA [214]	700501513
	IPO IP500 VCM 32 TAA [221]	700501518
	IPO IP500 VCM 32 TAA V2 [221]	700504033
Trunk Daughter Cards	**IPO IP500 TRNK BRI 4 UNI TAA** [226]	700501515
	IPO IP500 TRNK PRI UNVRSL SNGL TAA [227]	700501514
	IPO IP500 TRNK PRI UNVRSL DUAL TAA [227]	700501517
External Expansion Modules	**IPO IP500 EXP MOD ANLG TRNK 16 TAA** [229]	700501511
	IPO IP500 EXP MOD DGTL STA 16 TAA [231]	700501516
Telephones	**9608 IP Deskphone TAA Global**	700501428, 700507947
	9608G IP Deskphone TAA Global	700507946
	9611G IP Deskphone TAA Global	700501429, 700507948
	9621G IP Deskphone TAA Global	700500254, 700506516
	9641G IP Deskphone TAA Global	700501431, 700506519

Chapter 14.
Safety Statements

14. Safety Statements

The Avaya IP500 Office modules are intended to be installed by 'Service Personnel' and it is the responsibility of the Service Personnel to ensure that all subsidiary interconnected equipment is wired correctly and also meet the safety requirements of IEC60950 or UL60950 where applicable.

- CE
  The CE mark affixed to this equipment means that the module complies with the 1999/5/EC (R&TTE), 89/336/EEC (EMC) and 72/23EEC (LVD) Directives.
- The Declarations of Conformity (DoC) for the IP500 products are available on the IP Office Application DVD.
- ⚠ This warning symbol is found on the base of IP500 modules.
- Refer to Trunk Interface Modules 299 for information concerning which Trunk Interface module variants are fitted in which country.

In Finland, Norway and Sweden a protective earthing conductor must be attached to the protective earth point on the rear of the IP500 V2 control unit. See Grounding 93 for more information. In addition the Server must be located in a restricted access location where equipotential bonding has been applied, for example, in a telecommunication centre.

14.1 Lightning Protection/Hazard Symbols

Lightning protectors

The buildings lightning protectors must be verified as follow:

1. Check the lightning protectors, at the trunk cable entry point to the building housing the Avaya IP Office, paying special attention to the lightning protection grounding. Report any problems, in writing, to the telephone company.
2. Equipment that is designed to be connected using internal wiring is typically not lightning protected. Hence, Avaya IP Office extension cabling must not leave the building. For installations where telephones and/or other standard (tip/ring) devices are installed in another building then lightning protection is required (see Out of Building Telephone Installations 36).

Hazard Symbol

The shock hazard symbol is intended to alert personnel to electrical hazard or equipment damage. The following precautions must also be observed when installing telephone equipment:

1. Never install telephone wiring during a lightning storm.
2. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
3. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
4. Always use caution when working with telephone lines.

14.2 Trunk Interface Modules

To ensure the validation of the approvals, only the following types of trunk interface cards must be fitted in the following IP Office control units.

USA/Canada						
Product	Quad BRI	PRI E1		PRI T1		Analog Trunk Card
		Single	Dual	Single	Dual	
IP500 V2	✗	✗	✗	✓	✓	✓
IP500	✗	✗	✗	✓	✓	✓

Rest of World						
Product	Quad BRI	PRI E1/E1R2		PRI T1		Analog Trunk Card
		Single	Dual	Single	Dual	
IP500 V2	✓	✓	✓	✗	✗	✓
IP500	✓	✓	✓	✗	✗	✓

Notes

- E1R2 trunks are only supported in CALA and Korea.

14.3 Further Information and Product Updates

Further information, including Product and Reference Manual updates, can be obtained from Avaya Dealers and Distributors or from Avaya's web site: http://www.avaya.com.

This guide is also available from the Avaya's support web site: http://support.avaya.com.

Support Telephone Numbers

For initial help and support, contact your distributor/supplier. The following contact points are for Avaya authorized partners.

In the USA only

Avaya provides a toll-tree Customer Helpline 24 hours a day:

- Name: Avaya Technical Support Organization (TSO)
- Customer Helpline: 1 800 628-2888
- Address: 8744 Lucent Blvd., Highlands Ranch, Colorado, 80129 USA
- URL: http://support.avaya.com
  If you need assistance when installing, programming, or using your system, call the Helpline or your Avaya representative. Consultation charges may apply.

Outside the USA

If you need assistance when installing, programming, or using your system, contact your Avaya representative.

- URL: http://support.avaya.com

14.4 Port Safety Classification

The Avaya IP Office systems have the following ports which are classified as follows:

Port Name	Port Description	Port Classification
PRI port	PRI ISDN connection (NET)	TNV (Operating within the limits of SELV)
BRI ports	BRI ISDN connection (NET)	TNV (Operating within the limits of SELV)
Analog ports	Two wire analog trunk	TNV3
Power fail ports	Two wire analog trunk	TNV3
RS232 DTE port	Async Data connection.	SELV
Analog Telephone Ports	Telephone Extension ports	TNV2
Digital Telephone Ports	Telephone Extension ports	SELV
LAN ports	10/100 BaseT attachment to LAN.	SELV
Expansion ports	Expansion Module connector.	SELV
Audio port	Connector for Music on Hold.	SELV
External Control port	Connector for Controlling Ancillary circuits.	SELV
DC Input port	Connector for DC input power.	SELV

Interconnection circuits shall be selected to provide continued conformance with the requirements of EN 609050:1992/A3:1995 clause 2.3 for SELV circuits and with the requirements of clause 6 for TNV circuits, after connections between equipment.

Página2961 de 3226.

14.5 EMC Directive

889/336/ EEC (EMC Directive) CISPR 22:1993 including A1 + A2, AS/NZ 3548:1995 (ROW)

- ⚠ **WARNING**
  This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

Canadian Department of Communications (DOC)

''NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment."

EMC Caution for China

警示

注意：此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。仅适用于商业或工业环境。

14.6 Regulatory Instructions for Use

14.6.1 Australia

Connection
Connection of IP Office products must be via a Line Isolation Module with a telecommunications compliance label.

BRI Interface
During the configuration, ensure "000" emergency number is not barred, by performing the following:

- Short Code: 000
- Telephone No: 000;
- Function: DialEmergency

Connections to TS013, the following Bearer Capabilities shall not be used:

- 7kHz Audio, Video, Restricted Digital Information.

If unknown type of number is used in calling party number, the network will use the default CLI.

The system must be configured for Point to Multi point connection to comply with Austel requirements for connecting to TS013 circuits.

As the IP Office does not support emergency dialing after loss of power, the following warning notice should be recognized:

- **WARNING**
  This equipment will be inoperable when mains power fails.

PRI Interface
During the configuration, ensure "000" emergency number is not barred, by performing the following:

- Short Code: 000
- Telephone No: 000;
- Function: DialEmergency

- **WARNING**
  This equipment will be inoperable during mains power failure.

14.6.2 Canada

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met.

It does not imply that Industry Canada approved the equipment.

''NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 1. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.''

Página2963 de 3226.

14.6.3 China

AVAYA

700433220
February 2007
Copyright© 2007, Avaya Inc. All Rights Reserved

所有在中华人民共和国境内进口或销售的电子信息产品必须附上本文件

Include this document with all Electronic Information Products imported or sold in the People's Republic of China

部件名称 (Part Name)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 (Metal Parts)	×	○	○	○	○	○
电路模块 (Circuit Modules)	×	○	○	○	○	○
电缆及电缆组件 (Cables & Cable Assemblies)	×	○	○	○	○	○
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	○
电路开关/断路器 (Circuit Switch/Breakers)	○	○	○	○	○	○
电源组件 (Power Assemblies)	×	○	○	○	○	○
显示器 (LCD, Monitor)	○	○	○	○	○	○
玻璃 (Glass)	○	○	○	○	○	○

○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363 2006 标准规定的限量要求以下。
Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363 2006 standard.

×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363 2006 标准规定的限量要求。
Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363 2006 standard.

本表显示，所附的亚美亚电子信息产品中，从生产日期起，可能包含这些物质。注意：所附产品可能包含或不含以上所列的某些组件。
This table shows where these substances may be found in Avaya's electronic information products, as of the date of manufacture of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

除非有另外特别的标注,此标志将作为所附产品及零部件的环保使用期标志. 某些产品会有一个不同的环保使用期(例如,电话机)并贴在其产品上.此环保使用期限只适用于产品在产品手册中所规定的条件下使用

The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain products have a different EFUP (for example, telephones) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

Página2964 de 3226.

14.6.4 Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい

14.6.5 European Union

1. 999 and 112 calls must not be barred. Doing so will invalidate the approval.
2. All connections at the MDF shall be identifiable by suitable labeling.
3. The CE mark displayed on IP Office equipment indicates the systems compliance with the EMC, LVD, and R&TTE Directives and common technical regulations for Primary Rate and Basic Rate ISDN.
4. All ports for the connection of other non-telecommunications apparatus have a Safety Extra Low Voltage (SELV) safety status.

CE European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

14.6.6 New Zealand

The grant of a Telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom's network services.

Página2965 de 3226.

14.6.7 FCC Notification

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection

Connection of this equipment to the telephone network is shown in the following table.

Port	FIC	SOC	USOC Jack	REN
IP500 PRI 1U, IP500 PRI2U	04DU9.BN, 04DU9.DN, 04DU9.IKN, 04DU9.ISN	6.0Y	RJ48C	NA
IP500 ATM4U	OL13A, OL13B, OL13C, 02AC2, 02LA2, 02LB2, 02LC2, 02LR2, 02LS2	9.0Y	RJ45S	0.1B
IP500 ATM16	OL13A, OL13B, OL13C, 02AC2, 02GS2, 02LA2, 02LB2, 02LC2, 02LR2, 02LF2 02GS2, 02LS2	9.0Y	RJ45S	0.1B

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

A. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.
   - Routed to a dial prompt

B. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN. Permissible exceptions are:
   - A call is unanswered.
   - A busy tone is received.
   - A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

1. Remain on the line and briefly explain to the dispatcher the reason for the call.
2. Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and Least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

14.6.8 Compliance with FCC Rules

Transmit and Receive Gain Settings for PRI/T1 and Analog Ports

The Gain settings are password controlled for use by qualified installation personnel only and must not be made available to the end user. The default gain settings of 0dB ensures compliance with FCC part 68 section 68.308(b)(5) and TIA/EIA-IS-968 Section 4.5.2.5. "Through transmission amplification from ports for the connection of separately registered equipment or from other network connection ports". Gain setting adjustment by unqualified personnel may result in violation of the FCC rules. Qualified personnel may adjust gain settings above these levels only where:

1. Measurement is made to ensure that the power levels sent to line at each network interface connected does not exceed the maximum levels specified in FCC part 68 section 68.308(b) and TIA/EIA-IS-968 Section 4.5 for that specific interface type.
2. Where gain adjustment away from the default values are made, precautions should be taken to ensure that the connection of terminal equipment is controlled by qualified installation personnel.
3. To conform with the Receive Objective Loudness Rating at distances greater than 2.7km from the central office, on analog trunks a receive gain of 1.5dB must be set.

Chapter 15.
Document History

15. Document History

Date	Issue	Change Summary
15th November 2017	33a	Update for IP Office Release 11.0.
14th February 2018	33b	• Conversion to HMv7 authoring tool. • Removal of Integrated Contact Reporter.
26th April 2018	33c	• Correction to display of table headers in outputs.
10th May 2018	33d	• Equinox not supported on macOS 10.10. • IE10 supported only on Windows Server 2012.
16th May 2018	33e	• Addition of Dell R630 Server.
18th May 2018	33f	• Avaya Communicator for Windows incorrectly dropped from supported on R11.0. • Clarified Communicator advanced mode system licensing for IP500 V2. • Fixed error in PDF output metadata/HTML title properties.
22nd May 2018	33g	• Split tables that were causing excessively slow HTML load.
20th August 2018	33h	• Simplify Admin suite .NET installation note. • Update for R110.0 SP1. Addition of J139, K155 and H200 Series phone support. • Removed incorrect statement of Equinox support on K100 phones.
21st August 2018	33i	• Republish to correct missing image (SVG) and blank table headers.
13th September 2018	33j	• Correct to supported power supplies for current modules. • H229 incorrect listed as analog. Moved to SIP IP phones. • Internal music on hold not supported in Basic Edition. • Basic Edition HTML output incorrectly labeled Essential Edition.
9th October 2018	33k	• More than two JBM24s requires mains power supply for phone rather than PoE.
6th November 2018	33l	• Correction to the Equinox support table. • Updates for Release 11.0 SP2: ○ Equinox desktop/shared control mode.
30th January 2019	34a	• Updates for 11.0.3.0/11.0.4.0: • Support for JEM24 module and J179 Bluetooth.
15th February 2019	34b	• What's New section updated for 11.0.4.0.
7th August 2019	34c	• Correction. Equinox on Vantage now supported as of 11.0.4.0.

20th November 2019	35a	• Updates for R11.0.4.2.0:
		  ○ Support for J100 4.0.3 firmware and J159 phones.
		  ○ Equinox rebranding to Avaya IX Workplace.

27th November 2019	35b	• Reinstatement and update of wall/rack mount details.
3rd December 2019	35c	• Additional note. Maximum DS extension capacity in IP Office Basic Edition modes.
4th December 2019	35d	• Remove E159/E169 phones. Now end of service support from Avaya.
9th December 2019	35e	• Correct missed links.
6th January 2020	35f	• Update IP Office Knowledgebase link.

© 2020 AVAYA All Rights Reserved.

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)
Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Página2972 de 3226.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software
"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components
"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider
THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Página2973 de 3226.

Compliance with Laws
Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud
“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention
If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities
Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation
For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support
See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Index

A

Analog
- Phone Barrier Boxes 189
- Phone Region Availability 39, 249
- Port 264, 267

Application
- Call Center 45
- Call Logging 45
- CD/DVD 42
- CTI 45
- Maintenance 43
- Manager 253
- Monitor 255
- SoftConsole 257
- System Status Application 257
- TAPI 258
- User 44
- Voicemail 44
- VoiceMail Pro 259

Assessments
- Network 40
- VoIP 40

Audio
- Codec Conversion 41
- Port 264

Audio Port 267

Availability of Equipment 12

B

Backup
- SD Card 149

Barrier Boxes
- Analog Phone 189
- Rack Mounting 190

Base Card
- Analog Phone 22, 209
- Digital Station 22, 209
- Legacy Card Carrier 22, 209
- VCM 22, 209

BRI
- (So) Port 268
- (Trunk) Port 269
- Port 264

C

Cable
- Access Requirements 53
- Clearance Requirements 53

Cables
- Maximum Cable Distances 33, 265
- Standard IP Office 33, 265

Cabling
- Lightening Protection 36, 187

Call Logging Application 45

Call Status
- Application 43

Cards
- IP500 Analog Phone Base 213
- IP500 Digital Station Base 218
- IP500 VCM 221

Castle Rock 192

Channels
- Compression 41

Clock 107

Compact Business Center
- Application 45

Compact Contact Center
- Application 45

Compression Channels 41

Conference Center
- Application 44

Configuration
- Create New 76
- Erase 170

Connections
- Grounding 35
- Out of Building 36, 187

ContactStore
- Application 44

Control Unit
- IP406 V2 18
- IP412 18
- IP500 System Unit 18
- Rack Mounting 37
- SOE 18
- Wall Mounting 37

Copy
- SD Card 152

Country
- Languages 42
- Supported Locales 42

Create Configuration 76

D

Daughter Cards
- Analog Trunk 25, 224
- BRI Trunk 25, 226
- PRI Trunk 227
- PRI-U Trunk 25
- Trunk 25

DC I/P
- Port 264

DCI I/P Port 271

DECT
- Phone 39, 249
- Region Availability 39, 249

DevLink Application 45

DS
- IROB 188
- Phone 39, 188, 249
- Port 264, 271
- Region Availablility 39, 249

DTE Port 198
- Cable requirement 278
- RS232 278
- Settings 278

E

Embedded Voicemail
- Application 44

EMC Cautions
- Canadian Department of Communications 301
- EMC Caution for China 301
- Federal Communications Commission 301

Envirmental Requirements 51

Equipment Availability 12

Expansion
- Port 264

Expansion Modules
- IP400 Analog Trunk 16 241

Página2976 de 3226.

Expansion Modules
IP400 Digital Station V2 243
IP400 Phone V2 245
IP500 Analog Trunk 16 229
IP500 Digital Station 26, 231
IP500 Phone 26, 238
IPO 500 Analog Trunk 26
IPO 500 BRI So8 26
Expansion Port 273
Exporting Settings 77
EXT O/P
Port 264
EXT O/P Port 191, 273
Extension Numbers
Swapping 186
External Expansion Modules 26

F

Faulty Units 12
FCC Rules 307
Feature Key Server
Application 43
Feature Keys
Parallel 21
Serial 21
Smart Card 21
USB 21
Firewall Exceptiong 260

G

General Information
Training Courses 46
Web Sites 46
Grounding Control Units 35

H

H323
Phones 39, 249
Region Availability 39, 249
Hazard Symbols 298
Hazardous Substances 12
Homologation Statement 298
HP OpenView 192

I

Importing Settings 77
IP Office Operation in
Australia 302
Canada 302
China 303
European Union 304
New Zealand 304
USA 305
IP500
Analog Phone Base Card 22, 209
Analog Trunk Daughter Card 25
BRI Trunk Daughter Card 25
Digital Station Base Card 22, 209
Legacy Card Carrier Base Card 22, 209
PRI-U Trunk Daughter Card 25
Reset Button 197
Trunk Daughter Card 25
VCM Base Card 22, 209
IP500 Installation
Admin Applications 64
Card 82
Check Card LED 95
Connect Manager 67
Documentation 60
Grounding 93
Rack Mounting 89
Start Manager 68
Tools 59
Unpacking 60

L

LAN
Port 264
LAN Port 274
Licences
Manager 253
Monitor 255
SoftConsole 257
Syatem Status Application 257
TAPI 258
VoiceMail Pro 259
Licenses
PC-Base 21
PC-Less 21
Lightening Portection 298
Lightening Protection 36, 187

M

Maintenance
Applications 43
Manager
Application 43
Clock Quality 107
Components 253
License Requirements 253
PC Requirements 253
Prefix Dialing 109
Trunks 105
Upgrade Software 180
Memory card
Removal 142
Modules
Trunk Interface 299
Monitor
Application 43
Components 255
License Requirements 255
PC Requirements 255
Protocols 260
MS-CRM
Application 44

N

Network Assessments 40
New Configuration 76

O

Out of Building
Connections 36, 187

P

Parallel Feature Key 21
PC-Base Licensing 21
PC-Less Licensing 21
PF
Port 264
PF Port 275
Phone (POT)
Port 264
Phone (POT) Port 276

Página2977 de 3226.

Port
Analog 264, 267
Assigned 260
Audio 264, 267
BRI 264
BRI (So) 268
BRI (Trunk) 269
DC I/P 264
DCI I/P 271
Door 191
DS 264, 271
Expansion 264, 273
EXT O/P 191, 264, 273
IP Office 260
LAN 264, 274
PF 264, 275
Phone (POT) 264, 276
PRI 264, 277
RS232/DTE 264
RS323 DTE 278
Safety Classification 300
USB 264
Used 260
WAN 264
Power Supplies
1151C1 30
1151C2 30
Cords 31
Type 40w PSU 30
Type 45W Earthed PSU 30
Type 60W Earthed PSU 30
Uninterrupted Power Supply 32
PRI
Port 264
PRI Port 277
Protocols 260

R

Rack Mounting Control Units 37
Region Availability
Analog Phone 39, 249
DECT Phone 39, 249
DS Phone 39, 249
H323 Phone 39, 249
Remove
SD Card 142
Requirements
Cable Access 53
Cable Clearance 53
Enviromental 51
Space 53
Wall Mounting 51
Restore
SD Card 150
RoHS 12
RS232/DTE
Port 264

S

Safety Statement 298
SD Card
Backup 149
Copy 152
Removal 142
Restore 150
Security Settings
Default 173
Serial Feature Key 21
Settings
CSV File Formats 77
Exporting 77
Importing 77
Smart card Feature Key 21
SNMP 192
Enabling 195
Installation 193
Port 195
respond 195
Trap Sending 195
SNMP MIBs
Application 43
SoftConsole
Application 44
Components 257
License Requirements 257
PC Requirements 257
Software
Erase Core Software 199
Space Requirements 53
Statement
Homologation 298
Safety 298
Supported
Language 42
Locales 42
System Status
Application 43
System Status Application
Components 257
License Requirements 257
PC Requirements 257

T

TAPI
Components 258
License Requirements 258
PC Requirements 258
WAV Driver Application 45
TAPILink Lite
Application 44
TAPIlink Pro Application 45
Training Courses 46
Trunk Interface Modules 299

U

USB
Feature Key 21
Port 264

V

Voice Compression Channels 41
Voicemail Lite
Application 44
VoiceMail Pro
Application 44
Components 259
License Requirements 259
PC Requirements 259
VoIP Assessments 40

W

Wall Mounting Control Units 37
Wall Mounting Requirements 51

Página2978 de 3226.

WAN
Port 264
Web Sites 46

Página2979 de 3226.

© 2020 Avaya Inc. All rights reserved.

IP Office™ Platform 11.0

IP Office Platform Security Guidelines

Contents

1. Introduction
1.1 Intended Audience 6
1.2 Document Changes since Last Issue 6

2. Overview
2.1 Disclaimer 8
2.2 Information Classifications and NDA Requirements 8
2.3 Applicability 9
2.4 Responsibility for IP Office Security 9
2.5 Responsibility for Security Updates 9

3. IP Office Security Fundamentals
3.1 Encryption 13
3.1.1 Message Authentication 14
3.1.2 Security Database 14
3.2 Data Privacy 15
3.3 Authentication and Authorization Framework 16
3.4 Linux Platform Security 17
3.5 IP Office Services 18
3.6 Default Security Settings 19

4. User Accounts and Rights of Access
4.1 Service Users 23
4.1.1 Changing Administrative Users, Rights Groups and Authentication 24
4.1.2 Default Administrative Users and Rights Groups 24
4.2 Security Settings on Upgrade 29

5. Password and PIN Management
5.1 Password and PIN Policy 33
5.2 Administrative User Passwords 34
5.3 IP Office User Passwords and Login Codes 36

6. Certificates and Trust
6.1 Certificate Terminology 39
6.1.1 Components of a Certificate 40
6.1.2 Certificate Security 41
6.1.3 Certificate Checks 41
6.1.4 Certificates and the Transport Layer Security (TLS) Protocol 41
6.1.5 Certificate File Naming and Format 42
6.2 IP Office Certificate Support 43
6.2.1 Interface Certificate Support 44
6.2.2 Initial Certificate Settings 44
6.2.3 Certificate Name Content 50
6.2.4 Certificate Check Controls 52
6.2.5 Certificate Distribution 53
6.2.6 Determining Trust Policy 56
6.2.7 IP Office PKI Trust Approaches 57
6.2.8 Selecting IP Office PKI 59
6.2.9 Implementing IP Office PKI 59
6.2.10 Certificates from External Certificate Authorities 62
6.2.11 Certificate Maintenance 64

7. VoIP Security
7.1 IP Office Platform Media Security 68
7.2 VoIP Signalling Security 70
7.3 Endpoint Provisioning Security 70
7.4 SRTP Performance & Capacity 71
7.5 Secure Call Indications 71
7.6 VoIP Security Planning Considerations 72

8. Securing the IP Office Platform Solution
8.1 General Guidelines 75
8.2 Assessing IP Office Security Requirements 76
8.3 Security Administration 76
8.4 Change Security Defaults 76
8.5 Remove Unnecessary Accounts 76
8.6 Disable Unused Services/Interfaces 77
8.7 Ensure Minimum Rights of Access 78
8.8 Enforce a Password Policy 79
8.9 Update Certificates 80
8.10 Securing Telephony Users & Extensions 81
8.11 Hardening for Remote Worker Operation 82
8.12 Securing Trunks/Lines 83
8.13 Secure Voice Media 83
8.14 Preventing Unwanted Calls 84
8.14.1 Call Barring 84
8.14.2 User Based Barring 85
8.14.3 Protecting Phones 86
8.14.4 Making Calls from Protected Phones 86
8.14.5 Forwarding Protection 87
8.14.6 Remote Forwarding Controls 87
8.14.7 SMDR Reporting of Barred Calls 87
8.14.8 Error Handling in Voicemail Pro Call Flows 87
8.15 Securing CTI Interfaces 88
8.16 Securing IP Office Applications 88
8.16.1 Securing IP Office Manager 89
8.16.2 Securing IP Office Web Manager/Web Control 89
8.16.3 Securing Web Licence Manager 89
8.16.4 Securing System Status Application 90
8.16.5 Securing System Monitor 90
8.16.6 Securing Voicemail Pro 91
8.16.7 Securing Embedded Voicemail 92
8.16.8 Securing Contact Recorder 92
8.16.9 Securing one-X Portal for IP Office 93
8.16.10 Securing WebRTC Gateway 94
8.16.11 Securing Media Manager 94
8.16.12 Securing Integrated Call Reporter 94
8.16.13 Securing Avaya Contact Center Applications 94
8.17 Configuration and Other Sensitive Data 94
8.18 Limiting IP Network Exposure 95
8.18.1 Firewall 95
8.18.2 Session Border Controller 95
8.18.3 Remote Maintenance Access 95
8.19 Secure Maintenance Interfaces 96
8.20 Restricting Physical Access 96
8.21 Securing Server Edition Servers 97

Página2983 de 3226.

8.22 Securing Linux Application Server/Unified Communications Module 99

9. Monitoring the IP Office Platform

9.1 Checks and Tests 103
9.2 Activating Reporting 106
9.2.1 IP Office Reporting 106
9.2.2 Voicemail Pro Reporting 106
9.2.3 Contact Recorder Reporting 106
9.2.4 one-X Portal for IP Office Reporting 107
9.2.5 Linux-Based Server Reporting 107
9.2.6 Other Components Reporting 107
9.3 Avaya Security Advisories and IP Office Updates 107
9.4 Response to Incidents 107

10.Appendices

10.1 Appendix A - Avaya Product Security Support 111
10.1.1 Accessing Avaya Security Advisories 111
10.1.2 Interpreting an Avaya Security Advisory 111
10.2 Appendix B - Default Trusted Certificates 112
10.2.1 Symantec Class 3 Secure Server CA - G4 in PEM format 113
10.2.2 Entrust Certification Authority - L1K in PEM format 113
10.2.3 GTS Root R1 in PEM format 114
10.2.4 GTS Root R2 in PEM format 114
10.2.5 GlobalSign Root CA - R2 in PEM format 115
10.2.6 ISRG Root X1 in PEM format 115
10.2.7 DigiCert Global Root CA in PEM format 116
10.2.8 DigiCert SHA2 Secure Server CA in PEM format 116
10.2.9 Let's Encrypt Authority X3 in PEM format 117
10.2.10 Removing a Default Trusted Certificate 117
10.3 Appendix C - Windows Certificate Management 118
10.3.1 Windows Certificate Store Organization 118
10.3.2 Certificate Store Import 119
10.3.3 Certificate Store Export 119
10.3.4 Certificates Console 120
10.4 Appendix D - SRTP Troubleshooting 121
10.4.1 Troubleshooting Tools 121
10.4.2 Troubleshooting Tips 121
10.5 Appendix E - IP Office Interface Certificate Support 123
10.6 Appendix F - IP Office VoIP Endpoint Security 127
10.7 Appendix G - Using the IP Office Certificate Authority 131
10.7.1 Generating the CA Server's Own Identity Certificate 131
10.7.2 Generating Identity Certificates for Other Devices 132
10.7.3 Exporting the Signing Certificate 132
10.7.4 Renewing/Replacing the Signing Certificate 133
10.8 Appendix H - Certificate Signing Requests 134
10.8.1 Creating a CSR using Microsoft MMC Certificates Snap-in 135
10.8.2 Creating a CSR using the OpenSSL Package 138
10.8.3 Creating a CSR using the Linux Server Command Line 140
10.8.4 Converting Certificate Files 141
10.9 Appendix I - Secure Provisioning of 9600 Series H.323 Phones 142
10.9.1 Recommended Staging Process 142
10.9.2 Automated Process 143
10.9.3 Changing a Root CA Certificate 143
10.10 Appendix J - Application/Client Security Dependencies 144

11.Document History

Index 155

Página2984 de 3226.

Chapter 1. Introduction

1. Introduction

This document provides guidelines for implementing and maintaining IP Office Platform security. It contains an overview of security policy and describes the security tools available to an IP Office Platform solution.

1.1 Intended Audience

This document is intended for installation, administration, service and support personnel who required knowledge of the available IP Office security tools and information on how to implement an IP Office security policy.

1.2 Document Changes since Last Issue

Updates for IP Office Release 11.1

- Data Privacy
- IP Office security settings defaults
- Default trusted certificates
- SBC Policy
- Updated links

Updates for IP Office Release 11.1 FP1

- The voicemail password used to secure the connection between the IP Office and Voicemail Pro services is now fixed to 31-characters in length.
  - On new installs, a suitable 31-character password is automatically generated on first connection between the two services.
  - Existing systems can continue with existing shorter passwords. However, on any password change, the 31-character password length requirement is enforced.

Página2987 de 3226.

Chapter 2.
Overview

2. Overview

The following document is a practical guide to planning, checks and configuration changes required to help secure the IP Office solution. All IP Office existing and new installations, regardless of usage, must be assessed with the following sections and immediate action taken where indicated.

Implementing these recommendations will substantially reduce the risk of compromise from security threats such as Denial of Service, Toll Fraud and theft of data.

This document does not provide an analysis of security-related topics, define security policy or discuss theory – it also cannot guarantee security. This document does however aim to provide useful and understandable information that can be used by installation, service and support personnel as well as customers to help harden IP Office against attacks.

2.1 Disclaimer

Avaya has used reasonable efforts to ensure that the information provided here under is accurate at the date of publication. Avaya may change any underlying processes, architecture, product, description or any other information described or contained in this document. Avaya disclaims any intention or obligation to update or revise the document, whether as a result of new information, future events or otherwise. This document is provided "as is," and Avaya does not provide any warranty of any kind, express or implied.

2.2 Information Classifications and NDA Requirements

Avaya provides security-related information according to the following information classifications:

Classification	Description
Avaya Restricted	This classification is for extremely sensitive business information, intended strictly for use within Avaya. Unauthorized disclosure of this information can have a severe adverse impact on Avaya and the customers, the Business Partners, and the suppliers of Avaya.
Avaya Confidential	This classification applies to less sensitive business information intended for use within Avaya. Unauthorized disclosure of this information can have significant adverse impact on Avaya, and the customers, the Business Partners, and the suppliers of Avaya. Information that can be private for some people is included in this classification.
Avaya Proprietary	This classification applies to all other information that does not clearly fit into the above two classifications, and is considered sensitive only outside of Avaya. While disclosure might not have a serious adverse impact on Avaya, and the customers, Business Partners, and suppliers of Avaya, this information belongs to Avaya, and unauthorized disclosure is against Avaya policy.
Public	This classification applies to information explicitly approved by Avaya management as non-sensitive information available for external release.

As this document is generally available, the information herein is considered **Public**. This document contains references to additional information sources which may disclose both confidential and proprietary information and require a non-disclosure agreement (NDA) with Avaya.

Página2989 de 3226.

2.3 Applicability

The following information is applicable to IP Office IP500 V2, IP Office Server Edition, IP Office applications and endpoints for release 9.1, 10.0, 10.1, 11.0 and 11.1.

IP Office Technical Bulletin 169 covers releases 9.0 and prior, and can be found at: https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/bulletins/techbulls/tb169.pdf.

The following areas are not covered in this document:

- Physical security measures
- Non-Avaya component security
- Security policy definition
- Regulatory compliance

2.4 Responsibility for IP Office Security

Avaya is responsible for designing and testing all Avaya products for security. When Avaya sells a product as a hardware/software package, the design and testing process of the Avaya product also includes the testing of the operating system.

The customer is responsible for the appropriate security configurations of data networks. The customer is also responsible for using and configuring the security features on IP Office systems, gateways, applications and telephones.

2.5 Responsibility for Security Updates

When security-related applications or operating software updates become available, Avaya tests the updates if applicable before making them available to customers. In some cases, Avaya modifies the updated software before making updated software available to customers.

Avaya notifies customers of the availability of security updates through Security Advisories. Customers can subscribe to receive notification about Security Advisories by email. For more information, see Avaya Product Security Support.

When IP Office software security updates become available, the customer can install the updates or employ an installer from the customer services support group to install the updates. When Avaya installs the updates, the installer is responsible for following best security practices for server access, file transfers, and data backup and restore.

Chapter 3.
IP Office Security Fundamentals

3. IP Office Security Fundamentals

All telephony, management, data, services and interfaces offered by the IP Office solution have security features to help prevent security threats such as:

- Unauthorized access or modification of data
- Theft of data
- Denial of Service (DoS) attacks
- Viruses and Worms
- Web-based attacks such as Cross-Site Scripting and Cross-Site Forgery
- Detection of attempted attacks

The following table lists methods and techniques used to help counter security threats:

Mechanism	Usage	IP Office Examples
Identification and Authentication	Identification is the ability to uniquely identify a user, system or application of a system or an application that is running in the system. Authentication is the ability to prove that an entity is genuinely who they claim to be.	• Telephony and Service User accounts • Message authentication • X509 digital certificates
Authorization	Authorization protects resources by limiting access only to authorized users, systems or applications.	• Telephony and Service User accounts' access controls
Auditing	Auditing is the process of recording and checking events to detect whether any unexpected activity or attempt has taken place.	• Audit trail • System Status Application Alarms • Syslog reports
Confidentiality	Confidentiality keeps sensitive information private, protecting from unauthorized disclosure.	• TLS/SRTP encryption • Security database encryption
Data integrity	Data integrity detects whether there has been unauthorized modification of data.	• TLS/SRTP Message authentication

Table 1: Security Methods

Página2993 de 3226.

3.1 Encryption

Encryption ensures that all data stored on a system or sent by one system to another cannot be 'read' by anyone else. There are two main types of encryption

- **Symmetric encryption** is the application of a mathematical process at the originating end, and a reverse process at the receiving end. The processes at each end use the same 'key' to encrypt and decrypt the data.
- **Asymmetric encryption** uses different keys for encryption and decryption. A common usage is a certificate authority's private and public key. See Certificates and Trust 38 for more information.

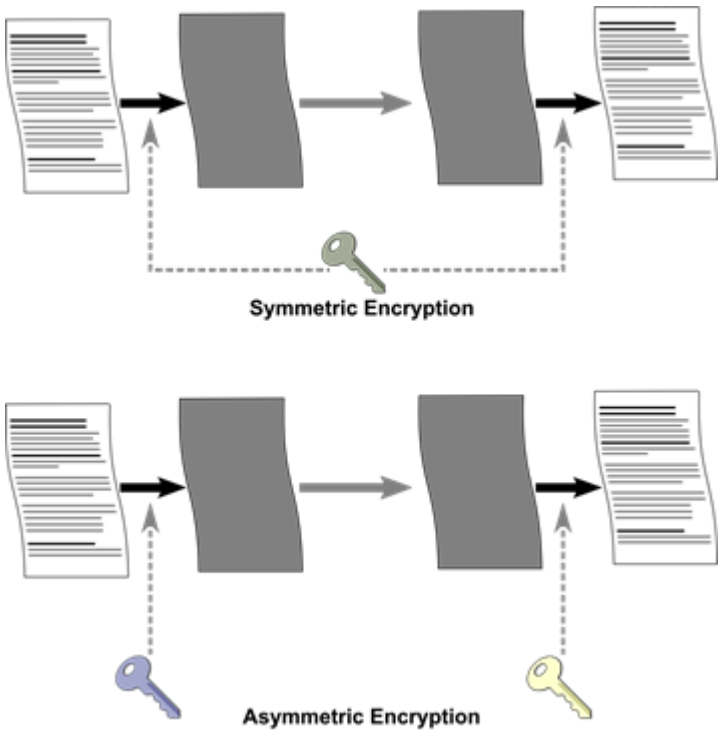


Figure 1: Symmetric/Asymmetric Encryption

Most message data encryption is symmetric. The data sent may be optionally encrypted using a number of well-known algorithms:

Algorithm	Effective key size (bits)	Use
DES-40	40	Not supported – insufficient strength
DES-56	56	Not supported – insufficient strength
3DES	112 (AKA two key DES)	Not supported – insufficient strength
3DES	168 (AKA three key DES)	'Low' security.
RC4-128	128	'Low' security.
AES-128	128	'Medium' security.
AES-256	256	'Strong' security.

Table 2: Encryption Algorithms

In general the larger the key size, the more secure the encryption. However, smaller key sizes usually incur less processing.

IP Office supports encryption using:

- Transport Layer Security (TLS v1.2 with v1.0 and v1.1 for legacy)
- Secure Shell (SSH v2)
- Secure RTP (SRTP)

Página2994 de 3226.

3.1.1 Message Authentication

Message authentication ensures that all data sent by either the system or Manager cannot be tempered with (or substituted) by anyone else without detection. This involves the originator of the data producing a signature (termed a 'hash') of the data sent, and sending that as well. The receiver gets the data and the signature, and checks both match.

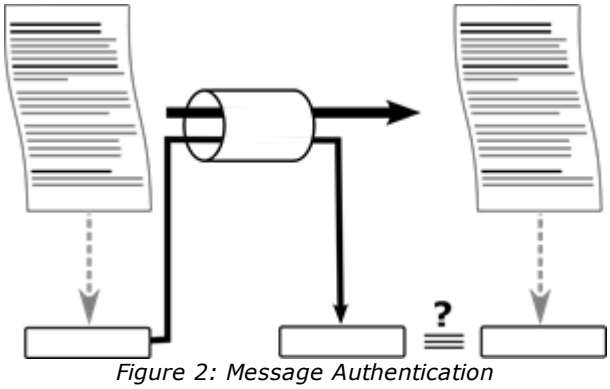


Figure 2: Message Authentication

Any data sent may be optionally authenticated using a number of well-known and cryptographically secure algorithms:

Algorithm	Effective hash size (bits)	Use
MD5	128	Not supported – insufficient strength
SHA-1	160	'Low/Medium' security for message authentication.
SHA-2	224, 245, 384, 512	'Strong' security

Table 3: Message Authenication

In general the larger the hash size, the more secure the signature. However, smaller hash sizes usually incur less processing. IP Office supports message authentication using Transport Layer Security (TLS v1.0, v1.1, and v1.2), Secure Shell (SSH v2), Secure RTP (SRTP) and IPsec protocols.

3.1.2 Security Database

A security database is located on the IP Office which controls all local access, plus remote access to other IP Office components. These security settings have initial default values, can be modified by IP Office Manager or IP Office Web Manager, and cover the following areas:

- Administrative accounts
- An inviolate security administration account
- Users' password and account policy
- Trust Store (Trusted Certificate Store)
- Identity certificates
- Received certificate checks
- Service interface security controls
- Legacy interface controls

The security settings are separate to the IP Office configuration, always secured and cannot be saved or edited offline.

In addition to the IP Office security settings, one-X Portal for IP Office, Voicemail Pro, Contact Recorder, WebLM and Web Control have local administrative accounts used under fall-back conditions, see User Accounts and Rights of Access 22.

Página2995 de 3226.

3.2 Data Privacy

In recent years legislation such as the California Consumer Privacy Act (CCPA) and the European General Data Protection Regulation (GDPR) have highlighted the need to keep personal data – that is, information that can be traced back to an individual – under a high degree of control.

IP Office can under certain conditions process and save personal data. Some examples are:

- Call Detail Records (SMDR) may contain an individual's personal telephone number
- Call Recordings might contain personal information spoken by a caller

Responsibility to keep such data protected is ultimately the responsibility of the 'Data Controller'. For IP Office the Data Controller typically would be the company using the system. that is, the customer or their agent. Under CCPA this is referred to as a 'Business'

Avaya IP Office, when used as part of a solution to process and save personal data on behalf of the customer is termed the 'Data Processor'. Under CCPA this is referred to as a 'Service Provider'. Note that IP Office will form only part of the Data Processor aspects, usually combined with other automated or manual processes.

IP Office cannot be individually certified to adhere to a specific data privacy requirement, but can be configured and operated by the Data Processor to achieve compliance with various data privacy regimes such as GDPR and CCPA.

The IP Office Platform adheres to the following set data privacy principles:

- Architected and designed with data privacy in mind
- No personal data captured by default
- Controls over what personal data can be captured, and how long it is retained.
- Notifications to individuals before personal data is captured, along with a record of acceptance.
- All personal data secure both at rest and in transit
- Personal data remains local to the servers; IP Office Cloud storage remains within the geographic region.
- Access to all personal data controlled via the IP Office Authentication and Authorisation framework, see Authentication and Authorization Framework 16.
- Personal data can be exported, modified or deleted in response to data privacy requests.
- Access to personal data logged. These logs may be viewed by the customer to provide an audit trail of personal data access.

A Product Privacy Statement for IP Office can be found at:
https://downloads.avaya.com/css/P8/documents/101049410.

Securing the IP Office Platform Solution 74 contains information for securing the IP Office solution and must be followed from both a security and Data Privacy perspective. In addition, the following documents must be read prior to solution deployment:

- Avaya IP Office Product Privacy Statement
- Avaya IX Workplace Product Privacy Statement
- Avaya Communicator for Web Product Privacy Statement
- Avaya IX Collaboration Product Privacy Statement
- Avaya Contact Center Select Product Privacy Statement
- Avaya Call Reporting For Avaya IP Office™ Product Privacy Statement

It is useful when reviewing these documents to understand the following terms. These definitions are broad in scope and may vary according to the data privacy regulations in force in a particular country/region.

- **Personal Data:** Means any information relating to an identified or identifiable natural person. This could include personal phone numbers, information recorded during calls, email addresses, location data, home address etc.
- **Data Subject:** An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name
- **Data Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. An example could be the customer operating the IP Office system.
- **Data Processor:** A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller. The IP Office system could form part of data processing.

Página2996 de 3226.

3.3 Authentication and Authorization Framework

IP Office has its own Authentication and Authorization (AA) framework, and requests to IP Office services are routed through the AA framework. The AA framework prevents unauthenticated, unauthorized access to IP Office services and data.

The following diagram shows the service interfaces covered by this framework:

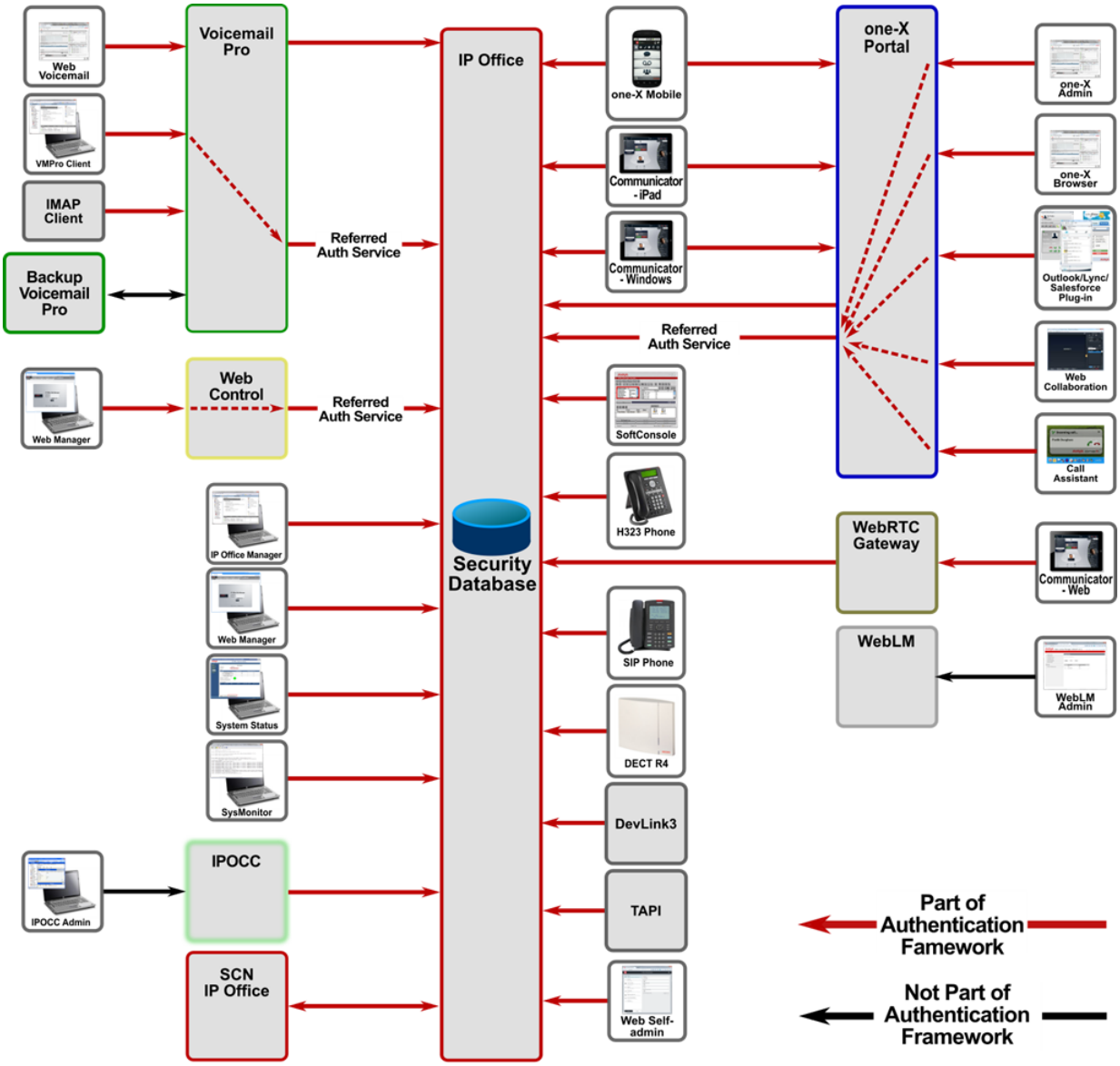


Figure 3: Authentication and Authorization Framework

one-X Portal for IP Office, Voicemail Pro and Web Control refer any administrative login to IP Office via an authentication/authorization web service.

There are some legacy interfaces which do not pass through the AA framework:

- TFTP user lists and directories
- TFTP file transfer
- SNMP (Note no SET operations supported)

These are disabled by default but can be enabled within an environment secured by other means.

Página2997 de 3226.

3.4 Linux Platform Security

A number of IP Office products run on the Linux operating system. Avaya uses the open source Linux operating system as a secure foundation for communications.

The open source foundation is beneficial because of the following reasons:

- Security experts worldwide review the source code for defects or vulnerabilities.
- Avaya works diligently to monitor both the enhancements and improvements created by the Linux community and to carefully review the changes before incorporating them into Avaya products.
- Linux-based Avaya servers help protect against many DoS attacks such as SYN floods, ping floods, malformed packets, oversized packets, and sequence number spoofing, among others.

Avaya has modified or hardened the Linux operating system in the following ways to minimize vulnerabilities and to improve security:

- **Minimal installation:**
  All unnecessary RPMs are removed. In addition to making the software file images smaller and more manageable, the operating system is more secure because attackers cannot compromise RPMs that are not present.
- **Least privilege:**
  All IP Office applications run as non-root. The root SSH access is disabled.
- **Ports:**
  Unnecessary IP ports closed.
- **Linux OS:**
  Security-Enhanced Linux (SELinux) is enabled, which provides increase security using kernel-level mechanisms that reduce the threat of compromise and limits potential damage from malicious or flawed applications.
- **Firewall protection:**
  The Linux-based products of Avaya use the IPTables firewall that protects the system against various network-based attacks.
- **Enhanced Access Security Gateway (EASG) support:**
  EASG is a certificate based authentication system that replaces passwords for technical support accounts.
- **Drive partition protection:**
  Processes that can write significant quantities of data to the hard drive such as the backup/restore HTTPS server and Voicemail Pro have quotas assigned to ensure disk space is not exhausted by malicious or unintentional actions.

Third-party security and management packages/tools

Several anti-virus and other security packages for Linux are available, however Avaya does not support the use of such software on the IP Office product as it has a level of natural immunity and the packages can severely impact performance.

Página2998 de 3226.

3.5 IP Office Services

All IP Office administrative and maintenance service interfaces are controlled by the security database for availability and security level. These services include:

Service	Usage
Configuration	IP Office Manager and Server Edition Manager configuration access
Security Administration	IP Office Manager and Server Edition Manager security settings (database) access
System Status Application Interface	System Status Application (SSA) access
Enhanced TSPI	one-X Portal for IP Office CTI access
HTTP	Phone and IP Office Manager file access, Voicemail Pro, IP Office Line, System Monitor (secure)
Web Services	IP Office Web Manager and SMGR
External	Services external to the IP Office application.

Table 4: IP Office Services

Each service has a configurable Service Security Level:

Service Security Level	Usage
Disabled	The service and corresponding TCP ports are inactive
Unsecure Only	This option allows only unsecured access to the service. The service's secure TCP port, if any, is disabled. This or Disabled are the only options supported for the Enhanced TSPI service
Unsecure + Secure	This option allows both unsecured and secure (Low) access.
Secure, Low	This option allows secure access to that service using TLS, and demands weaker (for example 3DES) encryption and authentication or higher. The service's unsecured TCP port is disabled.
Secure, Medium	This option allows secure access to that service using TLS, and demands moderate (for example AES-128) encryption and authentication or higher. The service's unsecured TCP port is disabled.
Secure, High	This option allows secure access to that service using TLS and demands stronger (for example AES-256) encryption and authentication, or higher. In addition, a certificate is required from the client (for Mutual Authentication). See Certificate Check Controls 52 for tests made on the received certificate. If no certificate is received from the client, the connection is rejected. The service's unsecured TCP port is disabled.

Table 5: Service Security Levels

Other service interfaces are controlled for activity.

Página2999 de 3226.

3.6 Default Security Settings

Defaults values for IP Office security settings are loaded on first start-up and on reset. They have a level of security and include enforced password changes for accounts.

- **Note:** IP Office release 9.0 and earlier require additional changes from default to make them more secure.

It is possible to reset the IP Office security settings via a management interface, IP500 V2 serial port or power-on reset buttons; for this reason it is important to make the IP Office installation physically secure.

For information about IP Office Administrative user defaults, see Default Administrative Users and Rights Groups 24 . For information about certificate defaults, see Initial Certificate Settings 44.

The following default security settings are applied to the various IP Office service interfaces.

Interface	Default Setting	Default Security?	Notes
Configuration	Secure, Medium	✓	IP Office Manager configuration access
Security Administration	Secure, Medium	✓	IP Office Manager security settings access
System Status Application Interface	Secure, Medium	✓	SSA access
Enhanced TSPI	Unsecure Only	✗	one-X Portal for IP Office CTI access
HTTP	Unsecure + Secure	✗	Phone and IP Office Manager file access, Voicemail Pro, IP Office Line, System Monitor (secure)
Web Services	Secure, Medium	✓	IP Office Web Manager and SMGR
TFTP Server	Active (IP500 V2) Inactive (Linux)	✗	Allows access for Manager upgrade and UDP whois discovery
TFTP Directory Read	Inactive	n/a	DECT R4 system directory
TFTP Voicemail	Inactive	n/a	Used for Voicemail Pro R9.0 and prior
Program Code	Active (IP500 V2) Inactive (Linux)	✗	Manager upgrade access
Devlink	Inactive	n/a	DevLink and System Monitor UDP/TCP access
Devlink3	Active	✓	DevLink3 access.
TAPI	Inactive	n/a	1st and 3rd party TAPI interfaces only.
HTTP Directory Read	Active	✗	one-X Portal for IP Office directory access, external directory feature
HTTP Directory Write	Active	✗	one-X Portal for IP Office directory access

Table 6: Default Security Settings

The local security settings for one-X Portal for IP Office, Voicemail Pro, IPOCC and Contact Recorder may be reset using the Linux console CLI and root access.

Chapter 4.

User Accounts and Rights of Access

4. User Accounts and Rights of Access

There are two main types of user accounts in the IP Office solution.

- A telephony user is called an **IP Office User**.
- An administrative user is called a **Service User**.

IP Office users are defined in the main configuration settings. Service users are defined in the security settings.

A special type of Service User is the Security Administrator, with permanent access to all security settings. An IP Office system can have no Service or IP Office users configured, but the Security Administrator cannot be removed or disabled.

In order to provide a central authentication database for the Authentication and Authorization (AA) framework a secure web service is provided by IP Office to other applications. Linux one-X Portal for IP Office, Voicemail Pro and Web Management use this service to 'Refer' administrative logins to the database.

Página3003 de 3226.

4.1 Service Users

Access to system settings is controlled by Service Users and Rights Groups stored in the control unit's security settings. These are stored separately from the system's configuration settings. All actions involving communications between Manager and the system require a service user name and password. That service user must be a member of a Rights Group with permissions to perform the required action.

Security Administrator:

The security administrator can access the system's security settings and the account cannot be removed or disabled.

In addition a further security setting can force this account to have exclusive security rights, preventing another Service Users from security settings access.

Service Users:

Each service user has a name, a password and is a member of one or more Rights Groups. The accounts may be in one of a number of states, including enabled, disabled, locked out and enforced password change.

IP Office supports a maximum of 64 Service Users.

Rights Groups:

The Rights Groups to which a service user belongs determine what actions they can perform. It can be thought of as a role, but has much more flexibility. Actions available to Rights Groups include configuration, security actions and maintenance actions. Where a service user has been configured as a member of more than one Rights Group, they combine the functions available in the separate Rights Groups

IP Office supports a maximum of 32 Rights Groups.

Application Roles:

In addition to rights of IP Office service access, Rights Groups can also contain 'Roles' for IP Office Manager and IP Office Web Manager; the settings of these roles determine what rights of access the Service User has within that application. It allows more granularity of access control within that application than the basic service access rights. For example, the IP Office configuration service has two basic rights of access: Read All and Write All. However, the Manager Operator roles can further constrain what can be written, viewed or edited.

Example Rights Assignment:

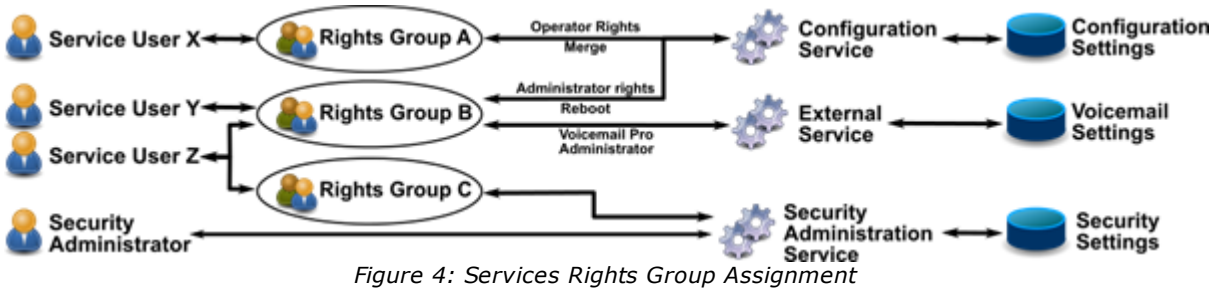


Figure 4: Services Rights Group Assignment

In the example illustrated above:

- Service user X can read and write the configuration. However they can only edit Operator settings and can only make changes that can be merged.
- Service user Y can read and write the configuration, edit all settings and make changes that require reboots or merges. They can also access the Voicemail Pro settings.
- Service user Z can read and write the configuration, edit all settings and make changes that require reboots. They can also access the security and the Voicemail Pro settings.
- The Security Administrator account can only access the security settings.

Página3004 de 3226.

4.1.1 Changing Administrative Users, Rights Groups and Authentication

IP Office Manager and IP Office Web Manager allow modification of Service Users and Rights Groups. Prior to any change, the following should be considered:

- A Server Edition or multi-site IP500 V2 deployment should have consistent Service Users and Rights Groups. IP Office Manager and IP Office Web Manager have synchronisation tools to assist.
- For all Linux-based servers, enable Referred Authentication to allow IP Office application to use the local IP Office
- All changes should follow security best practices such as password policy and minimal rights of access.

4.1.2 Default Administrative Users and Rights Groups

The following default service user settings are present on first start-up or following a security settings reset.

- Default Security Administrator 24
- Default Service Users 25
- Default Rights Groups 26
- Default Rights Group Assignments 27

4.1.2.1 Default Security Administrator

The following **Security Administrator** account is present on first start-up and security settings reset:

Name	Default Account Status	Usage	Rights Group Membership	Notes
security	Enabled, Force password change	This is the default security administration account. Has all rights to all security management and maintenance services	Implied all security rights	Cannot be removed or disabled.

Table 7: Default Security Administrator

4.1.2.2 Default Service Users

The following **Service User** accounts are present on first start-up and security settings reset:

Account Name	Default Account Status	Usage	Rights Group Membership	Notes
Administrator	Enabled, Force password change	This is the default account used for system configuration using the IP Office and IP Office Web Manager applications, including one-X Portal for IP Office/Voicemail Pro administration. Has all rights to all management and maintenance services including security settings.	Administrator, System Status Application, Business Partner	Should not be removed or disabled Should not be renamed
EnhTcpaService	Enabled	This account is used for one-X Portal for IP Office connections to the system.	TCPA Group	Although not enforced, the password should be change as soon as possible in both IP Office and one-X Portal for IP Office Enable only when one-X Portal for IP Office deployed
IPDECTService	Disabled	This account is used for DECT R4 system provisioning	IPDECT Group	Enable only when DECT R4 deployed and provisioning mode active
BranchAdmin	Disabled	This account is used for System Manager (SMGR) access in a branch deployment	SMGR Admin	Enable only when SMGR deployed; will be enabled when the Initial Configuration Utility (ICU) run and SMGR administration selected. Must not be renamed
BusinessPartner	Disabled	Similar access rights to Administrator and can be used as a separate account for Business Partners	Business Partner	Should be removed/disabled unless required
Maintainer	Disabled	Maintenance account without edit configuration or security access. Can be used for Manager (read-only), IP Office Web Manager (read-only), System Status Application (SSA), Backup/Restore, System Monitor, Upgrade	Maintainer	Should be removed/disabled unless required

Table 8: Default Service Users

Página3006 de 3226.

4.1.2.3 Default Rights Groups

The following **Rights Groups** are present on first start-up and security settings reset:

Group Name	Usage	Rights Group Users	Notes
Administrator Group	Allows full access to the IP Office Manager application to configure the system. No security or maintenance access	Administrator	All IP Office Manager operations are permitted Can use embedded file manager
Manager Group	Allows limited access to the IP Office Manager application to configure the system.	–	All IP Office Manager operations permitted except: - Delete Short Code - View LAN2 Settings Can use embedded file manager
Operator Group	Allows limited access to the IP Office Manager application to configure the system.	–	All IP Office Manager operations permitted except: - New object creations - View LAN2 Settings - Delete Directory - Delete Incoming Call Route Cannot use embedded file manager
System Status Application Group	Allows limited access to the SSA and Sys System Monitor applications.	Administrator	Sys Monitor access right only checked when using service users with Sys Monitor
TCPA Group	This group is used by the one-X Portal for IP Office application.	EnhTcpaService	
IPDECT Group	This group is used by the DECT R4 master base station to extract DECT settings from IP Office.	IPDECTService	
SMGR Admin	This group is used by SMGR to configure IP Office.	BranchAdmin	Do not change the access rights
Security Admin	Allows access to security settings only	–	
Backup Admin	Allows access to all backup and restore services only, including one-X Portal for IP Office	–	
Upgrade Admin	Allows access to the upgrade service	–	Allows upgrade of both IP Office applications and operating system
System Admin	Allows configuration of IP Office, one-X Portal for IP Office and Voicemail Pro	–	
Maint Admin	Allows configuration of IP Office, one-X Portal for IP Office and Voicemail Pro along with backup, restore and upgrade	–	Typically used for maintenance personnel
Business Partner	Full access to all configuration, security and maintenance services.	Administrator, BusinessPartner	
Customer Admin	Web Management , one-X Portal for IP Office and Voicemail Pro administration	–	No IP Office Manager access
Maintainer	Allows configuration view only, along with SSA, Sys Monitor backup, restore and upgrade	–	Typically used for maintenance personnel with no need for configuration changes.

Table 9: Default Rights Groups

Página3007 de 3226.

4.1.2.4 Default Rights Group Assignments

The following **Rights Group** assignments are present on first start-up and security settings reset:

Service	Rights Group > Access Right V	Administrator Group	Manager Group	Operator Group	System Status Application Group	TCPA Group	IPDECT Group	SMGR Admin
Configuration	Read all configuration	✓	✓	✓				
	Write all configuration	✓	✓	✓				
	Merge configuration	✓	✓	✓				
	Default configuration	✓	✓	✓				
	Reboot/Shutdown immediately	✓	✓	✓				
	Reboot when free	✓	✓	✓				
	Reboot at time of day	✓	✓	✓				
Security Admin	Read all security settings							
	Write all security settings							
	Reset all security settings							
	Write own service user password							
System Status Application	System Status Application Access				✓			
	Read all configuration				✓			
	System Control				✓			
	Sys Monitor				✓			
Telephony APIs	Enhanced TSPI Access					✓		
	DevLink 3							
	Location API							
HTTP	DECT R4 Provisioning						✓	
Web Services	Security Read All							✓
	Security Write All							✓
	Security Write Own Password							✓
	Config Read All							✓
	Config Write All							✓
	Backup							✓
	Restore							✓
	Upgrade							✓
External	Voicemail Pro Basic							
	Voicemail Pro Standard							
	Voicemail Pro Administrator							✓
	one-X Portal for IP Office Administrator							

Página3008 de 3226.

Service	Rights Group > Access Right V	Administrator Group	Manager Group	Operator Group	System Status Application Group	TCPA Group	IPDECT Group	SMGR Admin
	one-X Portal for IP Office Super User							
	Web Control Administrator							
	Web Control Security							
	WebRTC Administrator							

Service	Rights Group > Access Right V	Security Admin	Backup Admin	Upgrade Admin	System Admin	Maint Admin	Business Partner	Customer Admin	Maintainer
Configuration	Read all configuration				✓	✓	✓		✓
	Write all configuration				✓	✓	✓		
	Merge configuration				✓	✓	✓		
	Default configuration						✓		
	Reboot/Shutdown immediately						✓		
	Reboot when free						✓		
	Reboot at time of day						✓		
Security Admin	Read all security settings	✓					✓		
	Write all security settings	✓					✓		
	Reset all security settings	✓					✓		
	Write own service user password	✓					✓		
System Status Application	System Status Application Access						✓		✓
	Read all configuration						✓		✓
	System Control						✓		✓
	Sys Monitor						✓		✓
Telephony APIs	Enhanced TSPI Access								
	DevLink 3								
	Location API								
HTTP	DECT R4 Provisioning								
Web Services	Security Read All	✓					✓		
	Security Write All	✓					✓		
	Security Write Own Password	✓			✓		✓	✓	
	Config Read All				✓		✓	✓	
	Config Write All				✓		✓	✓	
	Backup		✓			✓	✓	✓	✓
	Restore		✓			✓	✓	✓	✓

Página3009 de 3226.

Service	Rights Group > Access Right V	Security Admin	Backup Admin	Upgrade Admin	System Admin	Maint Admin	Business Partner	Customer Admin	Maintainer
	Upgrade			✓		✓	✓	✓	✓
External	Voicemail Pro Basic								✓
	Voicemail Pro Standard				✓	✓		✓	
	Voicemail Pro Administrator						✓		
	one-X Portal for IP Office Administrator				✓	✓	✓	✓	
	one-X Portal for IP Office Super User		✓						✓
	Web Control Administrator						✓		✓
	Web Control Security	✓					✓		
	WebRTC Administrator								

Table 10: Default Rights Group Assignments

4.2 Security Settings on Upgrade

When the IP Office system is upgraded and new rights groups or services added, existing users will only be granted the new rights if the Service Users' accounts are at default. This prevents unexpected changes of rights on upgrade. If access to these new rights or services are required, they must be added manually after the upgrade process has been completed.

Chapter 5.

Password and PIN Management

5. Password and PIN Management

In general, password and PIN resistance to Guessing (attacks using default passwords, dictionary words, or brute force) and Cracking (attacks that attempt to match the login calculation without needing to know the actual password) can be greatly improved by 'strong' passwords and a password change policy.

A strong password is typically one that:

- Is long (for example at least 8 characters)
- Complex (for example contains upper, lower and numeric characters)
- Does not contain sequences or repeated characters
- Is not easily guessable. Guessable passwords include:
  - Password same as account name or extension number (or reversed)
  - Dictionary words
  - Dictionary words with number substitution
  - Backwards words
  - Personal or corporate information
  - Date of birth
  - Default passwords

A strong PIN/Login Code is typically one that:

- Is long. A 13 digit PIN is similar in strength to an 8 character case-sensitive password
- Does not contain sequences or repeated digits
- Does not contain keypad sequences (for example 2580)
- Is not easily guessable. Guessable PINs include:
  - PIN same as extension number (or reversed)
  - Personal or corporate information
  - Date, prevalent when 4, 6 or 8 digit minimum length is enforced
  - Default login codes

Password and PIN strength and management is not covered in detail here, but many publications exist including:

- **NIST Special Publication (SP) 800-118, Guide to Enterprise Password Management (Draft):** ttp://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
- **Centre for the Protection of National Infrastructure (CPNI), PROTECTING SYSTEMS AND DATA, PASSWORD ADVICE** http://www.cpni.gov.uk/documents/publications/2012/2012029-password_advice.pdf
- **US-CERT Security Tip (ST04-002), Choosing and Protecting Passwords:** https://www.us-cert.gov/ncas/tips/ST04-002

5.1 Password and PIN Policy

On a new installation of IP Office, when you ignite a Linux server or first login to Manager or IP Office Web Manager, you are required change the three system account passwords: Administrator, Security Administrator and system password.

Both Service and IP Office User password policy is configured in the **Security Settings | General** tab of IP Office Manager. The policy settings include:

- Service user minimum name and password length
- Service user minimum password complexity
- Number of consecutive failure attempts and the subsequent action; nothing, log, temporary disable, permanent disable
- Ensure no previous passwords are reused
- Enforced password change – both immediate and periodic
- Idle account timeout
- Separate set of IP Office User policy settings to allow differentiation

PINs are used on IP Office for telephony user login (Login Code), VoIP extension registration (Phone Password) and voice mailbox access (Voicemail Login Code). The policy is configured using **System | Voicemail | Voicemail Code Complexity** and **System | Telephony | Login Code Complexity**:

- Minimum login code & extension registration length
- Minimum login code & extension registration complexity
- Minimum voicemail code length
- Minimum voicemail code complexity

Página3014 de 3226.

5.2 Administrative User Passwords

There are various accounts used for administrative, maintenance and machine/service access. The following tables cover those interfaces, their password attributes, and where the account settings are located:

Login Interface	Account Settings	Notes
• **Manager** • **Server Edition Manager** • **IP Office Web Manager** • **System Status Application (SSA)** • **Web Control** • **Voicemail Pro client** • **System Monitor***	Service User name and password. Various rights of access Password: 1-31 Unicode characters	Change using Manager in security settings mode or Web Security Manager Security settings for Service User password policy apply Temporary or permanent lock out upon number of consecutive failed attempts. Current lockout status can be viewed in Manager under Security | Service Users | Service User Details *System Monitor will use this account when the **Security | System | Unsecured Interfaces | Use Service User Credentials** is active
• **Manager upgrade**	System password Password: 1-31 ASCII printable characters	Change using Manager in security settings mode
• **System Monitor*** • **DevLink**	System Monitor password Password: 1-31 ASCII 0-9, a-z, A-Z characters	Change using Manager in security settings mode *System Monitor will use this password when the **Security | System | Unsecured Interfaces | Use Service User Credentials** is inactive
• **Voicemail Pro client**	Three admin roles: - Administrator - Standard - Basic Password: 5-31 ASCII printable characters except \ / : * ? < > | , ;.	Change using VMPro client, Voicemail Pro Administrators tab Used for Voicemail Pro as a fallback account when IP Office Referred Authentication is not available.
• **Contact Recorder**	Two admin roles: - System Admin - Restricted Admin Password: 1-99 Unicode characters except space	Change using Contact Recorder web admin page, system tab
• **one-X Portal for IP Office admin**	Two admin roles: - Administrator - Backup/restore Password: 1-31 Unicode characters	Change using one-X Portal for IP Office admin web page, **Configuration | Users** panel. Used for one-X Portal for IP Office as a fall-back when IP Office Referred Authentication is not available
• **Linux Secure Shell (SSH)**	One admin role: 'Administrator' Password: 1-31 ASCII printable characters	Change using Web Control login screen Can only change password
• **Linux Console interface (CLI)**	Two admin roles: - Administrator - root Password: 1-31 ASCII printable characters	Change using Web Control login screen Change using Web Control, **Settings | System** tab Can only change passwords
• **VMPro <-> IP Office service interface**	VMPro password Password: 31 ASCII printable characters	Change using Manager in security settings mode Change using VMPro client, **System Preferences | General** tab.
• **one-X Portal for IP Office <-> IP Office service interface**	Service User name and password Password: 1-31 Unicode characters	Change using Manager in security settings mode or Web Security Manager. Change using one-X Portal for IP Office admin web page, **Configuration | Providers | Default-CSTA-Provider | Edit** panel

Página3015 de 3226.

Login Interface	Account Settings	Notes
• **TAPI Link Pro (3rd party TAPI)**	System password Password: 1-31 ASCII printable characters	Change using Manager in security settings mode TAPI Link Lite is covered in IP Office Users' Passwords and Login Codes 36 .
• **DECT R4 Provisioning**	Service User name and password Password: 1-31 Unicode characters	Change using Manager in security settings mode Change using base station web admin interface
• **DevLink3 API** • **Location API** • **Service Monitoring API** • **Web Management SDK API**	Service User name and password Password: 1-31 Unicode characters	Change using Manager in security settings mode

Table 11: Administrative User Passwords

5.3 IP Office User Passwords and Login Codes

The following table indicates which IP Office components use what password, voicemail PIN or login code when logging in to the various interfaces.

- Password is defined by the configuration field **User | User | Password** and typically used during application login.
- Voicemail code is defined by the configuration field **User | Voicemail | Voicemail Code** and used for mailbox login.
- Login code is defined by the configuration field **User | Telephony | Supervisor Settings | Login Code** and used for phone login. A new field in release 9.0+ allows VoIP phone login against the extension, not user record: **Extension | Extn | Phone Password**.

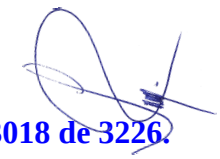
All passwords and login codes can be changed in IP Office and IP Office Web Manager.

Login Interface	Account Setting	Notes
• **SoftConsole** • **one-X Portal browser** • **one-X Mobile Preferred** • **Communicator Windows/iPad** • **IP Office Video Softphone** • **Outlook plugin, Call Assistant** • **Salesforce & Lync plugin** • **TAPI Link Lite (1st party TAPI)** • **RAS (dial in) Users** • **Web Self-Administration** • **Web Collaboration conference owner** • **Integrated Contact Reporter Agent/Supervisor** • **IP Office Web Client**	• Name: **User	User	Name** • Password: **User	User	Password** • Attributes: 0-31 ASCII 0-9, a-z, A-Z characters	Security settings for IP Office user password policy apply TAPI Link Pro and DevLink are covered in Administrative User Passwords 34. Temporary or permanent lock out upon number of consecutive failed attempts.
• **Voicemail Pro mailbox** • **Embedded Voicemail mailbox**	• User extension: **User	User	Extension** • Voicemail Code: **User	Voicemail	Voicemail Code** • Attributes: 0-15 ASCII digits	Voicemail settings for password/PIN policy apply: **System	Voicemail	Voicemail Code Complexity**. User's voicemail code input not required if accessing voicemail from a trusted extension.
• **IP Office User phone login**	• User extension: **User	User	Extension** • Login Code: **User	Telephony	Supervisor Settings	Login Code** • Attributes: 0-31 ASCII digits	System settings for password/PIN policy apply: **System	Telephony	Login Code Complexity**. Temporary lock out upon number of consecutive failed attempts.
• **H323 Phone registration** • **SIP Phone registration**	• Phone extension: **Extension	Extn	Base Extension** • Login Code: **User	Telephony	Supervisor Settings	Login Code** • Attributes: 0-31 ASCII digits	System settings for password/PIN policy apply: **System	Telephony	Login Code Complexity**. Temporary lock out upon number of consecutive failed attempts For R9.0+, H323 **Extension	Extn	Phone Password** field is used if set. Current lockout status can be viewed and reset in SSA under **System	VoIP Security	Blacklisted Extensions** and **Blacklisted Addresses**.

Table 12: User Passwords and Login Codes

Página3017 de 3226.

Chapter 6.
Certificates and Trust



6. Certificates and Trust

Digital certificates are used within the IP Office solution for a number of purposes:

- Signing firmware, applications and Java applets to assure their origin.
- Identifying IP Office to other systems, applications and users.
- Verifying the identity of other systems, applications and users.
- Setting up Transport Layer Security (TLS) links, including HTTPS and SIP.
- Incorporating IP Office into a wider trust domain.

Digital certificates are defined by the X509v3 format and have become the de facto standard for most security operations that involve identity verification. The identity of individuals, systems and applications can be asserted by a certificate with a 'public' key and its corresponding 'private' key. The public key is part of the certificate, along with other identity information and other digital security data.

For example, Avaya signs its applications with its private key and makes the corresponding certificate public. Anyone wishing to check the application, can take the certificate and use the public key to unlock the signature and verify:

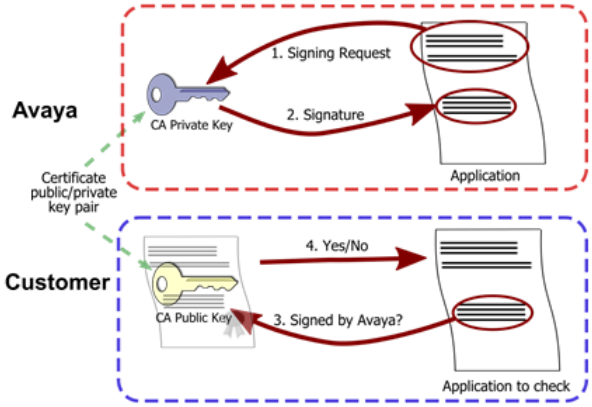


Figure 5: Avaya Application Key Checking

One point from the above example is that the private key must remain private; anyone with access to the key can masquerade as Avaya.

To ensure greater trust, a trusted party can sign the public key and the information about its owner. A trusted party that issues digital certificates is called a certification authority (CA), similar to a governmental agency that issues drivers' licenses. A CA can be an external certification service provider or a government, or the CA can belong to the same organization as the entities it serves. CAs can also issue certificates to other subordinate CAs, which creates a tree-like certificate trust called a Public-Key Infrastructure (PKI):

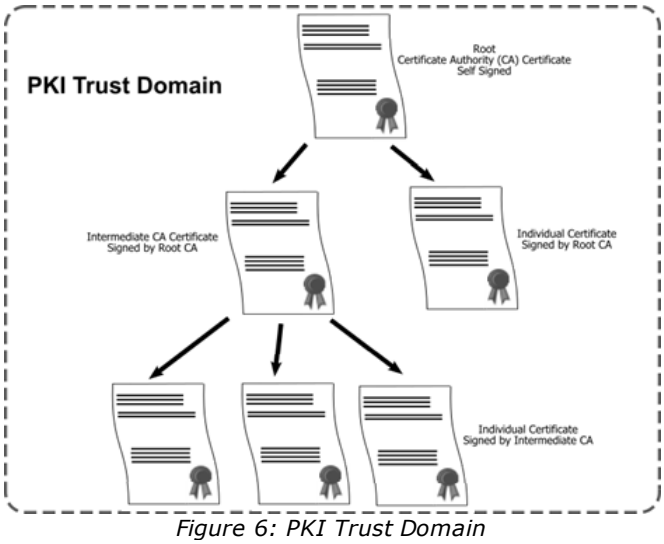


Figure 6: PKI Trust Domain

Página3019 de 3226.

6.1 Certificate Terminology

Throughout this document the following terms and definitions will be used in the context of certificates:

- **Certificate**
  A digital certificate containing identity information, a public key and other digital security data conforming to the X.509 v3 standard.
- **Certificate Authority (CA)**
  An entity that can issue identity certificates signed by another certificate.
- **Root CA Certificate**
  A 'self-signed' certificate (that is, A certificate that has been signed by itself) representing the certificate authority's root of the certificate hierarchy whose private key can be used for signing other certificates. Most operating systems and browsers ship with many root CA Certificates from public authorities that are trusted by default.
- **Intermediate CA Certificate**
  A certificate which has been created by signed by a CA for the purpose of signing other certificates.
- **Identity Certificate**
  A certificate used to represent an entity's identity. To be used as an identity certificate the associated private key must also be present.
- **Trusted Certificate**
  A certificate that is trusted by an entity.
- **Trust Store (Trusted Certificate Store/TCS)**
  A store of trusted certificates.
- **Trusted Root/Trust Anchor**
  The top level certificate that is trusted by an entity.
- **Certificate Chain**
  A list of certificates, starting with the Identity Certificate followed by one or more CA certificates (usually the last one being Root CA certificate) where each certificate in the chain is signed by the subsequent certificate.
- **Trust domain**
  A single PKI trust structure, for example, an 'island of authority'.
- **Server Authentication**
  The checking of a server's certificate by a client.
- **Mutual Authentication**
  The checking of a client's certificate by a server.
- **Certificate Identity Verification**
  The source of the certificate (IP address, URL, etc.) is checked against the contents of the certificate's Name and Subject Alternative Name fields.
- **Single Domain Certificate**
  A certificate created for a single server with just one name field/domain (that is, one identity).
- **Multi Domain Certificate** (also called **'Multi-SAN'** or **'Unified Communications'** certificate)
  A certificate created for a single server with many domains/identities, each identity is one name entry.
- **Wildcard Certificate**
  A certificate created for a multiple servers or a single server with many domains/identities. The name entry is of the form '*.example.com'. Wildcard certificates carry additional security risks and limitations. See Certificate Name Content 50.

6.1.1 Components of a Certificate

Certificates are made up of a number of fields some mandatory and some optional:

- **Version**
  Usually V3 – indicating X.509 v3 format
- **Serial Number**
  A unique number used to uniquely identify the certificate. There is no requirement that the number is actually serialised, just that it's unique.
- **Subject** (AKA **Issued to**)
  The entity (person, system etc.) identified by the certificate. This is divided into a number of sub fields: Common Name (CN), Organisation Unit (OU), email, etc. Typically the CN is referred to as the 'Name' of the certificate.
- **Subject Alternative Name**
  Alternative names by which the entity can be identified. These entries are often tested to assure the recipient the source of the certificate. For example the IP Address of the remote server should match one of the names in this field.
- **Issuer:** (AKA **Issued by**)
  The CA entity that verified the information and issued the certificate. This is also divided into a number of sub fields like Subject.
- **Valid From**
  The UTC time/date the certificate is first valid from.
- **Valid To**
  The expiration time/date.
- **Key Usage**
  Purpose for which the public key can be used (for example, certificate signing, encryption, etc.).
- **Signature Algorithm**
  The cryptographic algorithm used to create the signature.
- **Signature**
  The signature data to verify that it came from the issuer. Encrypted with the issuer's private key, can be decrypted with the issuer's public key found in the issuer's certificate.
- **Public Key Algorithm**
  The public key type (for example, RSA, DSA etc.).
- **Public Key**
  The public key.

There are other fields that may be present, see RFC5280 for more information.

6.1.2 Certificate Security

The size of the public key and the thumbprint algorithm used determine in part how resistant the certificate is to being compromised. Many government bodies now determine that certificates with MD5 and SHA-1 thumbprint algorithms, or public keys of less than 2048 bits are not secure.

6.1.3 Certificate Checks

When a certificate is received with a view to verifying identity, a number of tests and checks can be carried out:

- The certificate is assessed for basic validity such as integrity, start/end date, usage information, strength of public key, etc.
- The subject of the received certificate and any alternative names are verified against the source of the certificate; for example the IP address or the domain name. This is termed 'Certificate Identity Verification'.
- The Issuer is extracted and the Trusted Certificate Store (TCS) searched for a certificate that matches. When found the received certificate's signature is checked using the public key of the trusted certificate. This is repeated until a trusted Root CA certificate is found.
- If revocation information present in the Root CA certificate, the received certificate is checked with the CA to see if it has been revoked (that is, certificate has be cancelled or withdrawn by the authority).

Due to the variety of implementations, certificate content, configurable setting and heritage, many systems and applications differ greatly in their application of such tests.

6.1.4 Certificates and the Transport Layer Security (TLS) Protocol

Certificates are used by TLS in a number of ways:

- Exchanging the keys used for the symmetric encryption at the beginning of the session.
- Verifying the identity of the TLS server
- Verifying the identity of the TLS client

Due to the way TLS works, the server must always have a certificate else the TLS session cannot start, and that certificate is always presented to the client. In order to obtain the client's certificate, the server must explicitly request it.

Typically the identity verification of both client and server is configurable, along with the exact set of checks carried out on the received certificate(s). Without such checks TLS can be susceptible to man-in-the-middle attacks.

The IP Office platform supports TLS v1.0, v1.1 and v1.2. All TLS interfaces start with TLS v1.2 but can allow negotiation down to v1.1 or v1.0 for compatibility. There are IP Office, Voicemail Pro, IP Office Web Manager and one-X Portal for IP Office admin settings for 'Minimum TLS version' that enforce v1.2. Note that some Avaya clients do not support v1.2 at present. See Appendix F – IP Office VoIP Endpoint Security 127.

6.1.5 Certificate File Naming and Format

Like so many other aspects of certificates, there are various options and standards (both formal and informal) associated with certificate files.

File Formats

There are four main encodings/internal formats for certificate files. Note these are encodings, not file naming conventions:

Format	Description
DER	Distinguished Encoding Rules (DER) format, which is a binary format used to represent a certificate. Typically used to describe just one certificate, and cannot include a private key.
PEM	Privacy Enhanced Mail (PEM) is a Base 64 (that is, ASCII text) encoding of DER, one certificate is enclosed between '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' statements. Can contain a private key enclosed between '-----BEGIN PRIVATE KEY -----' and '-----END BEGIN PRIVATE KEY -----' statements. More than one certificate can be included. PEM be identified by viewing the file in a text editor. • This is an unsecure format and not recommended for private key use unless it is protected with a password.
PKCS#12	Public Key Cryptography Standard (PKCS) #12. A secure, binary format, encrypted with a password. Typically used to describe one certificate, and its associated private key, but can also include other certificates such as the signing certificate(s). This is the recommended format for private key use.
PKCS#7	A Base 64 (that is, ASCII text) encoding defined by RFC 2315, one or more certificates are enclosed between '—–BEGIN PKCS—–' & '—–END PKCS7—–' statements. It can contain only Certificates & Chain certificates but not the private key. Can be identified by viewing the file in a text editor.

Table 13: Certificate File Formats

Filename Extensions

There are many common filename extensions in use:

Extension	Description
.CRT	Can be DER or PEM. Typical extension used by Unix/Android systems' public certificates files in DER format.
.CER	Can be DER or PEM. Typical extension used by Microsoft/Java systems' public certificates files in PEM format.
.PEM	Should only be PEM encoded
.DER	Should only be DER encoded
.p12	Should only be in PKCS#12 format. Typical extension used by Unix/Android systems' identity certificates/private key pair files. Same format as .pfx hence can be simply renamed.
.pfx	Should only be in PKCS#12 format. Typical extension used by Microsoft systems' identity certificates/private key pair files. Same format as .p12 hence can be simply renamed.
.pb7	Should only be in RFC 2315 format. Typical extension used by Microsoft and Java systems for certificate chains.

Table 14: Certifictate Filename Extensions

3rd party tools such as OpenSSL and the Windows Management Console Certificate snap-in can be used to convert between the various formats, care should be taken not to expose any private key. See Creating a CSR using the Linux Server Command Line 146 for information on OpenSSL format conversion.

6.2 IP Office Certificate Support

The IP Office platform supports certificates in a number of ways, most of which are configurable via the security settings:

- An identity certificate for each system and their local applications, including an optional separate identity certificate for management and telephony interfaces.
- Unique identity certificate self-generated by all systems when required.
- Identity certificate can be administered via IP Office Manager or IP Office Web Manager, or obtained automatically using the Simple Certificate Enrollment Protocol (SCEP) or PKCS#10 (IP Office Linux only).
- DER and PEM for certificate file import/export, and PKCS#12 for certificate/private key pair import/export.
- A Certificate Authority on the Primary and Linux Linux Application Server including Subject Alternative Name support.
- The certificate processing can support 1024, 2048 and 4096 bit public RSA keys, and SHA-1, SHA-256, SHA-224 and SHA-512 hashes.
- A Trusted Certificate Store (TCS) of 64 entries minimum.
- Configurable default TCS content, restored on security settings reset.
- Individual per-service controls to enforce mutual certificate authentication where the client's certificate is requested and tested.
- Separate management and telephony received certificate check levels that provide increasingly rigorous tests. This includes a 'high' setting that tests not only the trust chain but also the presence of the received certificate in the TCS.
- Intermediate CA certificate support, both for the CAs and the identity certificate chain offered by IP Office and its applications.
- Errors, alarms and warnings to help identify certificate issues.

Currently IP Office certificate support does not include the following:

- Linux Applications (including one-X Portal for IP Office, Voicemail Pro and Contact Recorder) cannot be configured for mutual authentication. that is, they cannot check any received certificate against the TCS.
- SIP clients' certificates are not requested.
- The received certificate tests of IP Office do not include revocation checks such as OCSP or CRLs.
- The received certificate tests of IP Office do not include assuring the source of the certificate using Subject Alternative Name entries. that is, Certificate identity verification.
- No support for DSA or EC-DSA public key certificates, or RSA public keys above 4096 bits. It is recommended to use RSA public keys of 2048 bits.
    - The IP500 V2 servers does not support the manual generation of a Certificate Signing Request (CSR) where the private key is retained within the server. Either a web form based request or a 3rd party tool to create a CSR can be used. See Certificate Signing Requests 134 for more information on how to generate a CSR for IP Office.

6.2.1 Interface Certificate Support

Certificates are supported on all IP Office TLS and SSH interfaces including HTTPS, whether client or server.

- **Note:** SSLv2 and SSLv3 are not supported by IP Office.

For information about basic TLS functionality, see Certificates and the Transport Layer Security (TLS) 41.

There are a number of IP Office settings that affect certificate operation

The table in IP Office Interface Certificate Support 123 lists all TLS links in the IP Office platform solution and their security capabilities including certificate support.

The table in IP Office VoIP Endpoint Security 127 lists VoIP clients in the IP Office platform solution and their security capabilities.

6.2.2 Initial Certificate Settings

- **Interface Certificate Support** 44
- **Certificate Name Content** 50
- **Certificate Check Controls** 52
- **Certificate Distribution** 53
- **Determining Trust Policy** 56
- **IP Office PKI Trust Approaches** 57
- **Selecting IP Office PKI** 59
- **Implementing IP Office PKI** 59
- **Certificates from External Certificate Authorities** 62
- **Certificate Maintenance** 64

6.2.2.1 IP500 V2 Initial Certificate Settings

IP500 V2 will always create a unique self-signed CA certificate upon initial start-up and on security settings reset. It will contain the certificate fields listed below.

This certificate can be used for PKI operations in a limited manner; it has some security value, but is not part of a wider PKI and hence not trusted by anything else unless this certificate is installed in the relevant TCS.

Certificate Field	Contents	Notes
Version	V3	Always X.509 V3 format
Serial Number	Large random number	Ensures serial number unique Not more than 20 bytes
Subject (Issued To)	CN = ipoffice-nnnnnnnnnn.avaya.com O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Where *nnnnnnnnnn* is the LAN 1 mac address, for example *ipoffice-00e00705918e.avaya.com*
Subject Alternative Name(s)	1: DNS Name=ipoffice-nnnnnnnnnn.avaya.com 2: IP Address=a.b.c.d 3: IP Address=e.f.g.h	Where: - nnnnnnnnnn is the LAN 1 mac address - a.b.c.d is the LAN 1 IP address at the time of certificate creation - e.f.g.h is the LAN 2 IP address at the time of certificate creation
Issuer (Issued by)	CN = ipoffice-nnnnnnnnnn.avaya.com O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Same content as Subject: Self-signed certificate
Valid From	DD/MM/YY HH:MM:SS	Will reflect the UTC time/date minus 24 hours when the certificate was created. If the real time clock was corrupt/not set, the time will be fixed to 00:00:00 1st January of the year the software was released.
Valid To	Valid From plus 825 days	
Key Usage	keyAgreement keyEncipherment digitalSignature, nonRepudiation, dataEncipherment keyCertSign	Marked non-critical The certificate can be used for the set of IP Office certificate operations
Extended Key Usage	id-kp-serverAuth id-kp-clientAuth	Marked non-critical The certificate can be used for the set of IP Office certificate operations
Basic Constraints	cA: true pathLenConstraint: 0	Marked critical The certificate can be used in isolation as a CA, no other certificates may be signed by this one
Signature Algorithm	sha256RSA	
Signature	Signature data	
Public Key Algorithm	RSA	
Public Key	Size 2048 bits	

Table 15: IP500 V2 Initial Certificate Settings

Note

1. The correct LAN 1 and LAN 2 address should be set during initial installation and the identity certificate manually regenerated.

Página3026 de 3226.

6.2.2.2 Linux Servers Prior to Ignition

The Unified Communications Module and default Server Edition distributions before ignition has completed do not have a unique certificate. In order to connect a browser to ignite, this certificate requires to be temporarily accepted. It should never be stored permanently. It is self-signed and contains a subject and issuer of *'ipoffice-default.avaya.com'*.

Once ignition has completed, it is replaced by the relevant identity certificate according to the resultant server type.

6.2.2.3 Server Edition Primary/Linux Application Server Initial Certificate Settings

The Primary and Linux Application Server have an inbuilt certificate authority. During the ignition process the installer can chose to keep the default CA root certificate used for signing, or import another as a public/private key pair. This imported certificate can either be a root CA or an intermediate CA.

If the internal CA is retained, it has the contents listed below.

Certificate Field	Contents	Notes
Version	V3	Always X.509 V3 format
Serial Number	Large random number	Ensures serial number unique Not more than 20 bytes

Subject (Issued To)	CN = ipoffice-root-SubjectName.avaya.com
	O = Avaya Inc
	OU = GCS
	L = Basking Ridge
	S = New Jersey
	C = US
	E = support@avaya.com
		Where *SubjectName* is the hostname configured during ignition as follows:
		• Use the IP Office Web Manager | Platform View | Settings | System | Network | Host Name field if it is set to something other than:
		  • localhost
		  • localhost.localdomain
		  • the installer default (mac address)
		• If Hostname not used, use a DNS resolution of LAN1 if not then LAN2.
		• If Hostname not used and no successful DNS resolution, use the default name of 'Eth0 mac' for example, 'ipoffice-root-00e007057307.avaya.com'
		• The correct hostname should be set during ignition, if not the root CA certificate will need to be regenerated.

Subject Alternative Name(s)	1: DNS Name= ipoffice-root-hostname.avaya.com	A copy of the Subject CN
Issuer (Issued by)	CN = ipoffice-root-hostname.avaya.com O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Same content as Subject: Self-signed certificate
Valid From	DD/MM/YY HH:MM:SS	Will reflect the UTC time/date minus 24 hours when the certificate was created. If the real time clock was corrupt/not set, the time will be fixed to 00:00:00 1st January of the year the software was released.
Valid To	Valid From plus 10 years	
Key Usage	digitalSignature keyCertSign cRLSign off-line cRLSign	Marked non-critical The certificate can be used for the set of IP Office certificate operations
Extended Key Usage		Not present
Basic Constraints	cA: true pathLenConstraint: 1	Marked critical The CA certificate may sign further identity or intermediate CA certificates
Subject Key Identifier	Key Identifier	This value is placed in the Authority Key Identifier of any signed certificates
Signature Algorithm	sha256RSA	
Signature	Signature data	
Public Key Algorithm	RSA	
Public Key	Size 2048 bits	

Table 16: Default Primary CA Certificate

Página3028 de 3226.

Also as part of ignition, an identity certificate is created signed by the internal CA with the properties listed below.

Certificate Field	Contents	Notes
Version	V3	Always X.509 V3 format
Serial Number	Large random number	Ensures serial number unique Not more than 20 bytes

Subject (Issued To)	CN = SubjectName
	O = Avaya Inc
	OU = GCS
	L = Basking Ridge
	S = New Jersey
	C = US
	E = support@avaya.com
		Where *SubjectName* is the hostname configured during ignition as follows:
		• Use the IP Office Web Manager | Platform View | Settings | System | Network | Host Name field if it is set to something other than:
		  ○ localhost
		  ○ localhost.localdomain
		  ○ the installer default (mac address)
		• If Hostname not used, use a DNS resolution of LAN1 if not then LAN2.
		• If Hostname not used and no successful DNS resolution, use the default name of 'Eth0 mac' for example, 'ipoffice-root-00e007057307.avaya.com'
		• The correct hostname should be set during ignition, if not the root CA certificate will need to be regenerated.

Subject Alternative Name(s)	1: DNS Name= SubjectName 2: IP Address=a.b.c.d 3: IP Address=e.f.g.h	Where: - DN is the hostname configured during ignition - a.b.c.d is the LAN 1 IP address at the time of certificate creation - e.f.g.h is the LAN 2 IP address at the time of certificate creation (if present) See Note 1.
Issuer (Issued by)	CA certificate subject fields	Certificate signed by the internal CA
Valid From	DD/MM/YY HH:MM:SS	Will reflect the UTC time/date minus 24 hours when the certificate was created. If the real time clock was corrupt/not set, the time will be fixed to 00:00:00 1st January of the year the software was released.
Valid To	Valid From plus 825 days	
Key Usage	keyAgreement keyEncipherment digitalSignature, nonRepudiation, dataEncipherment	Marked non-critical The certificate can be used for the set of IP Office certificate operations
Extended Key Usage	id-kp-serverAuth id-kp-clientAuth	Marked non-critical The certificate can be used for the set of IP Office certificate operations
Basic Constraints	subjectType: endEntity pathLenConstraint: 0	Marked critical Indicates Identity certificate
Authority Key Identifier	Key Identifier	Matches the Subject Key Identifier field of the CA certificate
Signature Algorithm	sha256RSA	
Signature	Signature data	
Public Key Algorithm	RSA	
Public Key	Size 2048 bits	

Table 17: Default Primary Identity Certificate

Note 1:

- The correct LAN 1 and LAN 2 address should be set during ignition, if not the identity certificate will need to be regenerated.
- Identity certificate regeneration is done automatically if the IP Office Web Manager | Platform View | Settings | General | Certificates | Renew automatically setting is active (default).

Página3029 de 3226.

6.2.2.4 Server Edition Secondary/Linux Expansion Initial Certificate Settings

The Secondary Server and Linux Expansion do not have an inbuilt certificate authority. The ignition process creates a unique self-signed identity certificate with the properties listed below.

This identity certificate has limited value and should be replaced by one generated by the Primary Server or other external CA.

Certificate Field	Contents	Notes
Version	V3	Always X.509 V3 format
Serial Number	Large random number	Ensures serial number unique Not more than 20 bytes

Subject (Issued To)	CN = SubjectName
	O = Avaya Inc
	OU = GCS
	L = Basking Ridge
	S = New Jersey
	C = US
	E = support@avaya.com
		Where *SubjectName* is the hostname configured during ignition as follows:
		• Use the IP Office Web Manager | Platform View | Settings | System | Network | Host Name field if it is set to something other than:
		  ○ localhost
		  ○ localhost.localdomain
		  ○ the installer default (mac address)
		• If Hostname not used, use a DNS resolution of LAN1 if not then LAN2.
		• If Hostname not used and no successful DNS resolution, use the default name of 'Eth0 mac' for example, 'ipoffice-root-00e007057307.avaya.com'
		• The correct hostname should be set during ignition, if not the root CA certificate will need to be regenerated.

Subject Alternative Name(s)		None
Issuer (Issued by)	CN = SubjectName O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Same content as Subject: Self-signed certificate
Valid From	DD/MM/YY HH:MM:SS	Will reflect the UTC time/date minus 24 hours when the certificate was created. If the real time clock was corrupt/not set, the time will be fixed to 00:00:00 1st January of the year the software was released.
Valid To	Valid From plus 7 years	
Key Usage		None
Extended Key Usage		None
Basic Constraints		None
Signature Algorithm	sha256RSA	
Signature	Signature data	
Public Key Algorithm	RSA	
Public Key	Size 2048 bits	

Table 18: Default Secondary/Expansion Certificate

Página3030 de 3226.

6.2.3 Certificate Name Content

The certificate fields **Subject Name** (Common Name field) and **Subject Alternative Name** have particular significance to IP Office and its various clients.

Although IP Office does not process the Subject Alternative Name (SAN) field itself, specific content is required for SIP endpoints and other clients, typically as verification of the certificate's source. See IP Office VoIP Endpoint Security 127 for more Avaya client information.

When requesting or creating identity certificates for IP Office systems, all connected systems that process the received IP Office certificate should be reviewed for their Name and SAN requirements. This should also include any possible future systems connected within the lifetime of the certificate. If in doubt, all possible name entries should be included.

Typical considerations include:

- **System FQDN as the Subject Name**
  The system's Fully Qualified Domain Name (FQDN) for the Subject Name. If there is no relevant domain name, a meaningful and unique text name for the system should be used as this field can be displayed to users. The Name field should never be empty. **Example:** *example.com*
- **System FQDN as a SAN DNS Entry**
  The system's Fully Qualified Domain Name (FQDN) as one SAN entry in DNS format. This should always be present if any other SAN entries are required. This entry is typically used by web browsers and other clients when accessing IP Office using DNS resolution. When used by SIP endpoints, starting in IP Office release 10.0, this entry typically should have the value configured in Manager | LANx | VoIP | SIP Registrar | SIP Registrar FQDN. **Example:** *DNS:example.com*
- **Other Domain Names and FQDNs as SAN DNS Entries**
  Any other domain name or FQDN of the system as one SAN entry in DNS format. This entry is typically used when the system can be accessed using 'split' DNS. **Example:** *DNS:ipoffice.example.com*
- **SIP Domains as SAN DNS Entries**
  Any SIP domains in use as one SAN entry for each SIP domain, in DNS format. This is typically the value configured in Manager | LANx | VoIP | SIP Registrar | SIP Registrar FQDN. This entry is typically used by SIP endpoints, such as the H175, which verifies the server certificate against the SIP Domain it is registering to. **Example:** *DNS:sip.example.com*
- **SIP Domains as SAN DNS SIP Entries**
  Any SIP domains in use as one SAN entry for each SIP domain, in URI format. This is typically the value configured in Manager | LANx | VoIP | SIP Registrar | SIP Registrar FQDN. This entry is typically used by SIP endpoints when accessing IP Office using DNS resolution. **Example:** *URI:sip:sip.example.com*
- **LAN1 IP Address as a SAN IP Entry**
  The IP Address of LAN 1 as one SAN entry in IP format. This entry is typically used by web browsers and other clients when accessing IP Office using the LAN 1 IP Address. Example: IP:192.168.42.1 IP Address fields are not supported by many public Certificate Authorities. See the notes below.
- **LAN2 IP Address as a SAN IP Entry**
  The IP Address of LAN 2 as one SAN entry in IP format. This entry is typically used by web browsers and other clients when accessing IP Office using the LAN 2 IP Address. Example: IP:192.168.43.1 IP Address fields are not supported by many public Certificate Authorities. See the notes below.
- **NAT and Public IP Addresses as SAN IP Entries**
  Any NAT or public IP Address as one SAN entry in IP format. This entry is typically used by 96x1 H.323 phones in Cloud or Remote Worker deployments, web browsers and other clients when accessing IP Office using the external/public direct IP Address. Note that this entry is not added by default to identity certificates generated by the IP Office Primary Server CA. This entry is needed if phones or other clients are configured to connect to the IP Office's public IP address and not it's FQDN. Example: IP:135.11.53.53 IP Address fields are not supported by many public Certificate Authorities. See the notes below.
- **SIP IP Address as SAN URI Entries**
  Any SIP IP Address in use as one SAN entry for each SIP domain, in URI format. This entry is used by the Avaya E129 SIP endpoint when accessing IP Office using an IP Address. Example: URI:sip:135.11.53.53 IP Address fields are not supported by many public Certificate Authorities. See the notes below.
- **Wildcard Entries**
  Under certain circumstances, the use of 'wildcard' names might be considered. A wildcard name field contains an asterisk in the name (for example, '*.example.com') and covers all sub-domains. IP Office can support such fields in both Subject Name and SAN wildcard name fields, but carry additional security risks and limitations and hence are not recommended. See the notes below.

Certificate Name Content Notes:

- Public Certificate Authorities do not support IP address and private domains. DNS and public domains should be used for all clients if a public CA is to be used. Not using IP address can compromise the administration of 96xx and other endpoints. 11xx/12xx series phones do not support FQDNs and hence cannot be used with certificates provided by public Certificate Authorities.
- Wildcard certificates (or certificates with wildcard name fields) carry the following additional risks:
  - **Security:** If one server or sub-domain is compromised, all sub-domains may be compromised.
  - **Security:** If used for more than one server, private key may become exposed.
  - **Management:** If the wildcard certificate needs to be revoked, all sub-domains will need a new certificate.
  - **Compatibility:** Wildcard certificates may not work with all server-client configurations.
  - **Protection:** Wildcard Certificates are not protected by CA extended validation or warranty.
  - **Security:** They must not be used to secure more than one IP Office server in a deployment; each server must have a unique identity certificate.
- Wildcard certificates are not supported by Avaya SIP clients such as Equinox, Vantage or J1xx series.

IP500 V2 and Server Edition Primary/Linux Application Server support the creation of certificates with up to 8 SAN fields with the following options:

- **DNS** – used for hostname or FQDN
- **URL** – used for URLs and URIs
- **IP** – IP Address in v4 format
- **Email** – email address

These SAN fields can also be used for Certificate Signing Requests via SCEP.

See Initial Certificate Settings 44 for the default Name SAN fields added on initial certificate creation.

For many straightforward deployments only a single FQDN as the subject name is required, such as one-X Portal for IP Office and Voicemail Pro on Windows, Unified Communications Module or Linux Application Server where DNS always resolves itself to the same FQDN.

Other deployments where the identity of the system differs depending upon access (for example, LAN or WAN) or the use of SIP or H323 endpoints with secure signalling, SANs will typically be required.

6.2.4 Certificate Check Controls

There are three levels of received certificate checks performed by IP Office on supported interfaces; these apply to any certificate received from any remote TLS client or server.

- **Low**
  Only the received certificate is checked for validity (in date) and strength (public key >=1024 bits). This has no value in determining trust.
- **Medium**
  The received certificate is checked for validity (in date) and strength (public key >=1024 bits), then the TCS is searched for a complete trust chain to a root CA. This is typical of the way browsers check certificates. Note that these tests do not include Certificate Identity Checks using the Name and Subject Alternative Name fields.
- **High**
  This will not only perform Low and Medium checks, it will also check the public key >= 2048 bits, and that a copy of the received certificate is in the store. This allows a far smaller trust domain to be implemented where only individual certificates are accepted. This is a form of 'certificate pinning' and overcomes one of the limitations of the standard tree structure of PKI; every certificate issued by the root CA is always trusted.

See "*Administering Avaya IP Office™ Platform with Manager*" for a detailed list of checks performed.

The extended 'High' trust checks are activated with the settings:

- **Manager Security | System | Certificates | Received Certificate Checks (Telephony)** = ***High***
  Applies to all certificates received on the SIP-TLS interfaces
- **Manager Security | System | Certificates | Received Certificate Checks (Management)** = ***High***
  Applies to all certificates received on the Management TLS and HTTPS interfaces.
- **Manager Configuration | Line | Line | Security** = ***High***
  Applies to certificates received on that IP Office WebSocket Line, regardless of the management received certificate checks (WebSocket Lines use the IP Office HTTP/S server).

Mutual Authentication

Where IP Office acts as a TLS/HTTPS server, certain security settings activate a certificate request from the client. If no certificate is received the IP Office will reject the connection. If one is received, certificate checks will be applied. This is the main mechanism used to enforce trust checks by IP Office.

- **Note:** At present, IP Office never requests certificates from SIP or H323 endpoints connecting via TLS.

Mutual authentication is activated with the settings:

- **Manager Security | Services | Configuration | Service Security Level** = ***High***
  Applies to IP Office Manager configuration settings and Configuration Web Service (XO) DevConnect interfaces on port 50805.
- **Manager Security | Services | Security Administration | Service Security Level** = ***High***
  Applies to IP Office Manager security settings on port 50809.
- **Manager Security | Services | HTTP | Service Security Level** = ***High***
  Applies to HTTPS clients connecting to port 443 & 411, typically H323 phones, DECT R4, IP Office lines, Voicemail Pro, System Monitor, etc.
- **Manager Security | Services | Web Services | Service Security Level** = ***High***
  Applies to IP Office Web Manager interface on port 8443.
- **Manager Security | System | Certificates | Received Certificate Checks (Telephony)** = ***Low***, ***Medium*** or ***High***
  Applies to SIP and SM Lines on port 5061.
- **Manager Configuration | Line | Line | Security** = ***High***
  Applies to IP Office WebSocket Server Lines on port 443. This is separate to the **Security | Services | HTTP | Service Security Leve**l control.

See IP Office Interface Certificate Support 129 for more information.

6.2.5 Certificate Distribution

This section covers the processes of certificate distribution.

- Interface Certificate Support 44
- Initial Certificate Settings 44
- Certificate Name Content 50
- Certificate Check Controls 52
- Determining Trust Policy 56
- IP Office PKI Trust Approaches 57
- Selecting IP Office PKI 59
- Implementing IP Office PKI 59
- Certificates from External Certificate Authorities 62
- Certificate Maintenance 64

6.2.5.1 Identity Certificate Distribution

IP Office supports three main mechanisms to distribute identity certificates, the selection of which will depend upon the trust policy chosen. One unique identity certificate is required for each IP Office – two if a separate telephony trust domain is required.

Manual from an External CA

A Manual certificate Signing request (CSR) is created and sent to an external CA who verified the contents and creates an identity certificate signed by the CA.

Once the identity certificate/private key is obtained, Manager or IP Office Web Manager can be used to administer it on IP Office:

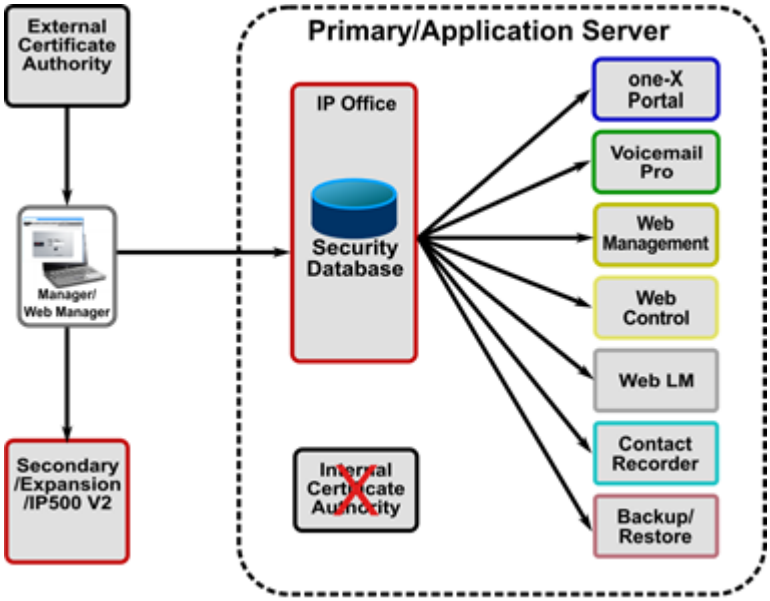


Figure 7: Cetrtification Distribution - External Certificate Authority

For more information on creation of a PKI based on an External CA, see Implementing IP Office PKI 59.

For more information on external Certificate Authorities, see Certificates from External Certificate Authorities 62.

Manual from the Primary or Linux Application Server

The internal certificate authority can be used to create a set of unique identity certificates in the secure PKCS#12 file format. The PKCS#12 file also includes the CA certificate.
These identity certificates can be utilized for any entity including IP Office, phones, Manager PCs etc. Once the identity certificate/private key file is saved to the local PC, Manager or IP Office Web Manager can be used to administer it on IP Office

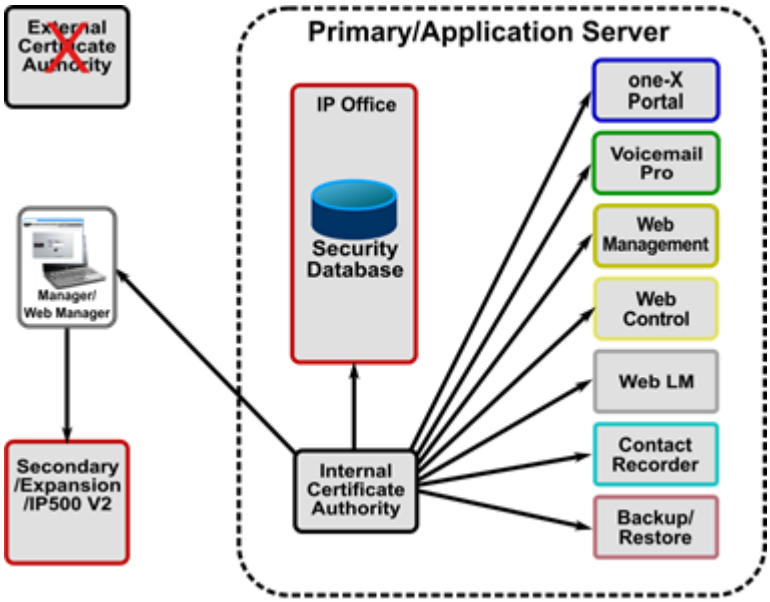


Figure 8: Certificate Distribution - Internal Certificate Authority

For more information on creation of a PKI based on an internal CA, see Implementing IP Office PKI 59.

Automatic using Simple Certificate Enrolment Protocol (SCEP)

Each IP Office is configured with the location of the SCEP server along with a password. The IP Office will periodically perform a CSR until it obtains its identity certificate. The private key is kept internally. The SCEP server must be administered to accept the signing request and issue the correct certificate.

As part of the enrollment process the CA certificate used to sign the SCEP request is placed into the TCS after which the IP Office will trust any other certificate signed by that CA. This is the mechanism used in IP Office branch deployments with System Manager (SMGR).

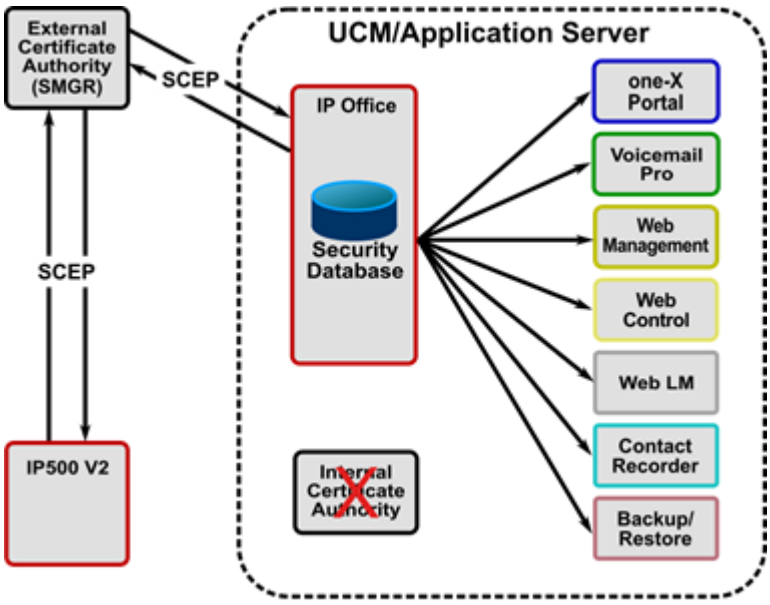


Figure 9: Certificate Distribution - Simple Certifcate Enrollment Protocol (SCEP)

In all cases (External CA, Internal CA, SCEP), when a new identity certificate is received by IP Office, all relevant interfaces/applications are updated.

For more information on creation of a PKI based on SCEP, see Implementing IP Office PKI 59.

Página3035 de 3226.

Manual Using a PKCS#10 CSR

A PKCS#10 certificate Signing request (CSR) is created on the IP Office Linux server via the command line interface (CLI). The private key is retained within the server. The CSR is sent to an external CA who verifies the contents and creates an identity certificate signed by the CA.

Once the identity certificate is returned the CLI is used to combine with private key and distributed with the server.

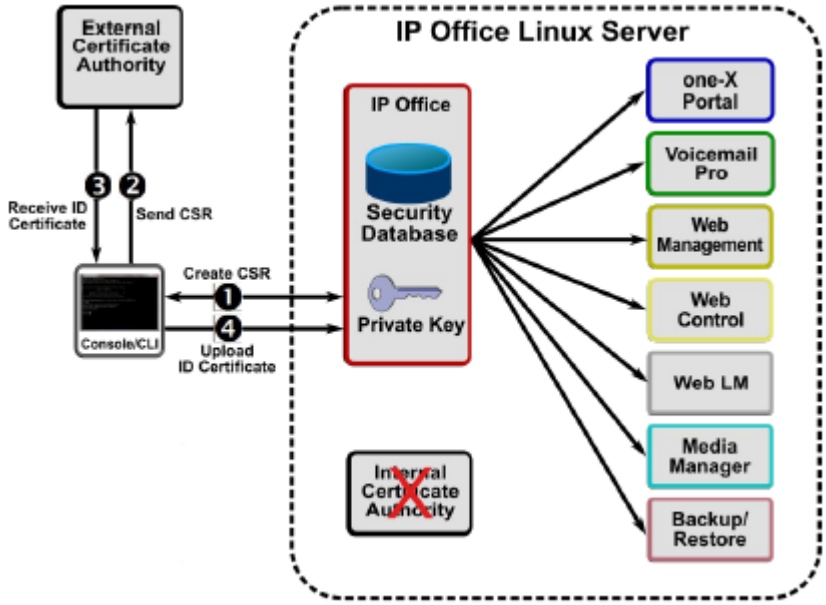


Figure 10: Certificate Distribution - External Certificate Authority

For more information on creation of a PKI based on an External CA, see Implementing IP Office PKI 59.

For more information on external Certificate Authorities, see Certificates from External Certificate Authorities 62.

6.2.5.2 Root CA Certificate Distribution

If the trust policy selected uses a well-known public CA (such as Verisign™), their root certificates are typically already installed in the relevant operating systems and browsers. However, IP Office does not have well-known public CA certificates in its TCS – these can be downloaded from the CA's web site and manually administered via Manager or IP Office Web Manager for each IP Office.

For more information on Root CA Certificate distribution, see Implementing IP Office PKI 59.

6.2.5.3 Intermediate CA Certificate Distribution

If the trust implementation additionally uses Intermediate CA certificate(s), the IP Office certificate chaining feature can be activated and the Intermediate CA(s) needs to be added to the TCS. This ID certificate chain is propagated to all local TLS interfaces.
This will remove the need to administer Intermediate CA certificates in the various clients' trusted certificate stores.

For more information on Intermediate CA Certificate distribution, see Implementing IP Office PKI 59.

6.2.6 Determining Trust Policy

With today's secure communication requirements, it is not possible to ignore the use of certificates to implement trust relationships, even if the identified needs are minimal. A trust policy must be selected and implemented before exposing IP Office services. This section provides some information to assist in the determination of such a policy; however it cannot provide definitive guidance or include outside factors.

Note: IP Office branch deployments have a specialized environment and requirements. See the documents:

- **Deploying Avaya IP Office Platform as an Enterprise Branch with Avaya Aura Session Manager**
  Document number 18-603853, https://downloads.avaya.com/css/P8/documents/101004861
- **Administering Centralized Users for an IP Office™ Platform Enterprise Branch**
  Document number 15-604263, https://downloads.avaya.com/css/P8/documents/101004857
- **Avaya IP Office Platform in a Branch Environment Reference Configuration**
  Document number 15-604253, https://downloads.avaya.com/css/P8/documents/101004855

When considering a trust policy for IP Office, the following questions can be considered:

- What international, national, corporate or other trust requirements exist?
- Is there an existing trust/PKI infrastructure that IP Office should be part of?
- Are IP Office services being exposed on public interfaces?
- Are IP Office platform components deployed on unsecure platforms or environments?
- Are IP Office clients/endpoints deployed on unsecure platforms or environments?
- What are the trust requirements for 3rd party systems that connect to IP Office?
- Is the ability to trust IP Office without administering certificates on clients/endpoints significant?
- Is there a need for a separate management and telephony trust domain?
- Which interfaces and services need to use trust checks and which do not?
- Does trust need to be one-way (for example, client checks sever), or both-way (for example, client and server check each other)?
- Is there a need to provide the extended trust checks of IP Office where all clients' certificates must be present in the TCS? This is useful when the PKI tree trust structure is insufficient.
- How many ID certificates are required? At least one unique certificate per IP Office server, two if a separate telephony trust domain is needed.
- How are certificates to be obtained, distributed and recovered?
- What certificate renewal and distribution methods should be supported?
- Is the CA able to provide the correct certificate content? For example Subject Alternative Name content

This list is by no means exhaustive, for further information see Assessing IP Office Security Requirements 76.

Página3037 de 3226.

6.2.7 IP Office PKI Trust Approaches

There are five main approaches that can be used with the IP Office Platform:

1. PKI Trust domain based on the Primary or Linux Application Server internal root CA.
2. PKI Trust domain based on the Primary or Linux Application Server internal Intermediate CA.
3. PKI Trust domain based on an external Certificate Authority.
4. PKI Trust domain based on an external Certificate Authority via SCEP.
5. No PKI trust domain.

Approach 1: PKI Trust Domain based on Primary or Linux Application Server root CA

This option allows identity certificates to be generated using the root CA certificate of the server.

Relative advantages include:

- Cost over a commercial CA.
- Control of the CA is internal.
- Certificate content format compatible with other Avaya components.
- The certificate policy is flexible and not subject to commercial considerations.
- The trust relationships do not extend outside of the deployment – that is, it remains a private domain.

Relative disadvantages include:

- The root CA certificate is untrusted by 3rd parties and other IP Office components and therefore needs to be distributed.
- The certificate creation and distribution process is manual.

Approach 2: PKI Trust domain based on Primary or Linux Application Server Intermediate CA

This option allows identity certificates to be generated on the Primary or Linux Application Server using an intermediate CA certificate obtained from an external Certificate Authority.

Potential advantages for intermediate CA certificate on the Primary/Linux Application Server:

- Generated ID certificates are part of a wider trust
- Control of the CA is internal.
- ID certificate content format compatible with other Avaya components.
- ID certificates with private domains and address ranges IP addresses can be created
- The root CA certificate is (typically) trusted by 3rd parties and therefore does not need to be distributed.

Potential disadvantages include:

- Cost - if using a commercial provider. Signing certificates are typically more expensive.
- The certificate policy is subject to commercial considerations.
- Many public certificate authorities will not issue intermediate CA certificates for private domains or IP address ranges.
- The root CA certificate is untrusted by IP Office components and therefore needs to be distributed.
- The certificate creation and distribution process is manual.
- All clients need to support certificate chains in the TLS exchange; if not the intermediate CA certificate needs to be distributed.

Approach 3: PKI Trust Domain Based on an External Certificate Authority

This option allows identity certificates to be obtained direct from an external Certificate Authority using a manual process.

Potential advantages for identity certificates from an external CA:

- Useful for small deployments when no Primary or Linux Application Server exists.
- Generated ID certificates are part of wider trust domain.
- The root CA certificate is (typically) trusted by 3rd parties and therefore does not need to be distributed.

Potential disadvantages include:

- Public certificate authorities will not issue certificates for private domains or IP address ranges.
- Cost - if using a commercial provider.
- Control of the CA is external.
- The certificate policy is subject to commercial considerations.ID certificate content format may not be compatible with Avaya components.
- The root CA certificate is untrusted by IP Office components and therefore needs to be distributed.
- The certificate creation and distribution process is manual.

Approach 4: PKI Trust Domain Based on an External Certificate Authority via SCEP

This option allows identity certificates to be obtained direct from an external Certificate Authority using an automated process.

Potential advantages for identity certificates obtained using SCEP:

- Generated ID certificates are part of a wider trust domain.
- ID certificate content format compatible with Avaya components.
- The root CA certificate is (typically) trusted by 3rd parties and therefore does not need to be distributed.
- The root CA certificate is always trusted by IP Office components and therefore does not need to be distributed.
- The certificate creation and distribution process is automated, supporting many systems efficiently.

Potential disadvantages include:

- Compatibility with SECP servers is currently limited to EJBCA – the CA present on Avaya Aura System Manager (SMGR).
- Public certificate authorities will not issue certificates for private domains or address ranges.
- Cost - if using a commercial provider.
- Control of the CA is external.
- The certificate policy is subject to commercial considerations.

Approach 5: No Trust Domain

This can only be considered used where a single IP500 V2 or Primary Server has no external/public interfaces and is completely within a secure/closed environment.

Installation/Creation is achieved by retaining the default identity certificate.

No trust relationships are active, no certificates are checked.

PKI Maintenance will consist of renewing the identity certificate by deleting the existing using IP Office Manager or IP Office Web Manager; this will create a new certificate for the next 7 years. Any existing browser exceptions will need to be re-asserted.

6.2.8 Selecting IP Office PKI

Existing customer security policy may already define the necessary approach. Where this has not yet been defined, an assessment of requirements should help identify the appropriate option. The following guidance may be helpful:

- A deployment with external interfaces and many external clients would suggest an external, public Certificate Authority (Approach 3).
- A deployment with no external interfaces, or few external clients would suggest an internal Certificate Authority (Approach 1).
- A deployment that requires IP Addresses or private domain names in the certificate fields cannot use a public Certificate Authority, therefore Approach 1 may be suitable.
- A deployment that offers any service to the public should use an external, public Certificate Authority (Approach 3).
- A branch deployment with System Manager will typically use SCEP (Approach 4)

Although five approaches are outlined above, a mix may be appropriate; for example external, public CA for public facing servers, internal CA for all others. A hybrid approach cannot be used when VoIP endpoint resilience is active; the root CA for both home and backup server must be the same.

6.2.9 Implementing IP Office PKI

Once the trust policy has been determined, the implementation process will depend on the option selected:

Approach 1: PKI Trust Domain based on Primary or Linux Application Server root CA

1. The Primary Server CA should be used for Server Edition deployments. The Linux Application Server for non-Server Edition deployments. The same CA must be used for all systems in a deployment.
2. Enable the setting **Platform View | Settings | General | Certificates | Identity Certificates | Renew automatically** on the Primary/Linux Application Server.
3. For every device (server, IP 500V2 etc.) use the CA to create a unique ID certificate for each with the correct name content and save to a local directory. The name fields of the certificate are important for correct interoperation with clients; see Certificate Name Content 50 for more information. See Using the IP Office Certificate Authority 131.
4. Save the root CA certificate in both PEM and DER formats to a local directory using the IP Office Web Manager setting **Platform View | Settings | General | Certificates | CA Certificate | Download (PEM-Encoded)** and **Download (DER-Encoded)**.
5. Use IP Office Web Manager or IP Office Manager to save the CA certificate in each TCS.
6. Use IP Office Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See Update Certificates 80.
7. If SIP or H.323 phones are using HTTPS for provisioning or TLS for signalling, the IP Office root CA certificate must be present on each phone. See VoIP Security 68.
8. Distribute the root CA certificate to all clients and browsers. The mechanisms vary and some require PEM format, some require DER. See the relevant client and browser documentation.
9. Verify that the correct ID certificate has been applied on each device using a browser or other diagnostic tool.
10. Enable certificate checking in the IP Office security settings and IP Office lines.
11. Verify using SE Manager that all IP Office systems are online with no alarms.
12. Enable secure connections for clients.
13. Verify each client can connect successfully.
14. Ensure all ID certificate files are stored securely.
15. Once all checks have been carried out, a configuration backup should be taken.

Approach 2: PKI Trust Domain based on Primary or Linux Application Server Intermediate CA

1. The Primary Server CA should be used for Server Edition deployments. The Linux Application Server for non-Server Edition deployments. The same CA must be used for all systems in a deployment.
2. Enable the setting **Platform | Settings | General | Certificates | Identity Certificates | Renew automatically** on the Primary/Linux Application Server.
3. Select an appropriate Certificate Authority that can fulfil the trust and certificate requirement of the deployment. For more information on external public authorities, see Certificates from External Certificate Authorities 62.
4. Request an Intermediate CA certificate/private key pair from a trusted Certificate Authority in PCKS#12 format. An intermediate CA certificate differs in content to a root CA or a device identity certificate. For more information on external public authorities, see Certificates from External Certificate Authorities 62 .
5. Download the root CA certificate (and any further intermediate CA certificates) from the Certificate Authority in PEM and DER format to a local directory.
6. Install Intermediate CA certificate the on the Primary or Linux Application Server. This can either be done during ignition, or post ignition via the IP Office Web Manager setting **Platform View | Settings | General | Certificates | CA Certificate | Import**.
7. For every device (server, IP 500V2 etc.) use the CA to create a unique ID certificate for each with the correct name content and save to a local directory. The name fields of the certificate are important for correct interoperation with clients; see Certificate Name Content 50 for more information. See Using the IP Office Certificate Authority 131.
8. Save the intermediate CA certificate in both PEM and DER formats to a local directory using the IP Office Web Manager setting **Platform View | Settings | General | Certificates | CA Certificate | Download (PEM-Encoded)** and **Download (DER-Encoded)**.
9. Use IP Office Web Manager or IP Office Manager to:
   - Save both the root and intermediate CA certificate in the TCS, then
   - Activate the certificate chaining feature Offer ID Certificate Chain.
10. Use IP Office Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See Update Certificates 80.
11. Distribution of the root CA certificate to phones, clients and browsers is as per PKI Trust Domain based on Primary or Linux Application Server root CA section above.
12. Verification and enabling steps are as per PKI Trust Domain based on Primary or Linux Application Server root CA section above, with the note that many external CAs provide online verification tools.
13. Once all checks have been carried out, a configuration backup should be taken.

Approach 3: PKI Trust Domain based on an External Certificate Authority

1. The CA on the Primary or Linux Application Server is not used.
2. Enable the setting **Platform | Settings | General | Certificates | Identity Certificates | Renew automatically**.
3. Select an appropriate Certificate Authority that can fulfill the trust and certificate requirement of the deployment. For more information on external public authorities, see Certificates from External Certificate Authorities 62.
4. For every device (server, IP 500V2 etc.) request the CA to create a unique ID certificate for each with the correct name content and save to a local directory. The name fields of the certificate are important for correct interoperation with clients; see Certificate Name Content 50 for more information. For more information on external public authorities, see Certificates from External Certificate Authorities 62.
5. For IP500 V2 devices, an external form based CSR must be used. For IP Office Linux devices a PKCS#10 CSR can be created using the CLI. For more information on the CSR process, see Certificate Signing Requests 134.
6. Download the root and any intermediate CA certificate from the Certificate Authority in PEM and DER format to a local directory.
7. Use IP Office Web Manager or IP Office Manager to:
   - Save both the root and intermediate CA certificate in the TCS, then
   - Activate the certificate chaining feature Offer ID Certificate Chain.
8. Use IP Office Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See Update Certificates 80.
9. Distribution of the root CA certificate to phones, clients and browsers is as per PKI Trust Domain based on Primary or Linux Application Server root CA section above.
10. Verification and enabling steps are as per PKI Trust Domain based on Primary or Linux Application Server root CA section above, with the note that many external CAs provide online verification tools.
11. Once all checks have been carried out, a configuration backup should be taken.

Approach 4: PKI Trust Domain based on an External Certificate Authority via SCEP

1. The CA on the Primary or Linux Application Server is not used; disable the setting **Platform View | Settings | General | Certificates | Identity Certificates | Renew automatically**.
2. Select an appropriate Certificate Authority that can fulfil the trust and certificate requirement of the deployment, including a SCEP service based on EJBCA.
3. The steps required to enable SCEP operation are covered in the IP Office Branch documentation.

6.2.10 Certificates from External Certificate Authorities

An external Certificate Authority (CA) provides a way of obtaining identity certificates that are trusted by 3rd parties. These CA providers typically perform the following functions:

- Validates the certificate requestor's identity and ownership of the domain
- Issues certificates
- Maintains certificate status information
- Updates Certificate Revocation Lists

Most commercial CAs are part of one or more industry organisations such as:

- **The Certificate Authority Security Council:** https://casecurity.org/
- **The CA/Browser Forum:** https://cabforum.org/

Both have online resources that can assist in selecting and using a CA. In addition there are other web resources from the CA providers themselves.

6.2.10.1 Selecting a Certificate Authority

Note: An external Certificate Authority cannot issue certificates with name content that cannot be externally verified. This includes any local domain names and private IP addresses. If local domain names or private IP addresses are required, the CA of the Primary or Linux Application Server should be used.

Select a Certificate Authority that can fulfil the trust and certificate requirement of the deployment. Selection criteria are outside of this document but should include for IP Office deployments:

- Is the Certificate Authority trusted?
- Can the Certificate Authority provide RSA 2048 bit + SHA-256 identity certificates for web servers? Code signing and other certificate type are not used by IP Office.
- Does the Certificate Authority support a secure web form based Certificate Signing Request (CSR)? If not, external tools are required to provide the CA with a text-based CSR. See Certificate Signing Requests 134 for more information about creating such text-based CSRs.
- Can the Certificate Authority provide identity certificates in PKCS#12 format? If not, external tools are required to convert the identity certificate to the correct format for import into IP Office.
  - See Certificate File Naming and Format 42 for more information on certificate file formats.
  - See Creating a CSR using IP Office Linux Command Line 140.
- If required, can the Certificate Authority provide multi-domain (AKA 'Multi-SAN' or 'Unified Communications') certificates?
- If required, can the Certificate Authority provide a signing CA certificate? The option would be required for Approach 2: PKI Trust domain based on Primary or Linux Application Server Intermediate CA above.
- Will the root CA already be in the client browsers and operating systems? Are all client browsers and operating systems covered?
- Are intermediate signing certificates used? This can increase deployment complexity if intermediates are used.
- Are the signing certificates provided in both PEM and DER format? See Certificate File Naming and Format 42 for more information on certificate file formats.
- What notification/assurance level is required? Providers typically offer a number of levels under various names:
  - Basic, AKA 'Domain Validation' – only the domain name is validated, not the company itself. Browsers should not raise an error/warning, but no company information is shown. This level is not recommended for IP Office interfaces where verification of company identity is important.
  - Intermediate, AKA 'Organization Validation' – the domain and company are validated. Browsers should not raise an error/warning, company information is shown.
  - Enhanced, AKA 'Extended Validation' – the domain and company are validated in detail. Browsers should display a green verified background and company information is displayed. Due to their security concerns, Wildcard certificates are not allowed for 'Extended Validation'.
- How long are the identity and signing certificates valid for? Shorter periods increase the maintenance overhead.

Página3043 de 3226.

- Can a free trial certificate be obtained to verify correct operation? IP Office has been tested successfully with a number of providers' certificates but due to quantity of providers, assurance cannot be given that all providers' certificates can be supported successfully.
- Are test and other support utilities provided?

6.2.10.2 Obtaining Identity Certificates

Once a provider has been selected, the certificate requirements need to be identified:

- The name fields of the certificate are vital for correct interoperation with clients; see Certificate Name Content 50 for more information.
- The certificate should be RSA2048 bit, with SHA-256 signature algorithm
- The quantity and duration
- The assurance level
- Whether single domain or multi-domain
- The certificate should be for a web server and not a signing certificate

Once requirements identified, a Certificate Signing Request (CSR) is made to the CA. This can use a number of methods:

- Form based, using the CA's web site or downloaded utilities: The private key and the certificate are created by the CA and sent/downloaded by the customer.
- Text based, using the OpenSSL package: The private key is created by OpenSSL and kept on the PC. The certificate is created by the CA and OpenSSL used to join the two parts together in a PKCS#12 file.
- Text based, using Microsoft windows tools: The private key is created by Microsoft OS tools and kept on the PC. The certificate is created by the CA and Microsoft OS tools used to join the two parts together in a PKCS#12 file.
- Automated via SECP: The private key is created by IP Office, kept on the system. The certificate is created by the CA and IP Office joins the two parts together.
- Web form based, using a 3rd party site. This is not recommended.

Currently IP Office Linux and IP500 V2 servers do not support the generation of a CSR where the private key is retained within the IP Office server. This means if the CA does not support form-based CSR, the OpenSSL or Microsoft windows tools methods of Certificate Signing Requests 134 must be used.

Once a CSR is submitted to the CA, they will review the application and if successful issue the identity certificate along with the signing certificate(s). The required format of IP Office identity certificates is PKCS#12. The required formats for the signing certificates are PEM and DER. See Certificate File Naming and Format 42.

If the file formats are not as required by IP Office utilities can be used to convert; these can be provided by the CA or 3rd party tools can be used. Examples of conversion using 3rd party tools are contained in Certificate Signing Requests 134.

6.2.11 Certificate Maintenance

Regardless of the certificate/trust structure used, all certificates expire and may under exceptional circumstances be compromised. It addition due to identity certificate naming requirements, update may be necessary due to hostname or IP address change. The certificate policy should include provision for replacement/update of CA and individual certificates, both trusted and identity.

If left at default, IP Office's identity certificates will expire seven years after installation and the root CA certificate in ten. For certificates obtained from an external authority it can be a little as 12 months.

For identity certificates derived from a CA, replacement is relatively straight forward as the CA (and hence the basic trust relationship) is unchanged: Obtain the relevant replacement before expiry with the same content and replace. If the root or intermediate CA requires changing, the process can be more extensive depending on whether the associated public/private key pair also changes. The IP Office internal CA on the Primary will optionally retain the public/private key pair if the CA certificate is recreated via Web Management (the **Renew existing** option).

If the root CA public/private key pair is changed, all identity certificates need to be renewed and should be done well before CA expiry. The new CA should be installed in the relevant trust stores alongside the old; this allows a transition period during which all identity certificates can be replaced.

Administrative logins to Manager and IP Office Web Manager will display an identity certificate expiry warning, along with the number of days remaining. IP Office release 10.0 and onwards will raise an alarm – a daily system event in SSA, SNMP, syslog, email – whenever any certificate is within 60 days of expiry.

6.2.11.1 Renewing an IP500 V2/Secondary/Expansion Certificate

If the default self-signed certificate or SCEP is being used, deleting the current or restarting the system will force another to be generated/obtained. When creating the new certificate the Common Name and Subject Alternative Name files can be specified in the Manager security settings – if not the default values will be used. For Server Edition all processes will restart, for IP500 V2 the transition will be smooth.

If the ID certificate has been obtained from an external CA, a replacement can be administered using IP Office Manager or IP Office Web Manager.

6.2.11.2 Renewing a Primary/Linux Application Server ID Certificate

If the ID certificate has been created by the internal CA, the setting Web Management **Platform | Settings | General | Certificates | Renew automatically** determines whether the creation and application is automatic due to expiry or change hostname or IP Address. If not automatic, Generate and Apply can be used.

If the ID certificate has been obtained from an external CA, a replacement can be administered using IP Office Manager or IP Office Web Manager.

6.2.11.3 Renewing a Primary/Linux Application CA Certificate

A new one can be created using Web Management **Platform View | Settings | General | CA Certificate | Create new**. This command must be used with caution as it will create a completely new root CA certificate – it will also require new ID certificates for all entities, and CA certificate distribution to all devices. To keep all existing ID certificates Renew existing should be selected; this will create a new certificate with the same content and public/private keys, but a different serial number and start/end date. Only this new root CA requires distribution, in-date existing ID certificates signed by the previous CA will still be valid. Care must be taken not to abuse the convenience of this feature as the longer the public/private keys are unchanged, the greater the risk of compromise.

See Using the IP Office Certificate Authority 131.

6.2.11.4 Recovering a Certificate

All certificates are part of the security settings backup/restore process. To recover an ID certificate, the latest backup set should be restored. For Server Edition, all processes will restart.

6.2.11.5 Certificate Troubleshooting

The certificates exchanged by any IP Office interface can be displayed using 3rd party tools like Wireshark. The IP Office identity certificate can also be displayed in Manager, IP Office Web Manager and browsers.

Failure of received certificate checks by IP Office result in an alarm event which contains the cause. These alarms also include certificate check failures as reported by the far end via TLS Alert messages. IP Office Manager and browsers also report certificate checks failures.

If an HTTP/TLS interface appears to have certificate issues it may be possible to temporarily disable certificate checking or enable an unsecure version of that interface.

The IP Office Manager security settings interface to IP Office should always be accessible; IP Office will always ensure it has an identity certificate (creating a self-signed one if the previous is deleted or corrupted), and Manager can be configured to accept any certificate. See Securing IP Office Manager 89.

It has been found on rare occasions that low-end routers when performing Network Address Translation (NAT) will modify IP addresses within the certificate name fields, rendering them corrupt. Changing the firewall/router is the best solution, but a temporary workaround may be to remove any IP address entries subject to NAT.

Chapter 7.
VoIP Security

7. VoIP Security

VoIP media security provides a means by which two endpoints capable of communication can engage in more secure media exchanges. There are a number of approaches that can be used:

- Secure Real-time Transport Protocol (SRTP)
- Datagram Transport Layer Security (DTLS)
- A Virtual Private Network (VPN) implemented using IPsec or another VPN technology such as SSL VPN.
- Other IP transports with security support such as Multiprotocol Label Switching (MPLS).

VPN and other IP transport security is briefly discussed in Limiting IP Network Exposure 95, however the relative merits for each media security approach is outside the scope of this document.

SRTP supports RTP media protection on a point to point basis providing confidentiality, message authentication and replay protection. SRTP also supports authentication and replay protection for the RTP Control Protocol (RTCP). Note that RTCP is not used as the signaling channel for VoIP calls, but contains Quality of Service (QoS) information.

The confidentiality (implemented by symmetric key encryption) and authentication (implemented by Hashed Message Authentication Code, HMAC) are optional and independent of each other.

SRTP encryption relies upon dynamically generated secure keys to be sent to the far endpoint. This cannot be achieved via the SRTP protocol so an alternative secure mechanism is required, typically via the associated signaling channel, for example SIP-TLS for SIP and 'Annex H' for H.323.

As SRTP is point to point, all individual links involved in the VoIP call – including key exchange/signaling – must be secure for the call to be secure end to end.

7.1 IP Office Platform Media Security

IP Office support both SRTP and IPsec for VoIP media security. IP Office's IPsec feature can be utilised, but it is not recommended as it limited to the IP500 V2 platform and uses a legacy key exchange mechanism (IKEv1).

VoIP media security using SRTP is supported on IP Office in Standard Edition, Server Edition, Select and hosted, without the need for extra licensing, for the connections:

- IP Office Line
- SIP Line
- SM Line
- Avaya H.323 extensions: 9608, 9611, 9621, 9641
- Avaya SIP extensions: 9608, 9611, 9621 and 9641 (in centralized branch deployments), 1100 Series, 1200 Series, B179, E129, H175, J100 Series, K100 Series (Vantage), Scopia XT series
- Avaya Communicator for iPad and Windows
- one-X Mobile Preferred for iOS and Android
- 3rd Party SIP extensions that support SRTP

Some IP Office connections do not support SRTP media security:

- Analogue and digital extensions
- Analogue and digital lines/trunks
- IP Office <-> Voicemail Pro link
- H.323 trunks
- Avaya H.323 extensions: 96x0, 16xx, 36xx, 46xx, 56xx
- Avaya SIP extensions: D100, E159, E169
- Avaya IP DECT and DECT R4
- Avaya IP Office Softphone (Mac)
- 3rd Party SIP extensions that do not support SRTP

The following configurable SRTP options are supported by IP Office:

SRTP feature	Options	Support	Default	Notes
SRTP Operation	Disabled	✓	✓	All SRTP settings are per system with a per line and per extension override
	On: Best Effort	✓		
	On: Enforce	✓		
RTP Encryption	Off	✓		
	On: AES128-CTR	✓	✓	
	On: AES128-F8	✗		
RTP Authentication	Off	✓		RTP Authentication should not be disabled
	On: SHA-1/32	✓		
	On: SHA-1/80	✓	✓	SHA-1/80 provides stronger authentication for a small bandwidth increase
RTCP Encryption	Off	✓	✓	
	On: AES128-CTR	✓		Some Avaya and 3rd party endpoints do not support encrypted RTCP
	On: AES128-F8	✗		
RTCP Authentication	On: SHA-1/32	✓		RTCP Authentication always active
	On: SHA-1/80	✓	✓	SHA-1/80 provides stronger authentication for a small bandwidth increase.

Table 19: SRTP Options

IP Office supports a per-system SRTP set of controls, with a per-line and extension override, including encryption and authentication settings. By default SRTP operation is disabled, however upgrades of IP Office branch systems from previous releases using the SM line and SRTP will maintain their settings.

The SRTP operation control is the setting Media Security and has the following values:

- **Disabled** – SRTP is not available
- **Enforce** – RTP is not available on that call leg. Note: This doesn't enforce end to end SRTP, only SRTP on the call leg configured as **Enforce**.
- **Best Effort** – always offer both SRTP and RTP and given a choice, choose SRTP.

Where SIP soft clients connect to IP Office in simultaneous-registration mode (that is, another device is registered for the same user), they do not have a per-extension override of media security settings. IP Office will handle calls of these devices according to its system-level Media Security settings

Each leg of a call is regarded independently by IP Office for SRTP control; the appropriate SRTP Line or Extension setting will determine the support by each leg. Conferencing or recording of calls with SRTP legs by IP Office will retain SRTP wherever possible.

In order to provide complete call security, the SRTP key exchange also requires to be secured, see VoIP Signalling Security 70.

7.2 VoIP Signalling Security

Securing the signalling of VoIP links is necessary when SRTP is enabled and is a security measure in itself: It should be enabled when the SIP registrar or H323 Gatekeeper is exposed on a public interface, with the other unsecure options disabled.

The security mechanism is dependent upon the type of link:

Link Type	Key Security Mechanism	Notes
IP Office Line	WebSocket HTTPS	Only the IP Office Line with WebSocket transport and Security setting of Medium or High should be used.
SIP Line	SIP-TLS	Additional line configuration is required to enable SIP-TLS. Also supports the SIPS URI scheme
SM Line	SIP-TLS	Additional line configuration is required to enable SIP-TLS Also supports the SIPS URI scheme
Avaya H.323 extensions	H.323-TLS	Supported from R10.0. Additional configuration is required to enable H.323-TLS.
	H.323-Annex H	No additional configuration required This does not secure the complete H.323 signalling channel, just the registration, key exchange and dialled digits.
Avaya SIP extensions	SIP-TLS	Additional SIP registrar configuration is required to enable SIP-TLS

Table 20: VoIP Signalling Security

For SIP extensions, the relevant LAN's SIP registrar layer 4 protocol setting should be configured to enable the TLS protocol. SIP-TLS requires the administration of certificates; see Certificates and Trust 38.

For SIP or SM lines, the Line's transport setting should be configured to use the TLS protocol and certificate checks enabled. A further consideration is the use of the SIPS URI scheme as defined by RFC 3261 and RFC 5630. Enabling the SIPS URI Type setting will cause all sessions originated from the trunk to use SIPS, indicating the requirement for secure SIP links for the call. The system setting System | VoIP Security | Strict SIPS when active, causes IP Office to reject any call to a SIP or SM Line that is not configured for SIP-TLS and the SIPS URI Scheme. When not set, IP Office permits the 'downgrading' of a SIP-TLS call to an unsecure SIP call.

Care should be taken when using SIPS URI scheme and Strict SIPS, as support by both Avaya clients and ITSPs is varied which could result in failed calls. This is of high importance for emergency call planning.

Current SIPS support of Avaya clients is covered in IP Office VoIP Endpoint Security 127.

See Secure Provisioning of 9609, 9611, 9621 and 9641 H.323 144 phones for information on 9608, 9611, 9621 and 9641 H323 secure phone provisioning.

For further details, see the relevant client documentation.

7.3 Endpoint Provisioning Security

When either media or signalling security is used, settings are required on the endpoints themselves. Some remote endpoint provisioning is supported directly by IP Office and can be more securely conveyed via HTTPS rather than the default HTTP.

Endpoint support of secure remote provisioning is covered in IP Office VoIP Endpoint Security 127.

Where remote endpoint provisioning is not supported by an endpoint, settings local to the device are used.

For further details, see the relevant client documentation.

7.4 SRTP Performance & Capacity

SRTP is more processing intensive than RTP to the extent that the concurrent call capacity of an IP500 V2 is reduced by 66% and Linux servers by 50%. See the Capacity Planning section in "*Deploying IP Office Server Edition Solution*". These reductions only occur when the media stream terminates or originates on IP Office. For this reason it is important to use direct media wherever possible.

SRTP direct media will occur when both external endpoints SRTP capabilities match, if they do not, IP Office will terminate both streams and convert. This will reduce the concurrent SRTP call capacity by two. This in turn places great importance on the various SRTP configuration settings within both IP Office and the various endpoints.

The following IP Office recommendations should be followed as a starting point, and only varied if necessary:

- RTP encryption and authentication should be kept on; some endpoints will not negotiate at all if either is off.
- RTP encryption/authentications setting should be AES-128/CTR plus SHA-1/80.
- RTCP encryption should be kept off; some systems (including Avaya Communication Manager) do not support RTCP encryption.
- All SIP extensions where possible should be configured for best effort (capability negotiation or 'cap-neg'); this allows the IP Office settings to dictate SRTP behaviour.
    - **Note:** When Auto generated configuration files that IP Office provides to 1100/1200 Series and B179 device types always indicates to the phones to do best effort, when the IP Office SRTP configuration is Best Effort or Enforce.
- Ensure consistency between the system and per-extension SRTP settings for SIP soft clients that connect to IP Office in simultaneous-registration mode (Avaya Communicator and one-X Portal for IP Office Mobile).
- All direct media settings on.
- Default codec selections which should ensure the mandatory G711 codec is always available.

Another performance consideration is the extra bandwidth incurred when SRTP is active; authentication adds 4 or 10 bytes to each packet for both RTP and RTCP. Given a 20ms sample period, active SRTP uses the following approximate IP bandwidth for a single call:

Codec	No SRTP	+RTCP auth	+RTP/RTCP auth	Notes
G.711	84 kbps	SHA1/80: 85 kbps SHA1/32: 84.5 kbps	SHA1/80: 86 kbps SHA1/32: 85 kbps	2.4% increase 1.2% increase
G.729	25 kbps	SHA1/80: 26 kbps SHA1/32: 25.5 kbps	SHA1/80: 27 kbps SHA1/32: 26 kbps	8% increase 4% increase
G.722	84 kbps	SHA1/80: 85 kbps SHA1/32: 84.5 kbps	SHA1/80: 86 kbps SHA1/32: 85 kbps	2.4% increase 1.2% increase

Table 21: SRTP Bandwidth

7.5 Secure Call Indications

There are no direct indications on phone displays that signal the call is secure. If assurance is required, Media Security should be set to Enforce and Strict SIPS activated.

The call leg SRTP status can be displayed by System Status Application and System Monitor, see SRTP Troubleshooting 121.

7.6 VoIP Security Planning Considerations

Secure media and signalling must be considered whenever VoIP endpoints or IP Office VoIP interfaces transit or are potentially accessible by untrusted networks, including the Internet.

Prior to deploying secure media or signalling using IP Office, the following should be reviewed:

- The IP Office SRTP feature supports media security natively without license or IP infrastructure requirements, but can add extra interoperation complexity with various endpoints.
- Signalling security must be considered whenever SRTP is contemplated. Signalling security can be considered on its own as a security improvement mechanism.
- Secure phone provisioning must be considered whenever media or signalling security is contemplated.
- When VoIP endpoint resilience is active with secure signalling or provisioning, the root CA certificate for both home and backup server must be the same.
- SRTP will reduce the concurrent call capacity of IP Office systems, therefore direct media should be used whenever possible. It may also reduce the capacity and performance of other connected systems.
- The exact SRTP support of each endpoint type should be assessed to determine how best to achieve security, direct media and other performance criteria.
- IP Office default SRTP settings should be retained wherever possible and only varied under exceptional circumstance.
- IP Office branch deployments have a specialized environment and requirements. See:
  - Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager, Document number 18-603853, https://downloads.avaya.com/css/P8/documents/101004861
  - Administering Centralized Users for an IP Office™ Platform Enterprise Branch, Document number 15-604263, https://downloads.avaya.com/css/P8/documents/101004857
  - Avaya IP Office™ Platform in a Branch Environment Reference Configuration, Document number 15-604253, https://downloads.avaya.com/css/P8/documents/101004855

Chapter 8.

Securing the IP Office Platform Solution

8. Securing the IP Office Platform Solution

IP Office can be made a very secure product, however only a certain number of features are active by default or on upgrade from previous releases. This is in order to ease the initial installation but will not help protect the system without following the suggestions listed in this document, other Avaya security publications and the relevant IP Office installation/Administration manuals. It is therefore necessary to check and implement the configuration options listed here.

Additional setting may be necessary to further secure the individual deployment. Avaya is presenting this information for guidance only; the customer is responsible for ensuring their system is secure.

- General Guidelines 75
- Assessing IP Office Security Requirements 76
- Security Administration 76
- Change Security Defaults 76
- Remove Unnecessary Accounts 76
- Disable Unused Services/Interfaces 77
- Ensure Minimum Rights of Access 78
- Enforce a Password Policy 79
- Update Certificates 80
- Securing Telephony Users & Extensions 81
- Hardening for Remote Worker Operation 82
- Securing Trunks/Lines 83
- Secure Voice Media 83
- Preventing Unwanted Calls 84
- Securing CTI Interfaces 88
- Securing IP Office Applications 88
- Configuration and Other Sensitive Data 94
- Limiting IP Network Exposure 95
- Secure Maintenance Interfaces 96
- Restricting Physical Access 96
- Securing Server Edition Servers 97
- Securing Linux Application Server/Unified Communications Module 99

8.1 General Guidelines

The recommended process for improving the security of IP Office is to; Assess the requirements, Implement changes as needed, then to monitor the system and respond in a timely manner to any detected threat.

All guidelines and steps should be followed regardless of the actual IP Office deployment.

Assess:

- Review existing installations
- Plan new deployments
- Identify security risks and requirements

Implement:

- Change security defaults
- Remove unnecessary accounts
- Disable unused services/interfaces
- Enforce password policy
- Update Identity Certificates and PKI
- Secure users and extensions
- Secure trunks/lines
- Secure voice media
- Prevent unwanted Calls
- Secure voicemail and one-X Portal for IP Office
- Limit IP network exposure
- Secure management applications & configuration data
- Secure servers
- Activate reporting/monitoring
- Checks and tests

Monitor:

- Monitor alarms and logs
- Detect other unusual activity
- Review Avaya Security advisories
- Review Avaya IP Office Software updates and technical bulletins
- Monitor telephony provider communication
- Periodic security reassessment

Respond:

- Investigate and react to any incident
- Report to appropriate organizations
- Ensure the latest software updates/service packs are installed

8.2 Assessing IP Office Security Requirements

It is vital that a security risk assessment is carried out on all IP Office installations, both initial (prior to deployment or for existing deployments if one has not yet been carried out), and periodically after initial assessment to review any change.

A primary differentiator of security risk for IP Office is whether the system is potentially accessible from external or unsecured networks or individuals, especially the Internet.

This document does not cover security assessments in any detail; however there are many resources available that cover this process, including for example:

- **US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology System**
  http://dx.doi.org/10.6028/NIST.SP.800-30r1
- **UK British Standards Institute (BSI) ISO/IEC 27001, Self-assessment questionnaire**
  http://www.bsigroup.co.uk/en-GB/iso-27001-information-security/ISO-27001-for-SMEs/
- The SANS Institute also provides a wide range of security-related information, including risk assessments and audits:
  http://www.sans.org/reading-room

8.3 Security Administration

The security settings are stored on the system and are separate from the system's configuration settings. To change a system's security settings, Manager must first be switched to security mode by selecting **File | Advanced | Security Settings** from the menu bar.

Security settings can only be loaded directly from a system. These settings cannot be saved as a file on the local PC, nor do they appear as a temporary file at any time. By default Manager and the system will always attempt to use a secured link for configuration and security settings exchanges.

8.4 Change Security Defaults

All default passwords must be changed to a unique and 'strong' password. See Password and PIN Management 32 for more information on password strength.

In IP Office Manager **Security Settings | General** tab:

1. For Security Administrator account:
   a. Change **Password** to a 'strong' password of 8 or more characters.
   b. Set **Minimum Password Complexity** to ***high***.
2. Change service user account '**Administrator**' password to a 'strong' password of 8 or more characters.
3. If required, add a customer administration account (again with strong password) with the minimum rights of access. The account status **Force New Password** should be set. This will enforce a password change at the next login (that is, during customer/ engineering Installation).
4. Change the System, VM Pro and Monitor passwords to 'strong' passwords of 8 or more characters.

8.5 Remove Unnecessary Accounts

All unnecessary administration and IP Office user accounts should be removed or disabled to reduce the likelihood of forgotten default accounts being used for unauthorized access. Any remaining accounts must have their passwords changed. See User Accounts and Rights of Access 22 for more information on the differing account types and locations.

1. In IP Office Manager | **Security Settings | Service User** tab, remove all unnecessary service user accounts; only retain accounts that are essential. The service user may be deleted or the account status set to Disabled.
2. For all remaining active Service User accounts, change password to a strong one of 8 or more characters. If using Server Edition, see Securing Server Edition Servers 97 for alternative Service User administration using IP Office Web Manager
3. In **Configuration | Users**: Delete any RAS telephony user accounts (for example 'RemoteManager') that are not required. For any that are required, change the password to a strong one of 8 or more characters.

Página3057 de 3226.

8.6 Disable Unused Services/Interfaces

All interfaces and services not required must be disabled. Additionally, consider enabling interfaces and services only when required.

1. In IP Office Manager **Security Settings | System | Unsecured Interfaces** tab: Uncheck all Application controls and enable only the minimum according to the following table:

Application Control	Affected Application	Notes
TFTP Server	IP Office Manager Upgrade Phone Manager DECT R4* Legacy Voicemail Pro UDP whois** Network Viewer	Disables all TFTP access, including TFTP Directory Read, TFTP Voicemail and Program Code. * When inactive, DECT will continue operating but without the system directory feature. ** TCP whois discovery should be used in Manager.
TFTP Directory Read	Phone Manager DECT R4* TAPI Install**	Also used for legacy applications: IP DECT*, Analog DECT, Conferencing Centre, CRM, MMM * When inactive, DECT will continue operating but without the system directory feature ** TAPI installation will generate a warning, but it can be ignored Also controlled by the general TFTP Server setting above.
TFTP Voicemail	Legacy Voicemail Pro	Enable only when Voicemail Pro R9.0 and prior used Not applicable to embedded voicemail Also controlled by the general TFTP Server setting above.
Program Code	IP Office Manager Upgrade	Used for upgrades from IP Office Manager, must be disabled when not required Also controlled by the general TFTP Server setting above.
DevLink	DevLink System Monitor*	Must be disabled when not required * When inactive, System Monitor can still use the HTTP/S access method.
TAPI	TAPI Link Lite (1st party TAPI) TAPI Link Pro (3rd party TAPI) Avaya Contact Center Select IP Office Contact Center	Enable only when TAPI required; note that TAPI driver installation will fail if the TAPI interface is not active. This setting will affect the IPOCC and ACCS CTI Link; when inactive, any IPOCC and ACCS sessions will require TLS and a trusted certificate from IPOCC/ACCS. This setting will not affect the one-X Portal for IP Office CTI Link.
HTTP Directory Read	IP Office Centralised Directory J129 Phone*	Enable only when J129 or IP Office Centralized Directory used. Access only via HTTPS. HTTP port 80 must be disable. * When inactive, J129 will continue operating but without the directory feature
HTTP Directory Write	J129*	Enable only when J129. Access only via HTTPS. HTTP port 80 must be disabled. * When inactive, J129 will continue operating but without the directory update feature

Table 22: Effect of Disabling Services

8.7 Ensure Minimum Rights of Access

Restrict Service Users' rights of access to the minimum necessary. See User Accounts and Rights of Access 22 for more information on the differing access levels.

1. In IP Office Manager | **Security Settings | Rights Groups**, remove all unnecessary access rights; only retain rights that are essential.
2. In IP Office Manager | **Security Settings | Service Users | Rights Group Membership**, remove all unnecessary rights group membership.
3. If necessary, create new rights groups with minimum access.
4. Rights groups that are defined but not assigned to any Service User do not present a security risk.
5. In IP Office Manager **Security Settings | Services** tab: Enable only the minimum services at the recommended **Service Security Level** according to the following table:

Service Name	Application	Service Security Level	Notes
Configuration	Manager, Configuration Web Service (DevConnect)	Secure, Medium	Should always be enabled
Security Administration	Manager	Secure, Medium	Should always be enabled
System Status Application Interface	SSA	Secure, Medium	Disable if SSA not present
Enhanced TSPI	one-X Portal for IP Office	Unsecure Only	Disable if one-X Portal for IP Office not present
HTTP	H323 Phones (HTTP or HTTPS) Embedded File Manager (HTTP), IP Office Softphone (HTTP or HTTPS) System Monitor (HTTP or HTTPS) VMPro (HTTPS) IP Office Line (HTTP or HTTPS)		Controls the IP Office HTTP server. Disable if not required, else if just HTTPS required, set to Secure, Medium. If HTTP must be enabled, set the **System	System	Avaya HTTP Client Only** setting active. This will reject all non-Avaya clients.
Web Services	IP Office Web Manager	Secure, Medium	Disable if Web Management or System Manager (SMGR) not used
External	Voicemail Pro, one-X Portal for IP Office, Web Control, WebRTC	n/a	Not a true service interface

Table 23: Minimum Access Rights

6. In IP Office Manager **Configuration | System | System** tab, check the File Writer IP Address setting. This specifies the IP address allowed to write files to the IP Office (IP500 V2 and Linux) using HTTP and TFTP protocols. It should be set to 0.0.0.0 (disabled) and set only when files need to be transferred.

8.8 Enforce a Password Policy

Change the security settings to enforce minimum password complexity, disable service users temporarily and IP Office users permanently on bad logins.

If a Service user fails to login 3 times within 10 minutes, the account will be locked for 60 seconds. If an IP Office user fails to login 5 times within 10 minutes, account will be locked permanently and the administrator will be required to unlock the account using Manager.

- **NOTE:** This recommended IP Office User password policy must always be enforced if the system is potentially accessible from unsecured networks including the Internet; for example when SIP trunks or VoIP remote worker/extensions are supported.

In IP Office Manager Security **Settings | General** tab:

1. **Set Service User Details:**
   - **Minimum Name Length** to 6.
   - **Minimum Password Length** to 8.
   - **Password Reject Action** to '***Log and Temporary Disable***'.
   - **Minimum Password Complexity** to '***Medium***'.
   - **Previous Password Limit (Entries)** to 4.
2. **Set IP Office User Details:**
   - **Password Enforcement** to on.
   - **Minimum Password Length** to 8.
   - **Minimum Password Complexity** to 'Medium'.
   - **Password Reject Limit** to 5.
   - **Password Reject Action** to '***Log and Disable Account***'.

- **Note:** The IP Office user password policy only applies to the password field, not the voicemail or user login code. See Password and PIN Management 32 for more information.

8.9 Update Certificates

1. It is essential to understand the information and recommendations of Certificates and Trust 38 to determine the certificate and trust requirements of the system prior to installation.
2. If required, administer a new platform identity certificate:
   - The new identity certificate should be in a 'p12' or 'pfx' file.
   - Ideally, all certificates used to sign the new identity certificate should be in the same file.
   - If the signing certificates are in separate files, use Manager **Security | System | Certificates | Trusted Certificate Store | Add** to upload each one.
   - Activate the Manager setting **Security | System | Certificates | Identity Certificate | Offer ID Certificate Chain**.
   - Use Manager **Security | System | Certificates | Identity Certificate | Set** to upload the identity certificate file.
   - The identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server, any signing certificates will be placed in the Trusted Certificate Store (TCS).
   - If a separate telephony identity certificate is required, it should be administered using Manager security settings.
3. The default certificates trusted by IP Office should be removed if not required. This is achieved by placing a copy of the certificate in the ***system/primary/certificates/tcs/delete*** directory using the Manager or IP Office Web Manager's File Manager.
   Any default certificates to be trusted by IP Office should be added to the ***system/primary/certificates/tcs/add*** directory. See Default Trusted Certificates 112 for more information and how to create the certificate files.
4. If there is a change to the server's LAN IP address, SIP domain or FQDN, the Identity certificate will require regeneration. An IP500 V2, Unified Communications Module, Secondary or Linux Expansion Server will always require manual regeneration. A Primary or Linux Application Server will be automatic if the **IP Office Web Manager | Platform | Settings | General | Certificates | Renew automatically** setting is active (default).
5. After ensuring that all other IP Office components' identity certificates are correctly configured, set the received certificate check levels appropriately using the Manager settings **Security | System | Certificates | Received Certificate Checks (Management)** and **Security | System | Certificates | Received Certificate Checks (Telephony)**.

8.10 Securing Telephony Users & Extensions

Users and extensions should be configured to restrict access to necessary features, default login codes changed and auto-create disabled.

1. All unused Users should be deleted – except NoUser.
2. The following auto-create settings must be disabled when not required:
   - **LAN1 | VoIP | H323 Gatekeeper | Auto-create Extn**
   - **LAN1 | VoIP | H323 Gatekeeper | Auto-create User**
   - **LAN1 | VoIP | SIP Registrar | Auto-create Extn/User**
   - **LAN2 | VoIP | H323 Gatekeeper | Auto-create Extn**
   - **LAN2 | VoIP | H323 Gatekeeper | Auto-create User**
   - **LAN2 | VoIP | SIP Registrar | Auto-create Extn/User**
   - **Line | IP DECT | Gateway | Auto-Create Extension**
   - **Line | IP DECT | Gateway | Auto-Create User**
3. If any auto-create feature is used to assist installation, the settings must be deactivated as soon as possible. Note that from 9.1, these settings will automatically be deactivated 24 hours after being set to avoid inadvertent exposure.
4. If no H.323 extensions are supported, the **LAN1/LAN2 | VoIP | H323 Gatekeeper Enable** must be set disabled. If H.323 extensions are supported, only the relevant LAN's gatekeeper should be enabled.
5. If no H.323 remote workers are supported, the **LAN1/LAN2 | VoIP | H323 Gatekeeper | H323 Remote Extn Enable** must be set disabled. If H.323 remote workers are supported, only the relevant LAN's Remote Extn should be enabled.
6. If no SIP extensions are supported, the **LAN1/LAN2 | VoIP | SIP Registrar Enable** must be set disabled. If SIP extensions are supported, only the relevant LAN's registrar should be enabled.
7. If no SIP remote workers are supported, the **LAN1/LAN2 | VoIP | SIP Registrar | SIP Remote Extn Enable** must be set disabled. If SIP remote workers are supported, only the relevant LAN's SIP Remote Extn should be enabled.
8. Enforce a Login Code (PIN) policy for all users and extensions by setting **System | Telephony | Login Code Complexity | Minimum length** to the minimum acceptable length, and activating Complexity tests. For more information on PIN and Login Code security see Password and PIN Management 32.
9. All VoIP (SIP, H323, DECT) users' **User |Telephony | Supervisor Settings | Login Code** or **Extension | Extn | Phone Password** must be set.
10. If any SIP registrar or H323 gatekeeper is exposed directly or indirectly to an unsecure network, even via an SBC, the additional steps of Hardening for Remote Worker Operation 82 must be followed.
11. All SIP extensions' **Extn | Force Authorisation** setting must be enabled.
12. All auto-created VoIP users must have their **User | Telephony | Supervisor Settings | Login Code** changed from the default. All auto-created non-VoIP (Digital, Analog) users should have their name and extension changed from the default.
13. Each user should have only the necessary **User | User | Profile** features enabled, all others disabled.
14. Each user should have only the minimum necessary **User | Web Self-Administration** interface features enabled, all others disabled. Web Self-Administration is a new feature from R9.1 and disabled by default. Each tab of the Web Self-Administration page may be controlled for view and edit on a per-user basis:

Tab	User Setting
Profile	User
Voicemail	Voicemail
Do Not Disturb	DND
Mobility	Mobility
Forwarding	Forwarding
Personal Directory	Personal Directory
Button Programming	Button Programming
Download	none (always available)

15. For IP Office release 8.1 and prior, disable all **User | Phone Manager Options** unless required. This can be achieved via the application of User Rights (User Rights | Phone Manager).
16. If different from the system-wide setting, change the **Extn | VoIP | Media Security** setting. See VoIP Security 68.

Página3062 de 3226.

17. If the VoIP extension is to be configured for secure media (SRTP) or operates in an unsecure environment, any settings file supplied by IP Office should be conveyed via HTTPS not HTTP. This will additionally require certificate administration; see Certificates and Trust 38.

8.11 Hardening for Remote Worker Operation

Whenever SIP or H323 remote worker operation is supported, or if any SIP registrar or H323 gatekeeper is exposed directly or indirectly to an unsecure network even via an SBC, extra considerations are required to ensure that the external access does not compromise IP Office security.

- **Important:**
  IP Office must only be connected externally via a properly configured Firewall. It must never be connected directly.

1. The RTP port range on the LAN interface must be set to no more than 50750. If more RTP ports are required, the minimum value may be changed.
   - **LAN1/LAN2 | VoIP | Port Number Range | Maximum**
   - **LAN1/LAN2 | VoIP | Port Number Range (NAT) | Maximum**
2. Any exposed SIP Registrar or H323 Gatekeeper should have the TLS option enforced and any unsecure options disabled. See VoIP Security 68. To reduce the overhead of security and certificate management, one LAN's registrar can be used for the external interface, the other LAN for internal extensions.
3. The SIP registrar ports should be changed from the default 5060/5061
4. Any settings file supplied by IP Office must be conveyed via HTTPS not HTTP. This will additionally require certificate administration; see Certificates and Trust 38.
5. SRTP for media security should be considered, see VoIP Security 68.
6. If any H323 Gatekeeper or SIP registrar is exposed directly or indirectly to an unsecure network, all remote worker's **Extension | Extn | Phone Password** must be set. The code must not be a sequence, repeated digits, or same as the extension number. It must not be less than 9 digits, preferably 13 digits. For R8.1 and prior, the setting **User | Telephony | Supervisor Settings | Login Code** can be used.
7. Each H323 or SIP remote worker extension's **Extension | VoIP | IP Address** should be set to the public IP Address of the phone.
   - **Note:** This cannot be used if more than one phone is behind the same firewall/NAT, or the remote IP address changes.
8. The steps of Securing Telephony Users & Extensions 81 must be followed.
9. The steps of Preventing Unwanted Calls 84 must be followed.
10. A Session Border Controller (SBC) must be considered for enhanced SIP remote worker security – the Avaya SBC for Enterprise (ABSCE) is a solution specifically tailored for IP Office SIP remote workers and SIP trunks. For more information see "*Configuring the Avaya Session Border Controller for IP Office Remote Workers*" in "*Administering Avaya IP Office Platform ™ with Manager*".
    - **Note:**
      If an SBC or SIP Application Level Gateway (ALG) is deployed, some of the IP Office security measures must be moved from the IP Office to the SBC/ALG; the IP Office source IP address blacklisting should be disabled with the No User Source Number 'B_DISABLE_SIP_IPADDR'. The SBC/ALG black/white listing must be activated to compensate.

8.12 Securing Trunks/Lines

SIP trunking and off-switch or trunks-to-trunk forwards/transfers should be disabled when not required, and a Session Border Controller (SBC) used for enhanced SIP security. Links between IP Office systems can be optionally secured.

1. If using SIP trunks, IP Office must be connected externally via a properly configured Firewall; see Limiting IP Network Exposure 95 for more information. IP Office must never be connected directly.
2. Unless SIP trunks are configured for a particular LAN interface, the **LAN1/LAN2 | VoIP | SIP Trunk Enable** setting must be disabled.
3. Many IP Office customers rely on the Services Providers to provide a secure SIP trunk environment. For a stronger security posture, implementation of the Avaya Session Border Controller for Enterprise (Avaya SBCE) is recommended as a best practice. Avaya SBCE also provides Advanced Services such as Secure Remote Worker and Encryption Service supporting VPN-less access to IP Office for SIP endpoints outside the enterprise firewall. The Avaya SBC for Enterprise is a solution specifically tailored for IP Office. For more information see: http://www.avaya.com/usa/product/avaya-session-border-controller-for-enterprise.
   - **Note:**
     If an SBC or SIP Application Level Gateway (ALG) is deployed, some of the IP Office security measures must be moved from the IP Office to the SBC/ALG; the IP Office source IP address blacklisting should be disabled with the No User Source Number 'B_DISABLE_SIP_IPADDR'. The SBC/ALG black/white listing must be activated to compensate.
4. Off-switch forwards/transfers should be disabled on a per-system or per-user basis, with the system setting taking precedence over the user.
   - Per-user setting is: **User | Telephony | Supervisor Settings | Inhibit Off-Switch Forward/Transfer**. This can also be set via User Rights.
   - System-wide setting is: **System | Telephony | Telephony | Inhibit Off-Switch Forward/Transfer**.
5. Analog trunks-to-trunk forwards/transfers should be disabled on a per-line basis unless required, using **Line | Analog Options| Analog Trunk to Trunk Connection**.
6. Other changes to restrict calls are contained in Preventing Unwanted Calls 84.
7. IP Office Lines (AKA SCN trunks) may be secured using the **Line | Line | Transport Type** of ***WebSocket Client/Server***, and a **Line | Line | Security setting** of ***Medium*** or ***High***.
   - One IP Office system must be the WebSocket client, the other the server. The Primary and Secondary should always be the WebSocket server.
   - For the ***High*** setting, certificate configuration is required; see Certificates and Trust 38 for more information.
8. For Server Edition deployments, Secure IP Office Lines should always be used.

8.13 Secure Voice Media

In an unsecure environment with no other VoIP security, IP Office's VoIP media security should be enabled.

- **Note:** Enabling VoIP media security will reduce the platform concurrent call capacity considerably. It will also require SIP call signalling security.

For more information, see VoIP Security 68. This should be reviewed prior to enabling any IP Office VoIP media security.

8.14 Preventing Unwanted Calls

The following recommendations cannot be precise due to the wide variation of national, international and customer dial plans, however they can be adapted as required for specific deployments.

- **Note:** It is strongly recommended that all IP Office deployments be protected from unwanted calls regardless of the perceived risk.

Toll fraud, dial-through attacks or general unwanted incoming or outgoing calls can be mitigated in IP Office by:

- Call barring
- Authorization Codes
- Call logging and monitoring
- Phone Lock
- Auto Logout
- Out of hours barring
- Blocking off-switch and trunk-to-trunk transfers
- Removing mobile call control
- Ensuring Emergency Numbers are defined
- Correct error handling in Voicemail Pro call flows.

8.14.1 Call Barring

The normal way of call barring is to have a default outgoing route and then lock down undesired numbers. When locking down un-desired numbers it is important to take in to account IP Office dialling rules and add an N after any dial string you are trying to block.

For example to block calls to Premium rate numbers (1900-xxx-xxxxx US or 09… UK):

	US	UK
Telephone Number	1900N	09N or 909N
Feature	Barred	Barred

It is important to ensure that the Telephone Number is followed by an N so that it matches even when dialled en-bloc (or redial).

Many countries have prefixes that may be dialled before normal PSTN numbers, for example to force Caller ID presentation, (*67(US)/141(UK) to Withhold Caller ID, *82(US)/1470(UK) to present Caller ID) it is important to include versions of all barred short codes including these prefixes or just bar any call attempts using these prefixes.

8.14.2 User Based Barring

There are several potential methods for achieving different routing/barring rules for Users.

One effective method that minimizes the per-user config, and can be part of user rights templates, centralizes the routing/barring config, and maintains features like secondary dial tone, is to create copies of the "50:Main" ARS for the different access levels required.

As 50:Main is the default it makes sense for that to be the one that is used for most users, or on sites with specific concerns about security the most restricted.

For this example we will define two alternate ARS entries for Local & Long Distance, and Unrestricted, by copying the default Main then restrict Main to be local only. All the ARS tables must route Emergency Calls.

The new Short Codes in the Main ARS will be:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0N;	0N	Barred	0
1N;	1N	Barred	0
XN;	N	Dial 3K1	0
XXXXXXXXXXN	N	Dial 3K1	0
*67N		Barred	0
*82N		Barred	0

The 0N; and 1N; codes have been changed to barred and barred codes added for *67 and *82. Note the addition of the N to ensure a match for redial, etc. Short codes can be added for areas where 7 digit local dialing is still available if required, also it might be useful to create Short Codes to trap local Area Codes that have been dialed with a leading 1, also Freephone dialing.

The Local & Long Distance Short codes will be:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0N;	0N	Barred	0
1XXXN;	1N	Dial 3K1	0
XN;	N	Dial 3K1	0
XXXXXXXXXXN	N	Dial 3K1	0
1900N		Barred	0
*67N		Barred	0
*82N		Barred	0

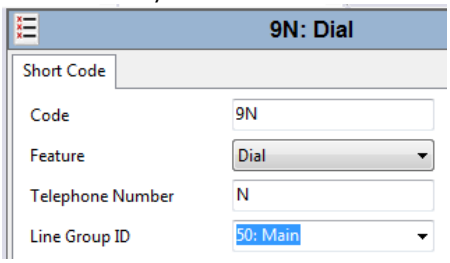
This will allow all calls starting '1' except Premium Rate (1-900 numbers), the 1N; Short Code is modified to 1XXXN; to avoid people pausing during dialing matching a simple "1N;" short code. The barring for *67 and *82 is repeated.

The Unrestricted ARS short codes will be:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
N;	N	Dial 3K1	0

This is totally un-restricted, in real operation it is unlikely that there will be totally un-restricted out-dialing.

The Default system short code for dialing is Unchanged:



Add specific User Short Codes for users who are allowed greater dialling privileges, similar to the default system Short code but pointing to the appropriate ARS entry. This can be done via User Rights Templates.

For more information on ARS operation, see the field descriptions for the Manager ARS tab in Administering Avaya IP Office ™ Platform with Manager.

Página3066 de 3226.

8.14.3 Protecting Phones

In some environments one of the risks is not from the normal Users of the phones but people who have physical access to the phone but you don't want them to use phones. There are several mechanisms that can be used to protect the phones when the normal users are away from their desks:

- **Phone Lock**
  Phones can be locked using the Lock feature on the phone Features menu. Locking the phone also locks the Features menu. The 1400, 9500, and 9600 series phones have an option to specify a timer where the phone will automatically lock itself after a specified period of inactivity.
- **Short codes**
  The "Outgoing Call Bar On" short code prevents the phone being used to make outgoing calls - Internal and Emergency calls are allowed. "Outgoing Call Bar Off" with the user's login code unlocks the phone
- **Logging out/Hot Desking**
  Users can log out of the phone - which will leave the phone with the special 'NoUser' account associated with it. This NoUser is Outgoing Call Barred. Users must have a login code to be able to log out of their default phone (the phone with their extension number).
- **Auto Logout**
  The **Extension | Telephony | Supervisor Settings | Login Idle Period** can be used to force a User to be logged out if their phone is idle for a period of time.
- **Out of Hours Call Routing**
  A time profile can be associated to an ARS so that when the time Profile is inactive a different ARS is used for routing calls - for our example above we will set the extra ARS tables to point to Main out of hours so that only Local and Emergency Calls can be made.
- **Trusted Voicemail Source**
  Where a phone is in an un-controlled area it is also advisable to remove the default Trusted Source Number for Voicemail access, so that all IP Office Voicemail access requires entering the Voicemail access code, even from the User's home extension.

8.14.4 Making Calls from Protected Phones

Once phones have outbound dialing locked down it often becomes necessary to provide occasional exceptions. Since release 5.0, it has been possible for a privileged User (Receptionist for example) to transfer secondary dial tone to a restricted user to allow them to make a call that they would not otherwise be able to make.

A more versatile solution is to use Authorization Codes. Authorization Codes permit a user with a Code to go to a restricted phone and make a call with their privileges without the necessity of Hot Desking for the call. This is sometimes called "Roaming Class of Service" on other systems. For information see the field descriptions for the Manager Authorization Codes tab in *Administering Avaya IP Office ™ Platform with Manager*.

Note that Emergency Calls are always permitted, hence the need to ensure Emergency Dialing has been correctly defined.

8.14.5 Forwarding Protection

When a user has forwarding active, any call routing, including barring for calls to that user, will be applied. If a user cannot make long distance call, and attempts to forward to a long distance number, the call will fail. As call routing/barring can vary by time of day it is not possible to block the attempt to configure long distance as the forwarding target.

Use the setting **System | Telephony | Telephony | Inhibit Off-Switch Forward/Transfer** to inhibit all off-switch forwarding and transfers. When enabled, this takes precedence over all user settings.

This setting can also be set per user using **User | Telephony | Supervisor Settings | Inhibit Off-Switch Forward/Transfer**.

8.14.6 Remote Forwarding Controls

By default IP Office and the IP Office Voicemail applications do not provide any mechanisms for remote modification of User Forwarding settings. However, Mobile Call Control can be enabled to give access. For information, see "Mobile Call Control" in Administering Avaya IP Office ™ Platform with Manager.

There is also a Voicemail Pro **Personal Options Menu** option that can be added to a custom call flow to allow users to remotely change their forwarding and other settings.

Before enabling either of these options the warnings in the manuals must be considered and a judgment made to decide if the benefit is worth the risk of unauthorized access.

8.14.7 SMDR Reporting of Barred Calls

To enable the detection of unauthorized call attempts, the string 'SMDR' can be included in the telephone field of the Barred short code. When included, an SMDR report will be generated with the relevant field indicating the calling party, call destination etc. The call will be zero duration, zero ring time, with the word 'Barred' in the 2nd party info field.

8.14.8 Error Handling in Voicemail Pro Call Flows

All call flows that can make internal or external calls, transfers or other potential call operations must ensure only the expected call destinations from valid users are allowed. All possible invalid operations should be detected and prevented by the use of call flow logic.

8.15 Securing CTI Interfaces

1. If not required, disable TAPI Link Lite/Pro (1st /3rd party TAPI) as per Disable Unused Services/Interfaces 77.
2. To secure the link between ACCS or IPOCC and IP Office, the setting IP Office Manager | **Security Settings | System | Unsecured Interfaces | TAPI** should be disabled. This will enable TLS and request a trusted certificate from IPOCC/ACCS.
3. Administer IPOCC/ACCS with an identity certificate. See the relevant IPOCC/ACCS documentation.
4. Administer the IP Office Trusted Certificate Store (TCS) with the root CA certificate of the IPOCC/ACCS.

8.16 Securing IP Office Applications

To help secure IP Office applications, use the following recommendations:

- General Guidelines 75
- Assessing IP Office Security Requirements 76
- Security Administration 76
- Change Security Defaults 76
- Remove Unnecessary Accounts 76
- Disable Unused Services/Interfaces 77
- Ensure Minimum Rights of Access 78
- Enforce a Password Policy 79
- Update Certificates 80
- Securing Telephony Users & Extensions 81
- Hardening for Remote Worker Operation 82
- Securing Trunks/Lines 83
- Secure Voice Media 83
- Preventing Unwanted Calls 84
- Securing CTI Interfaces 88
- Configuration and Other Sensitive Data 94
- Limiting IP Network Exposure 95
- Secure Maintenance Interfaces 96
- Restricting Physical Access 96
- Securing Server Edition Servers 97
- Securing Linux Application Server/Unified Communications Module 99

8.16.1 Securing IP Office Manager

1. Apply the following configuration settings on the Manager **File | Preferences | Security** tab to ensures more secure IP Office communications and help keep configuration data away from unauthorized users:

Configuration	Parameter Setting
Request Login on Save	Enabled
Close Configuration/Security Settings After Send	Enabled
Save Configuration File After Load	Disabled
Backup Files on Send	Disabled
Enable Application Idle Timer (5 minutes)	Enabled
Secure Communications	Enabled

2. The **Manager Certificate Check** on the **File | Preferences | Security** tab should be set according to the security policy. It should be set to ***None*** only for recovery purposes.
3. For more information see Certificates and Trust 38 and Windows Certificate Management 118.
4. If mutual certificate authentication is required (that is, the IP Office Configuration or Security Administration service will request a certificate from Manager) the **File | Preferences | Security | Certificate** offered to IP Office needs to be set with an identity certificate. See Windows Certificate Management 118. If Current User is selected, it will only apply the current Windows user. If Local Machine is selected, it will be used for all Windows users of that PC.
5. To prevent other administrators from modifying the **File | Preferences | Security** tab settings, ensure those Service Users do not have the rights to edit security settings, or have the Administrator Manager Operator Role.
6. In IP Office Manager's **File | Preferences | Directories** tab, change the **Working Directory (.cfg Files)** to be different to the **Binary Directory (.bin Files)**. If the two directory settings are the same, it potentially allows remote TFTP/HTTP file access to the folder containing copies of configuration files.
7. Ensure all offline configuration files, exported files or other configuration data are controlled.

8.16.2 Securing IP Office Web Manager/Web Control

Web Manger and the Linux Web Control Panel are browser-based online management tools that always use HTTPS communication.

1. Any browser used for web-based management should have the CA certificate/ID certificate of the IP Office installed in the relevant trusted certificate store. It is possible in some browsers to provide temporary or permanent exceptions, but this should be avoided. For more information about certificates and browser support, see Certificates and Trust 38.
2. Ensure all offline configuration files, exported files or other configuration data are controlled.

8.16.3 Securing Web Licence Manager

Web Licence Manager (WebLM) administrative accounts are separate to IP Office and logins to WebLM are not integrated into the IP Office AA framework.

WebLM administration is browser-based and always uses HTTPS communication.

1. Change the password of the default account as soon as possible.
2. All passwords must be 'strong' and of 8 or more characters (See Password and PIN Management 32).
3. For subsequent password management, go to the WebLM 'Manage Users' page. Any unused administrator accounts must be deleted.
   - Note: WebLM does not support referred authentication; local user accounts are used at all times.
4. Any browser used for web-based management should have the CA certificate/ID certificate of the IP Office installed in the relevant trusted certificate store. It is possible in some browsers to provide temporary or permanent exceptions, but this should be avoided. For more information about certificates and browser support, see Certificates and Trust 38.
5. If the application is not used, it should be disabled using the Web Control **Settings | System | Services | Automatic Start** setting.

Página3070 de 3226.

8.16.4 Securing System Status Application

SSA will always attempt to connect to the IP Office using the secure TLS service first if the login page setting **Secure Connection** is selected. However, if the TLS connection attempt fails, it will offer the user the option to connect over the unsecure connection.

1. To prevent the use of the unsecure connection, the Manager security setting **Services | System Status Application Interface | Service Security Level** should be set to ***Secure, Low*** or ***Secure, Medium***.
   - **Note:** The use of SSA with the TLS connection will limit the status monitoring capacity, particularly on the IP500 V2 platform. If high SSA events or call rates are anticipated, the unsecure connection should be used with alternative security arrangements.
2. There is no checking of the IP Office certificate by SSA when the TLS connection is used hence no certificate configuration is possible on SSA.
3. If not required by support personnel using SSA, the rights: **Rights Groups | System Status Application | Read all configuration** and **Rights Groups | System Status Application | System control** should be removed from the Service User account.
4. Any snapshot file saved by SSA may be read by any other SSA instance without authorization. This file can include configuration and other sensitive information and therefore access to the file must be controlled.

8.16.5 Securing System Monitor

System Monitor has a number of connection methods: Two legacy (UDP and TCP), and two contemporary (HTTP and HTTPS). Only the HTTPS method is fully secure, but has the highest processing overhead. UDP has the least.

IP Office support of the various System Monitor connection methods is controlled by the security settings as follows:

HTTP Service Security Level	HTTP	HTTPS	UDP	TCP
Disabled	Disabled	Disabled	n/a	n/a
Unsecure Only	Enabled	Disabled	n/a	n/a
Unsecure + Secure	Enabled	Enabled	n/a	n/a
Secure Low	Disabled	Enabled	n/a	n/a
Secure Medium	Disabled	Enabled	n/a	n/a
Secure High	Disabled	Enabled	n/a	n/a

Unsecured Interfaces | DevLink	HTTP	HTTPS	UDP	TCP
Disabled	Disabled	Enabled	Disabled	Disabled
Enabled	Enabled	Enabled	Enabled	Enabled

1. A Service User account should be used rather than the legacy Monitor Password, the Manager security using the setting **System | Unsecured Interfaces | Use Service User Credentials**. For default accounts that can use System Monitor in this way refer to Default Administrative Users and Rights Groups 24.
2. The legacy UDP and TCP connection methods should be disabled via the Manager security setting **System | Unsecured Interfaces | DevLink**.
   - **Note:** If the legacy connection methods are not disabled, the password exchange between System Monitor and IP Office is unsecure.
3. Select the correct connection methods in the System Monitor **File | Select Unit** tab. If HTTPS is used, an identity certificate (certificate plus private key) is requested. This is used by System Monitor to identify itself. For more information about certificates and PKI, see Certificates and Trust 38.
4. To ensure only HTTPS is used, the Manager security setting **Services | HTTP | Service Security Level** should be set to disable HTTP.
   - **Note:** The IP Office HTTP service is used by many components including H323 phones, IP Office lines, SoftConsole, Voicemail Pro and one-X Portal for IP Office.
5. Any log files saved by System Monitor may be read by any other System Monitor instance without authorization. This file can include configuration and other sensitive information and therefore access to these files must be controlled.

Página3071 de 3226.

8.16.6 Securing Voicemail Pro

1. Using the Voicemail Pro client, the password for the default administration account 'Administrator' must be changed to a 'strong' password of 8 or more characters. Any unused accounts must be deleted.

   - **Note:**
     For Voicemail Pro R9.0 and higher on Server Edition, Unified Communications Module and Linux Application Server, all authentication is referred to the 'local' IP Office – the default administration account is only used under failure conditions. For Unified Communications Module and Linux Application Server, the local IP Office is a management instance running on the server itself. See User Accounts and Rights of Access 22 for more information.

2. Using the Voicemail Pro client, configure the password used to access the IP Office in **Administration | Preferences | General | Voicemail Password**. This password must match the password entered in the Manager setting **Security | System | Unsecured Interfaces | Voicemail Password**. The password should be 31-characters.

   - For new systems, a suitable 31-character password is automatically generated and used on the first connection between the IP Office and Voicemail Pro services.
   - Existing systems upgraded to IP Office R11.1 FP1 can continue to use their existing shorter password but are forced to a 31-character password on any change.

3. The IP Office configuration setting **System | Voicemail | Voicemail IP Address** must not be left at 255.255.255.255, but set to the IP Address of the Voicemail Pro server.

4. Only users and groups that are entitled to use voicemail should have their mail box activated. All others should be disabled using the Voicemail Pro client disable mailbox feature.

   - **Note:**
     Disabling the mailbox will also disable IMAP, MAPI, email and Web Voicemail integrations for that user

5. All mailboxes must be protected by password/Voicemail Code access, except when connecting from trusted extensions (by the use of the **User | Source Numbers** field). The recommended minimum is 4 digits for internal use, 9 when the mailbox can be accessed externally.

6. The mailbox password/Voicemail Code policy should be enforced by setting the voicemail Default Telephony Interface to Intuity in the Voicemail Pro client, and minimum PIN Length to 4 or 9 using the Manager setting **System | Voicemail | Voicemail Code Complexity**.

   - **Note:** If IP Office voicemail TUI is used, the users are not forced to set a new password/Voicemail Code on initial mailbox access.

7. To prevent Toll fraud via the outdialling feature, it can be disabled on the IP Office Configuration **System | Voicemail** tab in IP Office Manager. Where outcalling is required, the call barring steps of Preventing Unwanted Calls 84 must be used.

8. To prevent Toll fraud via call flows, all call flows must have adequate protection against dialing unauthorized numbers. Where external calling is required, the call barring steps of Preventing Unwanted Calls 84 must be used.

9. Where a phone is in an un-controlled area the default Trusted Source Number for Voicemail access should be removed, so that all IP Office Voicemail access requires entering the Voicemail access code, even from the User's home extension.

10. Disable all unused services such as SMTP and MAPI.

11. If the SMTP send feature is used, authentication should be used. TLS is always enforced.

12. If the IMAP4 server feature is used, TLS should be used.

13. If the host server operating system is Microsoft Windows, consult the relevant Microsoft OS security guidelines, which can be found at https://technet.microsoft.com/en-us/library/windows-server-security.aspx. More general information can be found at https://technet.microsoft.com/en-us/security/default.aspx

14. If the application is not used, it should be disabled using the Web Control **Settings | System | Services | Automatic Start** setting.

8.16.7 Securing Embedded Voicemail

1. Only users and groups that are entitled to use voicemail should have their mailbox activated.
2. All mailboxes must be protected by password/Voicemail Code access, except when connecting from trusted extensions (by the use of the **User | Source Numbers** field). The recommended minimum is 4 digits for internal use, 9 when the mailbox can be accessed externally.
3. The mailbox password/Voicemail Code policy should be enforced by setting the **System | Voicemail | Voicemail Mode** to ***Intuity Mode***, and minimum PIN Length to 4 or 9 using the Manager setting **System | Voicemail | Voicemail Code Complexity**.
   - **Note:**
     If IP Office voicemail TUI is used, the users are not forced to set a new password/Voicemail Code on initial mailbox access.
4. Where a phone is in an un-controlled area, the default Trusted Source Number for Voicemail access should be removed, so that all IP Office Voicemail access requires entering the Voicemail access code, even from the User's home extension.

8.16.8 Securing Contact Recorder

- Contact Recorder gives full administrator rights to the first access of the web administration page, therefore is it important to configure the name and password as soon as possible. See the section General Setup > Recorder in "*Administering Avaya IP Office ™ Platform Contact Recorder*".
- All passwords must be 'strong' and of 8 or more characters (see Password and PIN Management 32). Any unused accounts must be deleted.
- The unsecure administrative interface (HTTP) should be disabled using the web admin interface and set **System | Manage Users | Allow unencrypted (http)** access to ***No***. See the section "General Setup > Recorder" in *"Administering Avaya IP Office ™ Platform Contact Recorder*".
- The Advanced Security section of the Contact Store documentation should be reviewed, however the changing of Contact Recorder ports is not recommended.
  - **Note:**
    Contact Recorder does not support referred authentication; local user accounts are used at all times.
- If the application is not used, it should be disabled using the Web Control **Settings | System | Services | Automatic Start** setting.

8.16.9 Securing one-X Portal for IP Office

1. Log in to the default one-X Portal for IP Office Administrator account and change the password to a strong password of 8 or more characters.

   - **Note:**
     This account is used by one-X Portal for IP Office if the IP Office authentication service is not available, see User Accounts and Rights of Access 22 for more information.

2. For subsequent password management, go to the one-X Portal for IP Office **Configuration | Users** page. Any unused administrator accounts must be deleted.

3. On the one-X Portal for IP Office administration page, navigate to **Configuration | Providers | CSTA-Provider | Edit** and configure the password used to access IP Office. The password must match the password configured for the IP Office Manager user ID EnhTcpaService.

4. If one-X Portal for IP Office clients are to be used externally, follow Hardening for Remote Worker Operation 82.

5. If external one-X Portal for IP Office clients are configured to support VoIP calls, follow Limiting IP Network Exposure 93.

6. one-X Portal for IP Office offers both an HTTP (8080 + 8069) and HTTPS (8443/9443 + 8063) interface for web clients. HTTPS must be used for external access. The HTTP ports can be disabled using the setting **Security | Protocol | Secure Connection (HTTPS)**.

7. To administer an Identity Certificate for the HTTPS interfaces on a Linux-based server, see Update Certificates 80.

8. To administer an Identity Certificate for the HTTPS interfaces of Windows-based servers, use the one-X Portal for IP Office administration web page and import the PKCS#12 format certificate file using the setting **Configuration | Certificate | Import**. Note this certificate is specific to the one-X Portal for IP Office HTTPS interfaces and not part of the Windows OS certificate store and must include all intermediate certificates.

9. Log in to the default Superuser backup and restore account and change the password to a strong password of 8 or more characters. For subsequent password management, go to the one-X Portal for IP Office AFA page **Configuration | Edit** page.

10. If the host server operating system is Microsoft Windows, consult the relevant Microsoft OS security guidelines, which can be found at https://technet.microsoft.com/en-us/library/windows-server-security.aspx. More general information can be found at https://technet.microsoft.com/en-us/security/default.aspx

11. The Openfire console should not be enabled under normal use, if under exceptional circumstances – and only under the direction of Avaya – it is enabled, the console must be disabled as soon as practical. The command to disable is at:
    http://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/oneXportaladmin/diabling_openfire_admin_consol.htm

12. If the application is not used, it should be disabled using the **Web Control Settings | System | Services | Automatic Start** setting.

8.16.10 Securing WebRTC Gateway

1. If the application is not used, it should be disabled using the Web Control settings **System | Services | Automatic Start** setting.

8.16.11 Securing Media Manager

1. If the application is not used, it should be disabled using the Web Control setting **System | Services | Automatic Start** setting.
2. If SMTP emails are used for alarms and events select the Secured Connection option using the IP Office Web Manager setting **Applications | Media Manager | Configuration**.

8.16.12 Securing Integrated Call Reporter

1. If the application is not used, it should be disabled using the Web Control setting **System | Services | Automatic Start** setting.

8.16.13 Securing Avaya Contact Center Applications

1. Whenever IP Office Contact Centre (IPOCC) and Avaya Contact Center Select (ACCS) are deployed with IP Office, the CTI link between IP Office and the application should be secured according to Securing CTI Interfaces 84.
2. Please refer to the relevant application documentation for all other security aspects:
   - Avaya IP Office Contact Center Feature Description
   - Avaya Contact Center Select Solution Description

8.17 Configuration and Other Sensitive Data

IP Office security settings are automatically encrypted and locked to the individual IP Office and cannot be exported, but configuration and other data for IP Office, Voicemail Pro and one-X Portal for IP Office contain some unencrypted information that may pose a security threat or privacy issue.

- Any backup data store (for example a file server used for backup/restore, copies of SD Cards) must be secured from unauthorised access
- Any backup/restore mechanism itself should be secure; IP Office, Voicemail Pro and one-X Portal for IP Office support secure backup/restore options such as HTTPS and SFTP
- Access to call recordings which are held as files on the Voicemail Pro or Contact Recorder server should be controlled
- Offline and exported configuration files, System Monitor logs and Linux server logs should be controlled using, for example, encryption with password protection. This should include any configuration or other sensitive data sent outside of the organisation.

Página3075 de 3226.

8.18 Limiting IP Network Exposure

It is vital to control the IP network access of IP Office to reduce the exposure to attack. Network security integration is outside the scope of this document; however the following section covers some items that must be reviewed as part of network security hardening.

If using any level of external IP access, IP Office must **only** be connected via a properly configured Firewall or other network security mechanism (for example, VPN, MPLS). It must **never** be connected directly.

If no external IP access is required, IP Office must be isolated using a firewall or other mechanism.

Using Manager, the IP Office IP Route table should be inspected for any gateway routes that may have been unintentionally acquired via DHCP. These should be deleted if not required and the DCHP settings modified to prevent re-occurrence.

8.18.1 Firewall

Any Firewall used must be selected, deployed, tested and managed by competent personnel to meet the needs of the IP Office deployment.

The NIST Special Publication (SP) 800-41, Guidelines on Firewalls and Firewall Policy: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf provides background information, including other helpful resources.

Only the absolute minimum of Firewall ports and protocols should be opened for use with IP Office. For example set only the port direction and protocol needed.

The relevant IP Office port matrix for each release must be used. A link to the port matrix document is located on the Avaya Product Security page at https://support.avaya.com/security.

Firewall guidelines:

- If a remote IP address is static – an ITSP SIP trunk for example – the source address should be configured to constrain the access further.
- IP Office unsecure ports/protocols should never be exposed to the Internet.
- If using a stateful Firewall, H.323 and SIP inspection should be turned off as this will interfere with IP Office operation.

8.18.2 Session Border Controller

The Avaya SBCE is recommended to be located behind the Enterprise firewall, and serves as a security and demarcation device between the IP-PBX and the Carrier facility. Avaya also supports an implementation of the Avaya SBCE parallel to the firewall, although it is better as recommended for best practices security to put it behind the firewall as part of a layered defence strategy. The Avaya SBCE performs NAT traversal, securely anchors signalling and media, and can normalize SIP protocol implementation differences between carrier and Enterprise SIP implementations.

- **Note:**
  If an SBC or SIP Application Level Gateway (ALG) is deployed, some of the IP Office security measures must be moved from the IP Office to the SBC/ALG; the IP Office source IP address blacklisting should be disabled with the No User Source Number 'B_DISABLE_SIP_IPADDR'. The SBC/ALG black/white listing must be activated to compensate.

8.18.3 Remote Maintenance Access

Both System Status Application and System Monitor access to IP Office can be secured, and events/alarms sent to syslog servers (including the IP Office Primary Server) using the TLS protocol.

IP Office SNMP should not be used without additional security measures such as Virtual Private Network (VPN).

All IP Office systems supports secure and high integrity SSLVPN connectivity, and Avaya offers IP Office Support Services (IPOSS) based on this technology. For more information, see Deploying IP Office ™ Platform SSL VPN Services.

For IP Office deployment in an enterprise or branch environment, Avaya's Secure Access Link (SAL) gateway can be utilised.

Página3076 de 3226.

8.19 Secure Maintenance Interfaces

Events and alarms can be securely sent to syslog servers (including the IP Office Primary Server) using the TLS protocol. This can be enabled using the Manager setting **System | System Events | Alarms | Syslog | Protocol**.

Both System Status Application and System Monitor access to IP Office can be secured. See Securing System Status Application 90 and Securing System Monitor 90.

SNMP should not be used as this is not secure.

- **Note:**
  Enabling security on these interfaces will increase the software processing of the IP Office and will be unsuitable for instances where high traffic is expected. In this instance local monitoring via unsecured interfaces or external secure solution are required. See Limiting IP Network Exposure 95.

Unsecure modems should not be left connected to the serial or analogue ports.

8.20 Restricting Physical Access

Any unauthorized physical access to the system could present attackers with an opportunity to reset the configuration and security settings, modify BIOS, access the unsecure serial port, install or modify software via the SD Card or other mechanisms.

It is essential to secure physical access to the IP Office platform; mechanisms of controlling such access outside the scope of this document.

Página3077 de 3226.

8.21 Securing Server Edition Servers

1. It is important to understand the information and recommendations of Certificates and Trust 38 to determine the certificate and trust requirements of the server as options are offered during the initial ignition process.
2. The ignition process will enforce a change to the Administrator and security passwords. It also updates the fall back accounts for one-X Portal for IP Office, Voicemail Pro and Web Control (the local Linux administration web interface).
3. All security administrator account passwords of all other systems in the Server Edition solution need to be the same. This can be done using IP Office Manager **Security | General | General** to change individual settings.
4. All Service User account credentials used for central management of all systems need to be the same. This can be done using IP Office Web Manager Security Manager **Service Users | Synchronize Service User and System Password**.
5. Apply a password policy to the Web Control application using IP Office Web Manager Platform **Settings | System | Password Rules Settings**.
6. Enable the setting IP Office Web Manager Platform **Settings | System | Authentication | Enable referred authentication**. This will refer all Web Control logins to the local IP Office. The local Linux Administrator account credentials are only used under failure conditions.
7. Disable the HTTP backup/restore server using IP Office Web Manager setting **Platform View | Settings | System | HTTP Server**. From R9.1, an HTTPS backup/restore server is always active for this purpose.
8. Enable the internal server firewall to apply DoS and DDos attack filters using IP Office Web Manager setting **Platform View | Settings | System | Firewall Settings | Activate**.
   - Note: The firewall support on Server Edition does not replace the need for an external firewall. For further information see Limiting IP Network Exposure 95.
9. Disable any unused unsecure TCP or UDP ports using IP Office Web Manager setting **Platform View | Settings | System | Firewall Settings | Enable TCP/UDP Ports**. This will apply filtering to all LAN 1 and LAN 2 traffic, regardless of source or destination.
10. If the ingress ports utilized by all IP Office operations conform to the following table, the setting **Platform View | Settings | System | Firewall Settings | Enable Filter** can be activated:

Protocol	Ports
TCP	22, 25, 37, 143, 389, 411, 443, 445, 514, 993, 1433, 1434, 1718:1720, 4097, 4560, 5060:5061, 5222, 5269, 5443, 5800:5899, 6514, 7070:7071, 7443, 8005, 8063, 8084, 8087, 8135, 8411, 8444, 8666, 8443, 8805, 9092, 9094, 9095, 9443, 9444, 9888, 32768:65280
UDP	37, 53, 67, 68, 123, 161, 162, 389, 500, 514, 520, 1024:65535

    For more information on IP Office port/protocol usage, see the relevant IP Office port matrix which can be found at https://support.avaya.com/security.
11. If not required, disable the syslog receiver on the **Primary Settings | General** tab.
12. If not required, remove the syslog client on the Secondary and each Expansion System using the Manager setting **System | System Events | Alarms | Destination Syslog**.
    - **Note:**
      Removing the syslog destination will stop audit trail and security events being sent to the Primary Server.
13. If not required, disable the Enhanced Access Security Gateway (EASG) support using the IP Office Web Manager setting **Platform View | Settings | EASG Settings | Status**.
14. If required, administer a new server identity certificate using IP Office Web Manager:
    a. The new identity certificate should be in a 'p12' or 'pfx' file.
    b. Set **Platform | Settings | General | Certificates | Renew automatically** active.
    c. Ideally, all certificates used to sign the new identity certificate should be in the same file.
    d. If the signing certificates are in separate files, use Security Manager | Certificates | +Add Certificate to upload each one.
    e. Set **Security Manager | Certificates | Edit | Offer ID Certificate Chain** active.
    f. Use **Security Manager | Certificates | Edit | Set** to upload the identity certificate file.
    g. The identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server, any signing certificates will be placed in the Trusted Certificate Store (TCS).
    - For more information, see Certificates and Trust on page 33 38.

Página3078 de 3226.

15. Follow Securing the IP Office Platform Solution 74.
    a. If Voicemail Pro is installed, follow Securing Voicemail Pro 91.
    b. If one-X Portal for IP Office is installed, follow Securing one-X Portal for IP Office 93.
    c. Any applications not used should be disabled using the Web Control **Settings | System | Services | Automatic Start** setting. Note that IP Office and Management Services should never be disabled.
16. Do not activate the server's Intelligent Platform Management Interface (IPMI) – this effectively grants physical access to the server.

8.22 Securing Linux Application Server/Unified Communications Module

The Linux Application Server and Unified Communications Module (Unified Communications Module) run a 'Management' IP Office instance. A management IP Office is a single installation of selected IP Office features running on Linux with management and maintenance services enabled. All telephony functions are disabled and no licensing is required.

1. It is important to understand the information and recommendations of Certificates and Trust 38 to determine the certificate and trust requirements of the server as options are offered during the initial ignition process.
2. The ignition process will enforce a change to the Administrator and security passwords. It also updates the fall back accounts for one-X Portal for IP Office, Voicemail Pro and Web Control (the local Linux administration web interface).
3. Apply a password policy to the Web Control application using **Settings | System | Password Rules Settings**.
4. Enable the setting **Settings | System | Authentication | Enable referred authentication**. This will refer all Web Control logins to the management IP Office. The local Linux Administrator account credentials are only used under failure conditions.
5. Use IP Office Manager to load the security settings of the IP Office Shell Server that co-resides on the Linux Application Server/Unified Communications Module at the same IP address.
   - **Note:** This is not the Unified Communications Module host IP500 V2 address.
6. Follow Securing the IP Office Platform Solution 74.
7. Disable the HTTP backup/restore server using **Settings | System | HTTP Server**. From R9.1, an HTTPS backup/restore server is always active for this purpose.
8. Disable any unused unsecure ports/protocols using **Settings | System | Firewall Settings**. This will apply filtering to all LAN 1 and LAN 2 traffic, regardless of source or destination.
   - **Note:**
     The firewall support on the Linux Application Server do not replace the needs for an external firewall. For further information see Limiting IP Network Exposure 95.
9. If not required, disable the Enhanced Access Security Gateway (EASG) support using the IP Office Web Manager setting **Platform View | Settings | EASG Settings | Status**.
10. If required, administer a new server identity certificate on the IP Office Shell Server using the IP Office Manager **System | Certificates | Identity Certificate | Set**; this identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server. Alternatively if the system is an Linux Application Server, the Web Control **Settings | General | Certificates | Identity Certificates** settings can be used. For more information see Certificates and Trust 38.
11. If required, administer a new server identity certificate on the IP Office Shell Server using the IP Office Manager **System | Certificates | Identity Certificate | Set**; this identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server. For more information see Certificates and Trust 38.
12. If Voicemail Pro is installed, follow Securing Voicemail Pro 91.
13. If Contact Recorder is installed, follow Securing Contact Recorder 92.
14. If one-X Portal for IP Office is installed, follow Securing one-X Portal 93.
15. Any applications not used should be disabled using the Web Control setting **System | Services | Automatic Start** setting. Note that IP Office and Management Services should never be disabled.
16. Do not activate the server's Intelligent Platform Management Interface (IPMI) – this effectively grants physical access to the server.

Chapter 9.

Monitoring the IP Office Platform

9. Monitoring the IP Office Platform

Constant and consistent monitoring ensures any threats can be identified early and reacted to. In addition to threat monitoring, existing installations should be reviewed for changes in security requirements that may be caused by customer needs, technology, or regulation.

- Activate all necessary reporting. See Activating Reporting 106.
- Monitor all alarms and logs, especially for repeated failed logins or other evidence of attack
- Detect other unusual activity, for example:
- New VoIP extensions
  - Forwarding set
  - Phones dialling unexpectedly
  - Unable to make outgoing calls
  - Unusual call destinations
  - Unusual call volumes or time of day/week
  - High phone bill
  - Unable to login to phones or applications
  - Unable to use voicemail
  - The string 'Barred' in SMDR reports
  - The syslog tag of 'IPTables-Rejected' in Linux server syslog events.
- Review Avaya Security advisories
- Review Avaya IP Office application notes, technical bulletins and tips
- Ensure the latest IP Office service packs are applied
- Monitor telephony provider communications
- Conduct periodic security reassessment

9.1 Checks and Tests

Thorough checks and tests should be carried out to ensure the deployment is secure and no previous attacks have compromised the system:

- **Note:**
  Care must be taken not to inadvertently expose sensitive data as a by-product of testing activities.
- Check LAN1/LAN2 do not have public IP addresses, that is, directly accessible from the internet.
- Check the IP Office for unsecure internet or inbound IP access by identifying the public IP address of the Firewall (for example, by using http://whatismyipaddress.com), then attempting access to the IP Office ports defined by the Port Matrix document. The following table contains some example ports that should be tested.

Note: This port list is not exhaustive and can vary from release to release. A link to the port matrix document is located at https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/general/port_matrix/index.htm.

Port	Protocol	Use	Possible test Tool	Notes
22	TCP	SSH	SSH, Nmap or other port scanner	Linux servers only
69	UDP	TFTP	Nmap or other port scanner	A TFTP RRQ of 'nasystem/who_is' can be used
80	TCP	HTTP	Browser, Nmap or other port scanner	http://[IP Address] can be used
143	TCP	IMAP	Nmap or other port scanner	Voicemail Pro only
161	UDP	SNMP	SNMP test tool, Nmap or other port scanner	
411	TCP	HTTP	Nmap or other port scanner	
443	TCP	HTTPS	Browser, Nmap or other port scanner	https://[IP Address] can be used
993	TCP	IMAP-TLS	Nmap or other port scanner	Voicemail Pro only
1300	TCP	H323-TLS	Nmap or other port scanner	
1720	TCP	H323	Nmap or other port scanner	
5060	UDP	SIP	Nmap or other port scanner	
5061	TCP	SIP	Nmap or other port scanner	
5443	TCP	HTTPS	Nmap or other port scanner	Linux servers only
7070	TCP	HTTPS	Browser, Nmap or other port scanner	Linux servers only https://[IP Address]:7070 can be used
7071	TCP	HTTPS	Browser, Nmap or other port scanner	Linux servers only https://[IP Address]:7071 can be used
8000	TCP	HTTP	Nmap or other port scanner	Linux servers only
8069	TCP	HTTP	Nmap or other port scanner	one-X Portal for IP Office only
8080	TCP	HTTP	Browser, Nmap or other port scanner	https://[IP Address]:8080/onexportal-admin.html can be used
8086	TCP	HTTP	Nmap or other port scanner	one-X Portal for IP Office only
8411	TCP	HTTPS	Nmap or other port scanner	
8443	TCP	HTTPS	Nmap or other port scanner	
9443	TCP	HTTPS	Nmap or other port scanner	one-X Portal for IP Office only
50791	TCP		VMPro Client, Nmap or other port scanner	
50792	UDP		Nmap or other port scanner	
50793	TCP		Nmap or other port scanner	IP500 V2 only
50794	UDP + TCP	SysMonitor	SysMonitor, Nmap or other port scanner	
50796	TCP	TLS	Nmap or other port scanner	
50804	TCP		IP Office Manager, Nmap or other port scanner	
50805	TCP	TLS	IP Office Manager, Nmap or other port scanner	
50808	TCP		SSA, Nmap or other port scanner	

Página3084 de 3226.

Port	Protocol	Use	Possible test Tool	Notes
50809	TCP	TLS	SSA, Nmap or other port scanner	
50812	TCP		IP Office Manager, Nmap or other port scanner	
50813	TCP	TLS	IP Office Manager, Nmap or other port scanner	
50814	TCP		Nmap or other port scanner	

Table 24: Example Ports

If access is successful, it can indicate a misconfigured Firewall or other network protection system.

- Attempt to log into the servers using the set of default administrator accounts and passwords in the following table.
  - Note: Default accounts from previous releases are not removed on upgrade.

Default Account Name	Domain	Possible test Tool	Notes
security **Administrator** **Manager** **Operator** **BusinessPartner** **Maintainer** **IPDECTService** **SMGRB5800Admin** **BranchAdmin**	IP Office	IP Office Web Manager IP Office Manager	All servers, including IP500 V2 and Unified Communications Module
Administrator	Voicemail Pro	VMPro client	Voicemail Pro only
Administrator	one-X Portal for IP Office	Browser	one-X Portal for IP Office only
Administrator	Web Control	Browser	Linux servers only
root	Linux	Console interface	Linux servers only

If access is successful, the account credentials should be changed or the account removed. See Remove unnecessary accounts 76 for more information on account removal

- Use IP Office Manager to load the configuration and review all errors and warnings with particular reference to passwords. None should be present.
- Check for unexpected Extensions and Users
- Check all users' settings for unusual forwarding destinations
- Ensure All SIP Extensions' **Extension | Extn | Force Authorisation** setting has not been disabled.
- Check the special IP Office user 'NoUser' **Source Number** field; any unexpected entries should be clarified with support personnel. NoUser source numbers are sometimes used to enable specific features or behaviour.
- Check that the padlock symbol is displayed on the bottom right of the screen, indicating a secure connection to IP Office.
- Use IP Office Manager to load the security settings and review all warnings; none should be present.
- Again, check that the padlock symbol is displayed on the bottom right of the screen, indicating a secure connection to IP Office.
- Log on to one-X Portal for IP Office administration page, if a warning is displayed 'Change Administrator Default Password' the administrator account is at default.
- For R9.0+, if login to Web Control, one-X Portal for IP Office or Voicemail Pro fails unexpectedly, check the IP Office security settings for the account being used; it must have a rights group assigned which contains the correct 'External' rights.
- Check successful and failed logins produce the expected reports and results.
- Test the call barring, emergency calls, authorisation codes, Voicemail Pro outcalling and call flows. Testing of Emergency Calls must be arranged in advance with the PCSP/Emergency Services to avoid prejudicing genuine emergency response.
- Review Firewall, SBC and call logger reporting.

Página3085 de 3226.

9.2 Activating Reporting

To ensure timely indication of any untoward activities on any component, various reporting mechanisms should be enabled. It is important to ensure that the reporting mechanisms themselves are reliable and secure.

- IP Office Reporting 106
- Voicemail Pro Reporting 106
- Contact Recorder Reporting 106
- one-X Portal for IP Office Reporting 107
- Linux-Based Server Reporting 107
- Other Components Reporting 107

9.2.1 IP Office Reporting

The following events and logging features are available for IP Office.

- System events for failed logins, blacklisted IP Addresses, and SSL/TLS failures, potentially indicating attempts to gain unauthorized access to the system. Available as syslog, SMTP (email), SNMP traps and displayable in SSA. For more information see:
  - "Service Alarms" in Using Avaya IP Office™ Platform System Status Application.
  - The description of the **System | System Events** tab in Administering Avaya IP Office™ Platform with Manager.
  - The file 'IP_Office_Alarms_N_N_N.xlsx' contained on the IP Office Admin DVD.
- Audit trail of administrative logins, their source and result. Available as syslog events, also displayable in SSA and Manager. NOTE that user/phone based changes are not currently captured. For more information see:
  - "Control Unit Audit" in Using *Avaya IP Office™ Platform System Status Application*.
  - **File | Advanced | Audit Trail** in Administering Avaya IP Office™ Platform with Manager.
- Detailed audit trail of all administrative changes, including security settings. Available as syslog events only.
- For Server Edition, all events are active and send via syslog to the Primary Server.
- Reports of all calls available as Station Message Detail Reporting (SMDR) message that can be sent to 3rd party call loggers. For information, see the SMDR section in Administering Avaya IP Office™ Platform with Manager

9.2.2 Voicemail Pro Reporting

The following events and logging features are available for Voicemail Pro server:

- Audit trail of administrative logins. Available as syslog events only. For more information see: "Voicemail Pro Syslog" in Administering Avaya IP Office™ Platform Voicemail Pro. By default for Server Edition, all events are active and send via syslog to the Primary.
- Voicemail box login failures are reported via the IP Office failed login alarms, see above.

9.2.3 Contact Recorder Reporting

Audit trail details of administrative logins are available as syslog events and are displayed on the web administration page. For information, see **System | Audit Trail** in Administering Avaya IP Office Platform Contact Recorder.

9.2.4 one-X Portal for IP Office Reporting

The following events and logging features are available for one-X Portal for IP Office server:

- Audit trail of administrative logins. Available as syslog events only. By default for Server Edition, all events are active and send via syslog to the Primary.
- one-X client login failures are reported via the IP Office failed login alarms, see the IP Office section above.

9.2.5 Linux-Based Server Reporting

Server Edition, Linux Application Server and Unified Communications Module servers generate security and audit logs via syslog, either saved internally or sent to a remote server.

- To enable the Linux OS security and audit logging, the following settings must be enabled on the **Web Control | Settings | General** tab.
  - Authentication and authorization privileges
  - Information stored by the Linux audit daemon (auditd)
  - Apache web server access_log and error_log
- By default for Server Edition, all events are active and send via syslog to the Primary where they can be stored, viewed and forwarded to external syslog servers. For more information see **Logs | Syslog Event Viewer** and **Settings | General | Syslog** in the Web Control application.

9.2.6 Other Components Reporting

- Firewall intrusion detection and reporting should be activated.
- SBC intrusion detection and reporting should be activated.
- Call logger unusual call activity detection and reporting should be activated.

9.3 Avaya Security Advisories and IP Office Updates

1. Register for Avaya Security Advisory notifications by using the E-Notification subscription procedures. See Avaya Product Security Support 111.
2. Register for IP Office Knowledgebase news, which includes updates on technical bulletins, application notes and technical tips using the options available at: https://ipofficekb.avaya.com/.

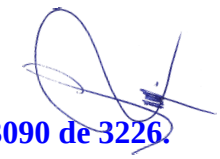
9.4 Response to Incidents

Containment, eradication and recovery is the recommended process to follow if a security incident has been detected:

- Attacked/compromised systems should be isolated or otherwise protected as soon as possible.
- Avaya customers with information regarding any discovered security problems with Avaya products should create a Service Request using the Self Service link on https://support.avaya.com, or by contacting the Customer Support phone number under the Maintenance Support link (1-800-242-2121 for US domestic customers). Non-Avaya customers wishing to report a security finding with Avaya products should send this information to securityalerts@avaya.com. See Avaya Product Security Support 111 for further information.
- Avaya provides a document to assist customers with security requests, see https://downloads.avaya.com/css/P8/documents/100161515.
- If the attack is IP based, it may be possible to trace the source IP address to the ISP it's registered to and report it. In addition the IP address or subnet can be blocked by the firewall.
- A general guide to incident handling is provided by NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Página3088 de 3226.

Chapter 10. Appendices



10. Appendices

- Appendix A - Avaya Product Security Support 111
  - Accessing Avaya Security Advisories 111
  - Interpreting an Avaya Security Advisory 111
- Appendix B - Default Trusted Certificates 112
  - Symantec Class 3 Secure Server CA - G4 in PEM format 113
  - Entrust Certification Authority - L1K in PEM format 113
  - GTS Root R1 in PEM format 114
  - GTS Root R2 in PEM format 114
  - GlobalSign Root CA - R2 in PEM format 115
  - ISRG Root X1 in PEM format 115
  - DigiCert Global Root CA in PEM format 116
  - DigiCert SHA2 Secure Server CA in PEM format 116
  - Let's Encrypt Authority X3 in PEM format 117
  - Removing a Default Trusted Certificate 117
- Appendix C - Windows Certificate Management 118
  - Windows Certificate Store Organization 118
  - Certificate Store Import 119
  - Certificate Store Export 119
  - Certificates Console 120
- Appendix D - SRTP Troubleshooting 121
  - Troubleshooting Tools 121
  - Troubleshooting Tips 121
- Appendix E - IP Office Interface Certificate Support 123
- Appendix F - IP Office VoIP Endpoint Security 127
- Appendix G - Using the IP Office Certificate Authority 131
  - Generating the CA Server's Own Identity Certificate 131
  - Generating Identity Certificates for Other Devices 132
  - Exporting the Signing Certificate 132
  - Renewing/Replacing the Signing Certificate 133
- Appendix H - Certificate Signing Requests 134
  - Creating a CSR using Microsoft MMC Certificates Snap-in 135
  - Creating a CSR using the OpenSSL Package 138
  - Creating a CSR using the Linux Server Command Line 140
  - Converting Certificate Files 141
- Appendix I - Secure Provisioning of 9600 Series H.323 Phones 142
  - Recommended Staging Process 142
  - Automated Process 143
  - Changing a Root CA Certificate 143
- Appendix J - Application/Client Security Dependencies 144

Página3091 de 3226.

10.1 Appendix A - Avaya Product Security Support

The Avaya Product Security Support Team (PSST) performs the following functions:

- Manages Avaya product vulnerabilities and threats.
- Maintains information posted at http://support.avaya.com/security.
- Performs security testing and auditing of the core products of Avaya.
- Resolves security-related field problems in support of Avaya Global Services.
- Manages the security at the securityalerts@avaya.com mailbox.

As a result, the PSST actively monitors security issues related to the following topics:

- Avaya products
- Products that are incorporated into Avaya products
- General data networking and telecommunications, as identified by government agencies

Before contacting Avaya on a security matter, please consult the Product Security Support Flow, which can be found at https://downloads.avaya.com/css/P8/documents/100161515. There is a link this document on the Avaya security support site at http://support.avaya.com/security.

When a security vulnerability is identified, the PSST determines susceptibility of Avaya products to those vulnerabilities and follows a process according to the Avaya's Product Security Vulnerability Response Policy defined at https://downloads.avaya.com/css/P8/documents/100045520. Depending on the category of risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

10.1.1 Accessing Avaya Security Advisories

Avaya Security Advisories are posted on the Security Support web site at http://support.avaya.com/security. Customers can register at Avaya Support web site to receive email notifications of Avaya security advisories.

10.1.2 Interpreting an Avaya Security Advisory

The precise definitions that PSST follows in classifying vulnerabilities relative to their potential threat to Avaya products is available in the Avaya's Product Security Vulnerability Response Policy at https://downloads.avaya.com/css/P8/documents/100045520.

10.2 Appendix B - Default Trusted Certificates

IP Office does not trust all certificate authorities by default; only the minimum required for initial operation are included. There are three certificates that are trusted by IP Office and are present on initial default and security settings reset:

Name	Duration	Thumbnail	Usage
Symantec Class 3 Secure Server CA - G4	30 October 2023 23:59:59	ff67367c5cd4de 4ae18bcce1d70fdabd7c866135	A Symantec intermediate certificate authority owned by Avaya. Trusts the Avaya SSLVPN server and on-boarding files used for the Avaya IP Office Support Services (IPOSS). Required for IP Office registration and connection to IPOSS.
Entrust Certification Authority - L1K	Start (yymmddhhmmss): 20151005191356Z End (yymmddhhmmss): 20301205194356Z		Required for Apple Push Notification Support and Avaya Spaces SSO
GTS Root R1	Start (yymmddhhmmss): 20160622000000Z End (yymmddhhmmss): 20360622000000Z		Required for Apple Push Notification Support and Avaya Spaces SSO
GTS Root R2	Start (yymmddhhmmss): 20160622000000Z End (yymmddhhmmss): 20360622000000Z		Required for Apple Push Notification Support and Avaya Spaces SSO
GlobalSign Root CA - R2	Start (yymmddhhmmss): 20061215080000Z End (yymmddhhmmss): 20211215080000Z		Required for Apple Push Notification Support and Avaya Spaces SSO
ISRG Root X1	Start (yymmddhhmmss): 20150604110438Z End (yymmddhhmmss): 20350604110438Z		Required to trust certificates issued by Let's Encrypt, used by IP Office Containerised
DigiCert Global Root CA	Start (yymmddhhmmss): 20061110000000Z End (yymmddhhmmss): 20311110000000Z		Required for Apple Push Notification Support and Avaya Spaces SSO
DigiCert SHA2 Secure Server CA	Start (yymmddhhmmss): 20130308120000Z End (yymmddhhmmss): 20230308120000Z		Required for Apple Push Notification Support and Avaya Spaces SSO
Let's Encrypt Authority X3	Start (yymmddhhmmss): 20160317164046Z End (yymmddhhmmss): 20210317164046Z		Required to trust certificates issued by Let's Encrypt, used by IP Office Containerised

Página3093 de 3226.

10.2.1 Symantec Class 3 Secure Server CA - G4 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFODCCBCCgAwIBAgIQUT+5dDhwtzRAQY0wkwaZ/zANBgkqhkiG9w0BAQsFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMTMxMDMxMDAwMDAwWhcNMjMxMDMwMjM1OTU5WjB+MQsw
CQYDVQQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24xHzAdBgNV
BAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxLzAtBgNVBAMTJlN5bWFudGVjIENs
YXNzIDMgU2VjdXJlIFNlcnZlciBDQSAtIEc0MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAstgFyhx0LbUXVjnFSlIJluhL2AzxaJ+aQihiw6UwU35VEYJb
A3oNL+F5BMm0lncZgQGUWfm893qZJ4Itt4PdWid/sgN6nFMl6UgfRk/InSn4vnlW
9vf92Tpo2otLgjNBEsPIPMzWlnqEIRoiBAMnF4scaGGTDw5RgDMdtLXO637QYqzu
s3sBdO9pNevK1T2p7peYyo2qRA4lmUoVlqTObQJUHypqJuIGOmNIrLRM0XWTUP8T
L9ba4cYY9Z/JJV3zADreJk20KQnNDz0jbxZKgRb78oMQw7jW2FUyPfG9D72MUpVK
Fpd6UiFjdS8W+cRmvvW1Cdj/JwDNRHxvSz+w9wIDAQABo4IBYzCCAV8wEgYDVR0T
AQH/BAgwBgEB/wIBADAwBgNVHR8EKTAnMCWgI6Ahhh9odHRwOi8vczEuc3ltY2Iu
Y29tL3BjYTMtZzUuY3JsMA4GA1UdDwEB/wQEAwIBBjAvBggrBgEFBQcBAQQjMCEw
HwYIKwYBBQUHMAGGE2h0dHA6Ly9zMi5zeW1jYi5jb20wawYDVR0gBGQwYjBgBgpg
hkgBhvhFAQc2MFIwJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cuc3ltYXV0aC5jb20v
Y3BzMCgGCCsGAQUFBwICMBwaGmh0dHA6Ly93d3cuc3ltYXV0aC5jb20vcnBhMCkG
A1UdEQQiMCCkHjAcMRowGAYDVQQDExFTeW1hbnRlY1BLSS0xLTUzNDAdBgNVHQ4E
FgQUX2DPYZBV34RDFIpgKrL1evRDGO8wHwYDVR0jBBgwFoAUf9Nlp8Ld7LvwMAnz
Qzn6Aq8zMTMwDQYJKoZIhvcNAQELBQADggEBAF6UVkndji1l9cE2UbYD49qecxny
H1mrWH5sJgUs+oHXXCMXIiw3k/eG7IXmsKP9H+IyqEVv4dn7ua/ScKAyQmW/hP4W
Ko8/xabWo5N9Q+l0IZE1KPRj6S7t9/Vcf0uatSDpCr3gRRAMFJSaXaXjS5HoJJtG
QGX0InLNmfiIEfXzf+YzguaoxX7+0AjiJVgIcWjmzaLmFN5OUiQt/eV5E1PnXi8t
TRttQBVSK/eHiXgSgW7ZTaoteNTCLD0IX4eRnh8OsN4wUmSGiaqdZpwOdgyA8nTY
Kvi4Os7X1g8RvmurFPW9QaAiY4nxug9vKWNmLT+sjHLF+8fk1A/yO0+MKcc=
-----END CERTIFICATE-----
```

10.2.2 Entrust Certification Authority - L1K in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIMDulMwwAAAABR03eFMA0GCSqGSIb3DQEBCwUAMIG+MQsw
CQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2Vl
IHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMDkg
RW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIwMAYDVQQD
EylFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjAeFw0x
NTEwMDUxOTEzNTZaFw0zMDEyMDUxOTQzNTZaMIG6MQswCQYDVQQGEwJVUzEWMBQG
A1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5lbnRydXN0Lm5l
dC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAt
IGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IC0gTDFLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmqAJqOV38pa9vH4SEkqjrQ
jUcj0u1yFvCRIdJdt7hLqIOPt5EyaM/OJZMssn2XyP7BtBe6CZ4DkJN7fEmDImiK
m95HwzGYei59QAvS7z7Tsoyqj0ip/wDoKVgG97aTWpRzJiatWA7lQrjV6nN5ZGhT
JbiEz5R6rgZFDKNrTdDGvuoYpDbwkrK6HIiPOlJ/915tgxyd8B/lw9bdpXiSPbBt
LOrJz5RBGXFEaLpHPATpXbo+8DX3Fbae8i4VHj9HyMg4p3NFXU2wO7GOFyk36t0F
ASK7lDYqjVs1/lMZLwhGwSqzGmIdTivZGwIDAQABo4IBDDCCAQgwDgYDVR0PAQH/
BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwMwYIKwYBBQUHAQEEJzAlMCMGCCsG
AQUFBzABhhdodHRwOi8vb2NzcC5lbnRydXN0Lm5ldDAwBgNVHR8EKTAnMCWgI6Ah
hh9odHRwOi8vY3JsLmVudHJ1c3QubmV0L2cyY2EuY3JsMDsGA1UdIAQ0MDIwMAYE
VR0gADAoMCYGCCsGAQUFBwIBFhpodHRwOi8vd3d3LmVudHJ1c3QubmV0L3JwYTAd
BgNVHQ4EFgQUgqJwdN28Uz/Pe9T3zX+nYMYKTL8wHwYDVR0jBBgwFoAUanImetAe
733nO2lR1GyNn5ASZqswDQYJKoZIhvcNAQELBQADggEBADnVjpiDYcgsY9NwHRkw
y/YJrMxp1cncN0HyMg/vdMNY9ngnCTQIlZIv19+4o/0OgemknNM/TWgrFTEKFcxS
BJPok1DD2bHi4Wi3Ogl08TRYCj93mEC45mj/XeTIRsXsgdfJghhcg85x2Ly/rJkC
k9uUmITSnKa1/ly78EqvIazCP0kkZ9Yujs+szGQVGHLlbHfTUqi53Y2sAEo1GdRv
c6N172tkw+CNgxKhiucOhk3YtCAbvmqljEtoZuMrx1gL+1YQ1JH7HdMxWBCMRON1
exCdtTix9qrKgWRs6PLigVWXUX/hwidQosk8WwBD9lu51aX8/wdQQGcHsFXwt35u
Lcw=
-----END CERTIFICATE-----
```

10.2.3 GTS Root R1 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
QzEUMBIGA1UEAxMLR1RTIFJvb3QgUjEwHhcNMTYwNjIyMDAwMDAwWhcNMzYwNjIy
MDAwMDAwWjBHMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNl
cnZpY2VzIExMQzEUMBIGA1UEAxMLR1RTIFJvb3QgUjEwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQC2EQKLHuOhd5s73L+UPreVp0A8of2C+X0yBoJx9vaM
f/vo27xqLpeXo4xL+Sv2sfnOhB2x+cWX3u+58qPpvBKJXqeqUqv4IyfLpLGcY9vX
mX7wCl7raKb0xlpHDU0QM+NOsROjyBhsS+z8CZDfnWQpJSMHobTSPS5g4M/SCYe7
zUjwTcLCeoiKu7rPWRnWr4+wB7CeMfGCwcDfLqZtbBkOtdh+JhpFAz2weaSUKK0P
fyblqAj+lug8aJRT7oM6iCsVlgmy4HqMLnXWnOunVmSPlk9orj2XwoSPwLxAwAtc
vfaHszVsrBhQf4TgTM2S0yDpM7xSma8ytSmzJSq0SPly4cpk9+aCEI3oncKKiPo4
Zor8Y/kB+Xj9e1x3+naH+uzfsQ55lVe0vSbv1gHR6xYKu44LtcXFilWr06zqkUsp
zBmkMiVOKvFlRNACzqrOSbTqn3yDsEB750Orp2yjj32JgfpMpf/VjsPOS+C12LOO
Rc92wO1AK/1TD7Cn1TsNsYqiA94xrcx36m97PtbfkSIS5r762DL8EGMUUXLeXdYW
k70paDPvOmbsB4om3xPXV2V4J95eSRQAogB/mqghtqmxlbCluQ0WEdrHbEg8QOB+
DVrNVjzRlwW5y0vtOUucxD/SVRNuJLDWcfr0wbrM7Rv1/oFB2ACYPTrIrnqYNxgF
lQIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNV
HQ4EFgQU5K8rJnEaK0gnhS9SZizv8IkTcT4wDQYJKoZIhvcNAQEMBQADggIBADiW
Cu49tJYeX++dnAsznyvgyv3SjgofQXSlfKqE1OXyHuY3UjKcC9FhHb8owbZEKTV1
d5iyfNm9dKyKaOOpMQkpAWBz40d8U6iQSifvS9efk+eCNs6aaAyC58/UEBZvXw6Z
XPYfcX3v73svfuo21pdwCxXu11xWajOl40k4DLh9+42FpLFZXvRq4d2h9mREruZR
gyFmxhE+885H7pwoHyXa/6xmld01D1zvICxi/ZG6qcz8WpyTgYMpl0p8WnK0OdC3
d8t5/Wk6kjftbjhlRn7pYL15iJdfOBL07q9bgsiG1eGZbYwE8na6SfZu6W0eX6Dv
J4J2QPim01hcDyxC2kLGe4g0x8HYRZvBPsVhHdljUEn2NIVq4BjFbkerQUIpm/Zg
DdIx02OYI5NaAIFItO/Nis3Jz5nu2Z6qNuFoS3FJFDYoOj0dzpqPJeaAcWErtXvM
+SUWgeExX6GjfhaknBZqlxi9dnKlC54dNuYvoS++cJEPqOba+MSSQGwlfnuzCdyy
F62ARPBopY+Udf90WuioAnwMCeKpSwughQtiue+hMZL77/ZRBIls6Kl0obsXs7X9
SQ98POyDGCBDTtWTurQ0sR8WNh8M5mQ5Fkzc4P4dyKliPUDqysU0ArSuiYgzNdws
E3PYJ/HQcu51OyLemGhmW/HGY0dVHLqlCFF1pkgl
-----END CERTIFICATE-----
```

10.2.4 GTS Root R2 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFWjCCA0KgAwIBAgIQbkepxlqz5yDFMJo/aFLybzANBgkqhkiG9w0BAQwFADBH
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
QzEUMBIGA1UEAxMLR1RTIFJvb3QgUjIwHhcNMTYwNjIyMDAwMDAwWhcNMzYwNjIy
MDAwMDAwWjBHMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNl
cnZpY2VzIExMQzEUMBIGA1UEAxMLR1RTIFJvb3QgUjIwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDO3v2m++zsFDQ8BwZabFn3GTXd98GdVarTzTukk3Lv
CvptnfbwhYBboUhSnznFt+4orO/LdmgUud+tAWyZH8QiHZ/+cnfgLFuv5AS/T3Kg
GjSY6Dlo7JUle3ah5mm5hRm9iYz+re026nO8/4Piy33B0s5Ks40FnotJk9/BW9Bu
XvAuMC6C/Pq8tBcKSOWIm8Wba96wyrQD8Nr0kLhlZPdcTK3ofmZemde4wj7I0BOd
re7kRXuJVfeKH2JShBKzwkCX44ofR5GmdFrS+LFjKBC4swm4VndAoiaYecb+3yXu
PuWgf9RhD1FLPD+M2uFwdNjCaKH5wQzpoeJ/u1U8dgbuak7MkogwTZq9TwtImoS1
mKPV+3PBV2HdKFZ1E66HjucMUQkQdYhMvI35ezzUIkgfKtzra7tEscszcTJGr61K
8YzodDqs5xoic4DSMPclQsciOzsSrZYuxsN2B6ogtzVJV+mSSeh2FnIxZyuWfoqj
x5RWIr9qS34BIbIjMt/kmkRtWVtd9QCgHJvGeJeNkP+byKq0rxFROV7Z+2et1VsR
nTKaG73VululycslaVNVJ1zgyjbLiGH7HrfQy+4W+9OmTN6SpdTi3/UGVN4unUu0
kzCqgc7dGtxRcw1PcOnlthYhGXmy5okLdWTK1au8CcEYof/UVKGFPP0UJAOyh9Ok
twIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNV
HQ4EFgQUu//KjiOfT5nK2+JopqUVJxce2Q4wDQYJKoZIhvcNAQEMBQADggIBALZp
8KZ3/p7uC4Gt4cCpx/k1HUCCq+YEtN/L9x0Pg/B+E02NjO7jMyLDOfxA325BS0JT
vhaI8dI4XsRomRyYUpOM52jtG2pzegVATX9lO9ZY8c6DR2Dj/5epnGB3GFW1fgiT
z9D2PGcDFWEJ+YF59exTpJ/JjwGLc8R3dtyDovUMSRqodt6Sm2T4syzFJ9MHwAiA
pJiS4wGWAqoC7o87xdFtCjMwc3i5T1QWvwsHoaRc5svJXISPD+AVdyx+Jn7axEvb
pxZ3B7DNdehyQtaVhJ2Gg/LkkM0JR9SLA3DaWsYDQvTtN6LwG1BUSw7YhN4ZKJmB
R64JGz9I0cNv4rBgF/XuIwKl2gBbbZCr7qLpGzvpx0QnRY5rn/WkhLx3+WuXrD5R
RaIRpsyF7gpo8j5QOHokYh4XIDdtak23CZvJ/KRY9bb7nE4Yu5UC56GtmwfuNmsk
0jmGwZODUNKBRqhfYlcsu2xkiAhu7xNUX90txGdj08+JN7+dIPT7eoOboB6BAFDC
5AwiWVIQ7UNWhwD4FFKnHYuTjKJNRn8nxnGbJN7k2oaLDX5rIMHAnuFl2GqjpuiF
izoHCBy69Y9Vmhh1fuXsgWbRIXOhNUQLgD1bnF5vKheW0YMjiGZt5obicDIvUiLn
yOd/xCxgXS/Dr55FBcOEArf9LAhST4Ldo/DUhgkC
-----END CERTIFICATE-----
```

10.2.5 GlobalSign Root CA - R2 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIDujCCAqKgAwIBAgILBAAAAAABD4Ym5g0wDQYJKoZIhvcNAQEFBQAwTDEgMB4G
A1UECxMXR2xvYmFsU2lnbiBSb290IENBIC0gUjIxEzARBgNVBAoTCkdsb2JhbFNp
Z24xEzARBgNVBAMTCkdsb2JhbFNpZ24wHhcNMDYxMjE1MDgwMDAwWhcNMjExMjE1
MDgwMDAwWjBMMSAwHgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEG
A1UEChMKR2xvYmFsU2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAKbPJA6+Lm8omUVCxKs+IVSbC9N/hHD6ErPL
v4dfxn+G07IwXNb9rfF73OX4YJYJkhD10FPe+3t+c4isUoh7SqbKSaZeqKeMWhG8
eoLrvozps6yWJQeXSpkqBy+0Hne/ig+1AnwblrjFuTosvNYSuetZfeLQBoZfXklq
tTleiDTsvHgMCJiEbKjNS7SgfQx5TfC4LcshytVsW33hoCmEofnTlEnLJGKRILzd
C9XZzPnqJworc5HGnRusyMvo4KD0L5CLTfuwNhv2GXqF4G3yYROIXJ/gkwpRl4pa
zq+r1feqCapgvdzZX99yqWATXgAByUr6P6TqBwMhAo6CygPCm48CAwEAAaOBnDCB
mTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUm+IH
V2ccHsBqBt5ZtJot39wZhi4wNgYDVR0fBC8wLTAroCmgJ4YlaHR0cDovL2NybC5n
bG9iYWxzaWduLm5ldC9yb290LXIyLmNybDAfBgNVHSMEGDAWgBSb4gdXZxwewGoG
3lm0mi3f3BmGLjANBgkqhkiG9w0BAQUFAAOCAQEAmYFThxxol4aR7OBKuEQLq4Gs
J0/WwbgcQ3izDJr86iw8bmEbTUsp9Z8FHSbBuOmDAGJFtqkIk7mpM0sYmsL4h4hO
291xNBrBVNpGP+DTKqttVCL1OmLNIG+6KYnX3ZHu01yiPqFbQfXf5WRDLenVOavS
ot+3i9DAgBkcRcAtjOj4LaR0VknFBbVPFd5uRHg5h6h+u/N5GJG79G+dwfCMNYxd
AfvDbbnvRG15RjF+Cv6pgsH/76tuIMRQyV+dTZsXjAzlAcmgQWpzU/qlULRuJQ/7
TBj0/VLZjmmx6BEP3ojY+x1J96relc8geMJgEtslQIxq/H5COEBkEveegeGTLg==
-----END CERTIFICATE-----
```

10.2.6 ISRG Root X1 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIRAIIQz7DSQONZRGPgu2OCiwAwDQYJKoZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQQDEwxJU1JHIFJvb3QgWDEwHhcNMTUwNjA0MTEwNDM4
WhcNMzUwNjA0MTEwNDM4WjBPMQswCQYDVQQGEwJVUzEpMCcGA1UEChMgSW50ZXJu
ZXQgU2VjdXJpdHkgUmVzZWFyY2ggR3JvdXAxFTATBgNVBAMTDElTUkcgUm9vdCBY
MTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK3oJHP0FDfzm54rVygc
h77ct984kIxuPOZXoHj3dcKi/vVqbvYATyjb3miGbESTtrFj/RQSa78f0uoxmyF+
0TM8ukj13Xnfs7j/EvEhmkvBioZxaUpmZmyPfjxwv60pIgbz5MDmgK7iS4+3mX6U
A5/TR5d8mUgjU+g4rk8Kb4Mu0UlXjIB0ttov0DiNewNwIRt18jA8+o+u3dpjq+sW
T8KOEUt+zwvo/7V3LvSye0rgTBIlDHCNAymg4VMk7BPZ7hm/ELNKjD+Jo2FR3qyH
B5T0Y3HsLuJvW5iB4YlcNHlsdu87kGJ55tukmi8mxdAQ4Q7e2RCOFvu396j3x+UC
B5iPNgiV5+I3lg02dZ77DnKxHZu8A/lJBdiB3QW0KtZB6awBdpUKD9jf1b0SHzUv
KBds0pjBqAlkd25HN7rOrFleaJ1/ctaJxQZBKT5ZPt0m9STJEadao0xAH0ahmbWn
OlFuhjuefXKnEgV4We0+UXgVCwOPjdAvBbI+e0ocS3MFEvzG6uBQE3xDk3SzynTn
jh8BCNAw1FtxNrQHusEwMFxIt4I7mKZ9YIqioymCzLq9gwQbooMDQaHWBfEbwrbw
qHyGO0aoSCqI3Haadr8faqU9GY/rOPNk3sgrDQoo//fb4hVC1CLQJ13hef4Y53CI
rU7m2Ys6xt0nUW7/vGT1M0NPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBR5tFnme7bl5AFzgAiIyBpY9umbbjANBgkq
hkiG9w0BAQsFAAOCAgEAVR9YqbyyqFDQDLHYGmkgJykIrGF1XIpu+ILlaS/V9lZL
ubhzEFnTIZd+50xx+7LSYK05qAvqFyFWhfFQDlnrzuBZ6brJFe+GnY+EgPbk6ZGQ
3BebYhtF8GaV0nxvwuo77x/Py9auJ/GpsMiu/X1+mvoiBOv/2X/qkSsisRcOj/KK
NFtY2PwByVS5uCbMiogziUwthDyC3+6WVwW6LLv3xLfHTjuCvjHIInNzktHCgKQ5
ORAzI4JMPJ+GslWYHb4phowim57iaztXOoJwTdwJx4nLCgdNbOhdjsnvzqvHu7Ur
TkXWStAmzOVyyghqpZXjFaH3pO3JLF+l+/+sKAIuvtd7u+Nxe5AW0wdeRlN8NwdC
jNPElpzVmbUq4JUagEiuTDkHzsxHpFKVK7q4+63SM1N95R1NbdWhscdCb+ZAJzVc
oyi3B43njTOQ5yOf+1CceWxG1bQVs5ZufpsMljq4Ui0/1lvh+wjChP4kqKOJ2qxq
4RgqsahDYVvTH9w7jXbyLeiNdd8XM2w9U/t7y0Ff/9yi0GE44Za4rF2LN9d11TPA
mRGunUHBcnWEvgJBQl9nJEiU0Zsnvgc/ubhPgXRR4Xq37Z0j4r7g1SgEEzwxA57d
emyPxgcYxn/eR44/KJ4EBs+lVDR3veyJm+kXQ99b21/+jh5Xos1AnX5iItreGCc=
-----END CERTIFICATE-----
```

10.2.7 DigiCert Global Root CA in PEM format

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```

10.2.8 DigiCert SHA2 Secure Server CA in PEM format

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```

10.2.9 Let's Encrypt Authority X3 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIEkjCCA3qgAwIBAgIQCgFBQgAAAVOFc2oLheynCDANBgkqhkiG9w0BAQsFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTE2MDMxNzE2NDA0NloXDTIxMDMxNzE2NDA0Nlow
SjELMAkGA1UEBhMCVVMxFjAUBgNVBAoTDUxldCdzIEVuY3J5cHQxIzAhBgNVBAMT
GkxldCdzIEVuY3J5cHQgQXV0aG9yaXR5IFgzMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAnNMM8FrlLke3cl03g7NoYzDq1zUmGSXhvb418XCSL7e4S0EF
q6meNQhY7LEqxGiHC6PjdeTm86dicbp5gWAf15Gan/PQeGdxyGkOlZHP/uaZ6WA8
SMx+yk13EiSdRxta67nsHjcAHJyse6cF6s5K671B5TaYucv9bTyWaN8jKkKQDIZ0
Z8h/pZq4UmEUEz9l6YKHy9v6Dlb2honzhT+Xhq+w3Brvaw2VFn3EK6BlspkENnWA
a6xK8xuQSXgvopZPKiAlKQTGdMDQMc2PMTiVFrqoM7hD8bEfwzB/onkxEz0tNvjj
/PIzark5McWvxI0NHWQWM6r6hCm21AvA2H3DkwIDAQABo4IBfTCCAXkwEgYDVR0T
AQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwfwYIKwYBBQUHAQEEczBxMDIG
CCsGAQUFBzABhiZodHRwOi8vaXNyZy50cnVzdGlkLm9jc3AuaWRlbnRydXN0LmNv
bTA7BggrBgEFBQcwAoYvaHR0cDovL2FwcHMuaWRlbnRydXN0LmNvbS9yb290cy9k
c3Ryb290Y2F4My5wN2MwHwYDVR0jBBgwFoAUxKexpHsscfrb4UuQdf/EFWCFiRAw
VAYDVR0gBE0wSzAIBgZngQwBAgEwPwYLKwYBBAGC3xMBAQEwMDAuBggrBgEFBQcC
ARYiaHR0cDovL2Nwcy5yb290LXgxLmxldHNlbmNyeXB0Lm9yZzA8BgNVHR8ENTAz
MDGgL6AthitodHRwOi8vY3JsLmlkZW50cnVzdC5jb20vRFNUUk9PVENBWDNDUkwu
Y3JsMB0GA1UdDgQWBBSoSmpjBH3duubRObemRWXv86jsoTANBgkqhkiG9w0BAQsF
AAOCAQEA3TPXEfNjWDjdGBX7CVW+dla5cEilaUcne8IkCJLxWh9KEik3JHRRHGJo
uM2VcGfl96S8TihRzZvoroed6ti6WqEBmtzw3Wodatg+VyOeph4EYpr/1wXKtx8/
wApIvJSwtmVi4MFU5aMqrSDE6ea73Mj2tcMyo5jMd6jmeWUHK8so/joWUoHOUgwu
X4Po1QYz+3dszkDqMp4fklxBwXRsW10KXzPMTZ+sOPAveyxindmjkW8lGy+QsRlG
PfZ+G6Z6h7mjem0Y+iWlkYcV4PIWL1iwBi8saCbGS5jN2p8M+X+Q7UNKEkROb3N6
KOqkqm57TH2H3eDJAkSnh6/DNFu0Qg==
-----END CERTIFICATE-----
```

10.2.10 Removing a Default Trusted Certificate

To remove that default trust a file can be used with, use the IP Office Trusted Certificate Store delete feature:

- Create a text file with an extension '.pem', open and copy the above PEM data including the 'BEGIN CERTIFICATE' and 'END CERTIFICATE' lines. The line termination can be Windows or Linux.
- One .pem, file per certificate
- Using the IP Office or IP Office Web Manager File Manager feature, copy the file to the ***system/primary/certificates/tcs/delete*** directory
- Restart IP Office

To add a default trusted certificate, the above steps can be followed, but copy the file to the ***system/primary/certificates/tcs/add*** directory

The default certificate feature also supports the binary DER format; see Certificates and Trust 38 for more information on certificate file formats.

Página3098 de 3226.

10.3 Appendix C - Windows Certificate Management

The certificate store used by a number of Avaya applications to save and retrieve X509 certificates is the default one provided by the Windows operating system. The Windows certificate store is relevant to the many applications running on Windows that uses certificates for security, either TLS or HTTPS, including:

- IP Office Manager
- Avaya Communicator
- Google Chrome Browser
- Safari Browser
- Microsoft Internet Explorer
- Microsoft IIS (Used by Windows Voicemail Pro)

There are some applications that currently do not use the Windows certificate store:

- IP Office SoftConsole – uses a local certificate file
- Firefox Browser – uses its own internal certificate store
- Java Runtime environment 1.6, 1.7 and 1.8 – uses its own internal certificate store
- one-X Portal on Windows server - uses a local certificate file.

- **Warning:**
  Avaya accepts no responsibility for changes made by users to the Windows operating system. Users are responsible for ensuring that they have read all relevant documentation and are sufficiently trained for the task being performed.

10.3.1 Windows Certificate Store Organization

By default, certificates are stored in the following structure:

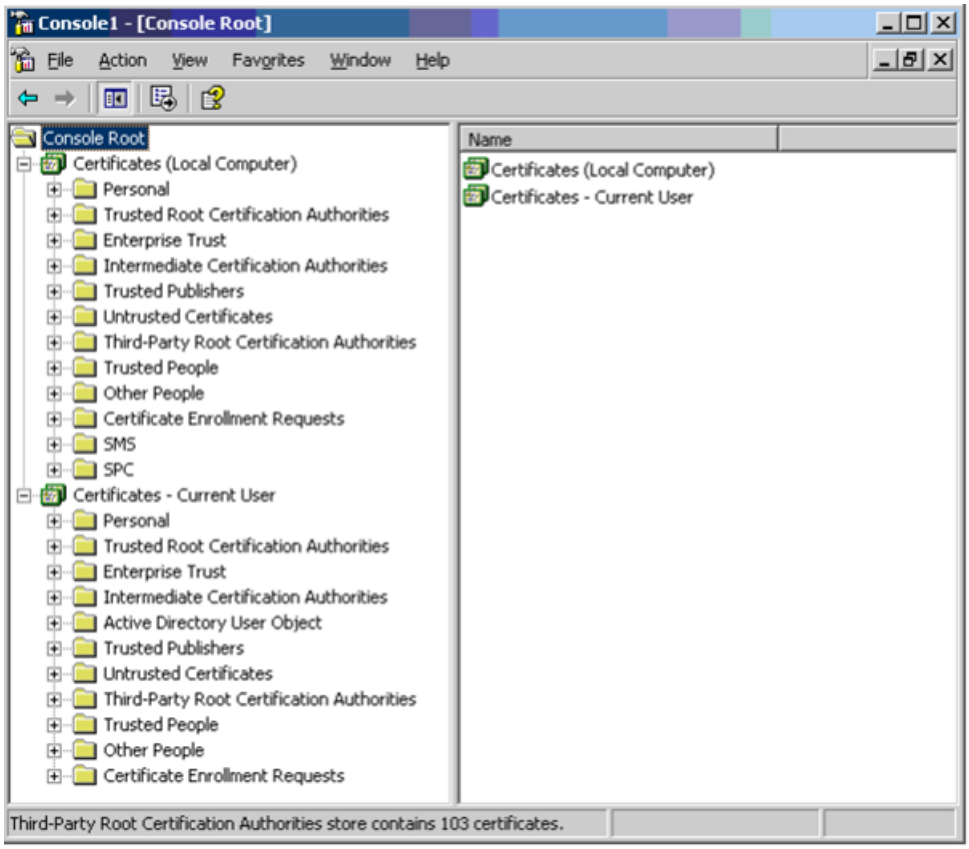


Figure 11: Default Certificate Storage Structure

Each of the sub folders has differing usage. The Certificates - Current User area changes with the currently logged-in windows user. The Certificate (Local Computer) area does not change with the currently logged-in windows user.

IP Office Manager and other Windows applications only access some of the certificate sub folders.

Página3099 de 3226.

Certificates (Local Computer) Folder	Usage
Personal | Certificates	Folder searched by Manager and some Web Browsers 1st for a certificate to send to the IP Office when requested. Certificate matched by the subject name contained in File | Preferences | Security | Certificate offered to the system. Folder accessed whenever 'Local Machine certificate store' used for Security Settings. Folder searched by Manager for matching certificate when certificate received from the system, and File |Preferences | Security | Manager Certificate Checks = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching root CA certificate when non-self-signed certificate received from IP Office, and File | Preferences | Security | Manager Certificate Checks = Medium or High. Folder searched by some browsers and other applications for matching root CA certificate when a certificate received from IP Office.

Certificates - Current User Folder	Usage
Personal | Certificates	Folder searched by Manager 2nd for a certificate to send to the IP Office when requested. Certificate matched by the subject name contained in File | Preferences | Security | Certificate offered to the system. Folder accessed whenever 'Current User certificate store' used for Security Settings. Folder searched by Manager for matching certificate when certificate received from IP Office, and File | Preferences | Security | Manager Certificate Checks = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self-signed certificate received from the system, and File | Preferences | Security | Manager Certificate Checks = Medium or High. This folder is not used by non-Microsoft applications such as Chrome or Safari browsers – the corresponding Local Computer folder is used.
Other People | Certificates	Folder searched by Manager for matching parent certificates when non-self-signed certificate received from the system, and File | Preferences | Security | Manager Certificate Checks = Medium or High. This folder is not used by non-Microsoft applications such as Chrome or Safari browsers – the corresponding Local Computer folder is used.

10.3.2 Certificate Store Import

In order to use certificates – either for security settings or Manager operation – they must be present in the windows certificate store. Certificates may be placed in the store by the Certificate Import Wizard. The Certificate Import Wizard can be used whenever a certificate is viewed. In order for Manager to subsequently access this certificate the Place all certificate in the following store option must be selected:

- If the imported certificate is to trust the IP Office, the Trusted Root Certification Authorities folder should be used, and the certificate imported should be the root CA certificate.
- If the certificate is to subsequently identify the Manager, the Personal folder should be used, and the associated private key saved as well.

10.3.3 Certificate Store Export

Any certificate required outside of the Windows PC must be first saved in the Certificate store then exported. If the certificate is to be used for identity checking (that is, to check the far entity of a link) the certificate alone is sufficient, and should be saved in PEM or DER format.

If the certificate is to be used for identification (that is, to identify the near end of a link) the certificate and private key is required, and should be saved in PKCS#12 format, along with a 'strong' password to access the resultant .pfx file.

10.3.4 Certificates Console

The Windows Certificates Console is a Microsoft Management Console (MMC) snap-in that can be used to manage the Windows certificate store including viewing, importing and exporting.

For more information on the Certificates Console, see
http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx

10.4 Appendix D - SRTP Troubleshooting

This section provides notes for SRTP troubleshooting.

10.4.1 Troubleshooting Tools

System Status Application

- Active Calls displays whether call is secure, direct media or relayed, whether SRTP is done by VCM or CPU on IP500 V2. Linux servers always use CPU.

System Monitor

- For capturing SRTP traces, set filters to default trace options plus:
  - **SIP | Sip + Verbose**
  - **Media | Media Events |Media handlers**
  - **Media | VoIP Events | VoIP + Verbose**
  - **Media | VoIP Events | Primitive + Verbose**
- During calls, in **Status | [S]RTP Sessions** window, column secure describes whether SRTP is used in that call and whether it is done by VCM or CPU on IP500 V2. Use **Show SRTP** button to display further details on SRTP sessions.

10.4.2 Troubleshooting Tips

First step in troubleshooting is to check whether the system and all participating devices are correctly configured. Some endpoints need to be registered using TLS to have SRTP available.

- Ensure that the system is using the default settings for advanced options. If that is not the case, check that it is intentional.
- If SIP devices are used and Best Effort is configured, check with SSA/System Monitor how SRTP is negotiated and whether the device supports cap neg (can be checked by placing a call to device with both SRTP and RTP and then checking whether it responds with SRTP or RTP – if it is SRTP, cap neg is supported). If not, override device media security settings and configure ***Enforce*** or ***Disabled***, as appropriate.
- IP Office lines with Best Effort configured and both crypto suites are enabled can result in large call initiation messages on IP Office lines, ~ 5000 bytes. If the link is slow and/or the call rate is high it can have a negative impact. Consider using only one crypto suite or the lines' **VoIP Settings | Media Security** setting to ***Enforce*** or ***Disabled***.
- Some phones do not support RTCP (SRTCP); verify operation with SRTCP disabled.

10.5 Appendix E - IP Office Interface Certificate Support

The following table provides an overview of certificate support for the IP Office Platform IP interfaces.

- **Note:** The relevant endpoint or server documentation should be consulted as supported features may vary with release.

For a full list of ports, see the relevant IP Office port matrix which can be found at https://support.avaya.com/security.

Link	Protocol	Cert Support	ID Cert Offered[1]	Cert Trust Checks[2]	Cert check Control[3]	Notes
IP Office						
SIP Line	SIP-TLS	✓	Tel	Bi	✓	
SM Line	SIP-TLS	✓	Tel	Bi	✓	
SIP Extension	SIP-TLS	✓	Tel	Client	✗	See IP Office VoIP Endpoint Security for more details.
H323 Extension – signalling	H323-TLS	✓	Man	Client	n/a	TLS option from R10.0 onwards See IP Office VoIP Endpoint Security for more details.
H323 Extension – provisioning	HTTPS	✓	Man	Bi	✓	See IP Office VoIP Endpoint Security for more details.
DECT R4 Provisioning	HTTPS	✓	Man	Bi	✓	See IP Office VoIP Endpoint Security for more details.
D100 Provisioning	HTTP	✗	n/a	n/a	n/a	
IP Office Line	HTTPS	✓	Man	Bi	✓	WebSocket
IP Office Manager - Security	TLS	✓	Man	Bi	✓	Manager and SE Manager
IP Office Manager - Configuration	TLS	✓	Man	Bi	✓	Manager and SE Manager
SoftConsole	HTTPS	✓	Man	IPO	✓	WebSocket
SSA	TLS	✓	Man	IPO	✗	
IP Office Web Manager (single)	HTTPS	✓	Man	Bi	✓	IP Office Web Manager single instance management over port 8443
IP Office Web Manager (solution)	HTTPS	✓	Man	Client	✗	IP Office Web Manager Server Edition management over port 7070
System Directory	HTTPS	✓	Man	Bi	✓	Central external directory feature
one-X Portal for IP Office CTI	TCP	✗	n/a	n/a	n/a	
IPOCC CTI	TLS	✓	Man	Server	✓	IP Office is the server
ACCS CTI	TLS	✓	Man	Server	✓	IP Office is the server

Página3104 de 3226.

Link	Protocol	Cert Support	ID Cert Offered[1]	Cert Trust Checks[2]	Cert check Control[3]	Notes
one-X Portal for IP Office Directory	HTTPS	✓	Man	Server	✓	IP Office is the server
Voicemail Pro	HTTPS	✓	Man	Server	✓	IP Office is the server
Backup/Restore client	HTTPS	✓	Man	Client	✓	
System Monitor	HTTPS	✓	Man	Server	✓	IP Office is the server
Voicemail Pro						
one-X Portal for IP Office status	TCP	✗	n/a	n/a	n/a	Message Status
one-X Portal for IP Office VM play	HTTPS	✓	Man	✗	✗	
Exchange WS client	HTTPS	✓	Man	Server	n/a	
SFTP Client	SSHv2	✓				Exporting voicemail and recording data
one-X Portal for IP Office						
one-XP Browser/ Call Assistant	HTTPS	✓	Man[4]	Client	✗	
Outlook, SalesForce, Lync Plugin	HTTPS	✓	Man[4]	Client	✗	
one-X Mobile Android	HTTPS	✓	Man[4]	Client	✗	See IP Office VoIP Endpoint Security 127 for more details.
one-X Mobile iOS	XMPP-TLS	✓	Man[4]	Client	✗	See IP Office VoIP Endpoint Security 127 for more details.
Communicator Windows	HTTPS	✓	Man[4]	Client	✗	See IP Office VoIP Endpoint Security 127 for more details.
Communicator iOS	XMPP-TLS	✓	Man[4]	Client	✗	See IP Office VoIP Endpoint Security 127 for more details.
Linux Server						
Backup/Restore server	HTTPS	✓	Man	Client	✗	
Web Control	HTTPS	✓	Man	Client	✗	
SSH Server	SSHv2	✓				
SFTP Server	SSHv2	✓				
WebLM Server						
Web Admin	HTTPS	✓	Man	Client	✗	WebLM is the server
Contact Recorder						
Web Admin	HTTPS	✓	Man	Client	✗	Contact Recorder is the server

Página3105 de 3226.

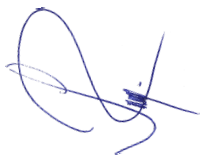
Table 25: IP Office Application Certificate Support

Notes:

1. Type of ID certificate presented:
   - **Tel** – Telephony or Management (configurable).
   - **Man** – Management certificate.
2. Support and direction of certificate trust checks:
   - **Bi** – Mutual certificate checks can be enabled.
   - **Server** – Only the server can check certificates.
   - **Client** – Only the client can check certificates.
3. The color indicates the grouping for the certificate check controls on the IP Office server component:

Color	Control	Notes
✓	Manager Security: **System | Certificates | Received Certificate Checks (Telephony)**	Any setting other than None will request a client certificate See Certificate Check Controls 52 for further information.
✓	Manager Security: **System | Services | HTTP | Service Security Level** Manager Security: **System | Certificates | Received Certificate Checks (Management)**	See Certificate Check Controls 52 for further information.
✓	Manager Configuration: **Line | Line | Security**	The HTTP service security level setting is applied first. This allows the general HTTPS server to have cert checks disabled, but still retain check for IP Office lines
✓	Manager Security: **System | Services | Security Administration | Service Security Level** Manager Security: **System | Certificates | Received Certificate Checks (Management)**	See Certificate Check Controls 52 for further information.
✓	Manager Security: **System | Services | Configuration | Service Security Level** Manager Security: **System | Certificates | Received Certificate Checks (Management)**	See Certificate Check Controls 52 for further information.
✓	Manager Security: **System | Services | Web Services | Service Security Level** Manager Security: **System | Certificates | Received Certificate Checks (Management)**	See Certificate Check Controls 52 for further information.
✓	Manager Security: **System | Certificates | Received Certificate Checks (Management)**	IP Office HTTP clients will check the server certificate against the TCS for a setting of Medium or High See Certificate Check Controls 52 for further information.
✓	Manager Security: **System | Unsecured Interfaces | TAPI = unchecked**	IP Office will check the ACCS or IPOCC server certificate against the TCS as per a setting of Medium See Certificate Check Controls 52 for further information.

4. one-X Portal for IP Office on Windows server uses a separately administered ID certificate.



10.6 Appendix F - IP Office VoIP Endpoint Security

The following table provides an overview of the various security aspects of Avaya endpoints with respect to IP Office.

- Note: The relevant endpoint or server documentation should be consulted as supported features may vary with release.

IP Office VoIP Endpoint	Secure Media	Secure Signalling[13]	Secure Remote Settings[1]	IP Office Auto-gen Settings	SIPS Support	Validate Server Cert?	Offer ID Cert?[7]	IP Office Subject Alt Name Required? [8]
Avaya H.323 Endpoint								
9608, 9611, 9621 and 9641	✓	✓ or partial[2]	✓	✓[10]	n/a	✓	✓	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1 IP.2: IP address of IP Office LAN2 IP.3: Public IP Address if remote.[14]
Other 9600 Phones	✗	✗	✓	✓	n/a	✓	✓	✗
1600 Series	✗	✗	✗	✓	n/a	✓	✓	✗
DECT R4	✗	✗	✓	✓	n/a	✓	✓	✗
IP Office[3]	✓	✓	✓	n/a	n/a	✓	✓	✗
Voicemail Pro[4]	✗	✗	✓	n/a	n/a	✗	✗	✗
Avaya SIP Endpoint								
9608, 9611, 9621, 9641[5]	✓	✓	✓	✗	✓	✓	✓	✗
1100/1200 Series[9]	✓[11]	✓	✓	✓	✗	✓	✓	IP.1: IP address of IP Office LAN1 IP.2: IP address of IP Office LAN2 IP.3: Public IP Address if remote
B179	✓[11]	✓	✓	✓	✓	✓	✓	✗
E129	✓	✓	✓	✓	✓	✓	✓	DNS.1: FQDN of IP Office DNS.2: IP address of IP Office if the phone is configured to connect to SIP server using IP address instead of FQDN[14] SIP URI: IP address of IP Office
E159	✗	✗	✗	✓	✗	✗	✗	✗
E169	✗	✗	✗	✓	✗	✗	✗	✗
H175	✓[11]	✓	✓	✓[11]	✓	✓	✓	DNS: SIP Domain Name
J129[9]	✓	✓	✓	✓	✓	✓	✓	IP.1: IP address of IP Office LAN1[14] IP.2: IP address of IP Office LAN2[14] IP.3: Public IP Address if remote[14] URI.1:'sip':SIP FQDN[14]

Página3108 de 3226.

IP Office VoIP Endpoint	Secure Media	Secure Signalling[13]	Secure Remote Settings[1]	IP Office Auto-gen Settings	SIPS Support	Validate Server Cert?	Offer ID Cert?[7]	IP Office Subject Alt Name Required? [8]
J139, J159, J169, J179	✓	✓	✓	✓	✓	✓	✓	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1[14] IP.2: IP address of IP Office LAN2[14] IP.3: Public IP Address if remote[14] URI.1:'sip':SIP FQDN[14]
K155, K165, K175 (Vantage)	✓	✓	✓	✓	✓	✓	✓	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1[14] IP.2: IP address of IP Office LAN2[14] IP.3: Public IP Address if remote[14]
Scopia XT series	✓	✓	n/a	✗	✓[6]	✓	✓	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1[14] IP.2: IP address of IP Office LAN2[14] IP.3: Public IP address if remote.[14]
Communicator iPad[12]	✓	✓	n/a	✗	✓[6]	✓	✗	✗
Communicator Windows[12]	✓	✓	n/a	✗	✓[6]	✓	✗	✗
one-X Mobile iOS	✓	✓	n/a	✗	✓[6]	✓	✗	✗
one-X Mobile Android	✓	✓	n/a	✗	✗	✓	✗	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1[14] IP.2: IP address of IP Office LAN2[14] IP.3: Public IP address of IP Office if remote[14]
D100 SIP DECT	✗	✗	✗	✓	✗	✗	✗	✗
Workplace	✓	✓	✓	✓	✓	✓	✓	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1[14] IP.2: IP address of IP Office LAN2[14] IP.3: Public IP address if remote.[14]
Avaya WebRTC Endpoint								
IP Office Web Client	✓	✓	n/a	✗	n/a	✓	✗	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1[14] IP.2: IP address of IP Office LAN2[14] IP.3: Public IP address if remote.[14]

Table 26: VoIP Endpoint Security

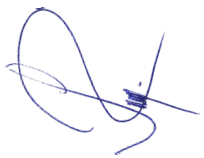
Notes:

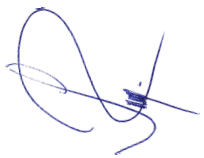
1. Ability for the phone to remotely download settings and configuration in a secure manner, typically via HTTPS.

Página3109 de 3226.

2. When H323-TLS is not used, signalling is not fully secured, but registration, SRTP Key exchange and dialled digits are.
3. IP Office line with WebSocket and security active.
4. Link between Voicemail Pro and its host IP Office. For Server Edition and Unified Communications Module this is an internal link.
5. 9608, 9611, 9621 and 9641 SIP phones only supported as Centralized Users in a branch deployment.
6. SIPS always active when Secure Signalling selected.
7. IP Office does not request certificates from SIP clients for the SIP-TLS session at present. It may request a certificate for any HTTPS transfer according to the **Mutual Authentication** setting; see Certificate Check Controls 52 for further information..
8. This column indicates whether the client requires Subject Alternative Name support within the received identity certificate from IP Office.
   Typically if DNS is used, the VoIP Endpoint only requires the FQDN of the IP Office in the SAN and no IP Address. IP Addresses and private domain names are not supported by public Certificate Authorities.
9. 1100/1200 Series and J129 phones do not support FQDNs and hence cannot be used with certificates provided by public Certificate Authorities.
10. The IP Office root CA certificate can be provisioned to the phone automatically by IP Office using the auto-generated settings file. See the Endpoint Configuration chapter of Deploying OnAvaya™ and Powered by Avaya IP Office and IP Office Contact Center For Business Partners for more information.
11. Direct media is disabled when SRTP is enabled.
12. Client does not fully support TLSv1.2; when one-X Portal for IP Office admin setting 'TLS v1.2 clients only' is active, Communicator for Windows will not connect, Communicator for iPad will operate, but without XMPP presence.
13. When VoIP endpoint resilience is active with secure signalling or secure provisioning, the root CA certificate for both home and backup server must be the same.
14. Certificate IP Address entries required only if configured to connect to signalling server using IP address. Unless a private, closed deployment utilising the Primary CA, IP addresses are not recommended.
15. Phone does not support secure RTCP (SRTCP).
16. 16. If IP address entries have to be used for the device with Public CAs which cannot have IP address name entries, some phone settings files can be enhanced to use the FQDN_IP_MAP entry. This maps IP Address entries to FQDNs. See the relevant phone documentation for support of this feature. If the IP Office Auto-gen Settings file feature is used, the FQDN_IP_MAP entry can be added to a '46xxspecials.txt' file at the same path where the phone binaries can be found. For example, to map IP Addresses to FQDN for 9608, 9611, 9621 and 9641 phones only:

```
IF $MODEL4 SEQ 9608 GOTO 96X1SETTINGS
IF $MODEL4 SEQ 9611 GOTO 96X1SETTINGS
IF $MODEL4 SEQ 9621 GOTO 96X1SETTINGS
IF $MODEL4 SEQ 9641 GOTO 96X1SETTINGS
GOTO END
# 96X1SETTINGS
SET FQDN_IP_MAP "ipol.ca.avaya.com=10.136.100.70,ipol2.ca.avaya.com=10.136.100.74"
# END
```





10.7 Appendix G - Using the IP Office Certificate Authority

The Certificate Authority (CA) feature of the Linux Application Server and Server Edition Primary can be used to:

- Generate an identity certificate for the server itself.
- Generate identity certificates for other devices including IP Office systems, phones and servers.
- Import a new signing certificate.
- Refresh the existing signing certificate.

The CA feature can be accessed via IP Office Web Manager **Platform View | Settings | Certificates | Identity Certificates**.

10.7.1 Generating the CA Server's Own Identity Certificate

By default, the Primary or Linux Applications Servers' own identity certificate is automatically created and signed by the internal CA. It is also automatically re-generated if the LAN1 IP Address, LAN2 IP Address or hostname is changed. This is controlled by the Web Management setting **Platform View | Settings | Certificates | Identity Certificates | Renew automatically**.

To manually create an identity certificate for the CA server:

1. Uncheck the setting **Platform View | Settings | Certificates | Identity Certificates | Create certificate for a different machine**.
2. Enter a unique subject name if the default offered is not acceptable. See Certificate Name Content 50 for more information.
3. Enter the subject alternative names if the default offered is not acceptable. See Certificate Name Content 50 for more information.
   It is recommended that a full set of subject alternative names are supplied to ensure compatibility with various Avaya clients and endpoints:

   DNS:<FQDN of server>, IP:<LAN1 IP address>, IP:<LAN2 IP address>, IP:<Public IP address>, DNS:<SIP domain>, URI:sip:<SIP domain>, URI: <LAN1 IP address>, URI: <LAN2 IP address>

   For example:

   ```
   DNS:example.com, IP:192.168.0.45, IP:192.168.1.45, IP:203.0.113.30, DNS:example.sip.com, URI:sip:example.sip.com, URI:192.168.0.45, URI:192.168.1.45, URI:sip:192.168.0.45
   ```

4. Enter the number of days the certificate will be valid for. The start date/time will be the current UTC time of the server. The end date/time will be start time + number of days. Identity certificates should not be valid for more than three years (1095 days). The longer the period, the greater the risk of certificate compromise.
5. Enter the Public Key Algorithm. This should be RSA-2048.
6. Enter the Secure Hash Algorithm. This should be SHA-256.
7. Check the settings and then click **Generate and Apply**. This will cause the server to generate and apply the new certificate to all interfaces during which service loss will occur.

Página3112 de 3226.

10.7.2 Generating Identity Certificates for Other Devices

To manually create an identity certificate for another device:

1. Check the setting **Platform View | Settings | Certificates | Identity Certificates | Create certificate for a different machine**.
2. Enter the Machine IP. This is used to create the file name, but not the certificate itself; an IPv4 address of that device should be entered.
3. Enter the Password; this is used to secure the identity certificate file and must conform to the complexity requirements.
4. Enter a unique subject name for the device. See Certificate Name Content 50 for more information.
5. Enter any subject alternative names. See Certificate Name Content 50 for more information.
6. Enter the number of days the certificate will be valid for. The start date/time will be the current UTC time of the server. The end date/time will be start time + number of days. Identity certificates should not be valid for more than three years (1095 days). The longer the period, the greater the risk of certificate compromise.
7. Enter the Public Key Algorithm. This should be RSA-2048 for all IP Office devices. RSA-1024 should only be used for legacy systems that cannot support RSA-2048.
8. Enter the Secure Hash Algorithm. This should be SHA-256 for all IP Office devices. SHA-1 should only be used for legacy systems that cannot support SHA-256.
9. Check the settings and then click Generate. This will cause the server to generate a PKCS#12 file containing the identity certificate, private key and signing certificate. The file is secured by the password entered and will be requested every time the file is opened.
10. A popup will prompt to save the file. Save the file to the local machine. Once the popup is close, the file will be deleted on the CA server.
11. The PKCS#12 file can now be imported into the IP Office deployment. See Update Certificates 80 and Implementing IP Office PKI 59 for more information.

10.7.3 Exporting the Signing Certificate

If the signing certificate is a root CA certificate, it will need to be exported in both PEM and DER formats for later import into various clients and servers in order to trust any identity certificate created by this CA. This does not export the private key, just the certificate.

To export the CA certificate in PEM format:

1. Select **Platform View | Settings | Certificates | CA Certificates | Download (PEM–encoded)**.
2. A popup will prompt to save the file which is named '***root-ca.pem***'. Save the file to the local machine for later distribution.

To export the CA certificate in DER format:

1. Select **Platform View | Settings | Certificates | CA Certificates | Download (DER–encoded)**.
2. A popup will prompt to save the file which is named '***root-ca.crt***'. Save the file to the local machine for later distribution.

10.7.4 Renewing/Replacing the Signing Certificate

To create a new signing certificate:

1. Select **Platform View | Settings | General | CA Certificate | Create new**.
2. This will create a completely new root CA certificate and will also require new ID certificates for all entities. The previous signing certificate will be deleted.

To keep all existing ID certificates but refresh the signing certificate:

Care must be taken not to abuse the convenience of this feature as the longer the public/private keys are unchanged, the greater the risk of compromise.

1. Select **Platform View | Settings | General | CA Certificate | Renew existing**.
2. This will create a new certificate with the same content and public/private keys, but a different serial number and start/end date.
3. Only this new root CA requires distribution, in-date existing ID certificates signed by the previous CA will still be valid.

To replace the existing signing certificate:

1. Select **Platform View | Settings | General | CA Certificate | Import**.
2. The format must be PKCS#12.
3. This will replace the signing certificate and may require new ID certificates for all entities

To back-up the signing certificate:

1. Select **Platform View | Settings | General | CA Certificate | Export**.
2. A password is requested to secure the PKCS#12 file
3. A popup will prompt to save the file which is named '***root-ca-p12***'. Save the file to the local machine and add a '***.p12***' extension.

To restore the signing certificate:

1. Select **Platform View | Settings | General | CA Certificate | Import**.

10.8 Appendix H - Certificate Signing Requests

One of the following methods can be used to obtain identity certificates based on a text-based Certificate Signing Request (CSR) to an external Certificate Authority (CA). In all cases the server used will retain the private key and therefore must be secured.

- Creating a CSR using Microsoft MMC Certificates Snap-in 135
- Creating a CSR using the OpenSSL Package 138
- Creating a CSR using the Linux Server Command Line 140
- Converting Certificate Files 141

For the Application server or Server Edition, either method can be used, but the OpenSSL package of the IP Office server itself must not; another PC should create the CSR and process the received certificate.

This section contains procedures for using each method. There are procedures for converting certificate files.

10.8.1 Creating a CSR using Microsoft MMC Certificates Snap-in

Use the following processes.

- Creating a CSR using the OpenSSL Package 138
- Creating a CSR using the Linux Server Command Line 140
- Converting Certificate Files 141

10.8.1.1 Create the CSR

1. If the selected CA provides instructions or utilities to generate CSRs using Microsoft tools, those can be used in preference to the following steps providing the correct format and content result. Any question on format or content should be clarified with the CA.
2. The following step cover use of the Microsoft Management Console Certificates Snap-in to generate a CSR and process the signed identity certificate. The identity certificate will reside in the Local Machine Personal certificate store and will not active on any machine interface by default.
3. All steps must be carefully followed to avoid errors.
4. Further information on the snap-in and certificate operations can be found at: https://technet.microsoft.com/en-us/library/cc771157.aspx
5. Ensure all naming information has been identified (Common name, Alternate subject names, organization details etc.)
6. You must be logged in and run the console session as administrator.
7. To open the Microsoft Management Console (MMC):
   a. Click **Start**.
   b. In the Search box, type ***mmc***.
   c. Click **mmc.exe**.
8. Click **File > Add/Remove Snap-in**.
9. Click **Certificates > Add > OK**.
10. Select **Computer Account** and click **Next**.
11. Select **Local Computer** and click **Finish** then **OK**.
12. Expand **Certificates (Local Computer)**.
13. Right-click **Personal**, then click **Select All Tasks > Advanced Operations > Create Custom Request**.
14. Click **Next**.
15. Select **Proceed without enrolment policy** and click **Next**.
16. Select **(No Template) Legacy Key**.
17. Select **PKCS #10** and click **Next**.
18. In the Certificate Information section, click arrow button next to **Details** and click **Properties**.
19. On the **General** tab, type the domain name of the certificate in the **Friendly Name** field.
20. On the **Subject** tab, in the **Subject Name** field, enter the information below, clicking **Add** after entering each type:

Type	Value	Notes
Country	Country Name (2 letter code)	The Country Name is a 2 letter code defined by https://www.iso.org/obp/ui/#home; select Country codes, and click search for example, US
State	State or Province name	Should not be abbreviated
Locality	Locality name	for example, City
Organization	Organization name	for example, Company Name
Organization Unit	Section/Department name	for example, IT
Common Name	FQDN of server	for example, www.example.com
Email	Contact email address	for example, contact@example.com

21. Any entries not required (for example Organizational Unit Name) or not requested by the CA should not be added.

Página3116 de 3226.

22. If the CSR is for a multi-domain/SAN certificate, in the Alternative Name field, enter the information below, clicking **Add** after entering each type:

Type	Value	Notes
DNS	DNS SAN entry	The first Alternative Name field should be DNS with the same value as the Common Name. for example, www.example.com for example, example.com
IP address (v4)	IP SAN entry	for example, 192.168.0.42 for example, 192.168.0.44
URL	URI SAN entry	for example, sip:example.com for example, 192.168.0.42

23. On the Extension tab, select **Key usage**.
24. Select **Non repudiation**, **Digital signature**, **Key encipherment**, **Data encipherment**, clicking **Add** after entering each option.
25. Unselect **Make these key usages critical**.
26. On the Extension tab, select **Extended Key Usage**.
27. Select **Server Authentication**, **Client Authentication**, clicking **Add** after entering each option.
28. Unselect **Make the Extended Key Usage critical**.
29. On the **Private Key** tab, select **Cryptographic Service Provider**, select **Microsoft Strong Cryptographic Provider (Encryption)** only.
30. On the Private Key tab, select **Key type**, select **Exchange**.
31. On the Private Key tab, select **Key options > Key size**, and set the value to ***2048***.
32. Select **Make Private Key Exportable**. Note: This step is important.
33. If presented, select **Select Hash Algorithm**, select **Hash Algorithm** and set the value to ***sha256***.
34. Review all entries; check the **Key options > Key size**, is still set to the value to ***2048***.
35. Click **OK** then **Next**.
36. Enter the filename (for example, yourdomain) and location to save the CSR to. Ensure **Base 64** is selected. Click **Finish**.
37. Open the CSR file yourdomain.req in a text editor and copy all of the text, including the start and end lines.
38. Go to the CA and follow instruction to paste the full CSR into the SSL enrolment form of the CA. If requested, the server software used to generate the CSR can be specified as Microsoft, or Microsoft IIS 7. If requested, SHA-256 should be selected for the hash algorithm. SHA-1 should not be used.

10.8.1.2 Download and Import the Signed Identity Certificate

1. After approval and generation, receive/download the certificate files from the CA. There should be two or more files:
   - The signed identity certificate which needs to be in PKCS#7/P7B or PEM format
   - Zero, one or more intermediate certificates in PEM format
2. The root certificate should be downloaded in PEM and DER format and put aside for later distribution to IP Office systems.
3. Copy all to the original CSR directory.
4. See Certificate File Naming and Format 42 for more information on certificate file formats.
5. On the same server the certificate request was created on, open the MMC Certificates snap-in for the Local Computer account.
6. Expand **Certificates (Local Computer)**.
7. Right-click **Personal**, then click **Select All Tasks > Import**.
8. Click **Next**.
9. Browse and select the signed identity certificate received from the CA, then click Open.
10. Ensure that these options are always selected:
    - **Mark the Private Key Exportable**

- **Import all Extended Properties**
- **Import all Certificates in the Chain**

11. Click **Next**.
12. Select **Place all certificates in the following store**. Under **Certificate Store**, make sure **Personal** is selected. and click **Next**.
13. Complete the Certificate Import Wizard and click **Finish**.
14. Check there is a key icon on the new certificate, if not the private key is not present.
15. Repeat the import process to import the intermediate certificate file(s); there will be no key icon with these new certificates. Again these must go into the Personal certificate store.
16. Select the identity certificate and click **Open**, select **Details** and verify the content are as expected. Select **Certification Path** and verify all the certificates are present to the root certificate.

10.8.1.3 Export the Signed Identity Certificate

1. The identity certificate and its private key, root and intermediate certificate(s) are now stored in the Local Machine Personal certificate store. These can now be exported in an appropriate format for IP Office.
2. On the same server the certificate request was created on, open the MMC Certificates snap-in for the Local Computer account.
3. Expand **Certificates (Local Computer)**.
4. Right-click the identity certificate (the one with the key icon), then click **Select All Tasks > Export**, click **Next**.
5. Select **Yes, export the private key**, click **Next**.
6. Select: **Personal Information Exchange - PKCS #12 (.PFX)**, **Export all Extended Properties**, and **Include all Certificates in the certification path if possible** .
7. When prompted, a strong password should be used to secure the file. This password will be requested when later importing into IP Office.
8. Click **Next**.
9. Enter a filename (for example, yourdomain) and then click **Next**, then **Finish**. The ID certificate file `yourdomain.pfx` should be renamed `yourdomain.p12`.
10. The PKCS#12 file `yourdomain.p12` now has the identity certificate, private key and all intermediate certificates.
11. `yourdomain.p12` can now be imported into the IP Office deployment using IP Office or IP Office Web Manager. See the relevant documentation and Implementing IP Office PKI 59 for more information.
12. The yourdomain.p12, root and intermediate certificate files should be retained and used for recovery purposes.

- **Note:** A password will always be required to open the PKCS#12 file.

10.8.2 Creating a CSR using the OpenSSL Package

Use the following processes.

- Creating a CSR using Microsoft MMC Certificates Snap-in 135
- Creating a CSR using the Linux Server Command Line 140
- Converting Certificate Files 141

10.8.2.1 Create the CSR

1. OpenSSL package is a third-party product and Avaya cannot provide assurance or warranty of purpose in any form.
2. OpenSSL is available for both Microsoft windows and Linux machines. See https://www.openssl.org/. The following has been tested on Windows 64-bit OpenSSL version 1.0.2d.
3. All steps must be carefully followed to avoid errors.
4. If the selected CA provides instructions or utilities for the use of OpenSSL, those should be used in preference to the following steps. Any question on format or content should be clarified with the CA.
5. Ensure all naming information has been identified (Common name, Alternate subject names, organization details etc.)
6. You must be logged in and run the console session as administrator.
7. Create a directory for the CSR and key and change to it.
8. Create a text file openssl.cfg with the following content, ensure no additional line breaks:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
countryName = Country Name (2 letter code)
stateOrProvinceName = State or Province Name (not abbreviated)
localityName = Locality Name (for example, City)
organizationName = Organization Name (for example, Company)
organizationalUnitName = Organizational Unit Name (for example, Section/Department)
commonName = Common Name (for example, www.example.com)
emailAddress = Email Address (for example, contact@example.com)
[v3_req]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.example.com
DNS.2 = example.com
IP.1 = 203.0.113.30
IP.2 = 203.0.113.40
URI.1 = sip:example.com
URI.2 = 203.0.113.30
URI.3 = sip: 203.0.113.30
```

9. The items in red must be replaced with the information specific to the CSR. Ensure that the information requested by the CA is supplied accurately.
10. The Country Name is a 2 letter code defined by https://www.iso.org/obp/ui/#home; select Country codes, and click Search.
11. Any entries not required (for example Organizational Unit Name) or not requested by the CA can be removed by removing the whole line.
12. If the certificate is for a single domain, remove all lines from `subjectAltName = @alt_names` and onwards.
13. If the certificate is for multiple domains, the first alt_name entry should be DNS.1 and the same as the Common Name (for example, www.example.com).
14. Create the CSR and private key using the command line, ensuring no line breaks. The items in red should be replaced with the domain name of the device.

```
openssl req -new -out example.csr -newkey rsa:2048 -sha256 -keyout example.key -config
openssl.cfg
```

Página3119 de 3226.

15. When requested ('Enter PEM pass phrase'), a strong password for the private key file should be entered. This will be requested later when combining the signed certificate.
16. Verify the CSR with the command line: `openssl req -text -noout -verify -in example.csr`
17. Check the output is as expected.
18. Open the CSR file example.csr in a text editor and copy all of the text
19. Go to the CA and follow instructions to paste the full CSR into the SSL enrolment form of the CA. If requested, the server software used to generate the CSR is OpenSSL, or 'Other'. If requested, SHA-256 should be selected for the hash algorithm. SHA-1 should not be selected.
20. Keep the example.key file for later use. Note a password will always be required to open the key file.

10.8.2.2 Download and Combine the Signed Identity Certificate

1. After approval and generation, receive/download the certificate files from the CA. There should be two or more files:
   - The signed identity certificate which needs to be in PEM format
   - Zero, one or more intermediate certificates which need to be in PEM format
2. If there are download options, selecting 'Other' or 'Apache' should provide the correct format.
3. Copy all to the original CSR directory. Rename the identity certificate to the domain name with a .crt extension.
4. The root certificate should be downloaded in PEM and DER format and put aside for later distribution to IP Office systems.
5. If there is more than one intermediate certificate file: In the original CSR directory , combine all the intermediate certificate files into one file using the single command line:

   ```
   cat intermediate1.crt intermediate2.crt intermediate3.crt > intermediates.crt
   ```

6. In the original CSR directory , join the files into a single PKCS#12 file along with the intermediate certificate file using the single command line:

   ```
   openssl pkcs12 -export -in example.crt -certfile intermediates.crt -inkey example.key -
   out example.p12
   ```

7. When prompted ('Enter pass phrase for example.key '), the password used to secure the private key file when creating the CSR should be entered.
8. When prompted ('Enter Export Password '), a strong password should be used to secure the output PKCS#12 file. This password will be requested when later importing into IP Office.
9. Review the PKCS#12 with the command line: `openssl pkcs12 -info -in example.p12`
10. The identity certificate, private key and all intermediates should be present.
11. The ID certificate file example.p12 and intermediates.crt can now be imported into the IP Office deployment using IP Office or IP Office Web Manager. See the relevant documentation and Implementing IP Office PKI [59] for more information.
12. The example.key, example.p12, root and intermediate certificate files should be retained and used for recovery purposes.
    - **Note:** A password will always be required to open the PKCS#12 and key file.

10.8.3 Creating a CSR using the Linux Server Command Line

Use the following processes.

- Creating a CSR using Microsoft MMC Certificates Snap-in 135
- Creating a CSR using the OpenSSL Package 138
- Converting Certificate Files 141

10.8.3.1 Create the CSR

All steps must be carefully followed to avoid errors.

1. Log in on the IPOL machine through the SSH service as Administrator, enter the certificates menu under the admin tab
2. Here the user can begin to create the CSR filling the SN and SAN parameters.
3. With the help of the csr_subjectName command the user can/should specify the following parameters: Country/State/Locality/Organization/OrganizationUnit/CommonName/Email as defined in the CSR parameters table above at the subject name fields.
4. Any entries not required (for example Organizational Unit Name) or not requested by the CA should not be added.
5. If the CSR is for a multi-domain/SAN certificate, the user has the possibility to add entries in the SAN fields with the help of the csr_subjectAltName (add) command. The valid values are DNS (DNS SAN entry), IP (IPv4 SAN entry), URI (URI SAN entry). We can specify multiple values for every entry, numbering them as per ex: DNS.1=test1csr.com, DNS.2=test2csr.com.
6. When all the parameters of the CSR have been filled the user should check the CSR generation configuration with the help of the csr_view_parameters command. The command will display the current configuration for the CSR. The user should see something similar on the console display:

```
[ req ]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[ req_distinguished_name ]
C=US
ST=Tennessee
L=Nashville
O=CSRsTest
OU=CSRsTestDep
CN=testcsr.com
emailAddress=admin@testcsr.com
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyAgreement, dataEncipherment, keyEncipherment
subjectAltName = @alt_names
subjectKeyIdentifier = hash
[ alt_names ]
DNS.1=testcsr.com
IP.1=192.168.42.1
URI.1=sip:testcsr.com
```

7. The user should then issue the generate_csr command which will generate the CSR, it will store the private key of the CSR in a location only accessible by root and it will display the generated CSR in the console.
8. The user should copy the from the console the generated CSR (that is view as text starting with the -----BEGIN CERTIFICATE REQUEST----- string and it ends with the -----END CERTIFICATE REQUEST----- string.
9. The CSR can be pasted in a text file and can be signed at a public CA or a private one resulting in a signed certificate based on a CSR generated on the IPOL machine.

10.8.3.2 Download and Combine the Signed Identity Certificate

1. After approval and generation, receive/download the certificate file(s) from the CA.
2. The user can import a signed certificate in CLI under the admin/certificates menu with the help of the **import_certid** command. This command does not need any arguments. After invokation the CLI awaits the input of a signed certificate beginning with the string -----BEGIN CERTIFICATE----- and ending with the string -----END CERTIFICATE-----. The certificate should be in pem format (text).
3. If the certificate is valid (the certificate text is valid and also the certificate Is based on a CSR generated on the same ipol machine) the ipol machine will import the certificate into ipoffice application.
4. Upon successful operation an Operation Successful will be reported to the user.
5. The user will be able to read and set the certificate distribution flag through the **read_distribution_flag** and **set_distribution_flag** (on/off) so the certificate will remain the default one only for the ipoffice application (distribution flag off) or it will be distributed for all the applications on the machine (distribution flag on).

10.8.4 Converting Certificate Files

The intermediate.crt file can be in PEM or DER format; it is PEM format if viewable using a text editor.

If other formats are required OpenSSL can be used:

To convert PEM to DER:

```
openssl x509 -outform der -in intermediate.crt -out intermediate.der
```

To convert DER to PEM:

```
openssl x509 -inform der -in intermediate.crt -out intermediate.pem
```

To convert PKCS#7 to PEM:

```
openssl pkcs7 -print_certs -in certificate.pb7 -out certificate.pem
```

To convert PKCS#7 and private key to PKCS#12:

```
openssl pkcs7 -print_certs -in certificate.pb7 -out certificate.pem
openssl pkcs12 -export -in certificate.pem -inkey privateKey.key -certificate.pfx -
certfile CAcert.cer
```

You will be asked for an encryption key for the resultant PKCS#12 file.

To convert PEM certificate and private key to PKCS#12:

```
openssl pkcs12 -export -in certificate.pem -inkey privateKey.pem -
certificate.pfx
```

You will be asked for an encryption key for the resultant PKCS#12 file. You may also be asked for the private key password.

See Certificate File Naming and Format 42 for more information.

10.9 Appendix I - Secure Provisioning of 9600 Series H.323 Phones

You can configure 9608, 9611, 9621 and 9641 H.323 endpoints with or without staging. The staging process is the most secure.

In the less secure alternative without staging, the phone does not authenticate the server with the initial HTTPS connection. If the initial phone connection to HTTPS is hijacked to an attacker's file server, the fraudulent file server can become trusted by the phone.

In deployments with stronger security requirements where this risk is not acceptable, the phones must be staged in a controlled environment.

10.9.1 Recommended Staging Process

Prepare the file server at the staging center. It can be an IP Office acting as the file server, and possibly also as the DHCP server, or it can be another HTTP file server. The following few steps list the files that have to be placed on the staging file server:

1. Put the phones upgrade file and firmware files on the staging file server.
2. Put the certificate of the root CA that signed the cloud IP Office identity certificate (or the root CA that signed the top intermediate CA in the certificate chain of the IP Office identity certificate) on the staging file server.
3. Edit the phones settings file per customer to contain the following settings, and put it on the staging file server:
4. **NVTLSSRVR**, **NVHTTPSRVR** and **NVMCIPADD** - all three settings should specify the DNS name (FQDN) of the cloud IP Office instance. This FQDN will be resolved by DNS to the public IP address of the cloud IP Office instance. Note that the cloud IP Office instance for each customer will have a different FQDN and public IP address, hence the settings file has to be edited for staging phones for each customer.
5. As an alternative to the above, the HTTPS Sever IP Address, HTTP Sever IP Address and Call Server IP Address can be manually configured on each phone using the CRAFT UI. But since programming phones manually via CRAFT UI can be very time consuming, the preferred method is setting the parameters using the staging settings file per the bullet above.
6. **SET TRUSTCERTS** <filename of root CA certificate>
7. **SET TLSSRVRVERIFYID 1** - This is a new parameter in the 9608, 9611, 9621 and 9641 H.323 phone R6.5. When set to 1, the phone will verify the server identity in TLS connections, which is recommended for security. The phone will verify that the DNS name of the TLS server (as set in **NVTLSSRVR**) matches the Common Name or subjectAltName in the server certificate.
8. Connect the phone to the staging center network, and provide it with the staging file server IP address, from DHCP or from the phone UI.
9. The phone will contact the staging file server via HTTP and will download the upgrade and settings files, the trusted root CA certificate, and the firmware files if needed.
10. After staging, the phone is shipped to customer site.
11. The phone is connected to the LAN at the customer site and powered up.
12. The phone contacts the cloud IP Office via HTTPS over TLS, using the NVTLSSRVR IP address it previously got from the staging settings file, and using port 411 (phone's default value of TLSPORT). The port 411 has to be open in the cloud firewall and in the IP Office. An authenticated TLS connection will be established, as the phone will verify the identity certificate (or identity certificate chain) that the cloud IP Office offers in the TLS connection, by checking it against the trusted root CA cert that the phone got during staging.
13. The phone will get the *96x1Hupgrade.txt* file and the auto-generated *46xxsettings.txt* file from the cloud IP Office through the HTTPS/TLS connection. The phone will also get the language files from the cloud IP Office through HTTPS.
14. The auto-generated 46xxsettings.txt will specify **HTTPPORT 8411**. The port number 8411 has to be open in the cloud firewall, whereas port 80 will probably be closed.
15. This is based on an enhancement on the IP Office. Port 8411 is hard-coded on the Linux IP Office and is open for restricted HTTP access allowing only Avaya IP phones to get only firmware files.
16. IP Office includes the setting **HTTPPORT 8411** in the auto-generated 46xxsettings.txt file sent to a phone if and only if the request for the settings file came in HTTPS (not HTTP) and IP Office determines that the phone is connecting from the Internet. IP Office makes this determination if the source IP address of the request is not an RFC 1918 private address and not in the customer's private network as can optionally be specified in **NUSN "PRIVATE_ADDR"**.
17. If new phone firmware is available on the cloud IP Office, as indicated in the upgrade file, the phone will get it from the cloud IP Office via HTTP on port 8411 as specified by the HTTPPORT in the auto-generated 46xxsettings.txt.
18. Ensure during initial provisioning the impact of a large number of sets performing firmware downloads.

Pagina3123 de 3226.

10.9.2 Automated Process

1. Make sure that the Root CA certificate, which was used to sign the IP Office identity certificate, is installed in the IP Office Trusted Certificate Store
2. If the trust policy selected for the IP Office uses a well-known public CA, download the PEM-encoded root CA certificate from the CA's web site and install it in the IP Office Trusted Certificate Store using IP Office Manager Security Mode **System | Certificates | Trusted Certificate Store | Add**.
3. If the trust policy selected for the IP Office uses its own internal CA, then the root CA certificate will already be in the IP Office Trusted Certificate Store.
4. Make sure that the IP Office identity certificate includes a Subject Alternative Name field containing the public IP address of the IP Office.
5. This is needed for the phones to be able to verify the server identity, when the phones are configured to connect to the IP Office's public IP address. It is not needed when the phones are configured through staging to connect to the IP Office's FQDN.
6. If IP Office is using an identity certificate generated by its own internal CA, then you need to generate a new identity certificate with the public IP address in Subject Alternative Name. Caution: Re-generate only the identity certificate and do not unnecessarily re-generate the root CA certificate, which can be disruptive (see Changing a Root CA Certificate 143).
7. Configure in each phone the following parameters through the phone's CRAFT menu: HTTPS Sever IP Address, HTTP Sever IP Address and Call Server IP Address. All three parameters have to be set to the IP address of the IP Office.
8. The phone is restarted, whereby it contact the IP Office and automatically obtains and installs the Root CA certificate of the IP Office.

10.9.3 Changing a Root CA Certificate

Caution: Changing the root CA that signed the IP Office identity certificate can lock out installed phones that have previously been provisioned to trust only the old root CA. Avoid doing this unnecessarily. If an identity certificate signed by an external CA is going to be installed on the IP Office, this should be done before installing the phones if possible.

If it is necessary to change the root CA then this has to be done with caution and will require some administrative effort:

One option is to do a preparation step before changing the IP Office identity certificate; place a manually-edited settings file on the IP Office with TRUSTCERTS specifying both the current root CA and the new root CA file, and place both root CA files on the SD card/disk. Then reset all the phones. The phones will successfully connect to the IP Office, will get the new settings file and will get and install the new trusted root CA. Then change the IP Office identity certificate and remove the manually-edited settings file. Next time the phones connect they will trust the new identity certificate.

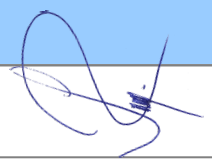
Another option is to clear the phone configuration using CRAFT on all the 96x1 phones and then repeat the configuration of the server address on each phone.

No effort is required if the phone is using HTTP and not HTTPS to get the settings file (which may not be possible in all environments). The next time the phone restarts it will automatically get a new settings file (with the new TRUSTCERT name) and will fetch the new root CA.

10.10 Appendix J - Application/Client Security Dependencies

The following tables provide an overview of IP Office components and their dependencies on various IP Office security settings.

Applications

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
IP Office Manager	IP Office Service: - Configuration (secure) - Security Administration (secure) Legacy Interface: - Program Code	Service User	Yes: - Management		Program Code used for Manager upgrade of IP500 V2 only
Web Management	IP Office Service: - Web Services	Service User	Yes: - Management		
Web Control	IP Office Service: - External	Service User	Yes: - Management		
Voicemail Pro	IP Office Service: - HTTP (secure)	Voicemail password	Yes: - Management		
one-X Portal for IP Office	IP Office Service: - EnhTSPI Legacy Interface: - HTTP directory read - HTTP directory write	Service User	No		
SSA	IP Office Service: - System Status Application	Service User	Yes: - Management		
SoftConsole	IP Office Service: - HTTP	IP Office User	Yes: - Management		
System Monitor	IP Office Service: - HTTP Legacy Interface: - DevLink	Service User or Monitor password	Yes: - Management	System Monitor will use a service user when the **Security | System | Unsecured Interfaces | Use Service User Credentials** is active	
TAPI	Legacy Interface: - TAPI	System password	No		TAPI installer requires IP Office TAPI service enabled
DevLink	Legacy Interface: - DevLink	Monitor password	No		DevLink installer requires IP Office DevLink service enabled (?)
Contact Recorder	None	Internal to Contact Recorder		Disable service in Web Control	

Página3125 de 3226.

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
WebRTC Client	IP Office Service: - External	Service User			See WebRTC client below
DECT R4 Master base station	IP Office Service: - HTTP (secure) Legacy Interface: - TFTP directory read	Service User	Yes: - Management		See DECT R4 extension below
ACCS		Internal to ACCS			See ACCS documentation
IPOCC		Internal to IPOCC			See IPOCC documentation
WebLM	Disable service	Internal to WebLM			See WebLM documentation

Lines

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
IP Office Line	IP Office Service: - HTTP	IP Office Line password	Yes: - Management		
SIP Line	Remove SIP line	SIP Line	Yes: - Management - Telephony		
Analogue/Digital	Remove line	No	No		Analogue/ Digital lines cannot be removed

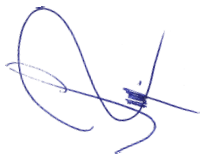
UC Clients

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
Avaya Communicator	one-X Portal for IP Office Service	IP Office User	Yes: - Management	HTTPS only can be enabled by the setting Protocol | Secure Connection (HTTPS)	
one-X Mobile	one-X Portal for IP Office Service	IP Office User	Yes: - Management		HTTPS only can be enabled
one-XP Browser/ Call Assistant	one-X Portal for IP Office Service	IP Office User	Yes: - Management		HTTPS only can be enabled
Outlook, SalesForce, Lync Plugin	one-X Portal for IP Office Service	IP Office User	Yes: - Management		HTTPS only can be enabled
Web Collaboration	one-X Portal for IP Office Service	IP Office User	Yes: - Management		HTTPS only can be enabled
WebRTC	WebRTC service SIP Registrar	IP Office User	Yes: - Management		

Página3126 de 3226.

Extension

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
DECT R4	IP DECT Line	IP Office User, SARI/ PARK	No	Auto-create DECT extension	
H.323	H323 Registrar	IP Office User Or Extension password	Yes: - Management	Auto-create H323 extension	TLS only can be enabled
SIP	SIP Registrar	IP Office User	Yes: - Management	Auto-create SIP extension	
Analogue/Digital	No	IP Office User	No		Analogue/ Digital extensions cannot be removed



Chapter 11.
Document History

11. Document History

Date	Issue	Change Summary
23rd September 2020	05a	Updates for R11.1 SP1. Align with ADMS168370 Version 13.
28th October 2020	05b	Remove obsolete external link.
5th March 2021	05c	Clarification round voicemail server password in 11.1 FP1 or higher.

© 2021 AVAYA All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

" Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link " Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

" Hosted Service" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK " Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS " YOU" AND " END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK " AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS " YOU" AND " END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (" AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. " Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. " Designated Processor" means a single stand-alone computing device. " Server" means a Designated Processor that hosts a software application to be accessed by multiple users. " Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (" VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A " Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Página3130 de 3226.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws
Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud
"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention
If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities
Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation
For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support
See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Table of Figures

Figure 1: Symmetric/Asymmetric Encryption 13
Figure 2: Message Authentication 14
Figure 3: Authentication and Authorization Framework 16
Figure 4: Services Rights Group Assignment 23
Figure 5: Avaya Application Key Checking 38
Figure 6: PKI Trust Domain 38
Figure 7: Cetrtification Distribution - External Certificate Authority 53
Figure 8: Certificate Distribution - Internal Certificate Authority 54
Figure 9: Certificate Distribution - Simple Certifcate Enrollment Protocol (SCEP) 54
Figure 10: Certificate Distribution - External Certificate Authority 55
Figure 11: Default Certificate Storage Structure 118

Table of Tables

Table 1: Security Methods 12
Table 2: Encryption Algorithms 13
Table 3: Message Authenication 14
Table 4: IP Office Services 18
Table 5: Service Security Levels 18
Table 6: Default Security Settings 19
Table 7: Default Security Administrator 24
Table 8: Default Service Users 25
Table 9: Default Rights Groups 26
Table 10: Default Rights Group Assignments 29
Table 11: Administrative User Passwords 35
Table 12: User Passwords and Login Codes 36
Table 13: Certificate File Formats 42
Table 14: Certifictate Filename Extensions 42
Table 15: IP500 V2 Initial Certificate Settings 45
Table 16: Default Primary CA Certificate 47
Table 17: Default Primary Identity Certificate 48
Table 18: Default Secondary/Expansion Certificate 49
Table 19: SRTP Options 69
Table 20: VoIP Signalling Security 70
Table 21: SRTP Bandwidth 71
Table 22: Effect of Disabling Services 77

Página3133 de 3226.

Table of Tables

Table 23: Minimum Access Rights 78

Table 24: Example Ports 104

Table 25: IP Office Application Certificate Support 125

Table 26: VoIP Endpoint Security 128

Página3134 de 3226.

Index

3

3DES 13

A

Access
  Physical 96
ACCS 94
Administrators
  Password 34
Advisories 107, 111
AES 13, 68
Algorithms 13
Anti-Virus Software 17
Application Server
  Secure 99
Applications
  Secure 88
ASBCE 95
Asymmetric Encryption 13
Audience 6
Auditing 12
Authentication 12, 14
  Framework 16
  RTP/RTCP 68
Authorization 12
Authroization
  Framework 16
Auto Logout 86
Avaya Session Border Controller 95

B

Bandwidth
  SRTP 71
Barring Calls 84
  Forwarding 87
  User 85
Best Effort 68
Border Controller 95
BranchAdmin 25
BusinessPartner 25

C

CA 39
Call Barring 84
  Forwarding 87
  User 85
Call Security 68
Capacity
  SRTP 71
CCPA 15
CER 42
Certificate 39
  Certificate Signing Requests 134
  Checks 41
  Convert 141
  Default Certificates 112
  Default Settings 44
  Distribution 53
  Extension 42
  Filename 42
  Format 42
  IP Office Support 43
  Issuer 40
  Maintenance 64
  Name Content 50
  Public Key 40
  Renewing 64
  Serial Number 40
  Signature 40
  Subject Alternate Name 40
  TLS 41
  Trust Policy 56
  Valid From 40
  Windows Certificate Management 118
Certificate Authority 39
Certificate Identity Verification 39
Certificate Signing Requests 134
Certificates 38
  Update 80
Changes 6
Checks 41
Confidentiality 12
Confidentual 8
Contact Center 94
Contact Recorder 92
  Reporting 106
Convert
  Certificate Files 141
CRT 42
CSR 134
CTI 88

D

Data Integrity 12
Data Privacy 15
Default
  Certificate Settings 44
  Certificates 112
  Rights Groups 26
  Security Administrator 24
  Security Settings 19
  Service Users 25
Defaults
  Change 76
DER 42
DES 13
DevLink 19
DigiCert 116
Disclaimer 8
Disk Quotas 17
DNS 50
Document Changes 6
DTLS 68

E

EASG 17
Embedded Voicemail 92
Encryption 13
  RTP/RTCP 68
Enhanced TSPI 18, 19
EnhTcpaService 25
Entrust 113
Export
  Windows Certificate 118
Extension 42
  Change Certificate 143
  Secure 81
  Staging 142

F

Filename Extension 42
Firewall 17, 95

Página3136 de 3226.

Format 42
Forwarding 87
FQDN 50
G
GDPR 15
GlobalSign 115
GTS 114
H
Hash Size 14
Hot Desking 86
HTTP Directory 19
I
ICR 94
Identification 12
Identity Certificate 39
Import
  Windows Certificate 118
Information Classifications 8
Integrated Call Reporter 94
IP 50
IP Office
  Certificate 43
  Manager 89
  Reporting 106
  Rights Groups 23
  Service Users 23
  Updates 107
  User Passwords 36
  Web Manager 89
IP Office Applications
  Secure 88
IP Office Services 18
IPDECTService 25
IPOCC 94
ISRG 115
Issuer 40
K
Key Size 13
Key Usage 40
L
Let's Encrypt 117
Line
  Secure 83
Linux Platform Security 17
Lock Phone 86
Logging Out 86
Login Code 32, 36
  System Policy 33
Logout 86
M
Maintainer 25
Maintenance 96
Maintenance Access 95
Manager 89
MD5 14
Media
  Secure 83
Media Manager 94
Media Security 68
Message Authentication 14
Monitor 90
Monitoring 102
MPLS 68
Multiple Domain Certificate 39
Multi-SAN 39
Mutual Authentication 39
N
NDA 8
O
one-X Portal
  Reporting 107
one-X Portal for IP Office 93
P
p21 42
Password 32
  Adminstrator Passwords 34
  Policy 79
  System Policy 33
Passwords
  User 36
pb7 42
PEM 42
Personal Data 15
pfx 42
Phone
  Change Certificate 143
  Provisioing 142
  Staging 142
Phone Lock 86
Physical Access 96
PIN Code 32
  System Policy 33
PKCS#12 42
PKCS#7 42
PKI Trust Domain 38
Planning 71
Platform Security 17
Ports 103
Prevent
  Forwarding 87
Privacy 15
Proprietary 8
Protocols 103
Public 8
Public Key 40
Public Key Algorithm 40
Q
Quotas 17
R
RC4 13
Remote Maintenance Access 95
Remote Workers 82
Renew
  Certificates 80
Renewing Certificates 64
Reporting 102
Responsibility
  IP Office Security 9
  Security Updates 9
Restricted 8
Rights Groups 23
  Default 26
  Default Assignment 27
root 17
Root CA Certificate 39
Root Certificate 39

Página3137 de 3226.

RTCP 68
RTP 68
S
SAN DNS 50
SBC 95
Secure
  ACCS 94
  Application Server 99
  Contact Recorder 92
  CTI 88
  Embedded Voicemail 92
  Extension 81
  Integrated Call Reporter 94
  IP Office Applications 88
  Maintenance 96
  Manager 89
  Media 83
  Media Manager 94
  one-X Portal for IP Office 93
  Phone Provisioning 142
  Server Edition Servers 97
  SSA 90
  System Monitor 90
  Trunk 83
  UCM 99
  Voicemail Pro 91
  Web Manager 89
  WebLM 89
  WebRTC 94
Security
  Planning 71
  VoIP 68
Security Administrator 24
Security Advisories 107, 111
Security Database 14
Server
  Reporting 107
Server Authentication 39
Service User 23
Service Users
  Default 25
  Remove 76
  Rights Groups 27
Services 18
  Default 19
  Disable 77
Session Border Controller 95
SHA-1 14, 68
SHA-2 14
Signature 40
Signature Algorithm 40
Single Domain Certificate 39
SIP 50
SMDR 87
SRTP 68
  Capacity 71
  Troubleshooting 121
SSA 90
Staging 142
Strong Password 32
Subject 40
Subject Alternate Name 40
Symantec 113
Symmetric Encryption 13
System Monitor 90
System Status Application 90
System Upgrade 29
T
TAPI 19, 88
TCS 39
Terminology 39
TFTP 19
Third-Party Security 17
TLS 41
Transport Layer Security 41
Troubleshooting
  Certificates 64
  SRTP 121
Trunk
  Secure 83
Trust Domain 38, 39
Trust Policy 56
Trust Store 39
Trusted Certificate 39
Trusted Certificate Store 39
Trusted Source 86
U
UCM
  Secure 99
Unified Communication Certificate 39
Update
  Certificates 80
Upgrade 29
URI 50
User
  Login Code 36
  Passwords 36
V
Valid From 40
Valid To 40
Voicemail
  Embbedded Voicemail 92
  Reporting 106
  Trusted Source 86
  Voicemail Pro 91
VoIP 68
  Planning 71
  Signalling Security 70
W
Web Control 89
Web Manager 89
Web Services 19
WebLM 89
WebRTC Gateway 94
Wildcard 50
Wildcard Certificate 39
Windows
  Certificate Management 118

Página3138 de 3226.

© 2021 Avaya Inc. All rights reserved.

Avaya Solution & Interoperability Test Lab

Application Notes for Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0.1 with AT&T IP Toll Free Service using IPv6 - Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya IP Office 11.0 and Avaya Session Border Controller for Enterprise 8.0.1 with the AT&T IP Toll Free service, using IPv6 and AVPN or MIS/PNT transport connections.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution providing toll-free services over SIP trunks for business customers.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

AT&T is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

©2020 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 4
2. General Test Approach and Test Results 5
   2.1. Interoperability Compliance Testing 6
   2.2. Test Results 7
   2.3. Support 8
3. Reference Configuration 9
   3.1. Illustrative Configuration Information 11
   3.2. Call Flows 12
      3.2.1. Basic Inbound 12
      3.2.2. Coverage to Voicemail 13
4. Equipment and Software Validated 14
5. Avaya IP Office Primary Server Configuration 15
   5.1. Licensing 16
   5.2. TLS Management 17
   5.3. System Settings 18
      5.3.1. LAN1 Tab 18
      5.3.2. Voicemail Tab 21
      5.3.3. Telephony Tab 22
      5.3.4. VoIP Tab 23
   5.4. IP Route 25
   5.5. SIP Line 26
      5.5.1. Creating a SIP Line from an XML Template 27
      5.5.2. SIP Line – SIP Line tab 28
      5.5.3. SIP Line - Transport Tab 29
      5.5.4. SIP Line – Call Details tab 30
      5.5.5. SIP Line - VoIP tab 31
      5.5.6. SIP Line – SIP Advanced Tab 32
   5.6. IP Office Line 33
   5.7. Users, Extensions, and Hunt Groups 34
      5.7.1. User 34
      5.7.2. Extension 35
      5.7.3. Hunt Groups 36
   5.8. Incoming Call Route 38
      5.8.1. Calls to IP Office Stations and Hunt Groups 38
      5.8.2. Calls to Voicemail Pro Scripts 40
   5.9. Call Center Provisioning in Voicemail Pro 41
   5.10. Save IP Office Primary Server Configuration 45
6. Avaya IP Office Expansion System Configuration 46
   6.1. Expansion System - Physical Hardware 46
   6.2. Expansion System - LAN Settings 47
   6.3. Expansion System - IP Route 47
   6.4. Expansion System - IP Office Line 48
   6.5. Save IP Office Expansion System Configuration 49

©2020 Avaya Inc. All Rights Reserved.

7. Configure Avaya Session Border Controller for Enterprise 50
7.1. Device Management – Status 51
7.2. TLS Management 53
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise 53
7.2.2. Server Profiles 54
7.2.3. Client Profiles 56
7.3. Network Management 58
7.4. Media Interfaces 59
7.5. Signaling Interfaces 60
7.6. Server Interworking Profiles 61
7.6.1. Server Interworking Profile – IP Office 61
7.6.2. Server Interworking Profile – AT&T 63
7.7. SIP Servers Profiles 65
7.7.1. SIP Server Profile – IP Office 65
7.7.2. SIP Server Profile – AT&T 67
7.8. Routing Profiles 69
7.8.1. Routing Profile – IP Office 69
7.8.2. Routing Profile – AT&T 70
7.9. Topology Hiding Profile 71
7.10. Application Rules 72
7.11. Media Rules 72
7.12. Signaling Rules 74
7.13. Endpoint Policy Groups 75
7.14. Advanced Options 76
7.15. End Point Flows - Server Flow 77
8. AT&T IP Toll Free Service Configuration 79
9. Verification Steps 79
9.1. AT&T IP Toll Free Service 79
9.2. Avaya SBCE 80
9.2.1. Incidents 80
9.2.2. Server Status 81
9.2.3. Protocol Traces 82
9.3. Avaya IP Office 83
9.3.1. System Status Application 83
9.3.2. System Monitor Application 85
10. Conclusion 86
11. Additional References 86

©2020 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps for configuring Avaya IP Office release 11.0 (Avaya IP Office) and the Avaya Session Border Controller for Enterprise (Avaya SBCE) release 8.0.1 with the AT&T IP Toll Free service using Internet Protocol version 6 (IPv6) and **AVPN** or **MIS/PNT** transport connections.

Avaya IP Office is a versatile communications solution that combines the reliability and ease of a traditional telephony system with the applications and advantages of an IP telephony solution. This converged communications solution can help businesses reduce costs, increase productivity, and improve customer service.

The Avaya Session Border Controller for Enterprise is the point of connection between Avaya IP Office and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling and media for interoperability. The Avaya SBCE also performs network address translations between the CPE private IPv4 network and the AT&T IP Toll Free IPv6 SIP trunk, at both the IP and SIP layers.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution providing toll-free services over SIP trunks for business customers. The AT&T Toll Free service utilizes AVPN[1] or MIS/PNT[2] transport services.

Note – The AT&T IP Toll Free service will be referred to as IPTF in the remainder of this document.

[1] AVPN uses compressed RTP (cRTP).
[2] MIS/PNT does not support cRTP.

©2020 Avaya Inc. All Rights Reserved.

2. General Test Approach and Test Results

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPTF and the Customer Premises Equipment (CPE) containing the Avaya SBCE and Avaya IP Office (see **Section 3.2** for call flow examples).

The test environment described in these Application Notes consisted of:

- A simulated enterprise with Avaya IP Office 11.0, Avaya SBCE 8.0.1, Avaya SIP, H.323, Digital and Analog telephones, as well as fax machine emulators (Ventafax).
- Laboratory versions of the IPTF service, to which the simulated enterprise was connected via AVPN/MIS transport.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the AT&T Toll Free service did not include use of any specific encryption features as requested by AT&T.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible.

2.1. Interoperability Compliance Testing

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPTF network. Calls were made from the PSTN across the IPTF test network, to the CPE.

The interoperability compliance testing focused on verifying inbound call flows (see **Section 3.2**) between Avaya IP Office, Avaya SBCE and the IPTF service.

The following SIP trunking VoIP features were tested with the IPTF service:

- Inbound calls from the PSTN, routed by the IPTF service, to the Avaya SBCE and the Avaya IP Office. These calls are via the Avaya IP Office SIP Line and may be generated/answered by Avaya SIP telephones/Softphones, H.323 telephones, Analog telephones, Digital telephones, Analog fax machines or via Hunt Groups. Coverage to Voicemail Pro, and Voicemail Pro auto-attendant applications were also used.
- Call and two-way talk path establishment between PSTN and IP Office telephones/ agents via IPTF.
- Basic telephony features such as call waiting, hold, transfer, and conference.
- AT&T IP Toll Free features such as Legacy Transfer Connect and Alternate Destination Routing
- Inbound fax using T.38 or G.711, and G3 or SG3 endpoints.
- Proper disconnect when the caller abandons a call before answer, and when the Avaya IP Office party or the PSTN party terminates an active call.
- SIP OPTIONS monitoring of the health of the SIP trunk. In the reference configuration Avaya IP Office sent OPTIONS to the IPTF service Border Element and AT&T responded with *405 Method Not Allowed* (which is the expected response). That response is sufficient for Avaya IP Office to consider the connection up.
- Incoming calls using the G.729A and G.711 ULAW codecs.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful voice mail navigation, including navigation of a simple auto-attendant application configured on Voicemail Pro, as well as IPTF DTMF generated features.

An Avaya Remote Worker endpoint (Avaya Equinox SIP softphone) was one of the Avaya endpoints used in the reference configuration. The Remote Worker resides on the public side of the Avaya SBCE (via a TLS connection), and registers/communicates with Avaya Session Manager via Avaya SBCE, as though it was an endpoint residing in the private CPE space. The configuration of the Remote Worker environment is beyond the scope of this document.

©2020 Avaya Inc. All Rights Reserved.

Página 3145 de 3226.

2.2. Test Results

The test objectives stated in **Section 2.1**, with limitations as noted below, were verified.

1. **Avaya IP Office only supports a packet size (ptime) of 20 msecs** – Although no issues were found during testing, AT&T recommends that for maximum customer bandwidth utilization, a ptime value of 30 should be specified.

2. **IP Toll Free Alternate Destination Routing (ADR) feature based on SIP error code response** – The IP Toll Free service can be configured to invoke the ADR call redirection feature upon receiving of an error response from the CPE.
   - The following error conditions were producible in the reference configuration and tested successfully: 480 Temporarily Unavailable, 486 Busy Here, 500 Server Internal Error and 503 Service Unavailable.
   - Even though the following error conditions were not producible in the reference configuration, the associated error codes were simulated during the tests via an Avaya SBCE signaling manipulation rule, allowing the associated ADR Call Redirection feature to be tested successfully in each case: 408 Request Timeout, 504 Server Timeout, and 600 Busy Everywhere.

3. **Disconnected calls do not release from IP Office –** When the PSTN caller disconnects the call and the IP Office user does not hang up, IP Office will not clear the call properly. AT&T sends a BYE with a "tgrp" parameter in the Request URI header that includes IPv6 addresses. IP Office is unable to parse the BYE message because of the contents within the tgrp parameter. A Server Interworking profile in the Avaya SBCE was used to remove the "tgrp" parameter. See **Section 7.6.1**. With the Server Interworking profile in place, the call clears correctly.

4. **DiffServ markings –** The IP header in RTP media and SIP signaling packets sent from the Avaya SBCE to AT&T do not contain the Quality of Service DSCP values configured on the Media and Signaling Rules under Domain policies (**Sections 7.11** and **7.12**). This issue seems to be restricted to Avaya SBCE interfaces configured with IPv6 addresses, and it is currently under investigation by Avaya.

5. **IP Office determines the codec priority** – IP Office will follow the codec priority based on the Codec Selection on the SIP Line VoIP tab, see **Section 5.5.5**. It will not follow the codec priority set by the IPTF service.

6. **Codec G.729B is not supported on IP Office Server Edition server** – Specific test cases on the AT&T Test Plan requiring the use of codec G.729B at the CPE could not be executed. Codec G729B is not supported on SIP trunks terminating on the Avaya IP Office Server Edition Linux server platform, as deployed on the test configuration. Codec G.729B is supported when the SIP trunk is terminated on an IP Office IP500 V2 standalone or expansion system.

©2020 Avaya Inc. All Rights Reserved.

7. **G.711 fax calls fail –** G.711 fax was tested in the reference configuration. After the initial voice setup is completed using code G.729A, Avaya IP Office does not send a re-invite to AT&T to transition to G.711 fax, unless the SIP Line Custom String **SLIC_PREFER _EXISTING_CODEC** is added to the Engineering tab of the SIP line. This issue is under investigation by the Avaya IP Office development team. When using the string above IP Office sent the re-INVITE at G.711, but after detecting the fax tone AT&T then sends a new re-INVITE at T.38 to the CPE. Since Fax Transport Support was set to G.711 on the SIP Line VoIP tab to run the test, IP Office returns a "488 Not Acceptable Here" and the fax call fails.
   G711 fax should not be used in this solution. T.38 fax was tested successfully, and it is the recommended method for fax.

8. **IP Toll Free services IP InfoPack** and **Landline/Mobility test cases could not be executed**. The AT&T supplied IP Toll Free test plan specifies test cases to verify the inbound transmission of INFOPAK and Landline/Mobility data by the IP Toll Free service. Due to network provisioning and lab support issues, these test cases could not be executed.

2.3. Support

AT&T customers may obtain support for the AT&T IP Toll Free service by calling (800) 325-5555.

Avaya customers may obtain documentation and support for Avaya products by visiting: http://support.avaya.com. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers (provided on http://support.avaya.com) to directly access specific support and consultation services based upon their Avaya support agreements.

©2020 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Note – Documents used to provision the test environment are listed in **Section 11**. References to these documents are indicated by the notation **[x]**, where *x* is the document reference number.

The reference configuration used in these Application Notes is shown in **Figure 1** on the next page and consists of the following components:

- Avaya IP Office provides the voice communications services for a particular enterprise site. In the reference configuration, Avaya IP Office runs on the Avaya IP Office Server Edition platform. Note that this solution is extensible to deployments using the standalone IP500 V2 platform as well.
- In the sample configuration, the Primary server runs the Avaya IP Office Server Edition Linux software. Avaya Voicemail Pro, running as a service on the Primary Server, provided the voice messaging capabilities in the reference configuration.
- The Expansion System (V2) is used for the support of digital, analog and additional IP stations. It consists of an Avaya IP Office 500 V2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module).
- Avaya endpoints are represented with an Avaya 9608 H.323 Deskphone, Avaya J169 SIP Deskphones, an Avaya 1140E SIP Deskphone, an Avaya 9508 Digital Deskphone, as well as Avaya Equinox for Windows (SIP) softphone. Fax endpoints are represented by PCs running Ventafax emulation software connected by modem to an Avaya IP Office analog port.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPTF service and the CPE. In the reference configuration, the Avaya SBCE runs on a VMware platform. This solution is extensible to other Avaya Session Border Controller for Enterprise platforms as well.

Note – In the reference configuration, the Avaya SBCE performs network address translations between the CPE private IPv4 network and the AT&T IP Toll Free IPv6 SIP trunk, at both the IP and SIP layers.

- The Avaya IP Office and the Avaya SBCE were deployed using the following configuration.
  - IP Office LAN1 interface connected to the CPE private network. (IPv4)
  - Avaya SBCE A1 interface connected to the CPE private network. (IPv4)
  - Avaya SBCE B1 interface connected to the AT&T network.(IPv6)
- TLS/5061 is the recommended transport protocol/port to use on the Avaya IP Office LAN1 connection to the Avaya SBCE A1 interface. However, TCP/5060 may be used for this connection if desired.
- UDP transport via port 5060 was used between the Avaya SBCE and AT&T.
- The AT&T IPTF service requires RTP port ranges 16384-32767.
- AT&T provided the inbound and outbound access numbers (DID and DNIS) used in the reference configuration. Note that the IPTF service may deliver various digit lengths in the SIP Invite Request-URI depending on the circuit order provisioning. In the reference configuration, the IPTF service delivered 15 digits.

©2020 Avaya Inc. All Rights Reserved.

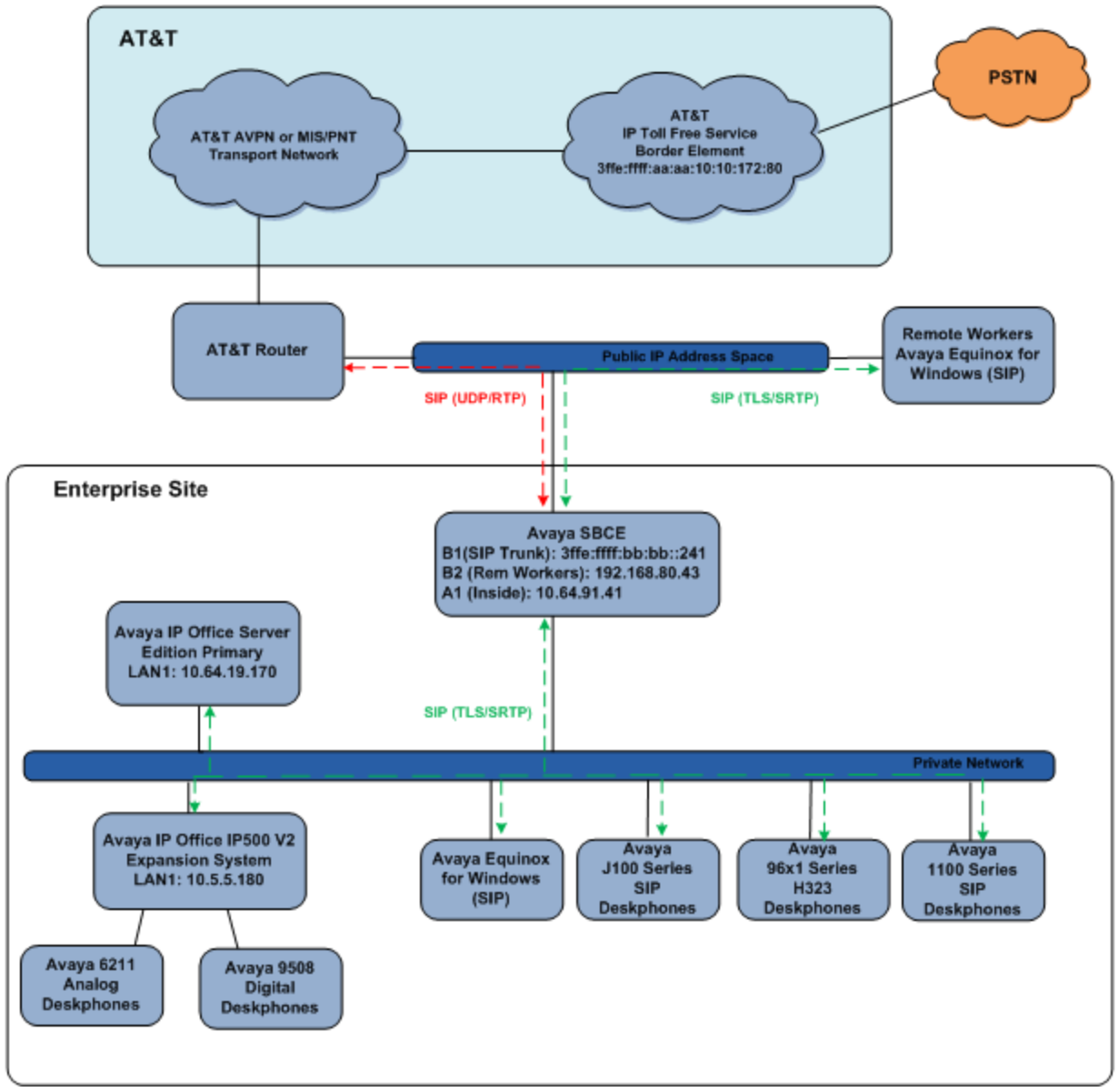


Figure 1: Test Configuration

An Avaya Remote Worker endpoint (Avaya Equinox for Windows) was used in the reference configuration. The Remote Worker endpoint resides on the public side of an Avaya SBCE (via a TLS connection), and registers/communicates with IP Office as though it was an endpoint residing in the private CPE space.

Note – The configuration of the Remote Worker environment is beyond the scope of this document. Refer to **[**7] on the **Additional References** section for information on Remote Worker deployments.

©2020 Avaya Inc. All Rights Reserved.

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes and are for illustrative purposes only. Customers must obtain and use the values based on their own specific configurations.

Note – The Avaya SBCE "B1" interface communicates with AT&T Border Element (BE) located in the AT&T IPTF network. For security reasons, the public IP addresses of the Avaya SBCE and AT&T BE are not included in this document. However, as placeholders in the following configuration sections, the IPv6 addresses **3ffe:ffff:bb:bb::241** (Avaya SBCE "B1"), and **3ffe:ffff:aa:aa:10:10:172:80** (AT&T BE address), are specified. In addition, AT&T DID/DNIS numbers shown in this document are examples as well. AT&T Customer Care will provide the actual Border Element IP addresses and DID/DNIS numbers as part of the IPTF provisioning process.

Component	Illustrative Value in these Application Notes
Avaya IP Office	
Primary Server, LAN1 interface	10.64.19.170
Expansion System, LAN1 Interface	10.5.5.180
Avaya SBCE	
"Inside Interface", A1	10.64.91.41
"Outside" Interface, B1	3ffe:ffff:bb:bb::241
AT&T IPTF Service	
Border Element IP Address	3ffe:ffff:aa:aa:10:10:172:80

Table 1: Illustrative Values Used in these Application Notes

©2020 Avaya Inc. All Rights Reserved.

3.2. Call Flows

To understand how inbound and outbound AT&T IPTF service calls are handled by Avaya IP Office, two basic call flows are described in this section.

3.2.1. Basic Inbound

The first call scenario illustrated in the figure below is an inbound AT&T IPTF service call that arrives on Avaya IP Office, which in turn routes the call to a hunt group, phone or a fax endpoint.

1. A PSTN phone originates a call to an IPTF service number.
2. The PSTN routes the call to the AT&T IPTF service network.
3. The AT&T IPTF service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any specified SIP header modifications, and routes the call to Avaya IP Office.
5. Avaya IP Office applies any necessary digit manipulations based upon the DID and routes the call to a hunt group, phone or a fax endpoint.

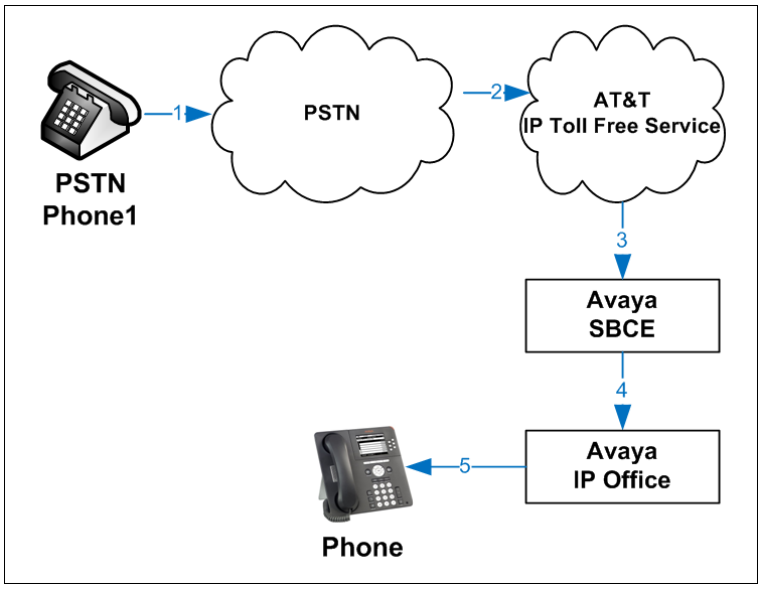


Figure 2: Inbound AT&T IPTF Call

©2020 Avaya Inc. All Rights Reserved.

Página 3151 de 3226.

3.2.2. Coverage to Voicemail

The call scenario illustrated in the figure below is an inbound call that is covered to Voicemail. In the reference configuration, the Voicemail system used is Voicemail Pro, running on the Application Server.

1. Same as the first call scenario in **Section 3.2.1**.
2. The Avaya IP Office phone does not answer the call, and the call covers to the external application Avaya IP Office Voicemail Pro.

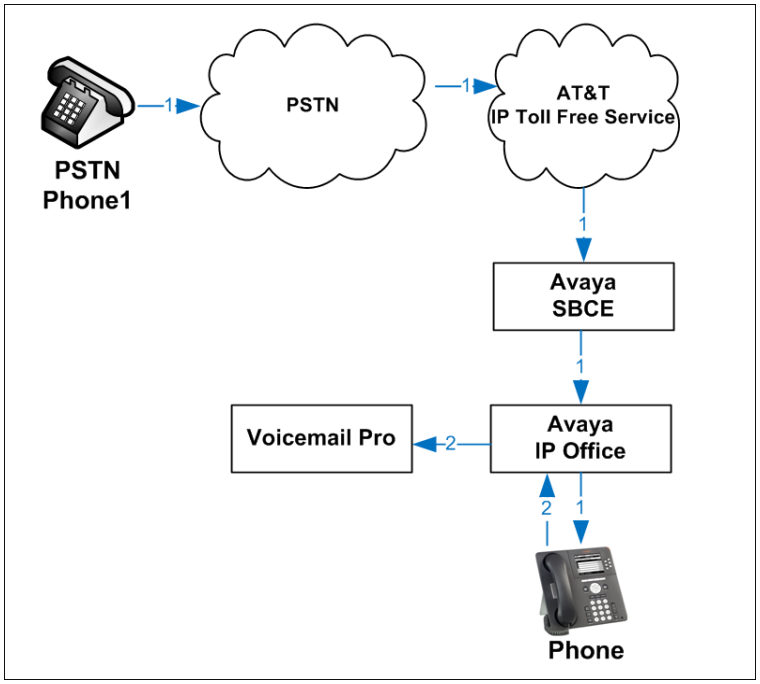


Figure 3: Coverage to Voicemail (Voicemail Pro)

©2020 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition Avaya IP Office Voicemail Pro	Release 11.0.4.1.0 Build 11 Release 11.0.4.1.0 Build 2
Avaya IP Office 500 V2 Expansion System	Release 11.0.4.1.0 Build 11
Avaya IP Office Manager	Release 11.0.4.1.0 Build 11
Avaya Session Border Controller for Enterprise	Release 8.0.1.0-10-17555
Avaya 96x1 Series IP Deskphone (H.323)	Release 6.8002
Avaya 1140E IP Deskphone (SIP)	Release 04.04.23.00
Avaya J169 IP Deskphone (SIP)	Release 4.0.3.0.10
Avaya 9508 Digital Deskphone	Release 0.60
Avaya Equinox for Windows	Release 3.6.4.31.2
Avaya Fax device	Ventafax 7.10

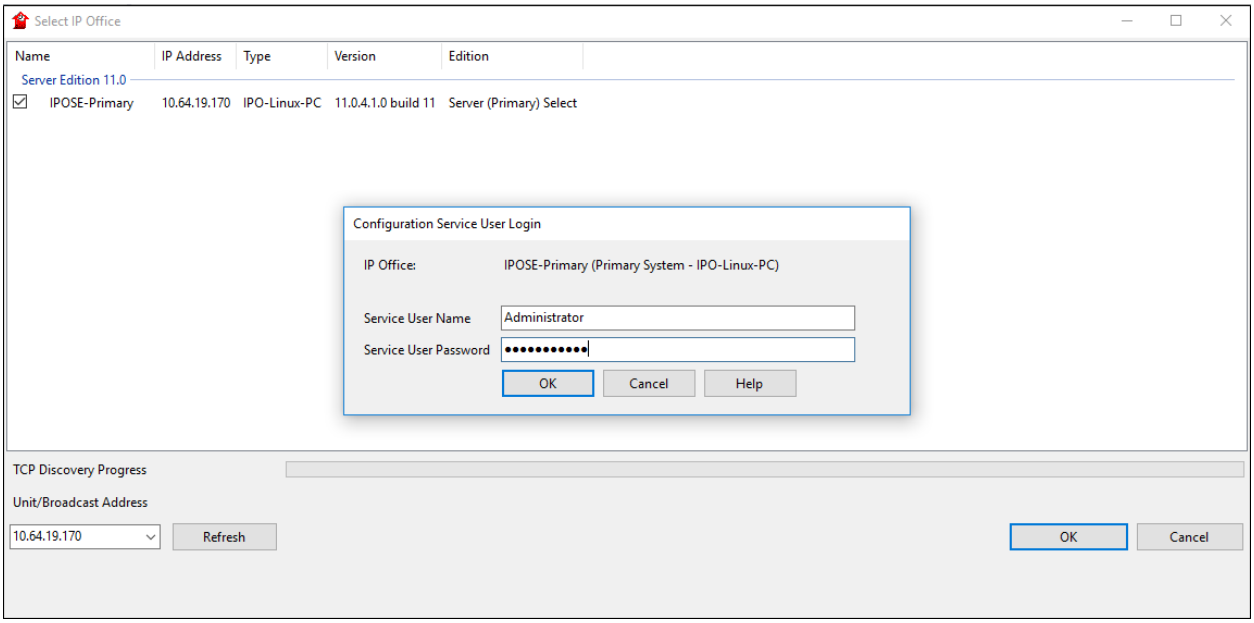
Table 1: Equipment and Software Versions

Note – Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2, and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

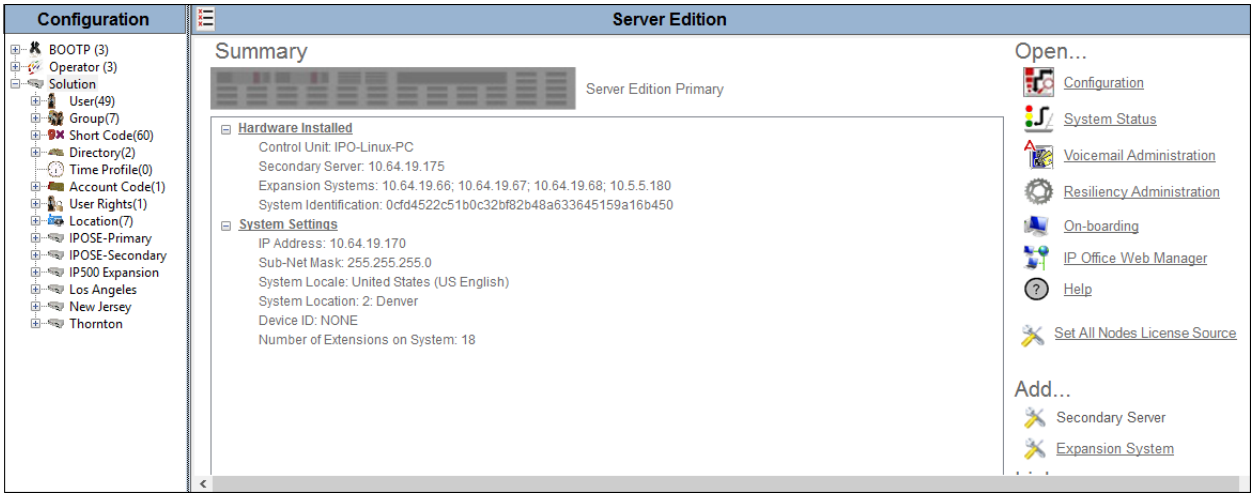
©2020 Avaya Inc. All Rights Reserved.

5. Avaya IP Office Primary Server Configuration

Avaya IP Office is configured through the Avaya IP Office Manager application. From the PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the Manager application. Log in using the appropriate credentials.



On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the "plus" sign next to the Primary server system name, e.g., **IPOSE-Primary**, on the navigation pane will expand the menu on this server.



©2020 Avaya Inc. All Rights Reserved.

In the screens presented in the following sections, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center and the Details pane on the right side. These panes will be referenced throughout the rest of this document.

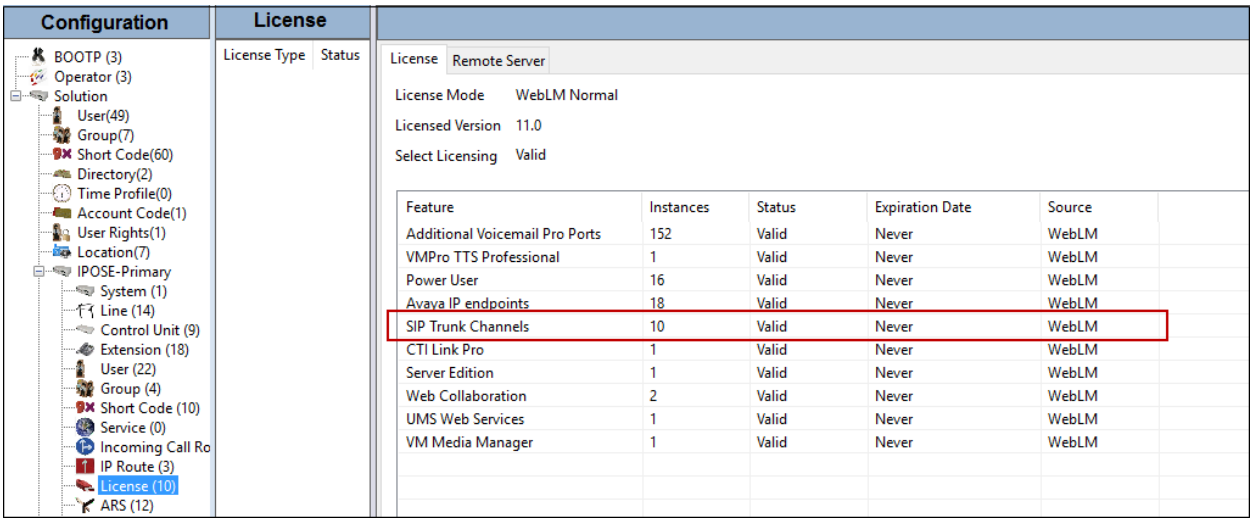
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

5.1. Licensing

The configuration and features described in these Application Notes require the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

In the reference configuration, **IPOSE-Primary** was used as the system name of the Primary Server and **IP500 Expansion** was used as the system name of the Expansion System. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane.

Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.



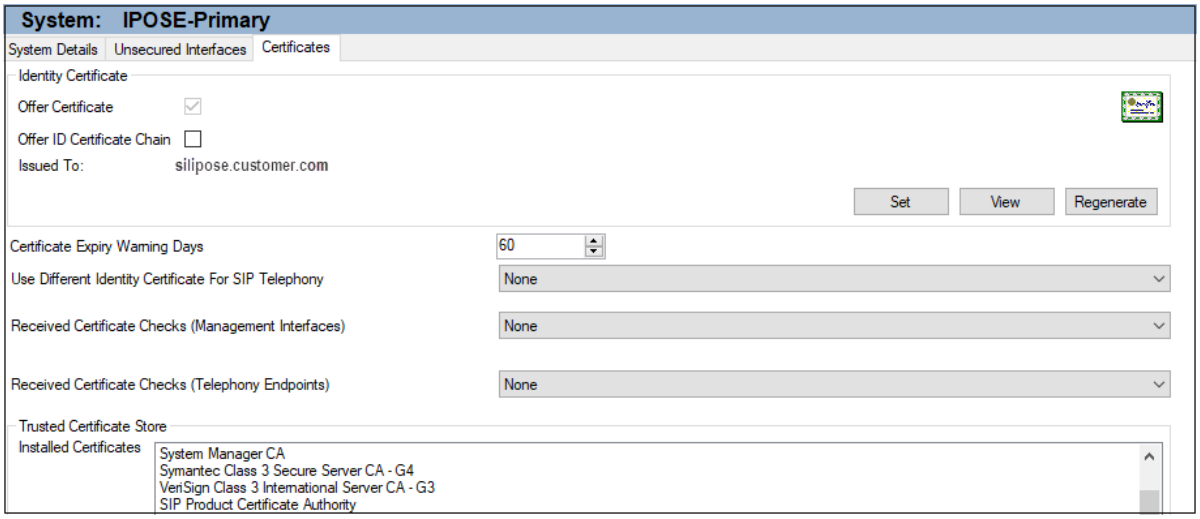
©2020 Avaya Inc. All Rights Reserved.

5.2. TLS Management

For the compliance test, the signaling on the SIP trunk between IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority **SystemManager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes. However, once the certificates are available they can be viewed on IP Office in the following manner.

To view the certificates currently installed on IP Office, navigate to **File → Advanced → Security Settings**. Log in with the appropriate security credentials (not shown). In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

To verify the identity certificate, locate the **Identity Certificate** section and click **View** to see the details of the certificate.



©2020 Avaya Inc. All Rights Reserved.

5.3. System Settings

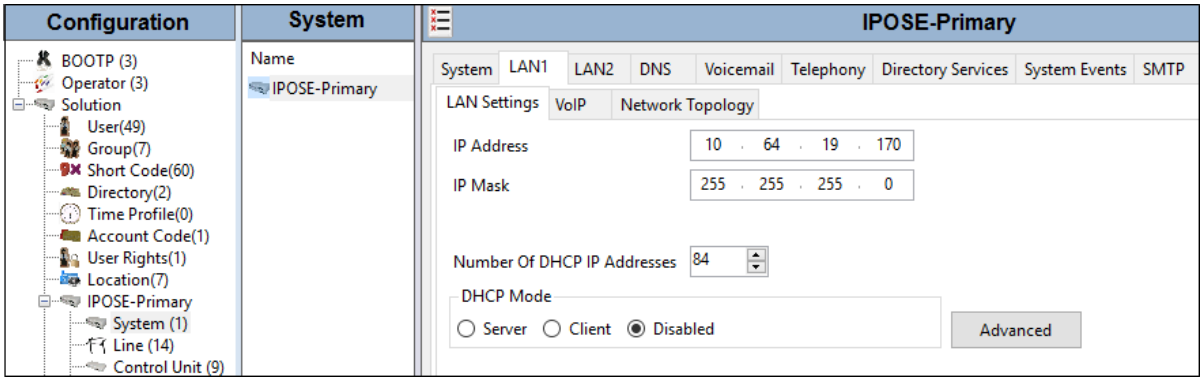
This section illustrates the configuration of system settings. Select **System** on the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings. For all the following configuration sections, the **OK** button (not shown) must be selected in order for any changes to be saved.

5.3.1. LAN1 Tab

In the sample configuration, LAN1 is used to connect the Primary Server to the enterprise private network.

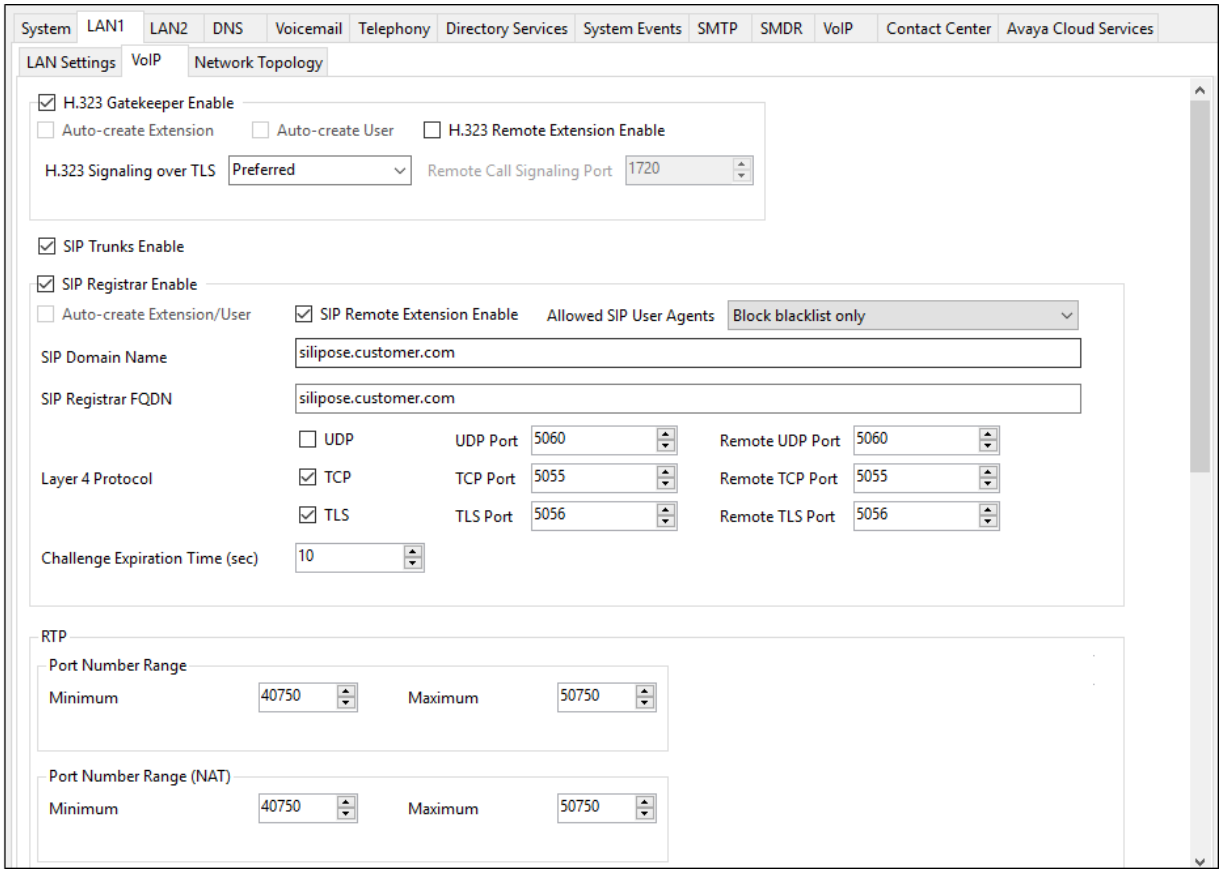
To view or configure the LAN 1 IP address and subnet mask, select the **LAN1 → LAN Settings** tab and enter the information as needed, according to customer specific requirements:

- **IP Address**: **10.64.19.170** was used in the reference configuration.
- **IP Mask**: **255.255.255.0** was used in the reference configuration.
- Click the **OK** button (not shown).



Select the **LAN1 → VoIP** tab as shown in the following screen. The following settings were used in the reference configuration:

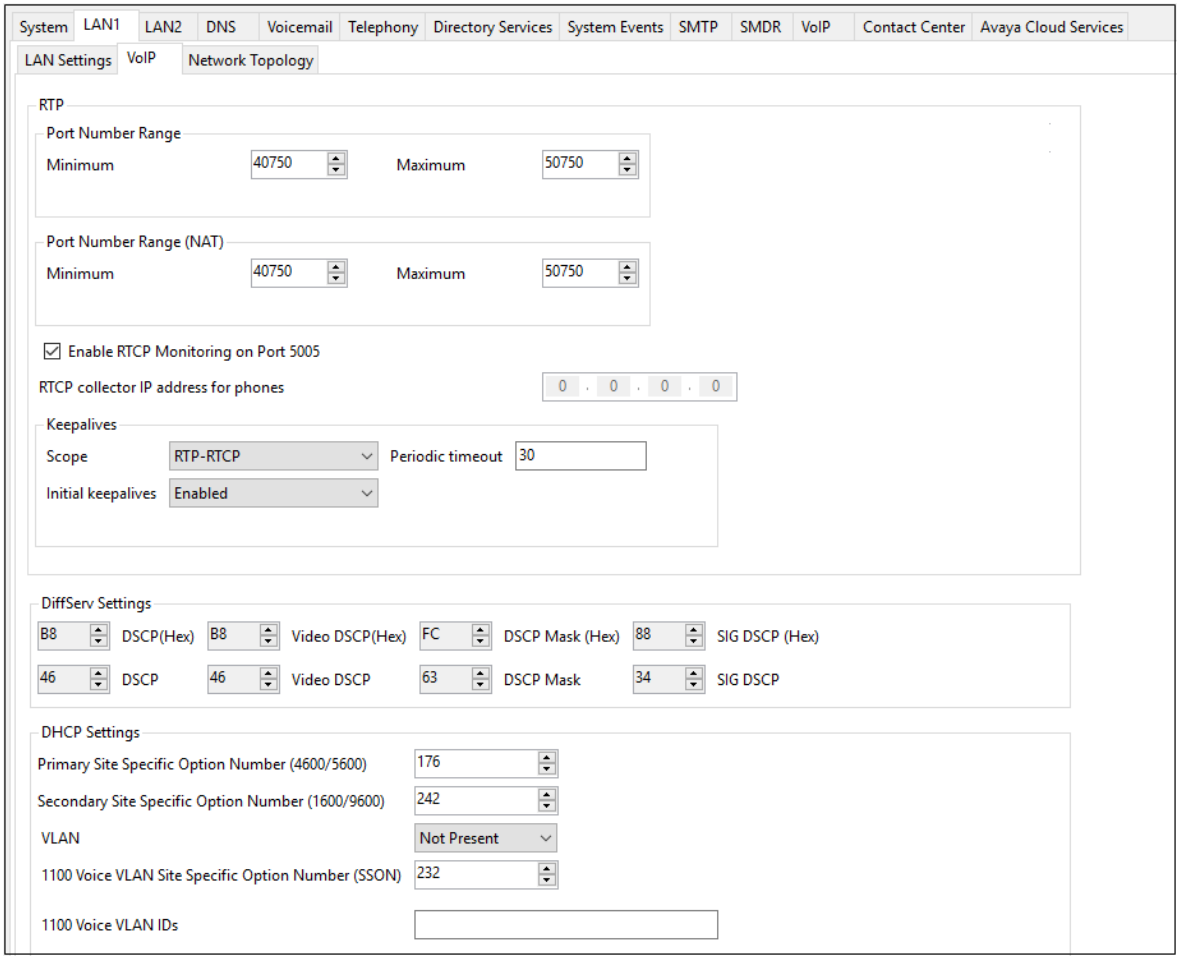
- The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 96x1-Series Deskphones used in the reference configuration.
- The H.323 Signaling over TLS should be set based on customer needs. In the reference configuration it was set to **Preferred**.
- The **SIP Trunks Enable** parameter must be checked to enable the configuration of SIP trunks to AT&T.
- The **SIP Registrar Enable** box was checked to allow Avaya J100-Series Deskphones, Avaya 1100-Series Deskphones and Avaya Equinox usage.
- The **Domain Name** and **SIP Registrar FQDN** may be set according to customer requirements. The values used in the reference configuration are shown.
- Set the **Layer 4 Protocol** section based on customer needs. In the reference configuration **TCP/5055** and **TLS/5056** were configured.



©2020 Avaya Inc. All Rights Reserved.

Scroll down the page:

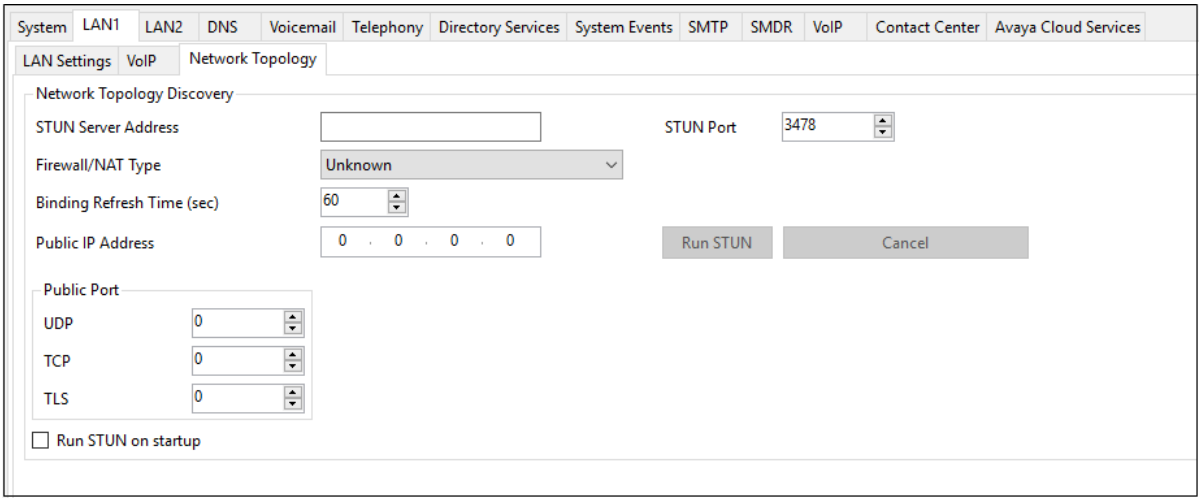
- Verify the **RTP Port Number Range**. Based on this setting, Avaya IP Office will request RTP media to be sent to a UDP port in the configurable range for calls using LAN1. The **Minimum** and **Maximum** port numbers were kept at their default values in the reference configuration.
- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. This is done to prevent possible issues with network firewalls closing idle RTP channels.
- In the **DiffServ Settings** section, IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services (QoS) policies for both signaling and media. The **DSCP** field is the value used for media, while the **SIG DSCP** is the value used for signaling. These settings should be set according to the customer's QoS policies in place. The default values used during the compliance test are shown.
- Click **OK** to commit (not shown).



©2020 Avaya Inc. All Rights Reserved.

Select the **LAN1 → Network Topology** tab as shown in the following screen, and enter the following:

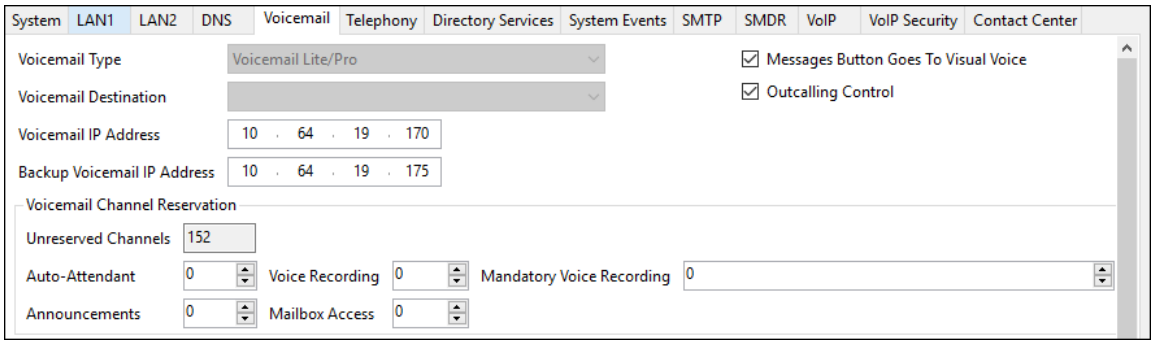
- **Firewall/NAT Type** was set to **Unknown** in the reference configuration.
- The **Public IP Address** and **Public Port** sections are not used for the AT&T IPTF SIP trunk service connection.
- Click the **OK** button (not shown).



5.3.2. Voicemail Tab

As described in **Section 3**, Voicemail Pro was used in the reference configuration.

- Set **Voicemail Type** to **Voicemail Lite/Pro**.
- Set **Voicemail IP Address** to the IP address of the server hosting voicemail. In the reference configuration, this is the Primary server, **10.64.19.170**.
- Other parameters on this screen are default. Click the **OK** button (not shown).

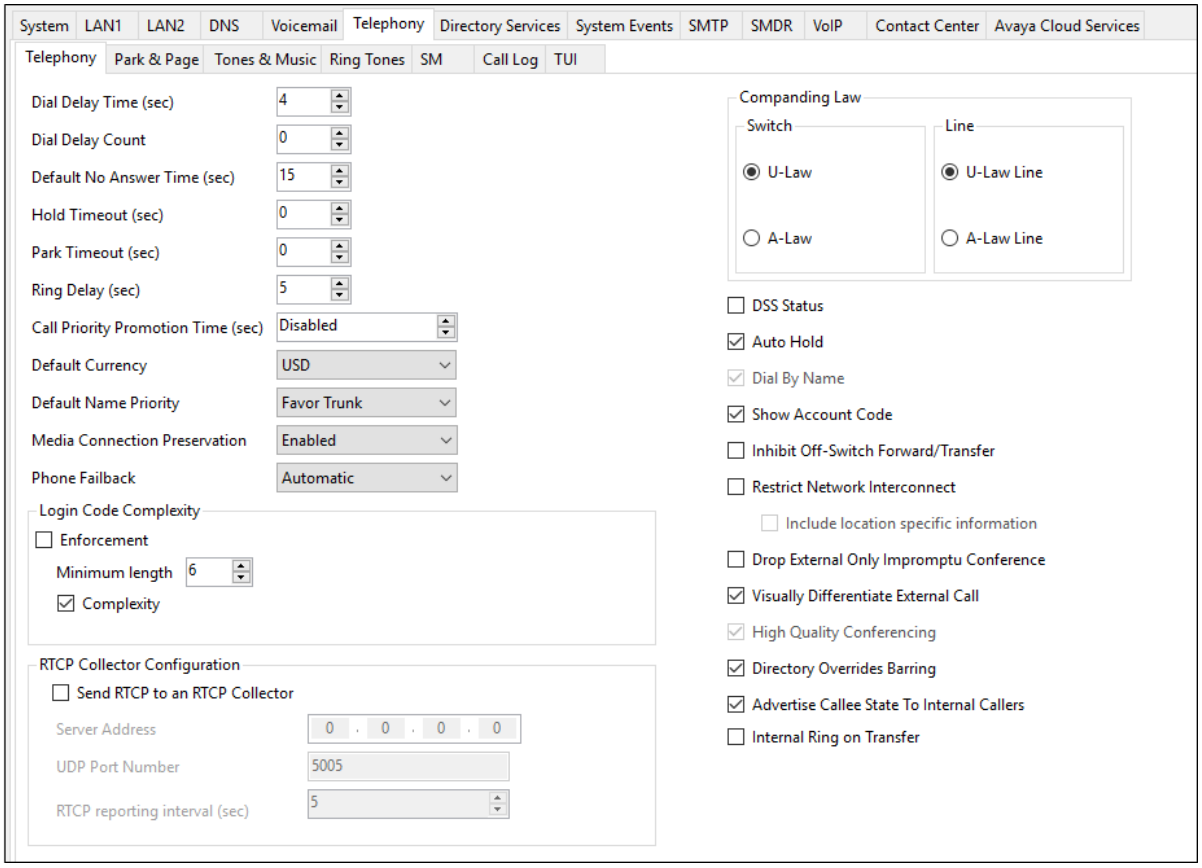


©2020 Avaya Inc. All Rights Reserved.

5.3.3. Telephony Tab

To view or change telephony settings, select the **Telephony** tab and **Telephony** sub-tab as shown in the following screen. The settings presented here simply illustrate the values used in the reference configuration and are not intended to be prescriptive.

- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave this setting checked.
- Set the **Companding Law** parameters to **U-Law** as is typical in North America.
- Default values are used in the other fields.
- Click the **OK** button (not shown).



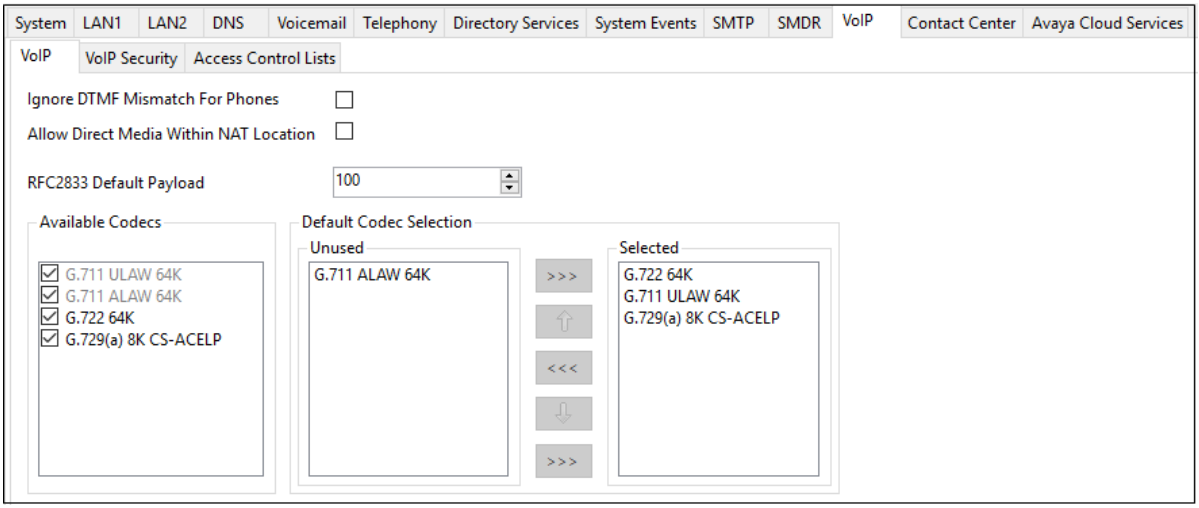
©2020 Avaya Inc. All Rights Reserved.

5.3.4. VoIP Tab

Navigate to the **VoIP** tab in the Details pane to view or change the system codecs and VoIP security settings.

Select the **VoIP → VoIP** tab. Configure the following parameters:

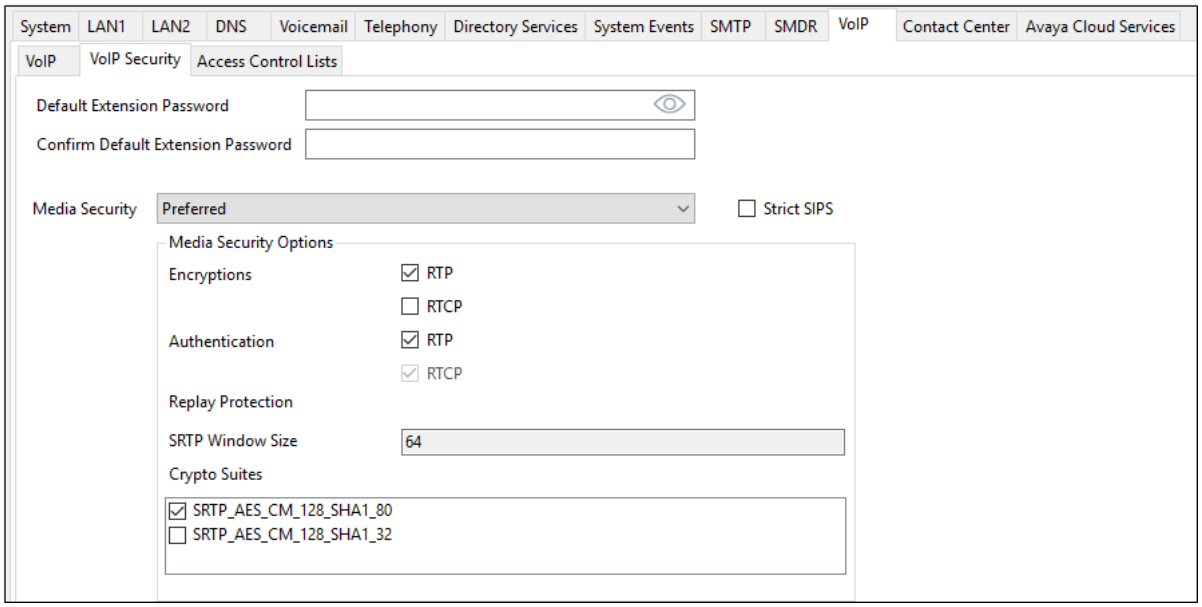
- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. During the compliance test, this was set to **100**, the value preferred by AT&T.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order were used.
- Click **OK** to commit (not shown).



©2020 Avaya Inc. All Rights Reserved.

During the compliance test, SRTP was used internal to the enterprise wherever possible. To view or configure the media encryption settings, select the **VoIP → VoIP Security** tab on the Details pane.

- Set the **Media Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields.
- Under **Crypto Suites**, select **SRTP_AES_CM_128_SHA1_80**.
- Click **OK** to commit (not shown).



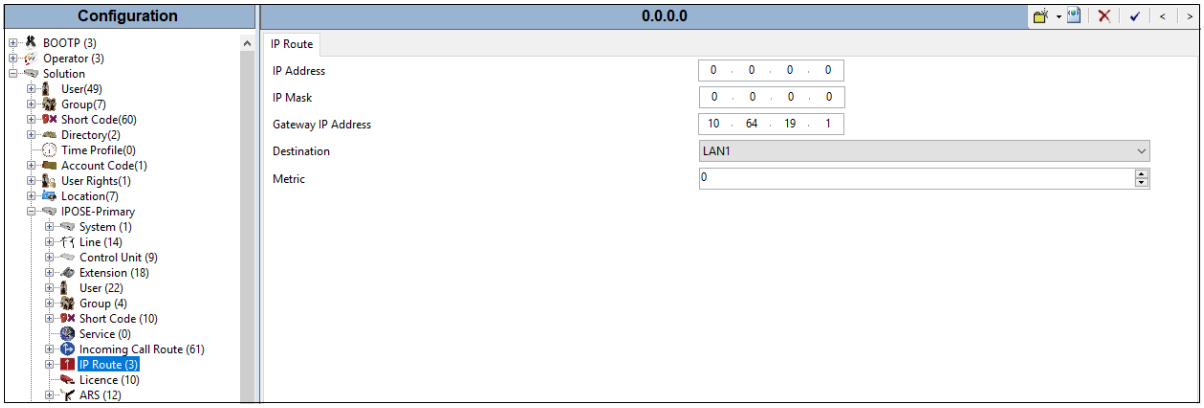
©2020 Avaya Inc. All Rights Reserved.

5.4. IP Route

In the sample configuration, the IP Office LAN1 port is physically connected to the local area network switch at the IP Office customer site. The Avaya SBCE resides on a different subnet and requires an IP route to allow SIP traffic between the two devices.

To create a new IP route, right-click on **IP Route** on the left navigation pane. Select **New** (not shown).

- Set the **IP Address** and **IP Mask** of the subnet of the private side of the Avaya SBCE, or enter **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the router in the IP Office subnet. The default gateway for this network is **10.64.19.1**.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).



5.5. SIP Line

The following sections describe the configuration of a SIP Line. The SIP Line terminates the CPE end of the SIP trunk to the AT&T IPTF service.

The recommended method for creating/configuring a SIP Line is to use the template associated with the provisioning described in these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a new SIP Line for SIP trunking with the AT&T IPTF service. Follow the steps in **Section 5.5.1** to create a SIP Trunk from the template.

Some items relevant to a specific customer environment are not included in the template or may need to be updated after the SIP Line is created. Examples include the following:

- IP addresses.
- SIP trunk registration credentials (if applicable).
- SIP URI entries.
- Setting of the **Use Network Topology** Info field on the Transport tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2** to **5.5.6**.

In addition, the following SIP Line settings are not supported on Basic Edition:

- SIP Line – Originator number for forwarded and twinning calls.
- Transport – Second Explicit DNS Server.
- SIP Credentials – Registration Requirement.
- SIP Advanced Engineering.

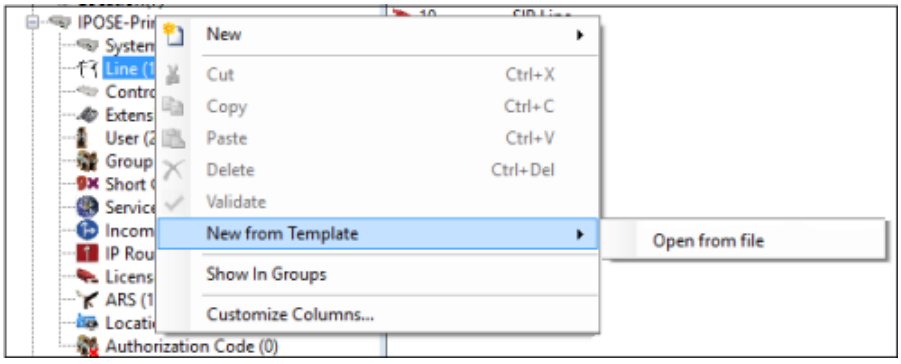
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.5.2** to **5.5.6**.

©2020 Avaya Inc. All Rights Reserved.

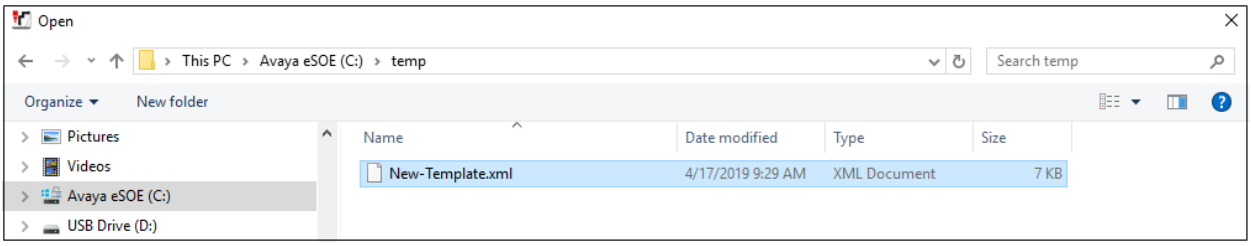
5.5.1. Creating a SIP Line from an XML Template

Note – DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (IP500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

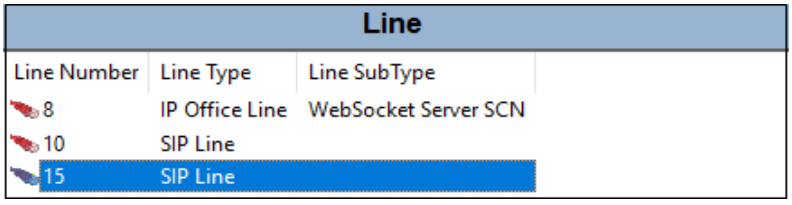
Copy a previously created template file to the computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New →New from Template**. Select **Open from file.**



Navigate to the directory where the template was copied on the local computer (e.g., *\temp*) and select it. Click **Open** (not shown).



The new SIP Line is created, and it will appear on the **Navigation** pane (e.g., SIP Line **15**). The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2** to **5.5.6**.

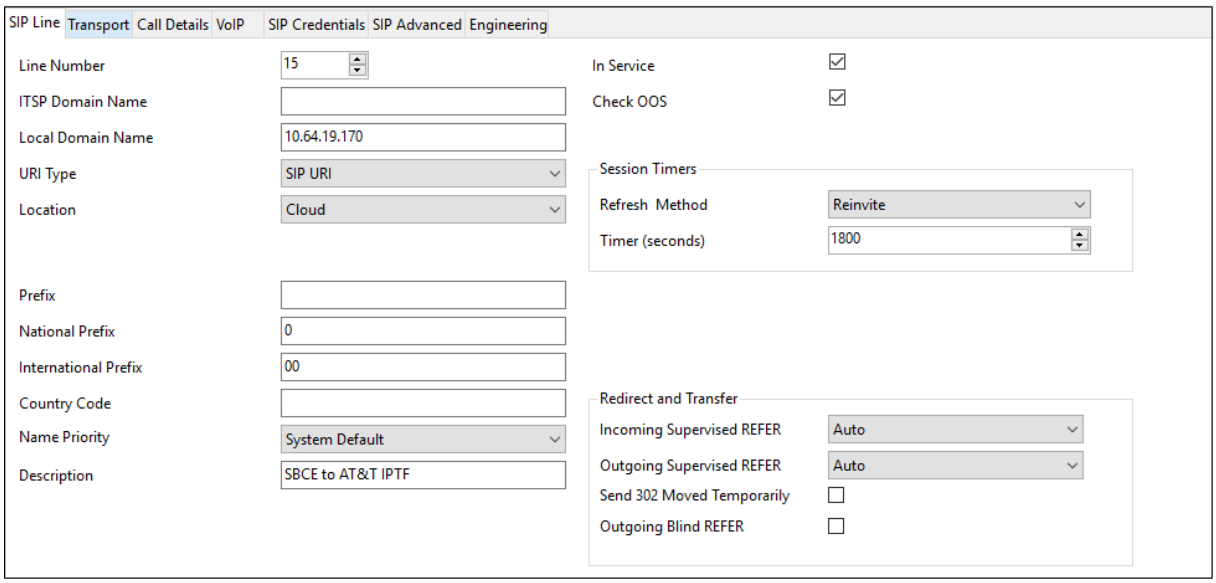


©2020 Avaya Inc. All Rights Reserved.

5.5.2. SIP Line – SIP Line tab

On the **SIP Line** tab in the **Details** pane, configure or verify the parameters as shown below:

- **ITSP Domain Name**: leave as the default (blank) to have IP Office send the **ITSP Proxy Address** as the domain name. See **Section 5.5.3**.
- **Local Domain Name:** Set to the public IP address of the Avaya IP Office LAN1 interface (e.g., **10.64.19.170**).
- Verify that **In Service** box is checked, the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- **Refresh Method:** Set to **Re-Invite**, as AT&T does not support UPDATE
- Set **Timer (seconds)** to **1800**. This field specifies the session expiry time. With this value, a session refresh message is sent every 15 minutes, at the half way point of the expiry time.
- **Incoming Supervised Refer**: Set this field to **Auto** (default).
- **Outgoing Supervised Refer**: Set this field to **Auto** (default).
- **Send 302 Moved Temporarily**: Verify this is unchecked (default).
- **Outgoing Blind Refer**: Verify this is unchecked (default).
- Use the default values for the other fields.
- Click **OK** (not shown).

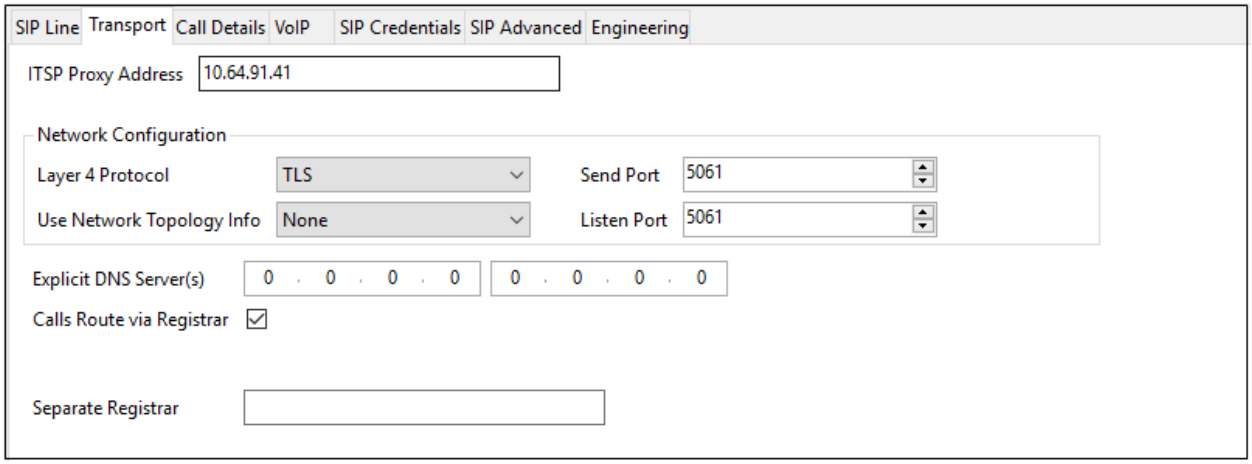


©2020 Avaya Inc. All Rights Reserved.

5.5.3. SIP Line - Transport Tab

Select the **SIP Line → Transport** tab and configure the following:

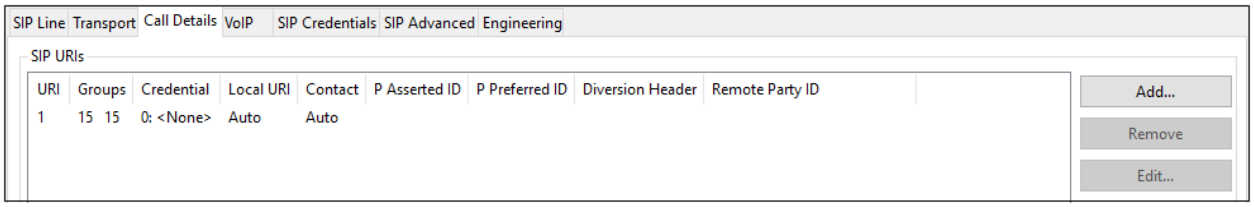
- **ITSP Proxy Address:** Set to the Avaya SBCE A1 IP address (e.g., **10.64.91.41**).
- **Network Configuration → Layer 4 Protocol**: Set to **TLS**.
- **Network Configuration → Send Port**: Set to **5061**.
- **Network Configuration → Use Network Topology Info**: Set to **None**.
- **Network Configuration → Listen Port**: Set to **5061**.
- Verify **Calls Route via Registrar:** Enabled (default)
- Click **OK** (not shown).



©2020 Avaya Inc. All Rights Reserved.

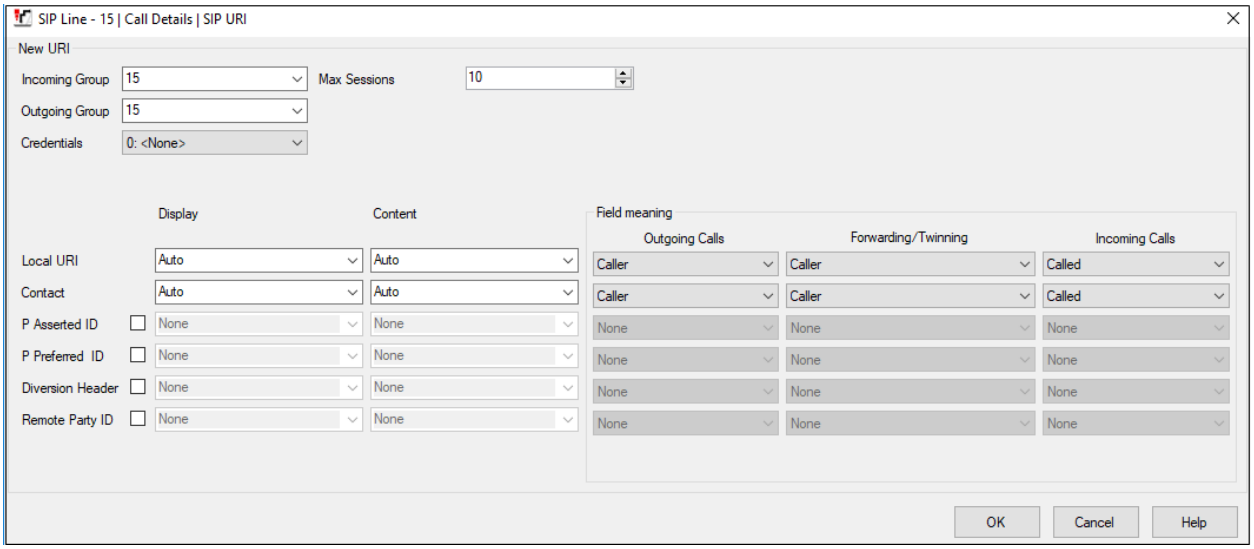
5.5.4. SIP Line – Call Details tab

Select the **Call Details** tab. To add a new SIP URI, click the **Add…** button. To review an existing SIP URI, select it and click the **Edit** button.



The **SIP URI** window will open. Configure the following:

- **Incoming Group:** Set to an unused group number, e.g., **15**. This value references the **Line Group ID** set on the **Incoming Call Routes** in **Section 5.8**.
- **Max Sessions:** In the reference configuration this was set to **10**. This sets the maximum number of simultaneous calls that can use the URI before Avaya IP Office returns busy to any further calls.
- **Outgoing Group:** Set to an unused group number, e.g., **15**.
- For the **Local URI**, and **Contact** fields, leave the selections under the **Display** and **Content** columns to the default **Auto**.
- On the **Field meaning** section, set the values as shown on the screenshot below.
- Click **OK**.



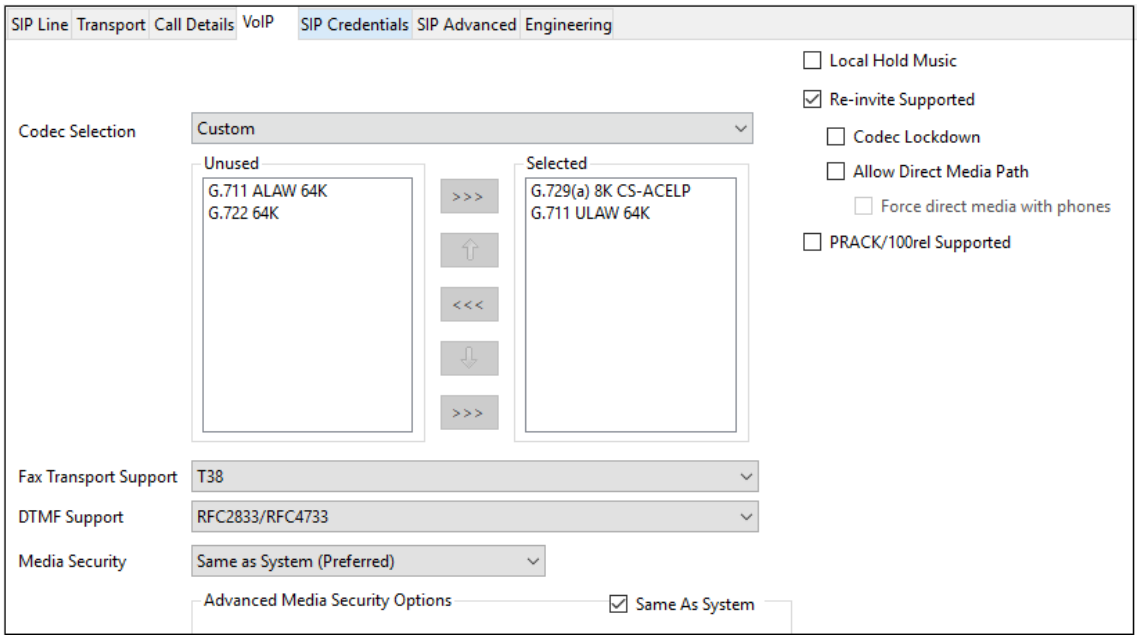
- To edit an existing entry, click an entry in the list and click the **Edit** button.
- When all SIP URI entries have been added or edited, click **OK** at the bottom of the screen (not shown).

©2020 Avaya Inc. All Rights Reserved.

5.5.5. SIP Line - VoIP tab

Select the **SIP Line → VoIP** tab. Set the parameters as shown below:

- The **Codec Selection** drop-down box → **System Default** will list all available codecs. In the reference configuration, **Custom** was selected with **G729(a) 8K CS-ACELP** and **G.711 ULAW 64K** specified. This causes Avaya IP Office to include these codecs in the Session Description Protocol (SDP) offer, and in the order specified. Note that in the reference configuration G.729A is set as the preferred codec on the SIP trunk to the AT&T IPTF network.
- T.38 fax is the preferred method for fax. Set the **Fax Transport Support** to **T.38** from drop-down menu. See **Section 2.2**, **item 7**.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** drop-down menu to **Same as System (Preferred)**. Verify that the **Same as System** parameter is checked. This setting will use the same media security level for the trunk as is defined for the system in **Section 5.3.4**. The system level media security is set to **Preferred,** specifying that SRTP is preferred over RTP.
- The **Re-invite Supported** parameter can be checked to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).



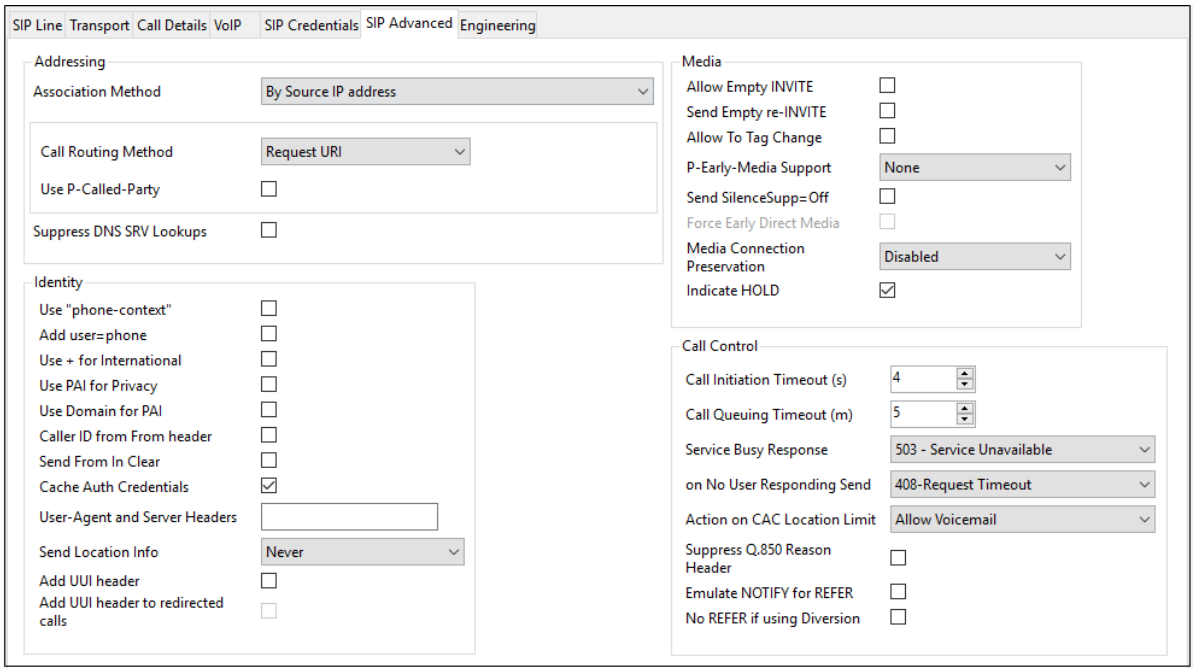
©2020 Avaya Inc. All Rights Reserved.

5.5.6. SIP Line – SIP Advanced Tab

IP Office can be configured to signal when a call is placed on hold by sending an INVITE with media attribute “sendonly”. AT&T in turn will respond with media attribute “recvonly” and will stop sending RTP media for the duration the call is on hold. When the call is taken off of hold, IP Office will send another INVITE with media attribute “sendrecv” indicating to AT&T to start sending RTP again.

To have Avaya IP Office signal to AT&T when a call is placed on/off hold, select the **SIP Line → SIP Advanced** tab and enter the following:

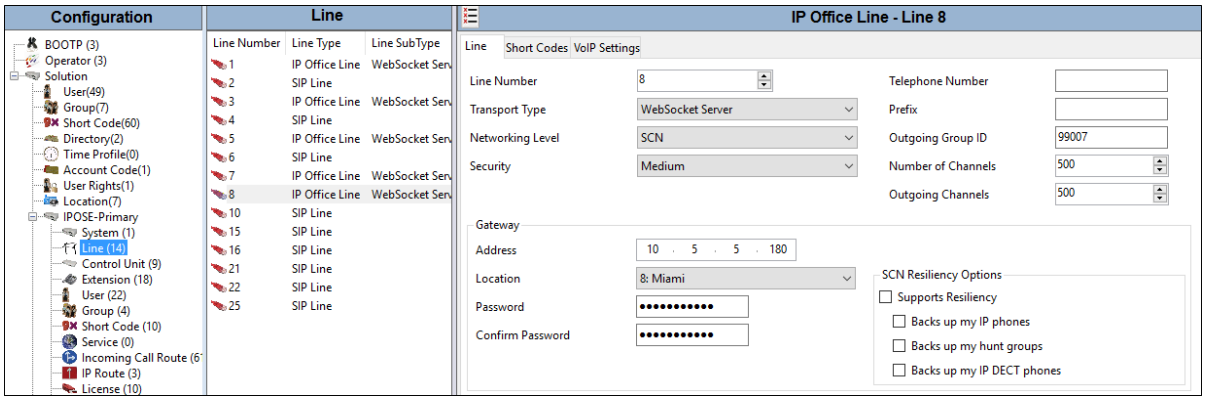
- Select **Indicate HOLD** in the **Media** section.
- Click **OK** to commit (not shown).



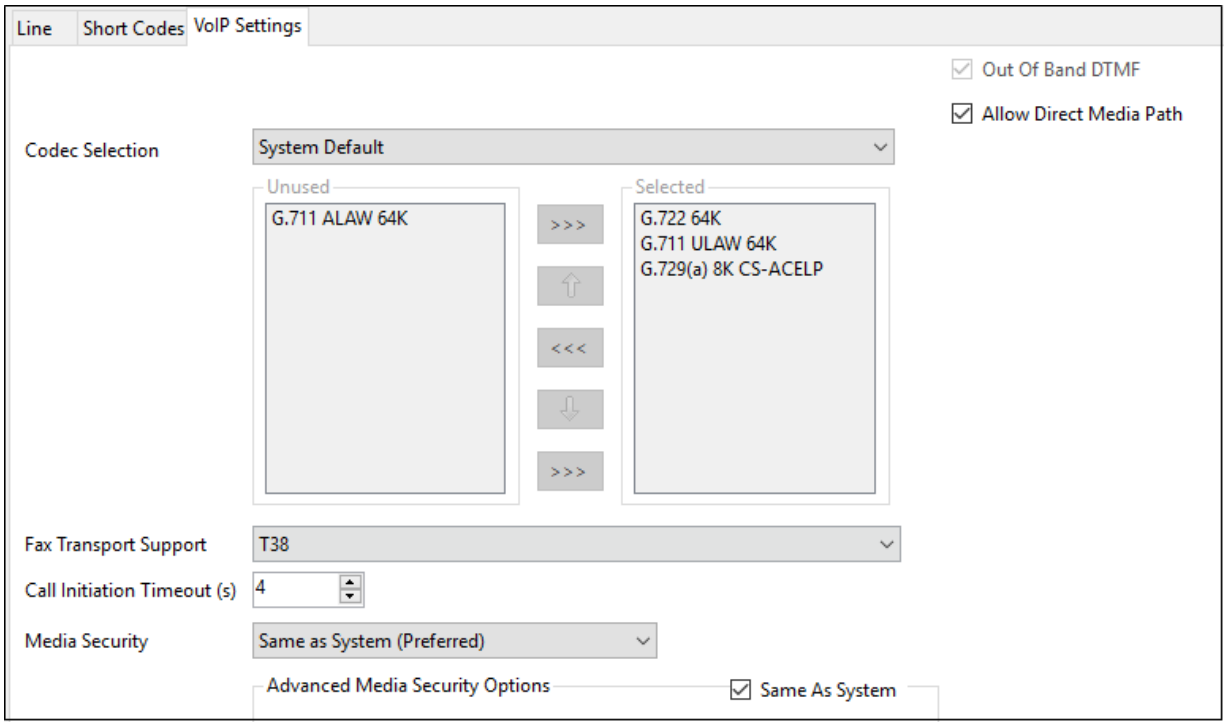
©2020 Avaya Inc. All Rights Reserved.

5.6. IP Office Line

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the IP500 V2 Expansion System.



The screen below shows the IP Office Line, **VoIP Settings** tab. In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. **Fax Transport Support** is set to **T.38**. Default values were used for all other parameters.



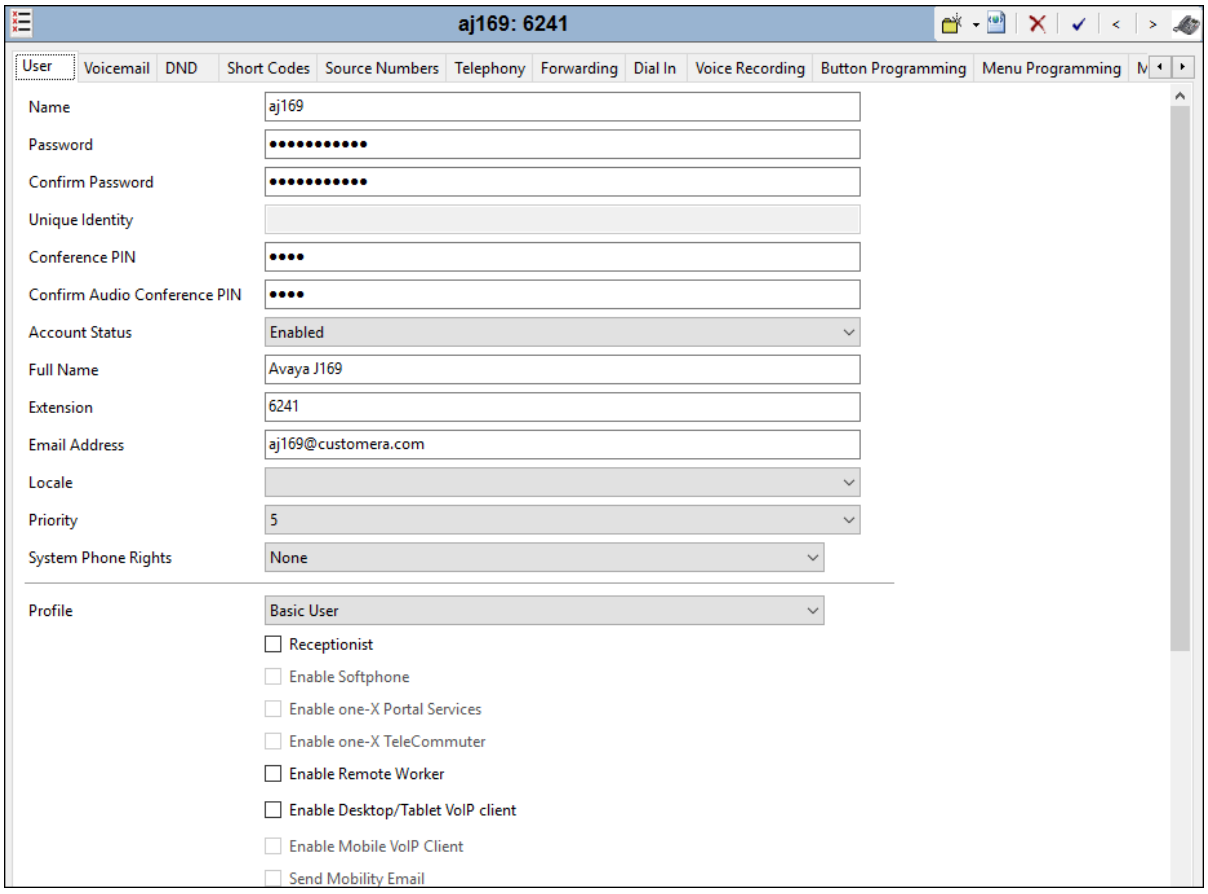
©2020 Avaya Inc. All Rights Reserved.

5.7. Users, Extensions, and Hunt Groups

In this section, examples of IP Office Users, Extensions, and Groups will be illustrated. In the interests of brevity, only one of the users and extensions shown in **Figure 1** will be presented, since the configuration can be easily extrapolated to other users. To add a User, right click on **User** in the **Navigation** pane, and select **New**. To edit an existing User, select **User** in the **Navigation** pane, and select the appropriate user to be configured in the **Group** pane.

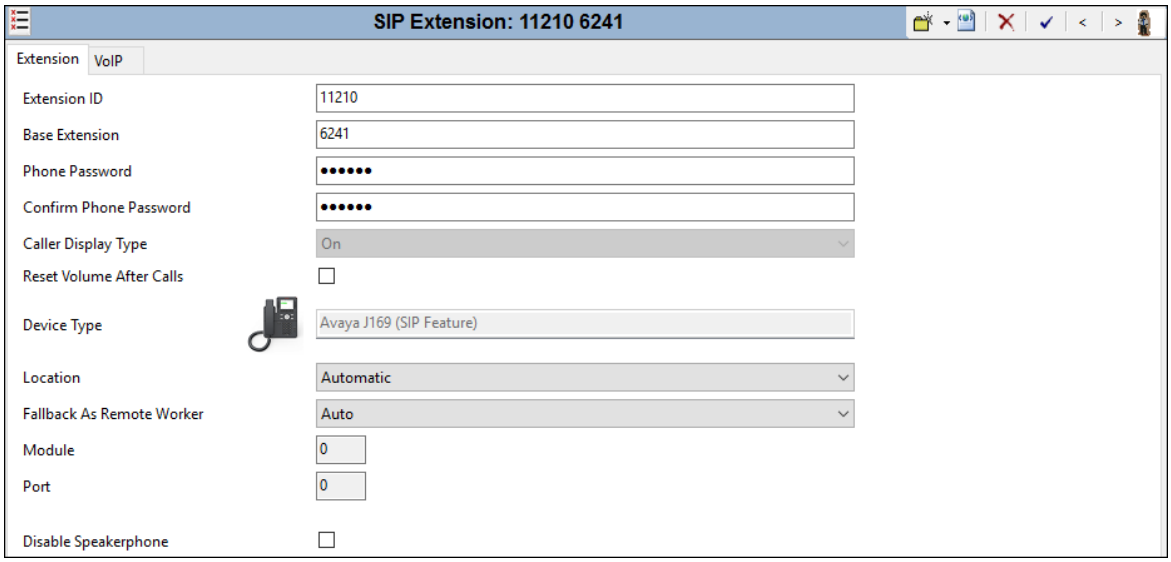
5.7.1. User

The following screen shows the **User** tab for user 6241. As shown in **Figure 1**, this user corresponds to the Avaya J169 SIP endpoint.

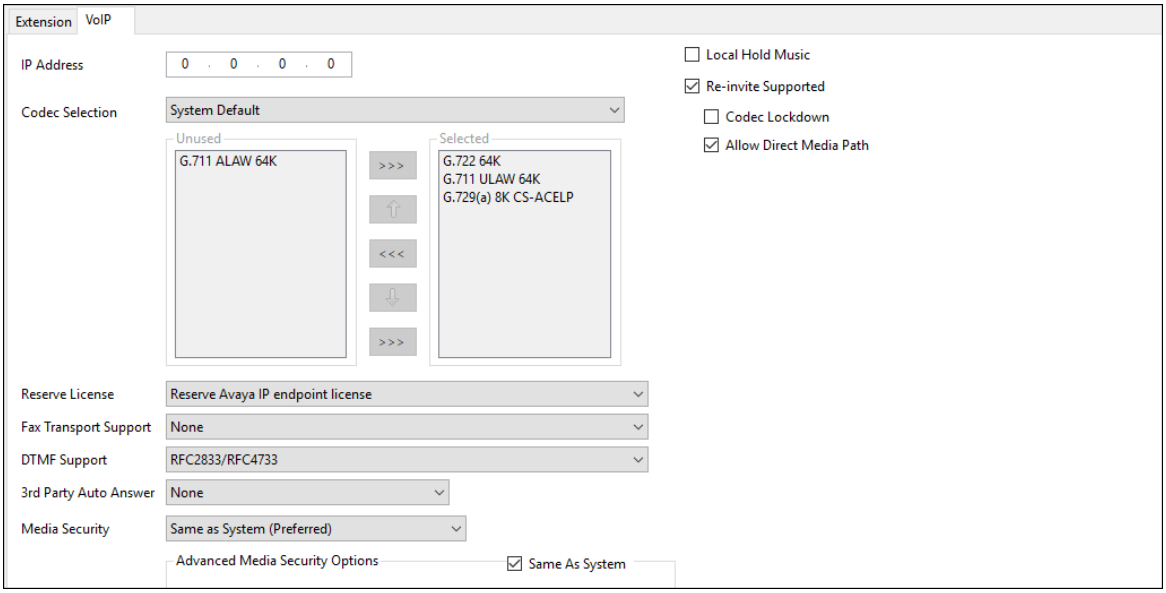


5.7.2. Extension

The following screen shows the Extension information for user 6241 (Avaya J169 SIP).
To view, select **Extension** from the Navigation pane, and the appropriate extension from the Group pane.



The following screen shows the **VoIP** tab for the extension. The **IP Address** field may be left blank. Check the **Reserve Avaya IP endpoint license** box. The **Codec Selection** parameter may retain the default setting "**System Default**" to follow the system configuration shown in **Section 5.3.4**. The Media Security parameter may also retain the default setting "**Same as System (Preferred)**" to follow the system configuring shown in **Section 5.3.4**.

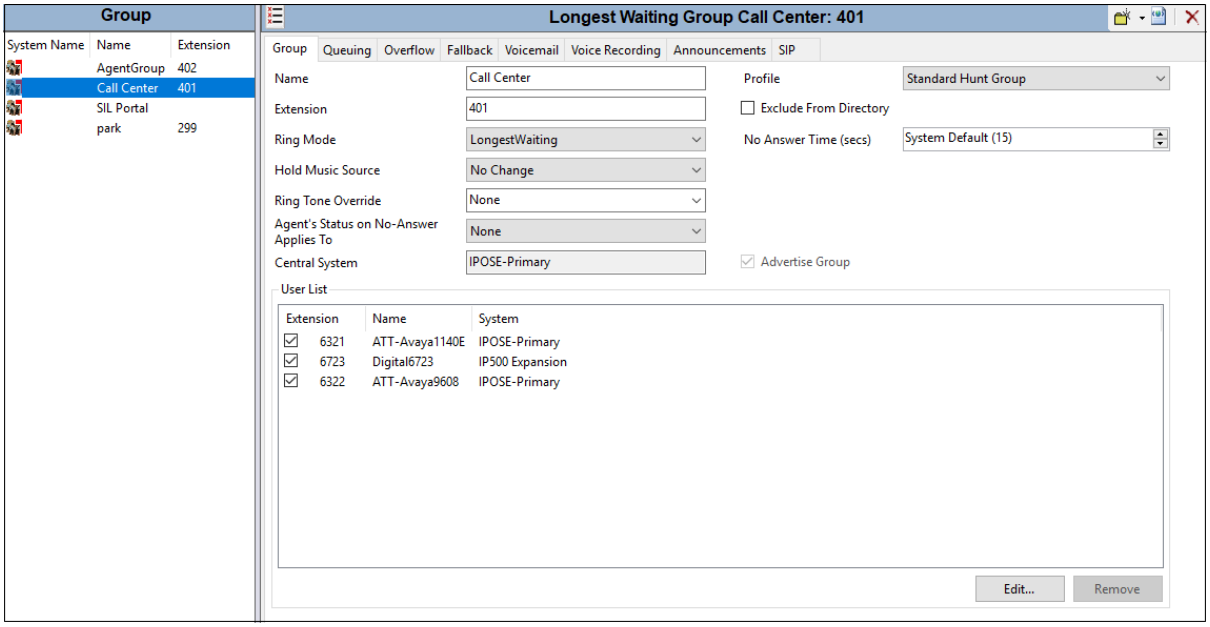


©2020 Avaya Inc. All Rights Reserved.

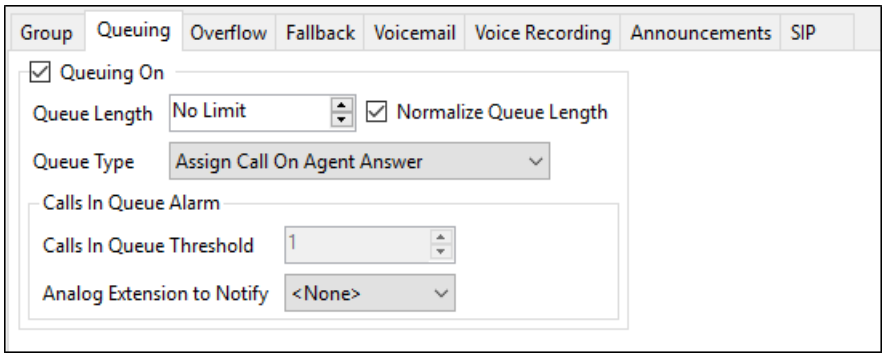
5.7.3. Hunt Groups

During the verification of these Application Notes, users could also receive incoming calls as members of a hunt group. To configure a new hunt group, right-click **Group** from the Navigation pane, and select **New**. To view or edit an existing hunt group, select **Group** from the Navigation pane, and the appropriate hunt group from the Group pane.

The following screen shows the **Group** tab for hunt group 401. The telephone extensions in the **User List** are rung based the extension that has been unused for the longest period, due to the **Ring Mode** setting "**Longest Waiting**" (i.e., "longest waiting", most idle user receives next call). Click the **Edit** button to change the **User List**.

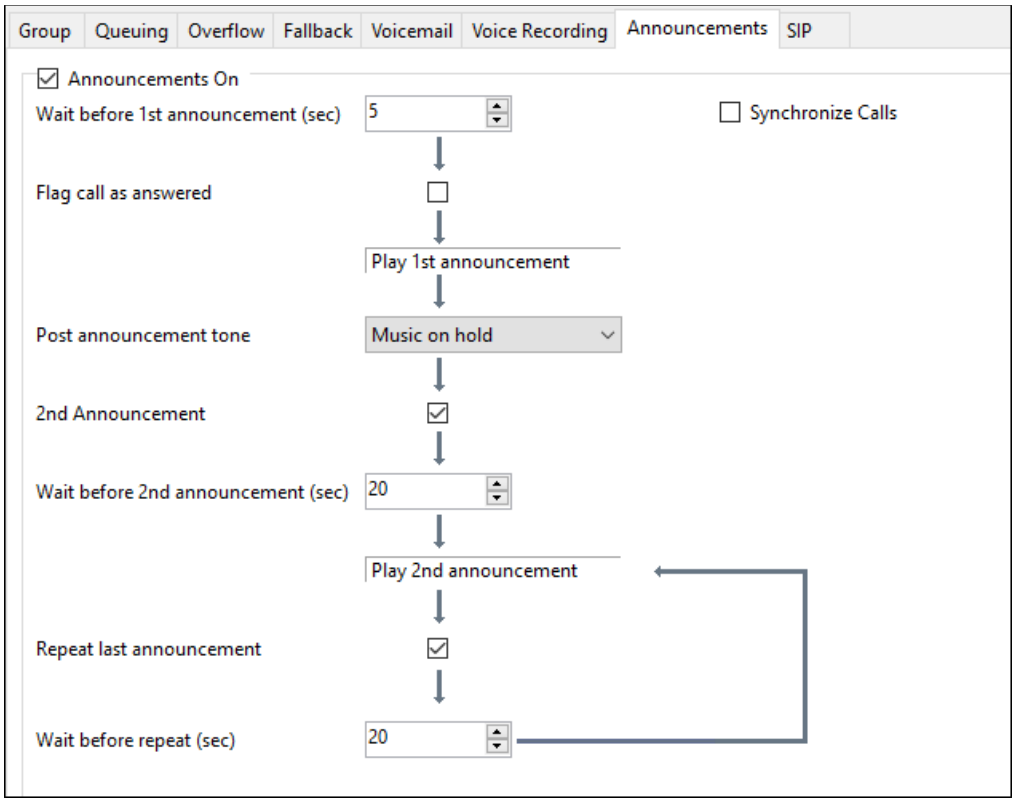


Under the **Queuing** tab, check the **Queuing On** box and set the **Queue Length** field to any desirable value. Use the default values for all the other fields.



©2020 Avaya Inc. All Rights Reserved.

Under the **Announcements** tab, check the **Announcements On** box. The wait time can be set to any desirable value. The **Synchronize Calls** box is checked to greatly reduce the number voicemail channels needed to play announcements. These announcements are played if an agent for a particular skill is unavailable.



In the reference configuration, these steps were used to create the additional Hunt Group "AgentGroup" (402).

©2020 Avaya Inc. All Rights Reserved.

5.8. Incoming Call Route

Note – The digits defined and matched in the Incoming Call Route table, are the DNIS digits specified in the AT&T Request-URI, not the DID digits dialed by the caller. The IPTF service may deliver various DNIS digit lengths in the SIP Invite Request-URI, depending on the circuit order provisioning. In the reference configuration, the IPTF service delivered 15 digits.

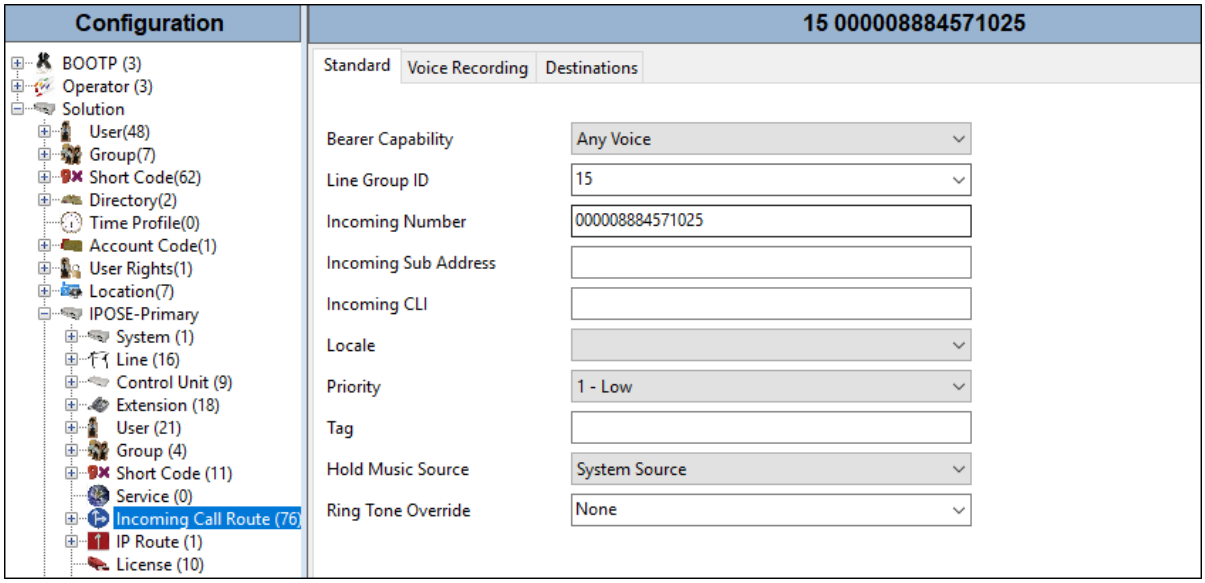
The Incoming Call Route table will map specific AT&T DNIS numbers to an IP Office User, or Hunt Group, as well as to Voicemail Pro scripts.

To add an incoming call route, right click on **Incoming Call Route** in the Navigation pane and select **New** (not shown). To edit an existing incoming call route, select an **Incoming Call Route** in the Navigation pane, and the associated call route information is displayed in the Group pane.

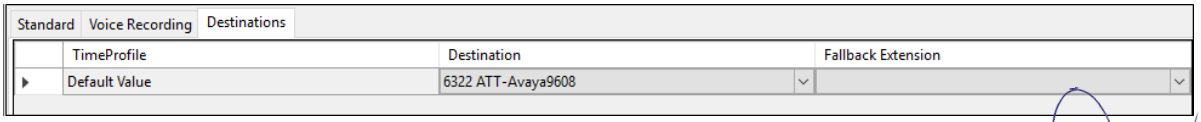
5.8.1. Calls to IP Office Stations and Hunt Groups

In the example below, the incoming number **000008884571025** is directed to H.323 phone 6322. On the **Standard** tab enter the following:

- **Line Group ID**: Enter the SIP Line defined in **Section 5.5** (e.g., **15**).
- **Incoming Number**: Enter the associated DNIS digits sent by AT&T (e.g., **000008884571025**).
- Use default values for the remaining fields and click **OK** (not shown).

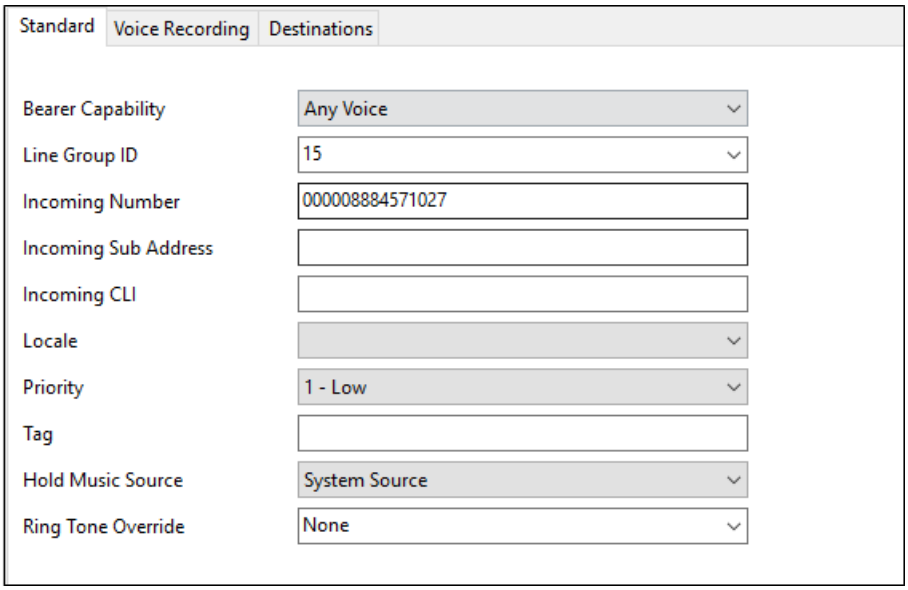


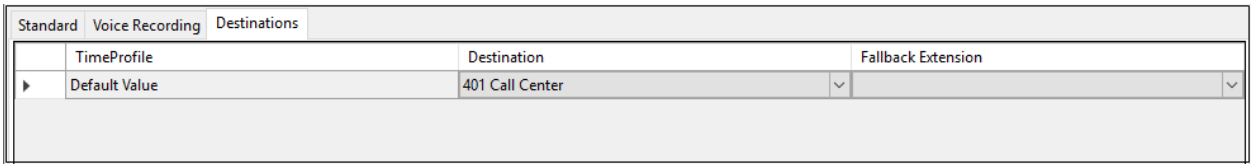
Select the **Destinations** tab. From the **Destination** drop-down menu, select the endpoint associated with this number, extension **6322** in this example.



©2020 Avaya Inc. All Rights Reserved.

Below is an example of a call for AT&T DNIS **000008884571027** being directed to Hunt Group **401** (Call Center).

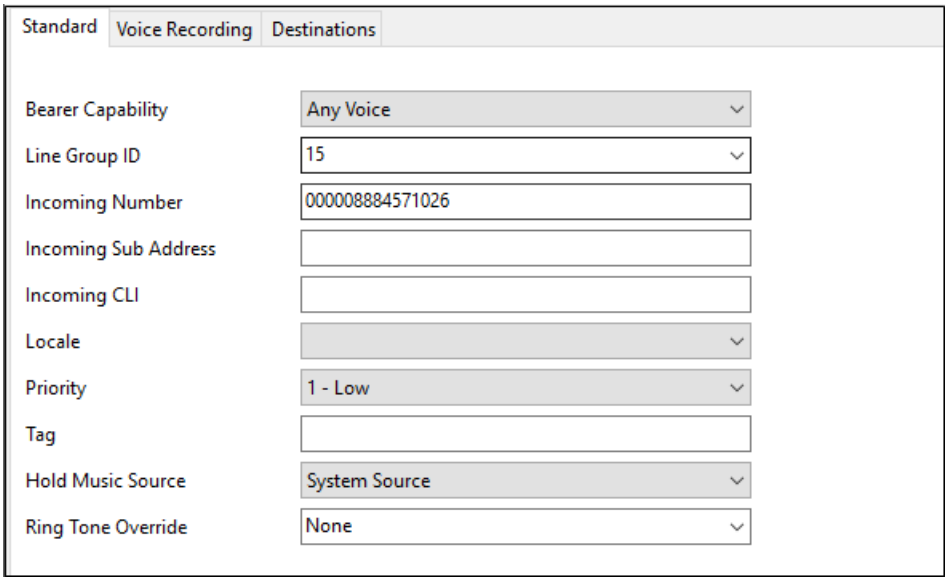


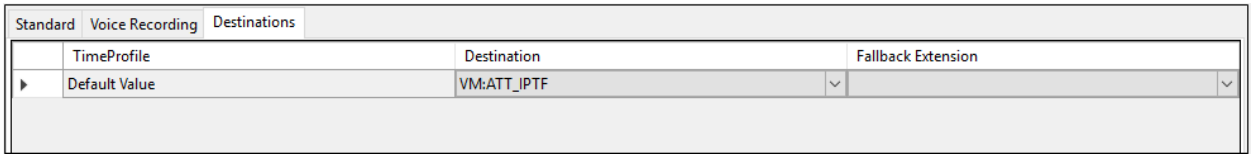


5.8.2. Calls to Voicemail Pro Scripts

As described next in **Section 5.9**, Voicemail Pro scripts are defined with specific names. These script names are specified as destinations in the Incoming Call Route table.
In the example below, incoming number **000008554571026** is directed to the Voicemail Pro Auto-Attendant script **ATT_IPTF**.

1. On the **Standard** tab repeat the steps in **Section 5.8.1**, with the following changes:
   - **Incoming Number**: Enter the associated DNIS digits sent by AT&T (e.g., **000008554571026**).
2. On the **Destinations** tab enter the following:
   - In the **Destinations** column, enter the string **VM:ATT_IPTF** from the drop down menu (note if the voicemail module does not appear in the list, enter the value manually).
   - Use default values for the remaining fields and click **OK** (not shown).





©2020 Avaya Inc. All Rights Reserved.
Página 3179 de 3226.

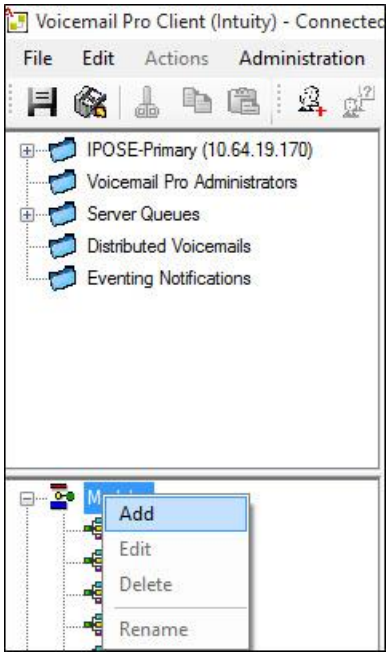
5.9. Call Center Provisioning in Voicemail Pro

Note – While Voicemail Pro provisioning and programming is beyond the scope of this document, a sample Auto-Attendant script is described below.

In the reference configuration, Voicemail Pro is used for Voicemail processing as well as for simulating basic Call Center functionality.

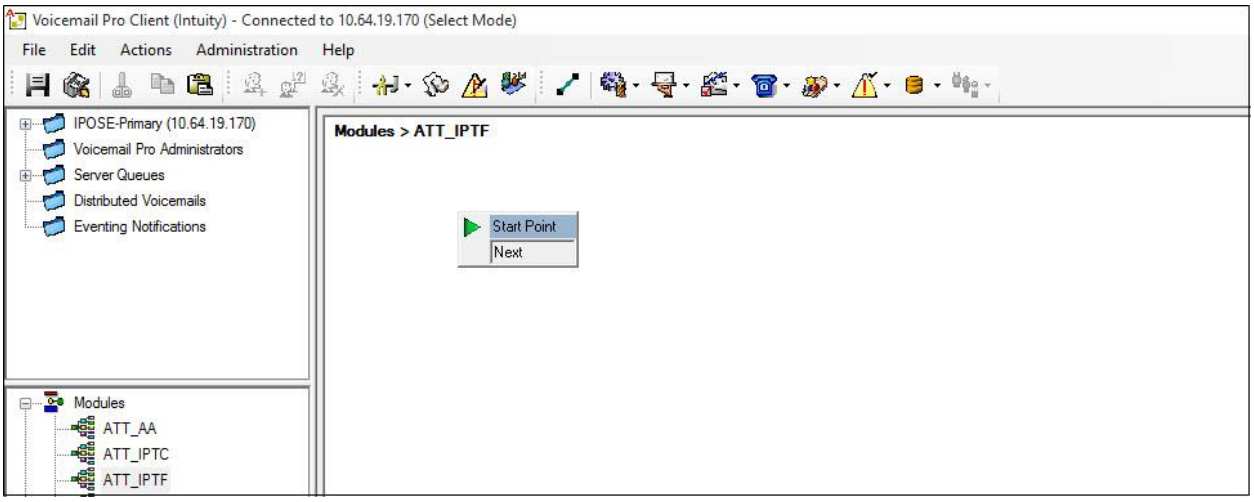
The Auto-Attendant function was provisioned to prompt callers to select a numeric option (1, 2, or 3), that would transfer the call to an associated Avaya IP Office Hunt Group (Call Center, AgentGroup), or to a specific extension. This is accomplished via the following steps:

1. Hunt Groups **Call Center** and **AgentGroup** are created in IP Office (**Section 5.7.3**).
2. User 6241 is created in IP Office (**Section 5.7.1**)
3. Incoming Call Route for DNIS digits **000008884571026** is defined for access to the Auto-Attendant script (**Section 5.8.2**).
4. Via the Voicemail Pro GUI interface:
    - Open the **Voicemail Pro Client** application and log in to the Voicemail Pro server (not shown).
    - Create a **Start Point** by right clicking on **Modules** and selecting **Add**.



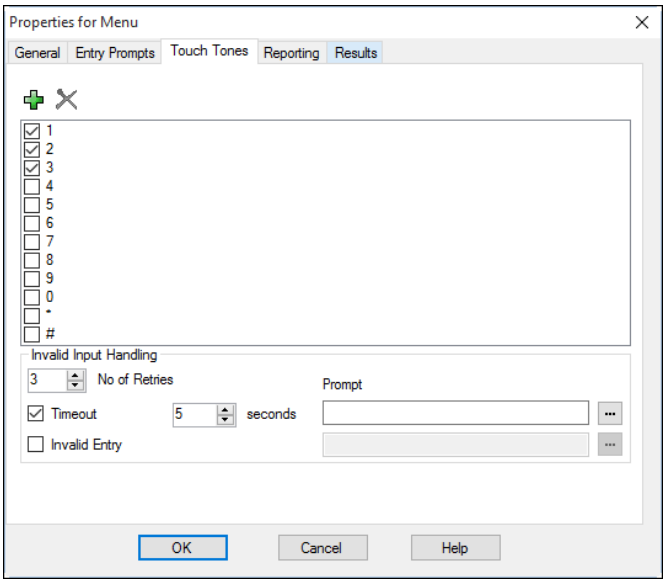
- Enter a name (e.g., **ATT_IPTF**) and click on **OK** (not shown). The new script "ATT_IPTF" will appear under Modules and a Start Point icon will appear in the work area.

©2020 Avaya Inc. All Rights Reserved.



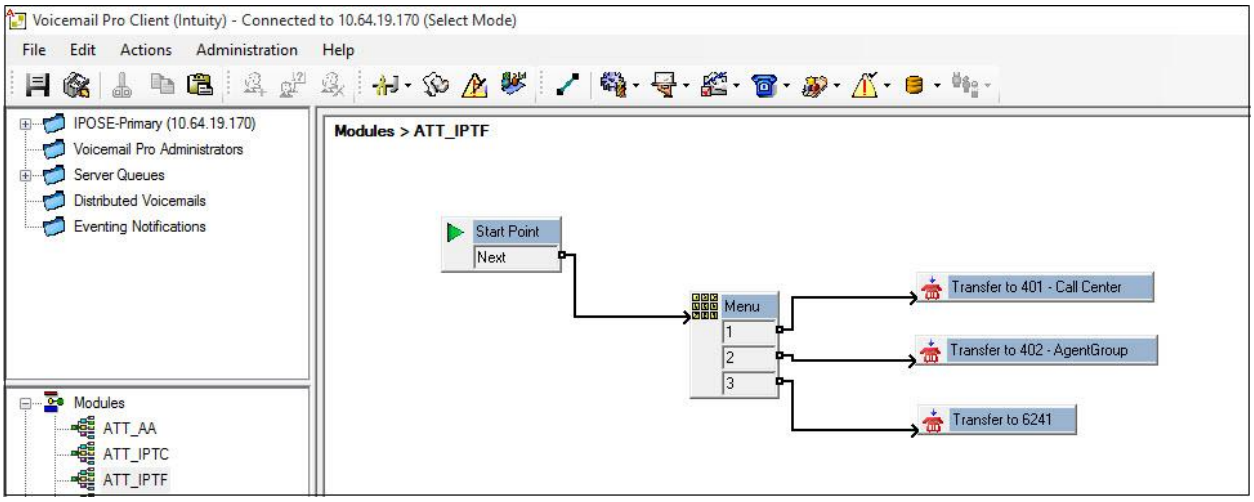
- Click on the **Start Point** icon to activate the script options at the top of the screen. From the options, select the **Basic Actions** icon , select the **Menu** icon , and click on the work area to place the **Menu** icon.
    i. Double click the **Start Point** icon.
        1. On the **General** tab → **Token Name**, enter **Start Point** and click **OK** (not shown).
    ii. Double click the **Menu** icon.
        1. On the **General** tab → **Token Name**, enter **Menu** (not shown).
        2. On the **Entry Prompts** tab (not shown), select or create an **Entry Prompt** that will tell the caller what digits to press (e.g., **mainmenu.wav**). To modify an existing recording, double click on the .wav file and rerecord. If no .wav files exist, double click on the icon to open the .wav editor.
        3. On the **Touch Tone** tab:
            a. Select **1, 2,** and **3** as the possible entry digits.
            b. Select **3** for **No of Retries**.
        4. Click on **OK**.

©2020 Avaya Inc. All Rights Reserved.



- Click on the Telephony Actions icon , select the Transfer icon , and click on the work area to place the **Transfer** icon in the work area. This will be used for "Call Center". Select and place two more Transfer Icons (these will be used for "AgentGroup" and "User 6241").
    i. Double click on the first **Transfer** icon.
        1. On the **General** tab → **Token Name** = **Transfer to 401 - Call Center** (not shown).
        2. On the **Specific** tab → **Destination = 401** (not shown).
    ii. Double click on the second **Transfer** icon.
        1. On the **General** tab → **Token Name** = **Transfer to 402 - AgentGroup** (not shown).
        2. On the **Specific** tab → **Destination** = **402** (not shown).
    iii. Double Click on the third **Transfer** icon.
        1. On the **General** tab, **Token Name** = **Transfer to 6241** (not shown).
        2. On the **Specific** tab, **Destination = 6241** (not shown).
- From the options bar, select the Connector icon and:
    i. Drag a connecting flow line from the **Start Point** box to the **Menu** box (see screen shot below).
    ii. Drag connecting flow lines from each of the **Menu** options to their associated **Transfer** boxes (see screenshot below).

©2020 Avaya Inc. All Rights Reserved.



5. From the top menu select **File → Save & Make Live** or select the icon.

When the associated AT&T DNIS number is received (e.g., **000008884571026**), IP Office will send the call to Voicemail Pro. The caller will be prompted to enter 1, 2, or 3 to access Call Center, AgentGroup, or user 6241. The associated Avaya IP Office extension (e.g., 401, 402, or 6241) will then ring.

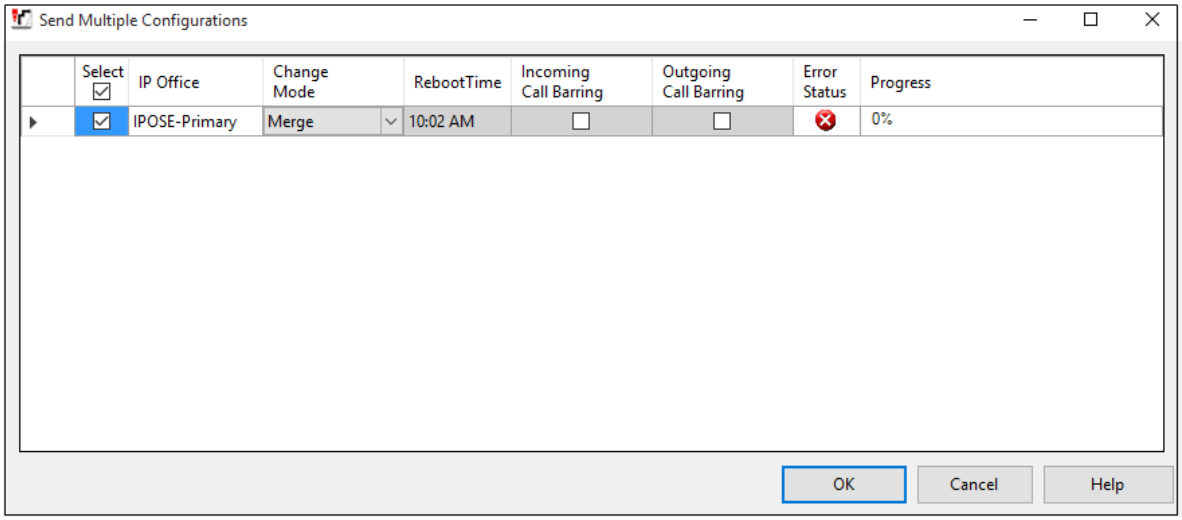
©2020 Avaya Inc. All Rights Reserved.

5.10. Save IP Office Primary Server Configuration

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. At the top of the Avaya IP Office Manager page, click **File → Save Configuration** (if that option is grayed out, no changes are pending).

A screen similar to the one below will appear, with either **Merge** or **Reboot** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Reboot** option will save the configuration and cause the Avaya IP Office server to reboot.

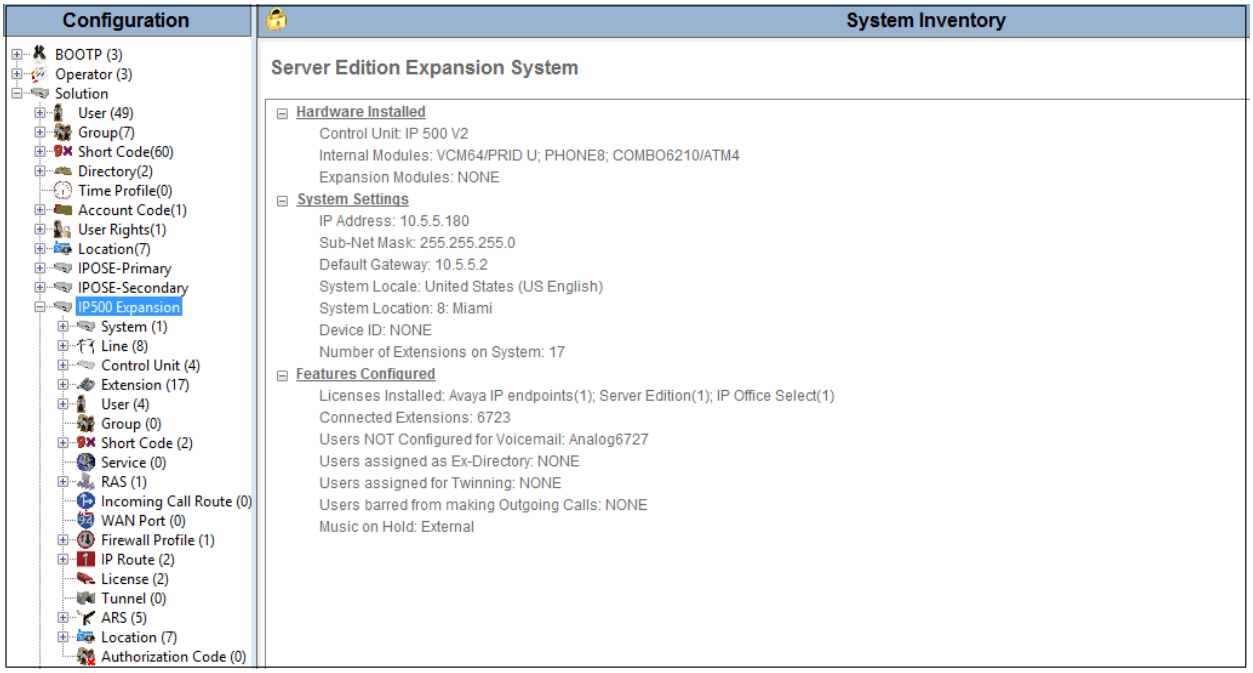
Click **OK** to execute the save.



©2020 Avaya Inc. All Rights Reserved.

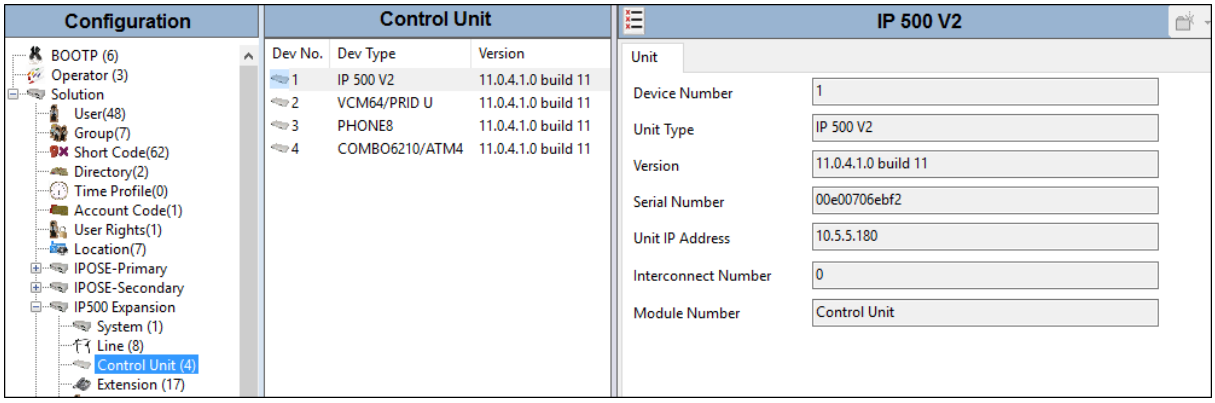
6. Avaya IP Office Expansion System Configuration

Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the "plus" sign next to **IP500 Expansion** on the left navigation pane will expand the menu on this server.



6.1. Expansion System - Physical Hardware

In the sample configuration, the IP500 V2 Expansion System contained a PHONE8 analog card and a COMBO6210 card, for the support of analog and digital stations. Also included is a VCM64 (Voice Compression Module). Both the VCM64 and the COMBO6210 cards provide voice compression channels to the control unit. Voice compression channels are needed to support VoIP calls, including IP extensions and or IP trunks.

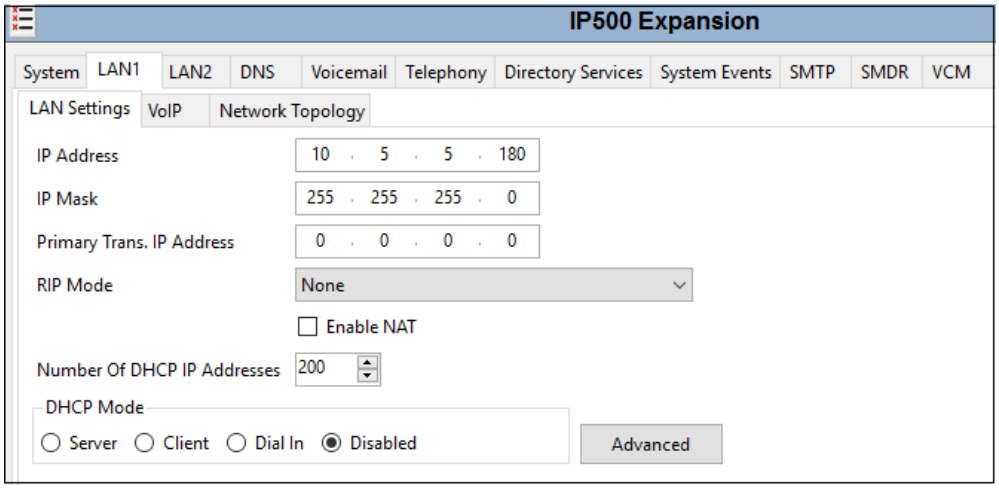


©2020 Avaya Inc. All Rights Reserved.

6.2. Expansion System - LAN Settings

In the sample configuration, LAN1 is used to connect the Expansion System to the enterprise network. To view or configure the LAN1 IP address, select **System** on the Navigation pane. Select the **LAN1 → LAN Settings** tab on the Details pane, and enter the following:

- **IP Address: 10.5.5.180** was used in the reference configuration.
- **IP Mask: 255.255.255.0** was used in the reference configuration
- Click the **OK** button (not shown).

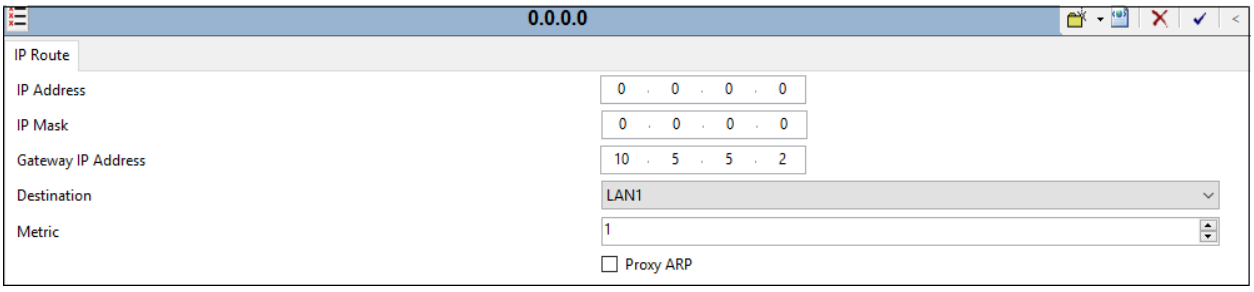


Defaults were used on the **VoIP** and **Network Topology** tabs (not shown).

6.3. Expansion System - IP Route

To create an IP route for the Expansion system, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown).

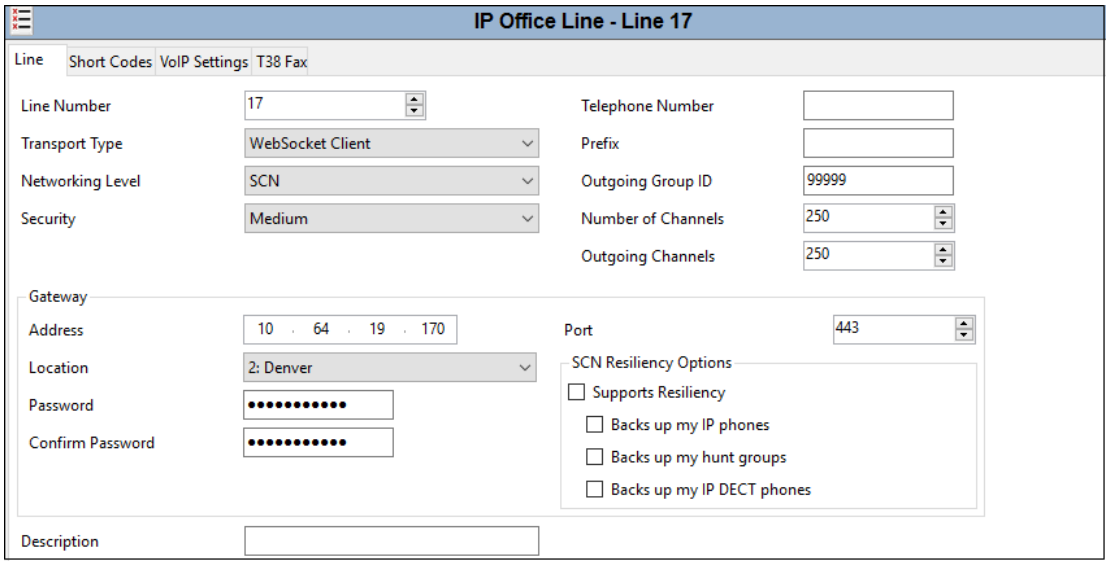
- Enter **0.0.0.0** on the **IP Address** and **IP Mask** fields to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet. The default gateway in the reference configuration was **10.5.5.2**
- Set **Destination** to **LAN1** from the pull-down menu.



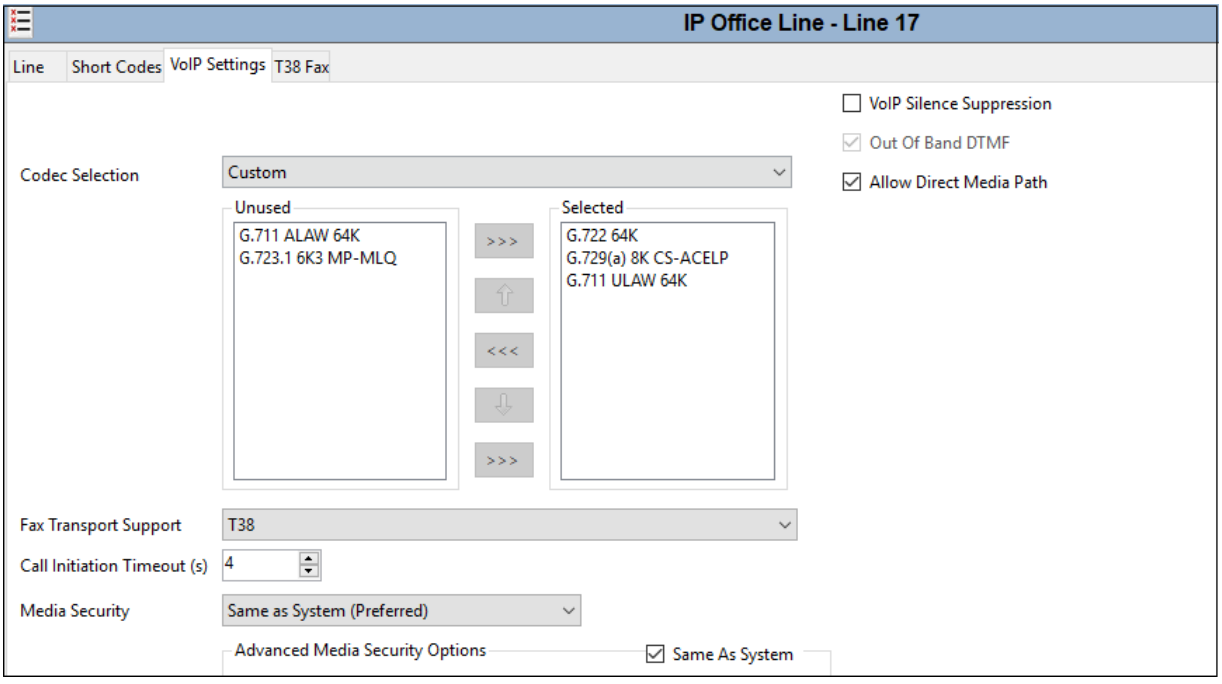
©2020 Avaya Inc. All Rights Reserved.

6.4. Expansion System - IP Office Line

The IP Office Line was automatically created on each server when the Expansion System is added to the solution. Below is the IP Office Line to the Primary server.

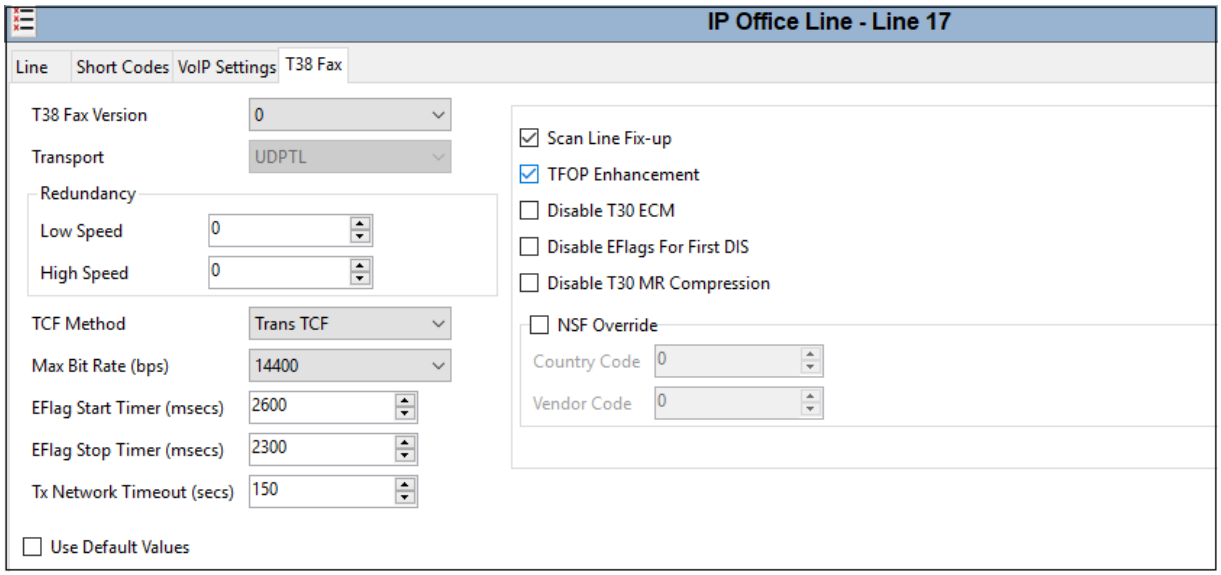


In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate T.38 fax, select the **VoIP Settings** tab and set **Fax Transport Support** to **T38.**



©2020 Avaya Inc. All Rights Reserved.

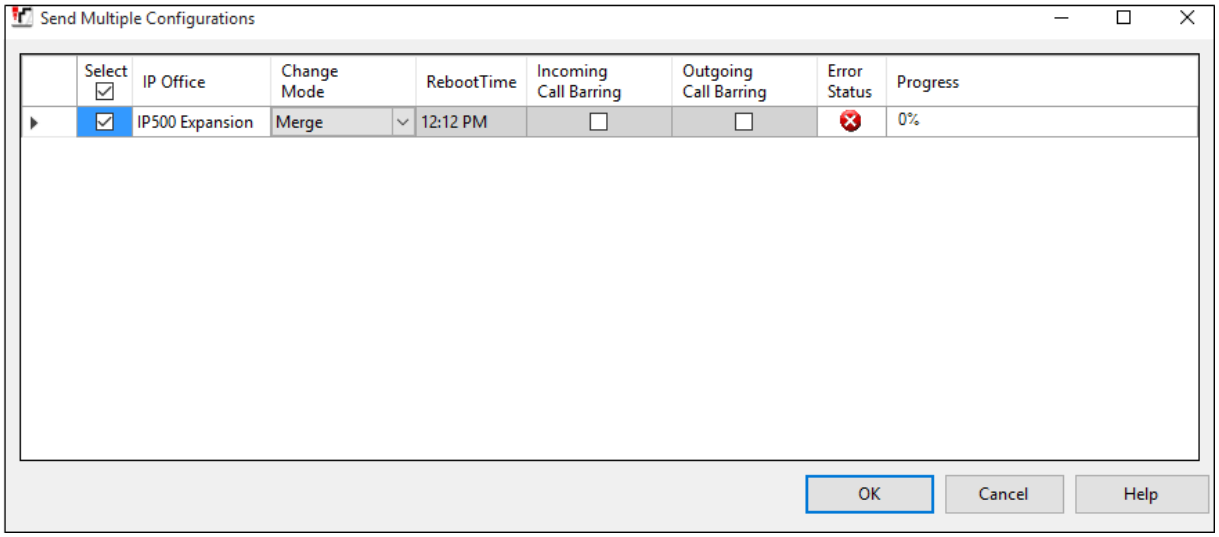
Select the **T38 Fax** tab. The **Use Default Values** box is unchecked, and the **T38 Fax Version** is set to "**0**". All other values are left at default.



6.5. Save IP Office Expansion System Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections

The following will appear, with either **Merge** or **Reboot** selected, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to proceed.



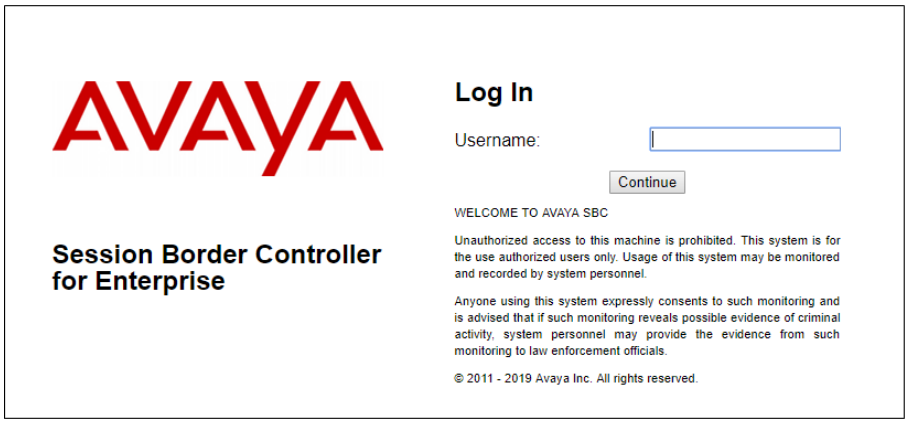
©2020 Avaya Inc. All Rights Reserved.

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the initial provisioning of the Avaya SBCE, including the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

Use a WEB browser to access the Element Management Server (EMS) web interface, and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE.

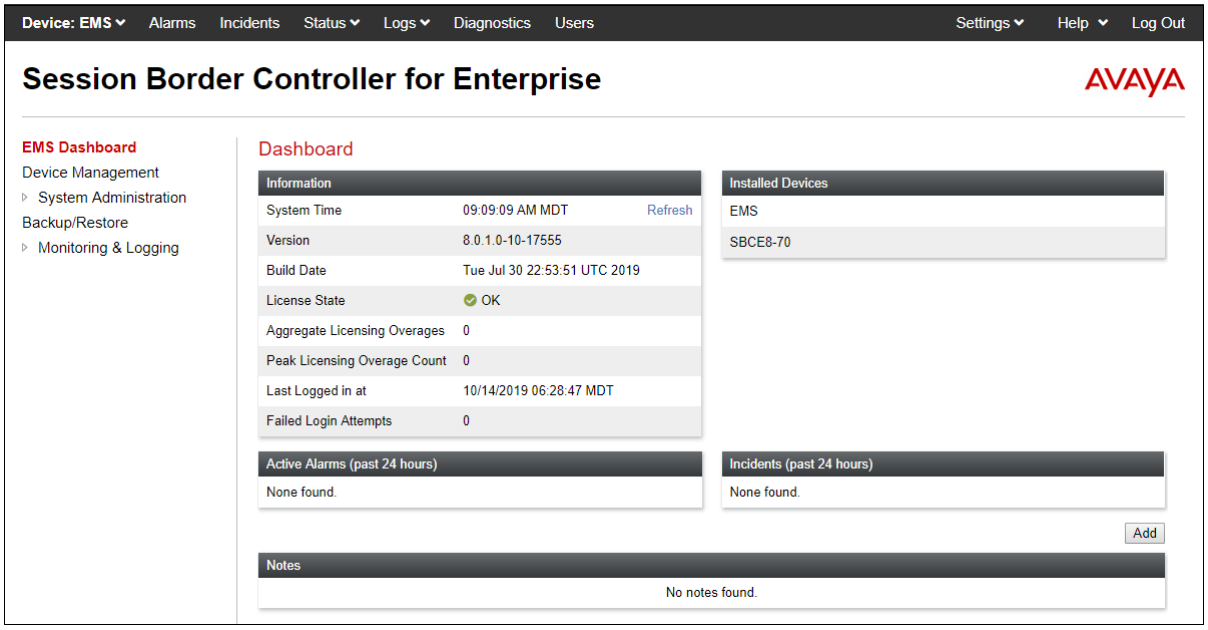
Enter the **Username** and click on **Continue**.



Enter the password and click on **Log In**.

©2020 Avaya Inc. All Rights Reserved.

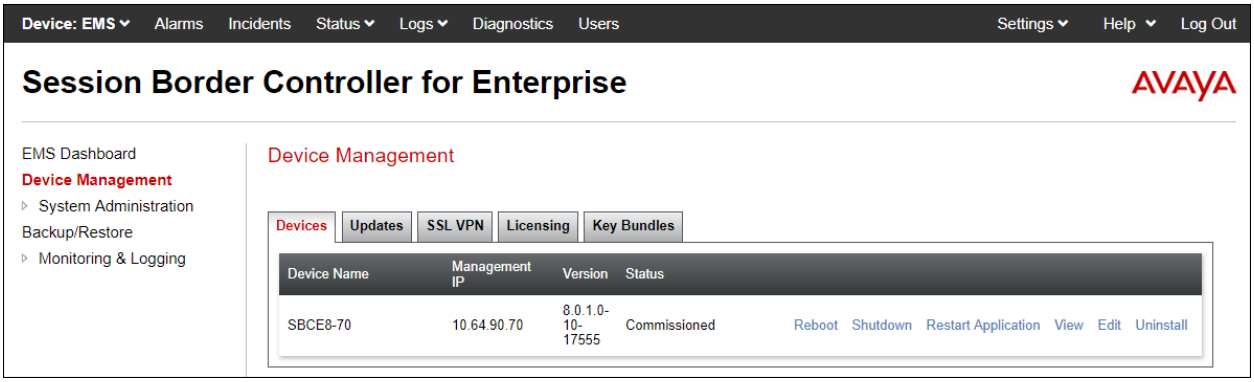
The EMS Dashboard page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.



7.1. Device Management – Status

Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **SBCE8-70** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya representative. To view the configuration of this device, click **View** on the screen below.

Note – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.



©2020 Avaya Inc. All Rights Reserved.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. In the shared test environment, the highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to AT&T.

System Information: SBCE8-70

General Configuration

Appliance Name	SBCE8-70
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	10	100
Advanced Sessions	10	100
Scopia Video Sessions	10	100
CES Sessions	10	100
Transcoding Sessions	10	100
CLID	---	
Encryption Available: Yes	☑	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.91.40	10.64.91.40	255.255.255.0	10.64.91.1	A1
10.64.91.41	10.64.91.41	255.255.255.0	10.64.91.1	A1
[redacted]	[redacted]	[redacted]	[redacted]	B1
3ffe:ffff:bb:bb::241	3ffe:ffff:bb:bb::241	64	3ffe:ffff:bb:bb::1	B1
[redacted]	[redacted]	[redacted]	[redacted]	B1
[redacted]	[redacted]	[redacted]	[redacted]	B2

DNS Configuration

Primary DNS	10.64.19.201
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.64.91.40

Management IP(s)

IP #1 (IPv4)	10.64.90.70

©2020 Avaya Inc. All Rights Reserved.

Página 3191 de 3226.

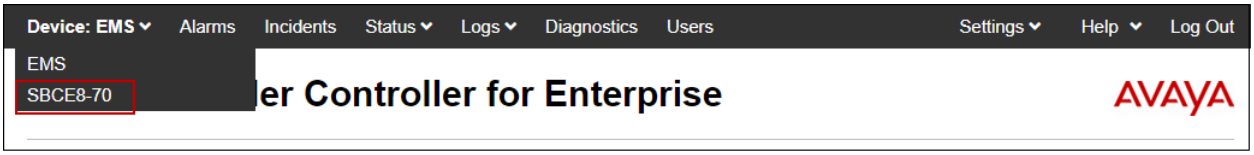
7.2. TLS Management

Note – Testing was done using identity certificates signed by a local certificate authority. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between IP Office and Avaya SBCE. The following procedures show how to view the certificates and configure the profiles to support the TLS connection.

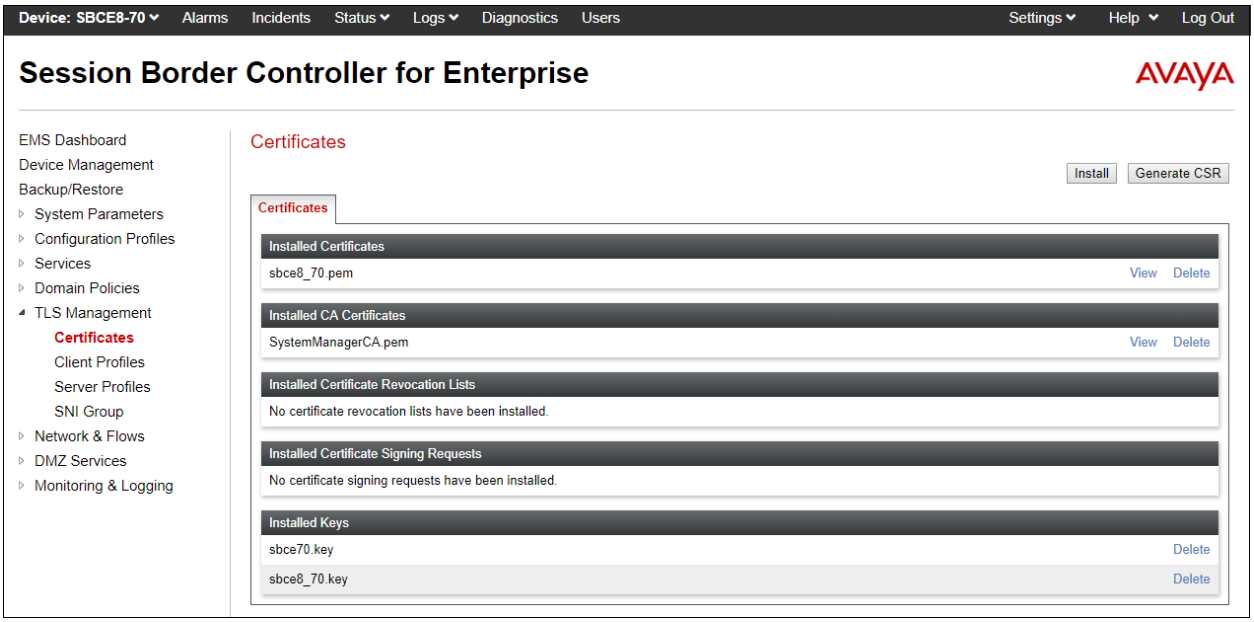
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.



Select **TLS Management → Certificates** from the left-hand menu. Verify the following:

- The root CA certificate is present in the **Installed CA Certificates** area.
- The signed identity certificate is present in the **Installed Certificates** area.
- The private key associated with the identity certificate is present in the **Installed Keys** area.



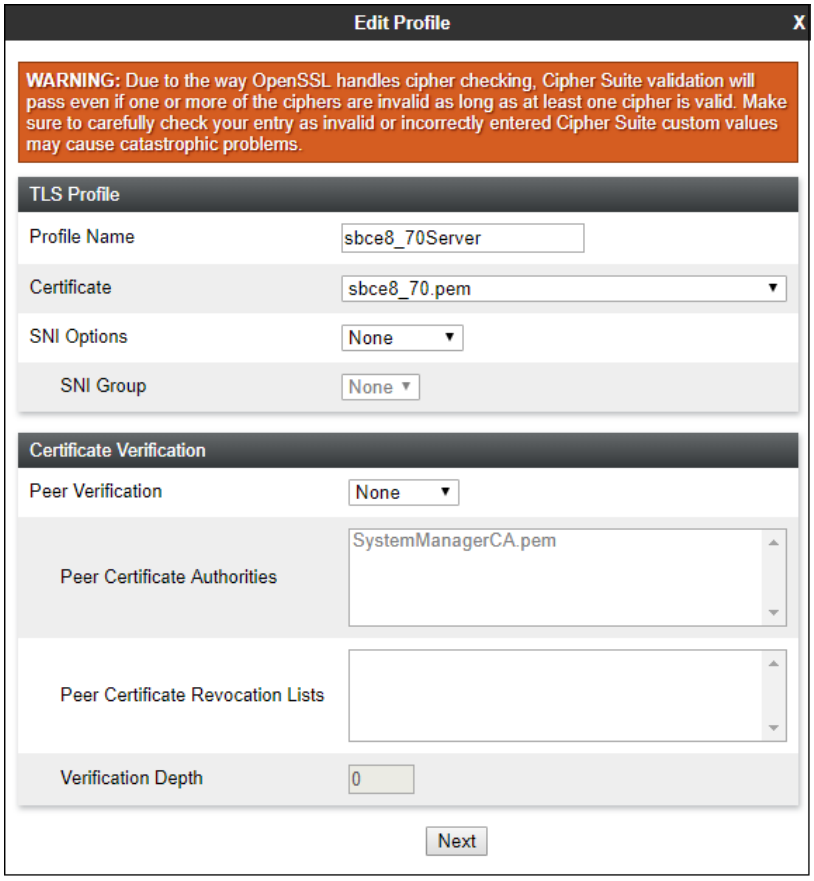
©2020 Avaya Inc. All Rights Reserved.

7.2.2. Server Profiles

Step 1 - Select **TLS Management → Server Profiles** and click on **Add**. Enter the following:

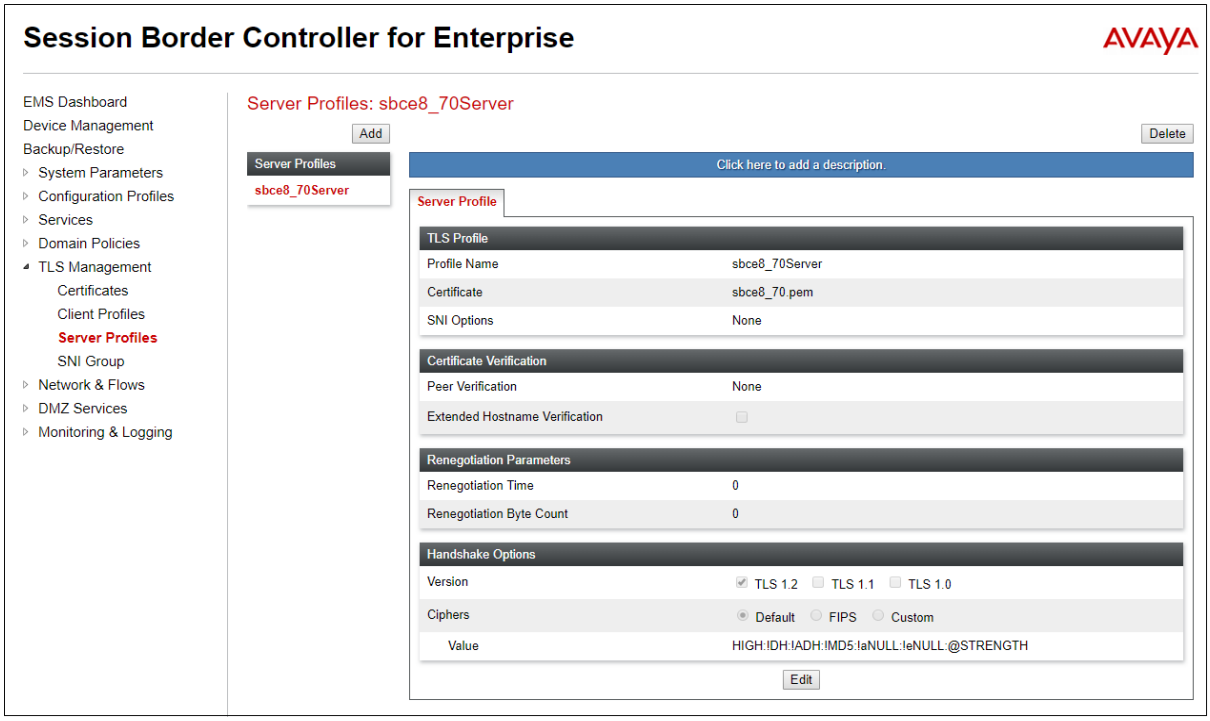
- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce8_70.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

The following screen shows the completed TLS **Server Profile** form:



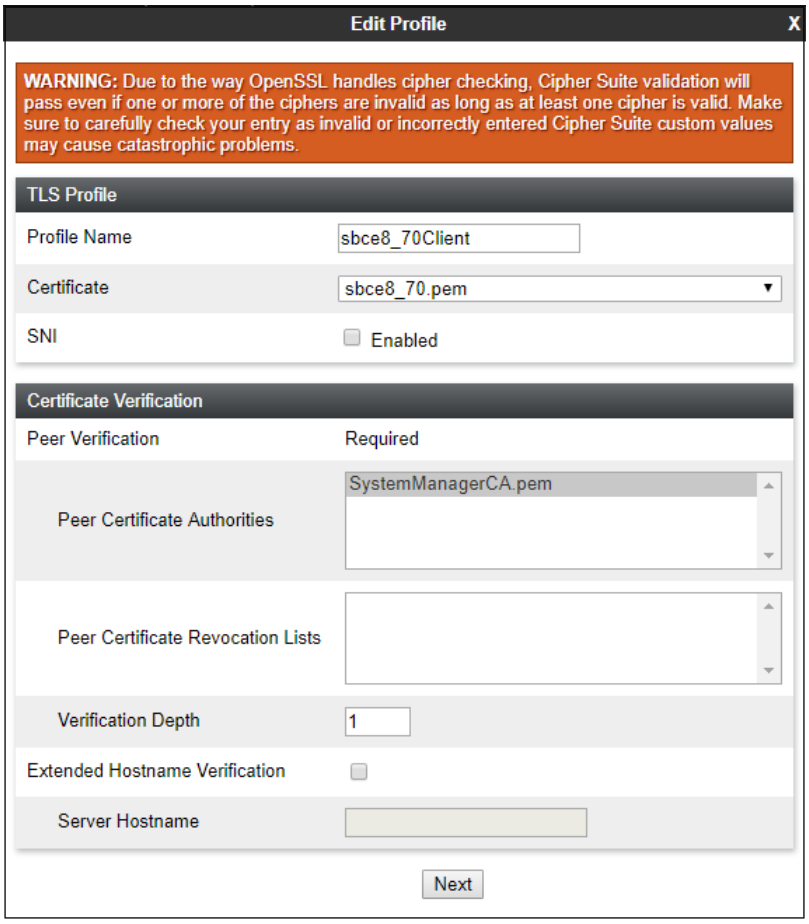
©2020 Avaya Inc. All Rights Reserved.

7.2.3. Client Profiles

Step 1 - Select **TLS Management → Client Profiles** and click on **Add**. Enter the following:

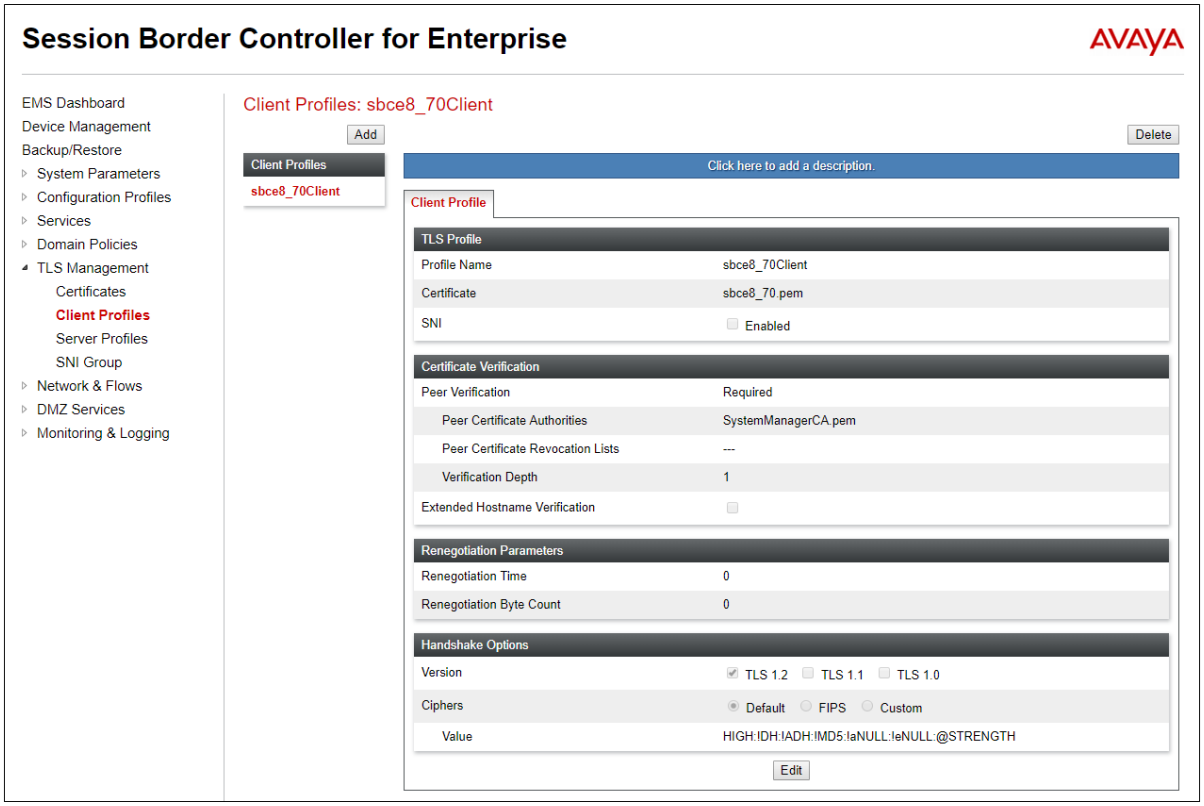
- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce8_70.pem**, from pull down menu.
- **Peer Verification** = **Required**.
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManagerCA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

The following screen shows the completed TLS **Client Profile** form:



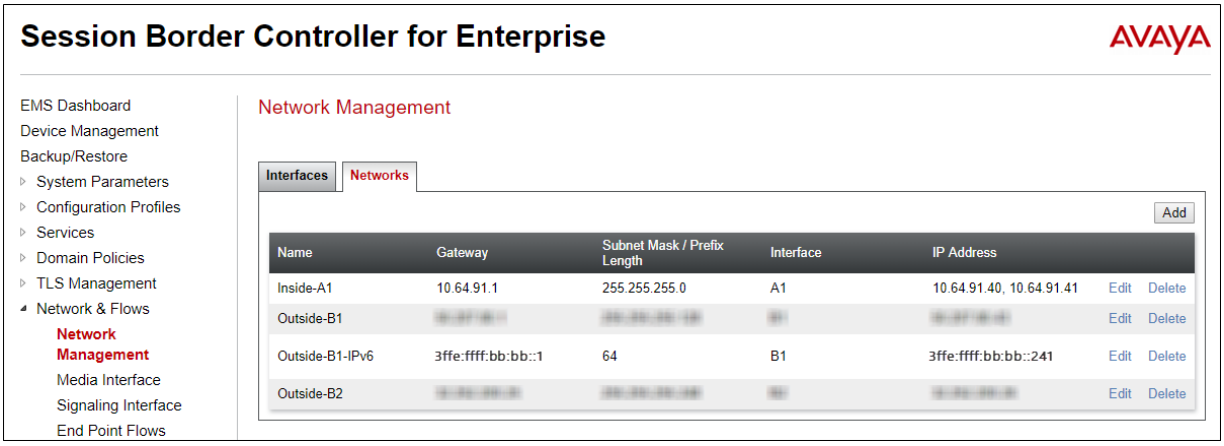
©2020 Avaya Inc. All Rights Reserved.

7.3. Network Management

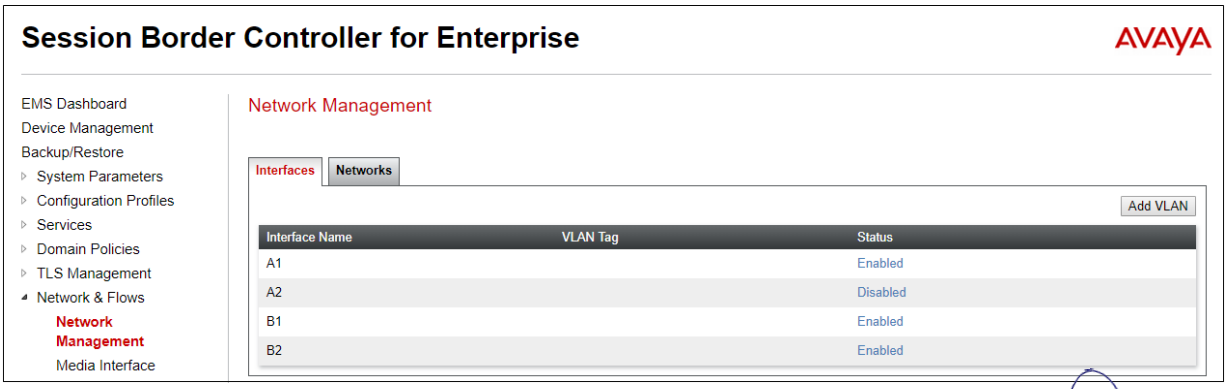
The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Networks & Flows → Network Management**. On the **Networks** tab, verify the IP addresses assigned to the interfaces. The following screen shows the enterprise interface is assigned to **A1** and the interface towards AT&T is assigned to **B1**.

The following Avaya SBCE IP addresses and associated interfaces were used in the sample configuration:

- **A1**: **10.64.91.41** – IPv4 address configured for AT&T IPTF to IP Office.
- **B1: 3ffe:ffff:bb:bb::241** – IPv6 address configured for the AT&T IPTF service. This address is known to AT&T. See **Section 3**.



Verify that the interfaces are enabled on the **Interfaces** tab. The following screen shows interfaces **A1** and **B1** with status **Enabled**. To enable an interface, click the corresponding **Disabled** link under the Status column to change it to **Enabled**.



©2020 Avaya Inc. All Rights Reserved.

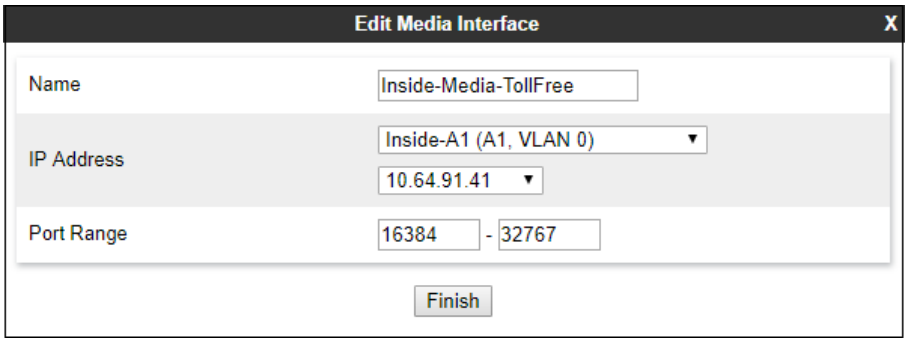
7.4. Media Interfaces

Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server.

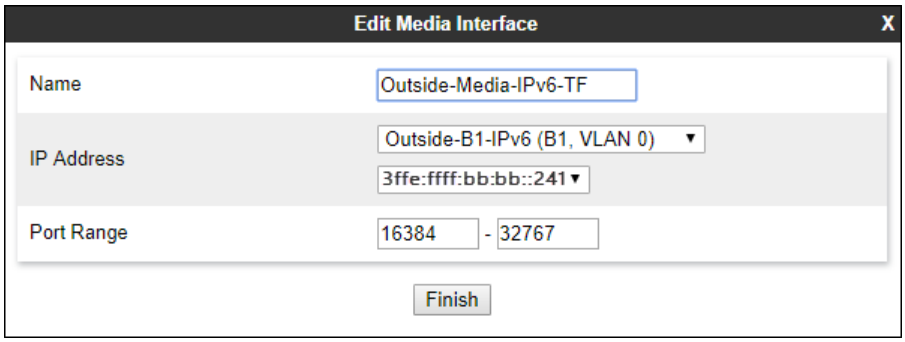
To create a new Media Interface in the enterprise direction, navigate to **Network & Flows** → **Media Interface** on the left-hand side menu, and click **Add** (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the Avaya SBCE private IP Address from the **IP Address** drop-down menu. Note that the **Port Range** was configured with the values required by AT&T (**16384** – **32767**). Click **Finish**.

Some ports in the range required by AT&T were already allocated by the Avaya SBCE for internal use, by default. See **Section 7.14** for the steps required to reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T could be accommodated.

The screen below shows the **Inside-Media-TollFree** media interface created in the reference configuration.



A second Media Interface towards the AT&T network was created with the name **Outside-Media-IPv6-TF**, as shown below. The outside IPv6 Address of the Avaya SBCE on the B1 interface was selected from the drop-down menu. The **Port Range** was configured with the values required by AT&T (**16384** – **32767**).

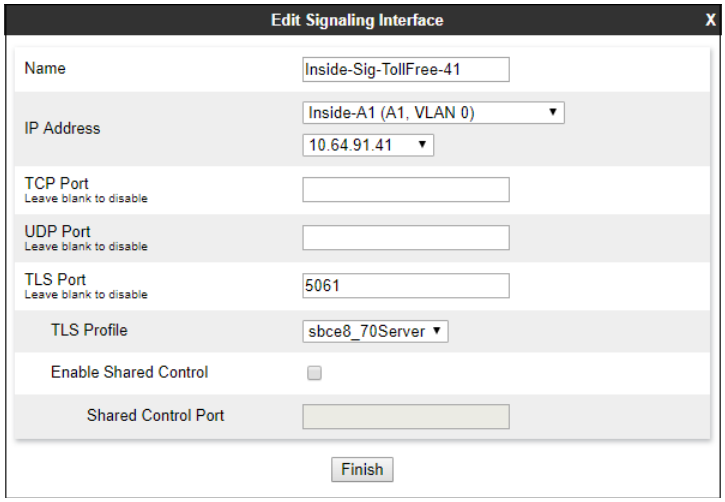


©2020 Avaya Inc. All Rights Reserved.

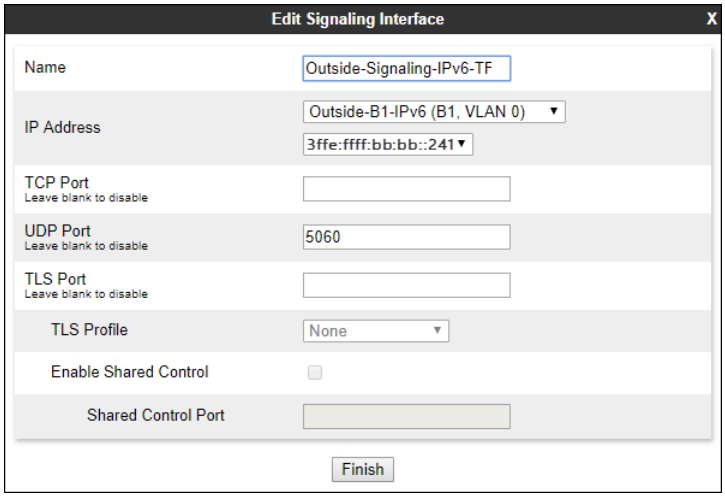
7.5. Signaling Interfaces

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a signaling interface for the inside and outside IP interfaces.

To create a new Signaling Interface on the enterprise direction, navigate to **Network & Flows** → **Signaling Interface** and click **Add**. On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. Since TLS is used in the sample configuration to listen for signaling traffic from the IP Office, **5061** is entered under **TLS Port**. The TLS Profile is set to the TLS server profile **sbce8_70Server** shown on **Section 7.2.2**. Click **Finish**.



A second Signaling Interface with the name **Outside-Signaling-IPv6-TF** was similarly created in the network direction. The outside IPv6 Address of the Avaya SBCE on the B1 interface was selected from the drop-down menu. Under **UDP Port,** enter **5060** as specified by AT&T. Click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

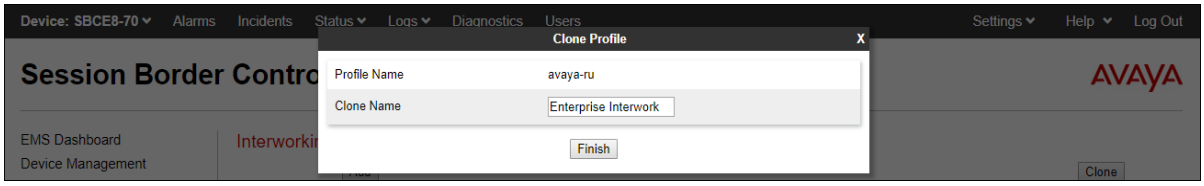
7.6. Server Interworking Profiles

The Server Internetworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

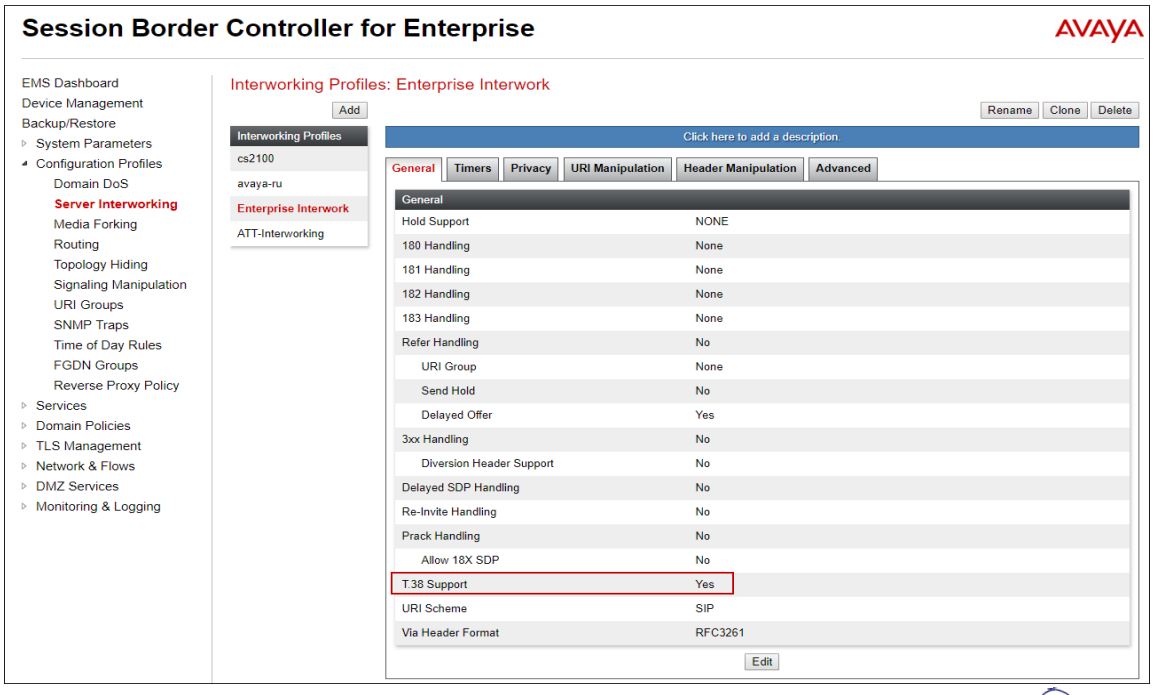
In the sample configuration, separate Server Interworking Profiles were created for IP Office and AT&T IPTF service.

7.6.1. Server Interworking Profile – IP Office

In the sample configuration, the IP Office Server Interworking profile was cloned from the default **avaya-ru** profile. To clone a Server Interworking Profile for IP Office, navigate to **Configuration Profiles → Server Interworking**, select the **avayu-ru** profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.



The following screen shows the **Enterprise Interwork** profile used in the sample configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish** (not shown).

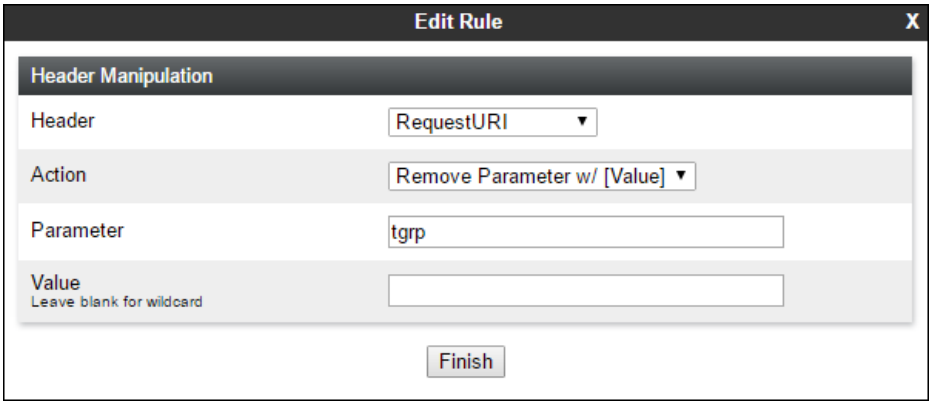


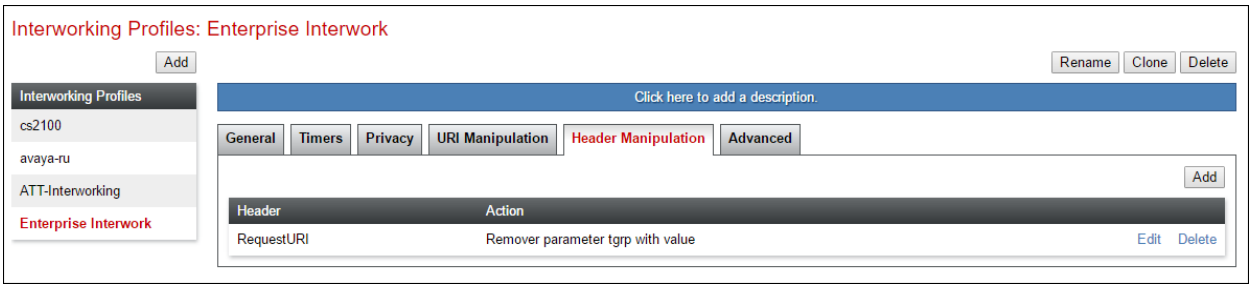
©2020 Avaya Inc. All Rights Reserved.

As described in **Section 2.2**, **item 3**, the BYE message received from AT&T contained a "tgrp" parameter that included IPv6 addresses on it. IP Office was unable to process this BYE message correctly. The following header manipulation rule of the Server Interworking profile will remove this parameter from the Request URI header in the BYE message arriving from AT&T.

Select the **Header Manipulation** tab. Click on **Add** and enter the following:

- **Header:** select **RequestURI** from the drop-down menu
- **Action:** select **Remove Parameter w/ [Value]** from the drop-down menu
- **Parameter** = **tgrp**
- **Value:** leave blank
- Click **Finish**

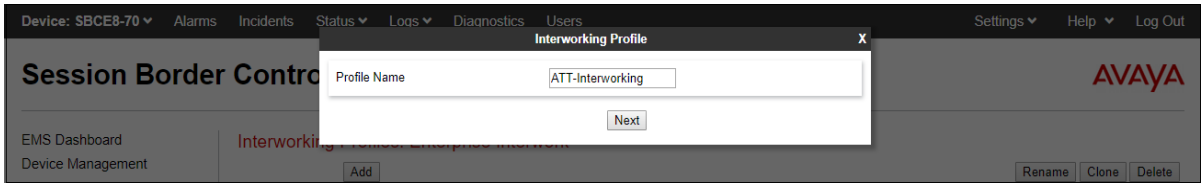




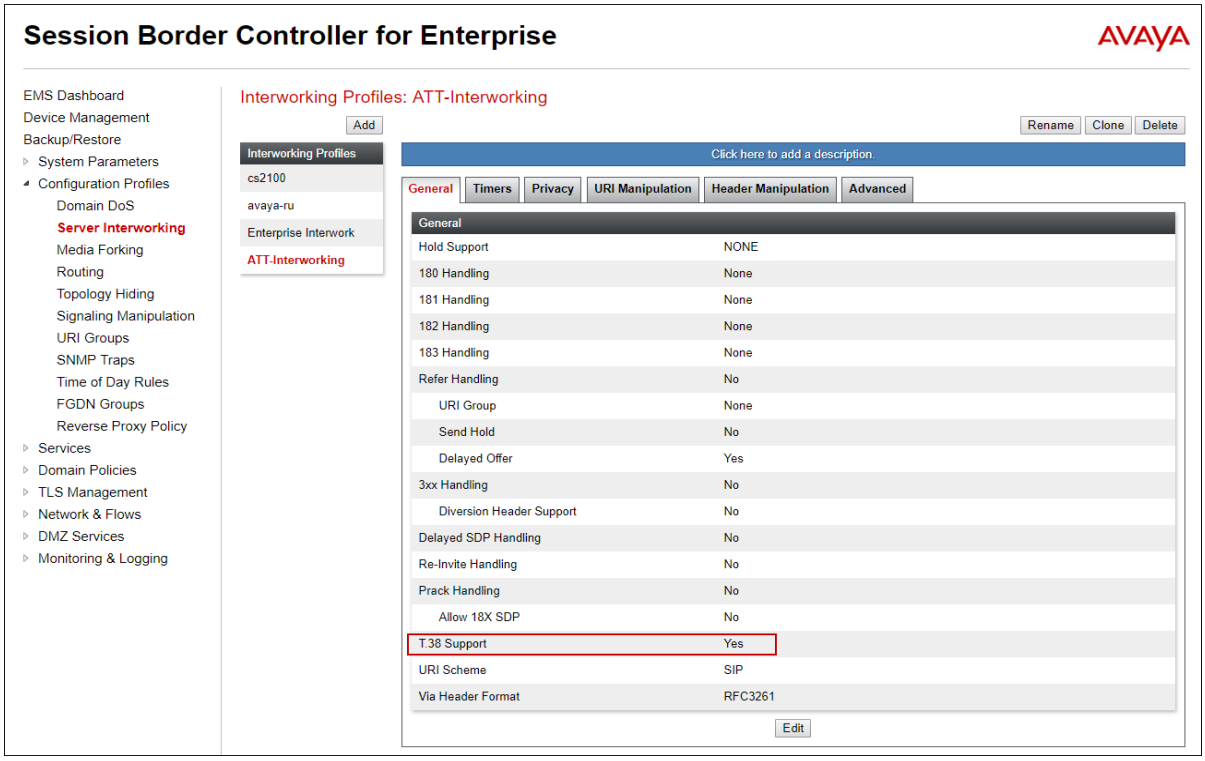
©2020 Avaya Inc. All Rights Reserved.

7.6.2. Server Interworking Profile – AT&T

To create a new Server Interworking Profile for AT&T, navigate to **Configuration Profiles → Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**.

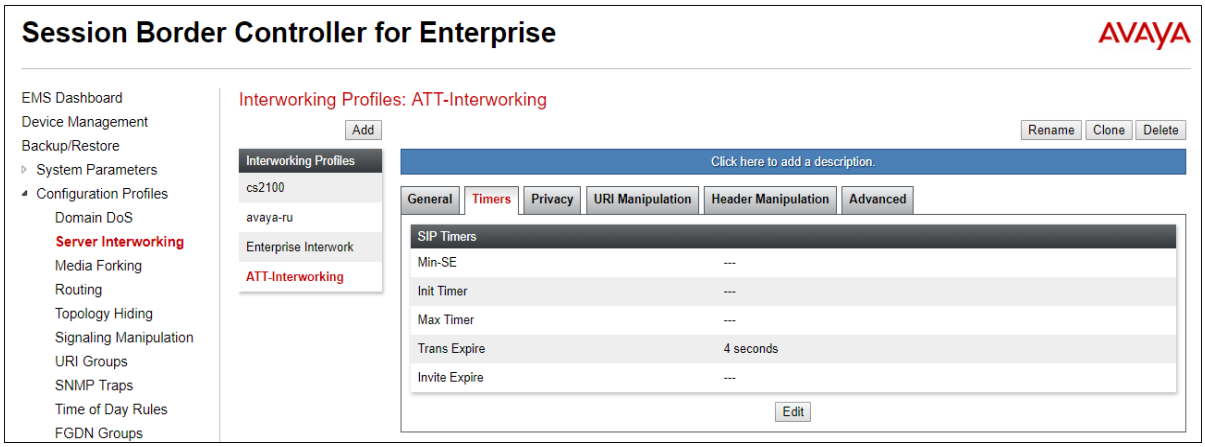


The following screens show the **ATT-Interworking** profile used in the sample configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to **Yes**.

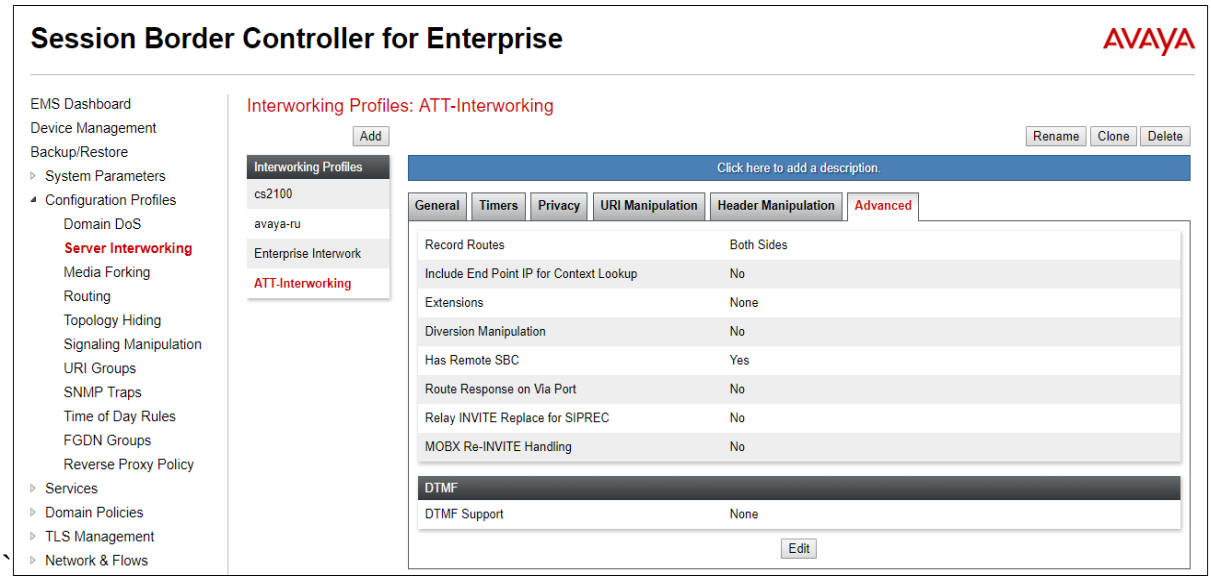


©2020 Avaya Inc. All Rights Reserved.

The **Timers** tab shows the values used for compliance testing for the **Trans Expire** field. The **Trans Expire** timer sets the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if one exists.



Click **Next** to accept default parameters for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown) and advance to the **Advanced** area. **Record Routes** is set to **Both Sides**. Default values can be used for all other fields.



©2020 Avaya Inc. All Rights Reserved.

Página 3203 de 3226.

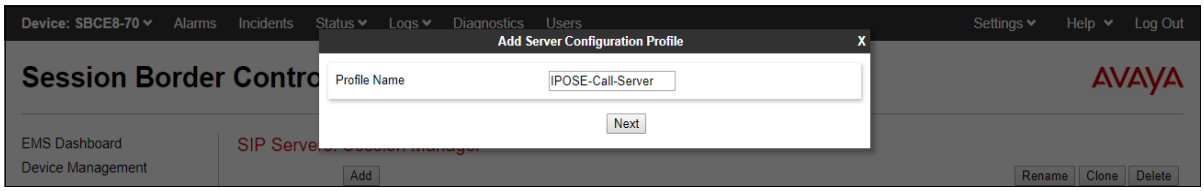
7.7. SIP Servers Profiles

The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

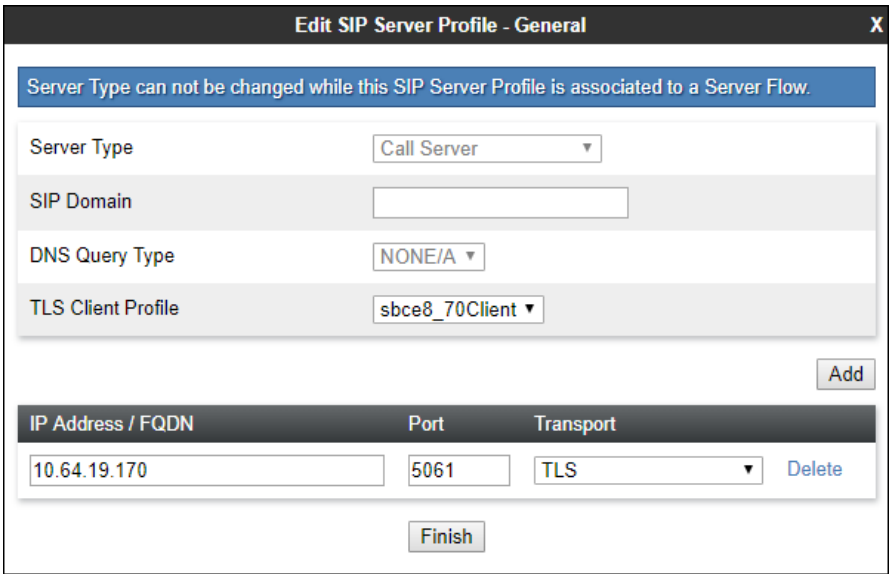
In the sample configuration, separate Server Configurations profiles were created for the IP Office and the AT&T IPTF service.

7.7.1. SIP Server Profile – IP Office

To add a SIP Server Profile for IP Office, navigate to **Services → SIP Servers** and click **Add**. Enter a descriptive name for the new profile and click **Next**.

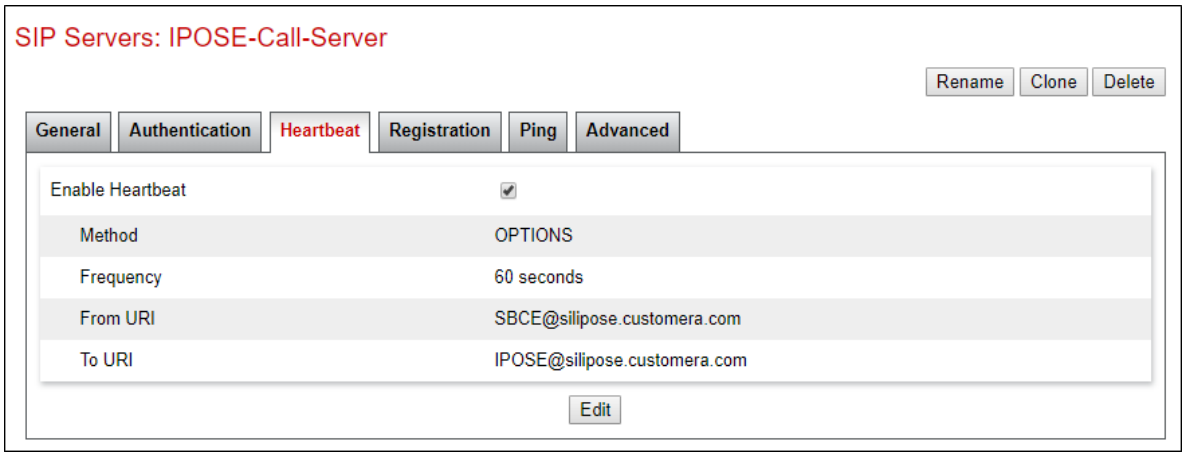


The following screens illustrate the SIP Server Profile named **IPOSE-Call-Server**. In the **General** parameters, the **Server Type** is set to **Call Server**. In the **IP Address / FQDN** field, the IP Address of IP Office LAN 1 interface in the sample configuration is entered. This IP address is **10.64.19.170**. Under **Port**, **5061** is entered, and the **Transport** parameter is set to **TLS**. The TLS profile **sbce8_70Client** created in **Section 7.2.3** is selected for **TLS Client Profile**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

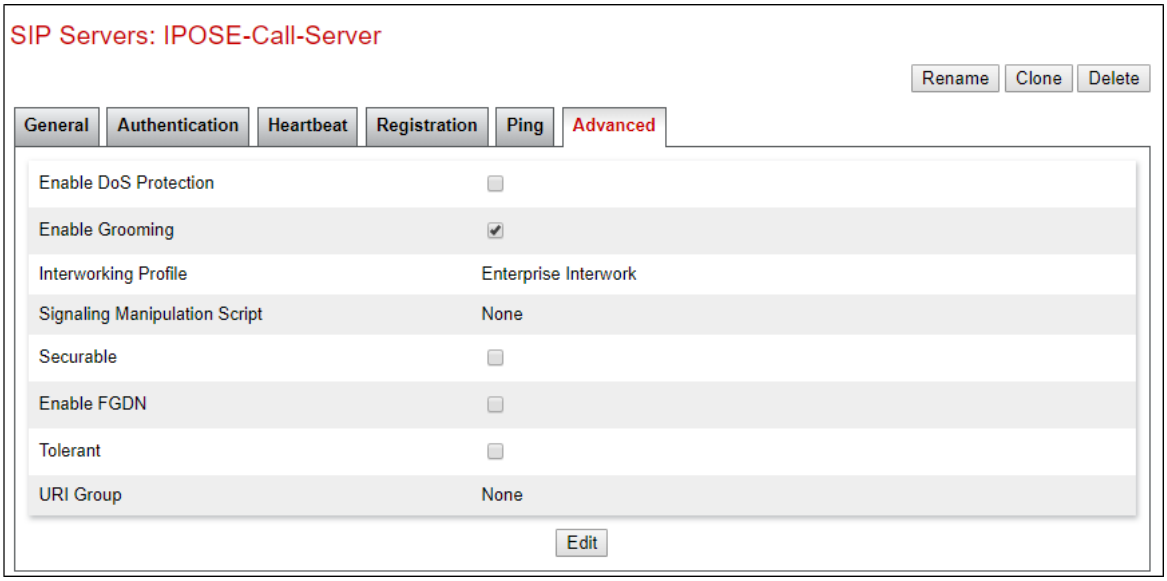


©2020 Avaya Inc. All Rights Reserved.

Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeat** tab. The Avaya SBCE can be optionally configured to source "heartbeats" in the form of PINGs or SIP OPTIONS towards IP Office. Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS towards IP Office.



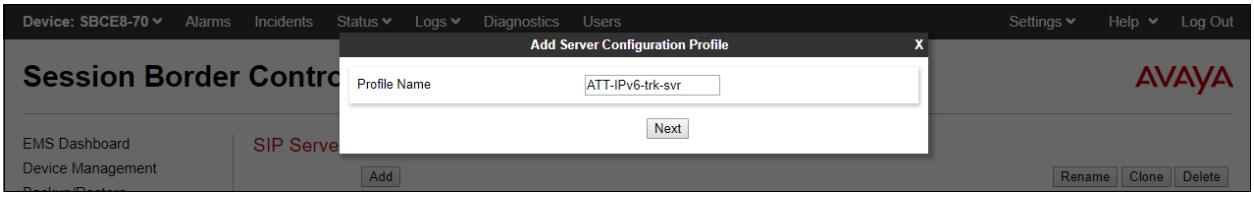
On the **Advanced** tab, **Enable Grooming** is check and the **Interworking Profile** is set to **Enterprise Interwork** created in **Section 7.6.1** for IP Office.



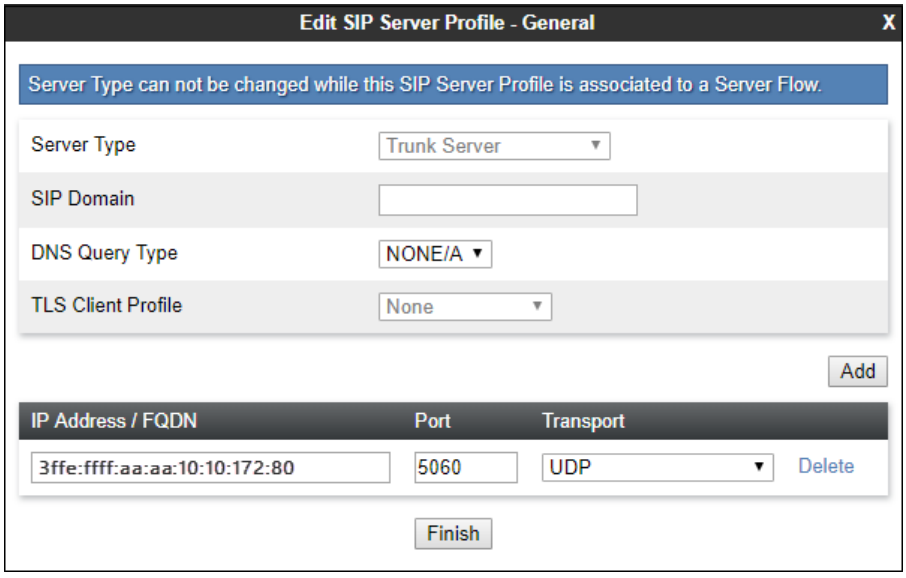
©2020 Avaya Inc. All Rights Reserved.

7.7.2. SIP Server Profile – AT&T

To add a SIP Server Profile for AT&T, navigate to **Services → SIP Servers** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



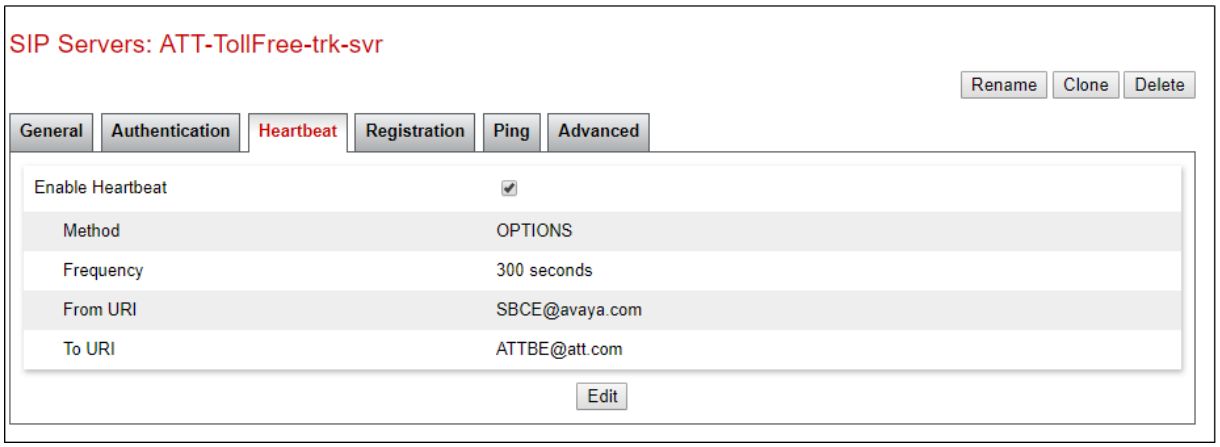
The following screens illustrate the SIP Server Profile **ATT-IPv6-trk-svr**. In the **General** parameters, the **Server Type** is set to **Trunk Server**. In the **IP Address / FQDN** fields, the AT&T-provided border element IP address is entered. This is **3ffe:ffff:aa:aa:10:10:172:80**. Under **Port**, **5060** is entered, and the **Transport** parameter is set to **UDP**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



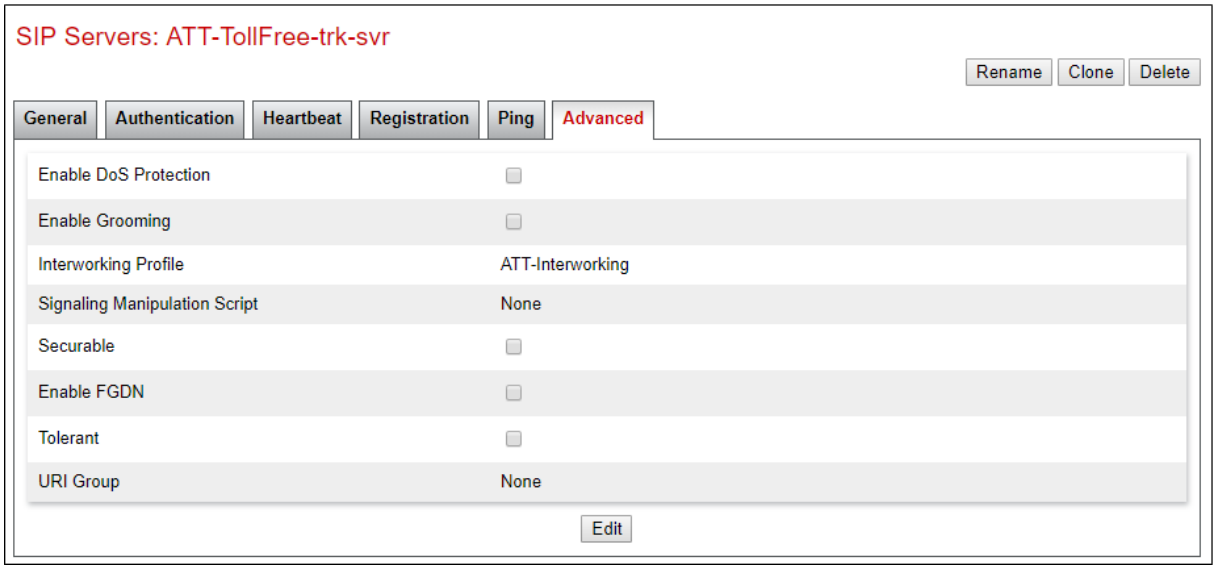
Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source "heartbeats" in the form of SIP OPTIONS towards AT&T. This configuration is optional. Independent of whether the Avaya SBCE is configured to source SIP OPTIONS towards AT&T, AT&T will receive OPTIONS from the IP Office site as a result of the **Check OOS** parameter being enabled on IP Office (see **Section 5.5.2**). When IP Office sends SIP OPTIONS to the inside private IP Address of the Avaya SBCE, the Avaya SBCE will send SIP OPTIONS to AT&T. When AT&T responds, the Avaya SBCE will pass the response to IP Office.

©2020 Avaya Inc. All Rights Reserved.

Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If adding a new profile, click **Next** to continuing to the **Advanced** settings.



On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and is left unchecked. The **Interworking Profile** is set to **ATT-Interworking** created in **Section 7.6.2** for AT&T.



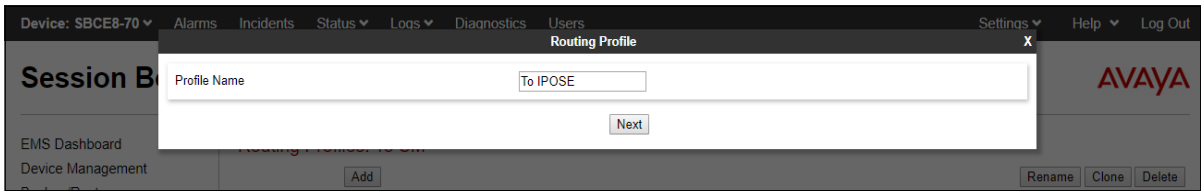
©2020 Avaya Inc. All Rights Reserved.

7.8. Routing Profiles

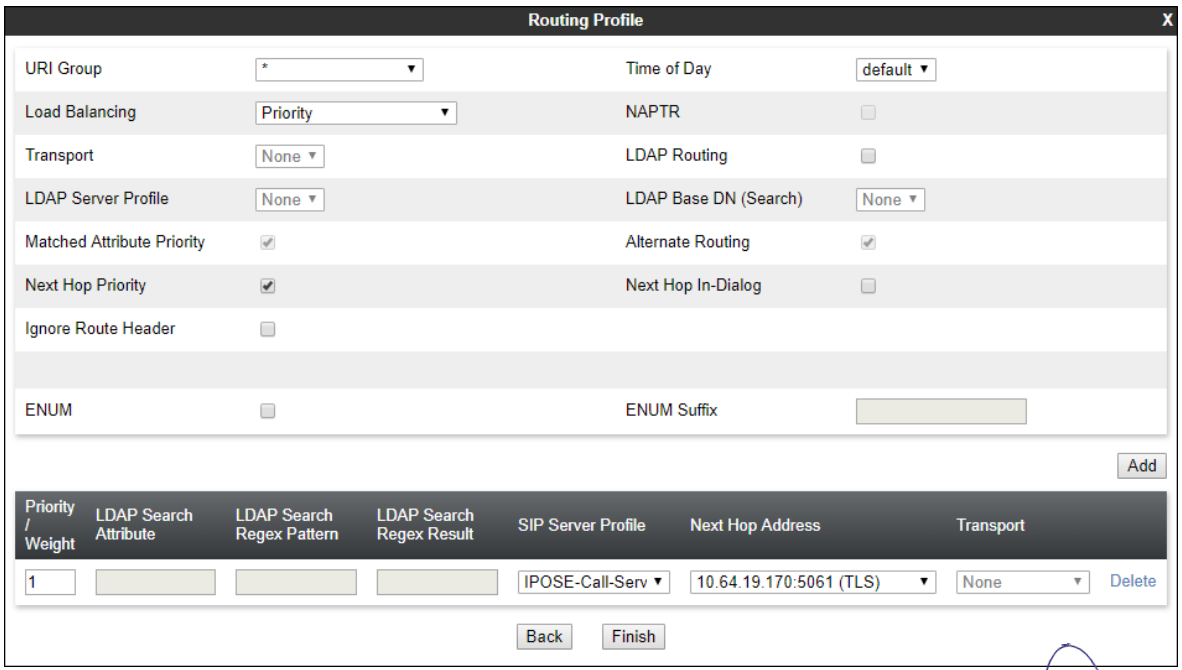
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types. Separate Routing Profiles were created in the reference configuration for IP Office and AT&T IPTF service.

7.8.1. Routing Profile – IP Office

To add the Routing Profile for the IP Office, navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.



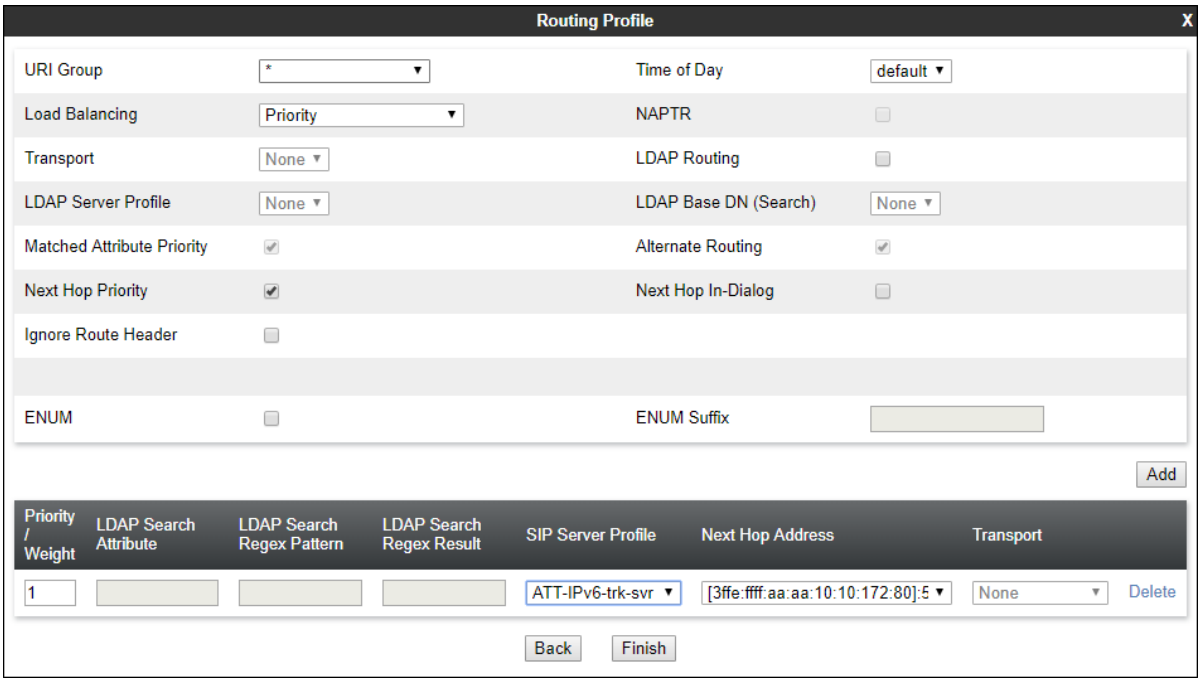
The following screen shows the Routing Profile **To IPOSE** created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. Clicking the **Add** button on this screen allows to enter the routing rule at the bottom of the profile. The **Priority / Weight** parameter is set to **1**, and the IP Office **SIP Server Profile**, created in **Section 7.7.1**, is selected from the drop-down menu. The **Next Hop Address** (IP address, port and transport) is automatically selected with the values from the IP Office SIP Server Profile, and **Transport** becomes grayed out. Click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

7.8.2. Routing Profile – AT&T

Similarly, add a Routing Profile to AT&T. The following screen shows the Routing Profile **To ATT IPv6** created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the AT&T **SIP Server Profile**, created in **Section 7.7.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the AT&T SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

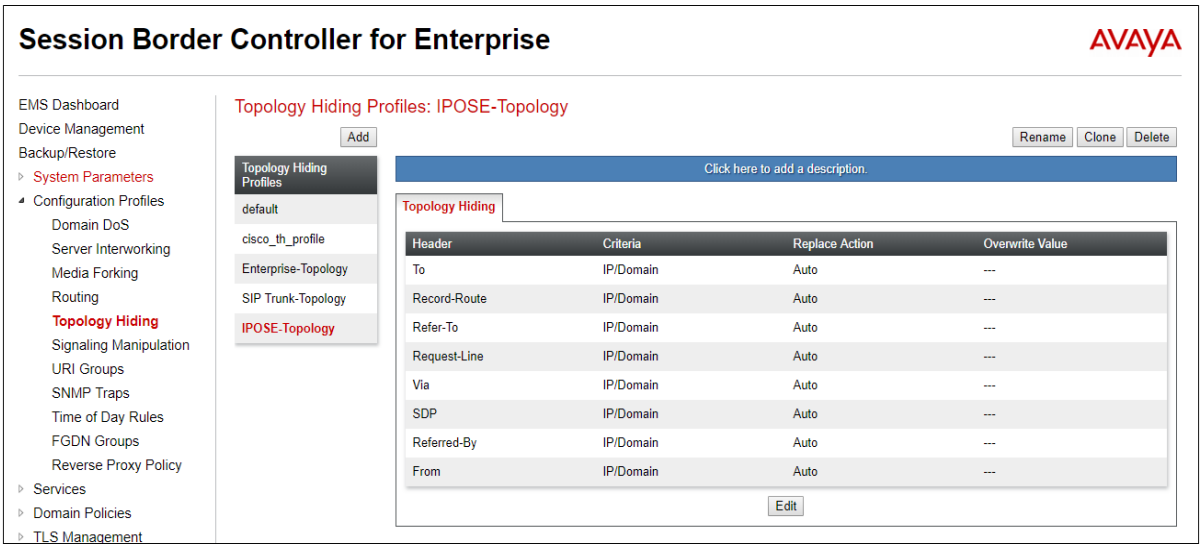
7.9. Topology Hiding Profile

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

To create the Topology Hiding profiles for IP Office and AT&T, navigate to **Configuration Profiles → Topology** Hiding. Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the sample configuration, the **default** profile was cloned for both IP Office and AT&T. They will later be applied to the Server Flows in **Section 7.15**.

In the **Replace Action** column an action of **Auto** will replace the header field with the IP address of the Avaya SBCE interface and the **Overwrite** will use the value in the **Overwrite Value**.

In the example shown, **IPOSE-Topology** was cloned from the default. A second profile, **SIP-Trunk-Topology** (not shown) was similarly cloned from the default.

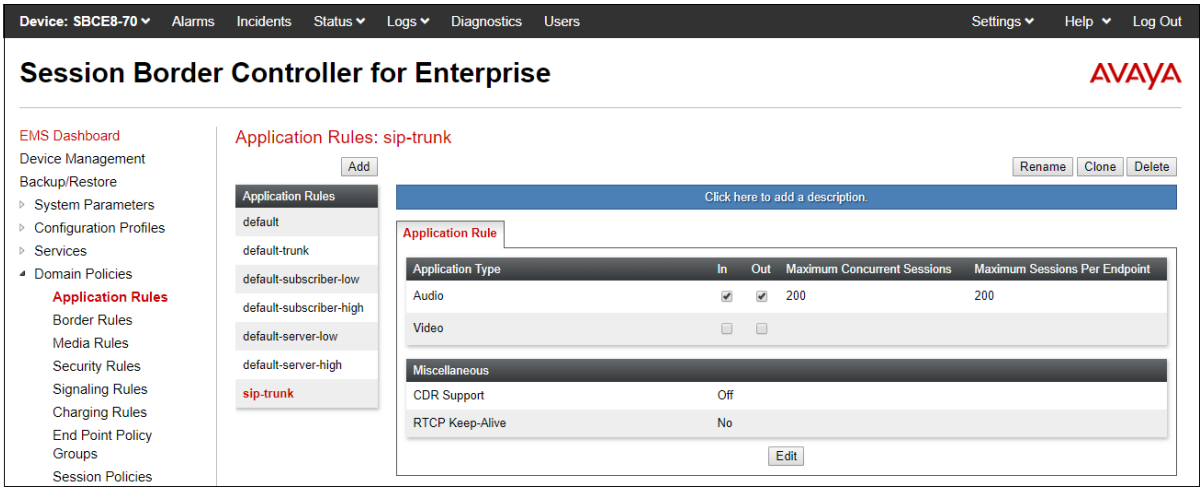


©2020 Avaya Inc. All Rights Reserved.

7.10. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Select **Domain Policies → Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing application rule to edit. In the sample configuration, the **sip-trunk** rule was created for IP Office and AT&T. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** and **Video** applications to a value slightly larger than the licensed sessions. For example, if licensed for 150 session set the values to **200**. The **Maximum Session Per Endpoint** should match the **Maximum Concurrent Sessions**.



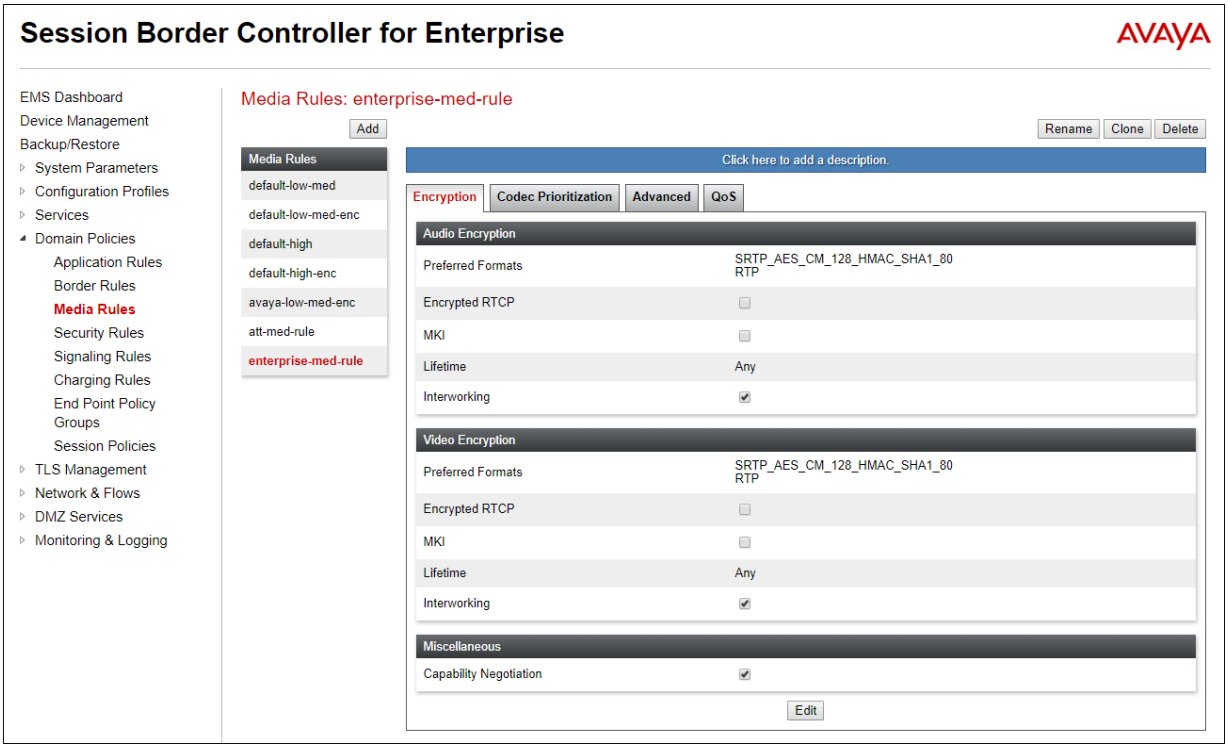
7.11. Media Rules

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

To create a Media Rule for the IP Office, select **Domain Policies → Media Rules** from the left-side menu. In the sample configuration, the default **avaya-low-med-enc** rule was cloned for IP Office, and then modified as shown on the screen below. With the **avaya-low-med-enc** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

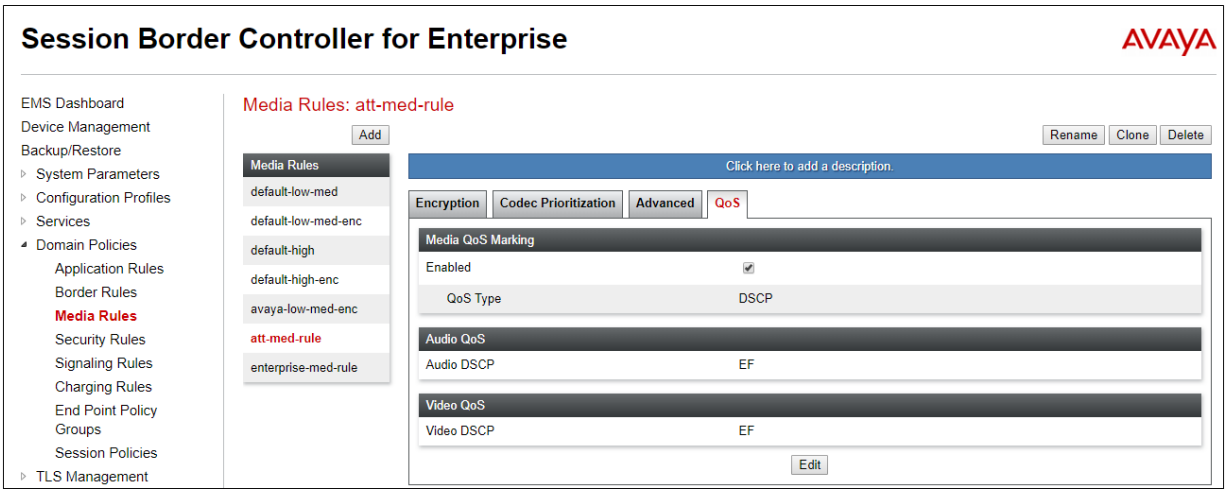
©2020 Avaya Inc. All Rights Reserved.

The Media Rule **enterprise-med-rule** created for the IP Office is shown below.



Similarly, the default **default-low-med** rule was cloned to create the Media Rule for AT&T.

The Media Rule named **att-med-rule** used in the sample configuration for AT&T IPTF is shown below, with the DSCP values **EF** for expedited forwarding (default value) for **Media QoS**. See **Section 2.2**, **item 4** for current limitations.

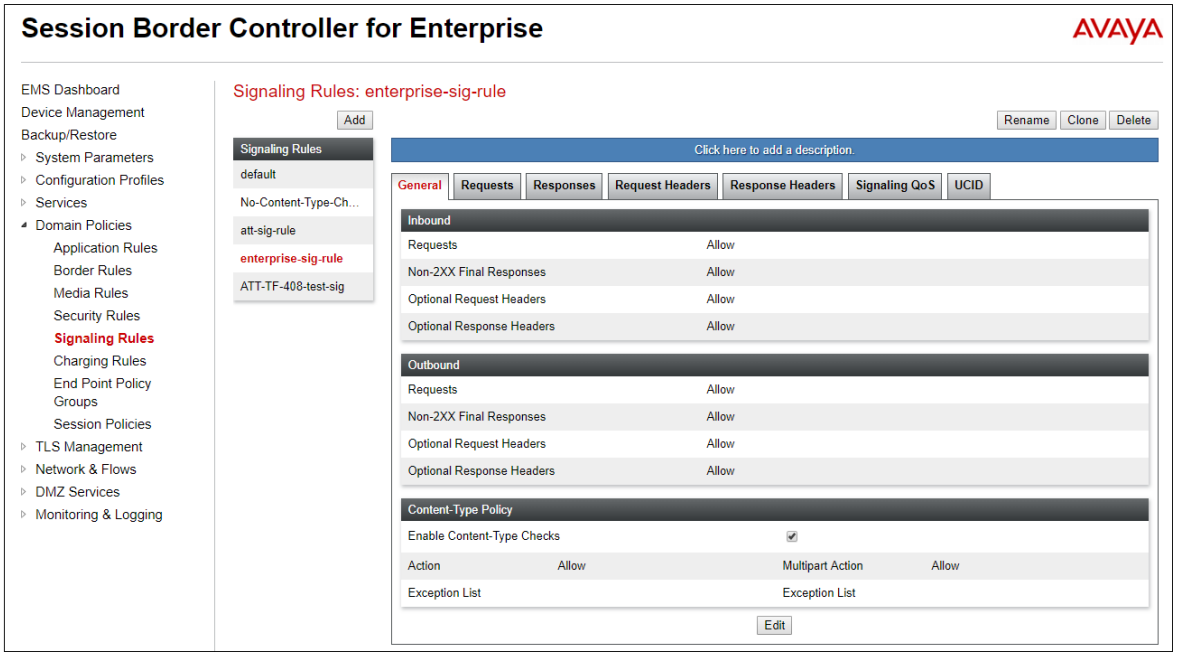


©2020 Avaya Inc. All Rights Reserved.

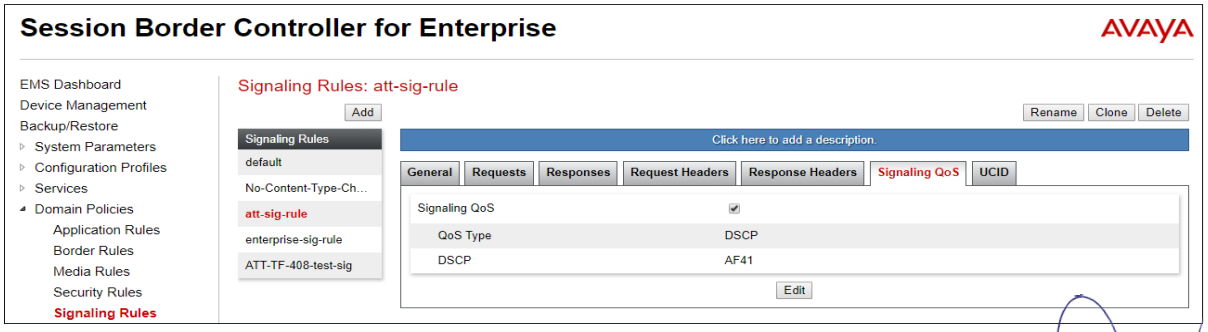
7.12. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Clone and modify the **default** signaling rule to add the proper quality of service to the SIP signaling. To clone a signaling rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown). In the sample configuration, signaling rule **enterprise sig rule** is unchanged from the default rule.



Signaling rule **att sig rule** was also cloned from the default rule and used for AT&T. The DSCP value **AF41** for assured forwarding (default value) was set for **Signaling QoS**. See **Section 2.2**, **item 4** for current limitations.

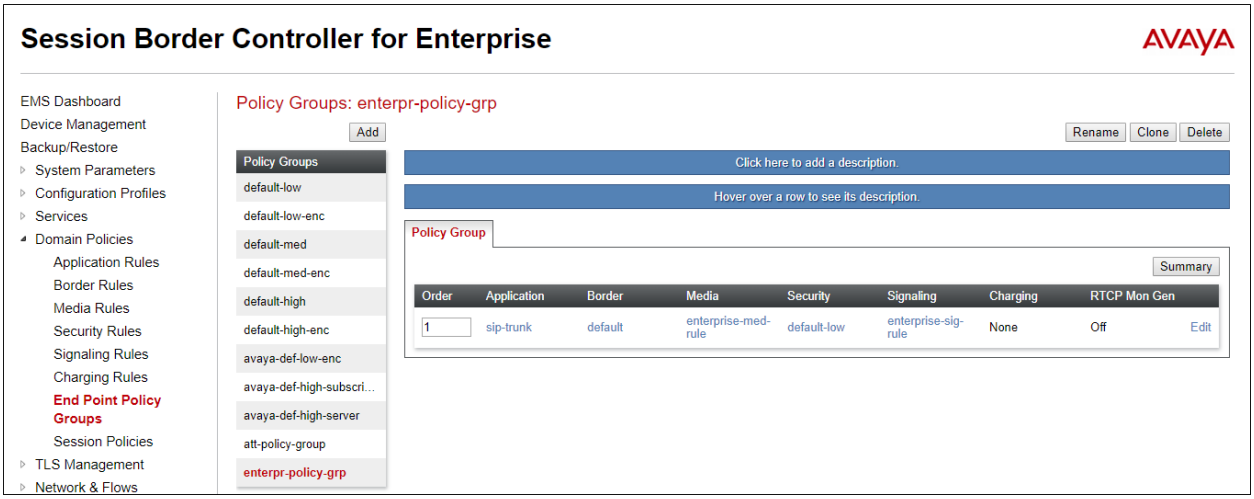


©2020 Avaya Inc. All Rights Reserved.

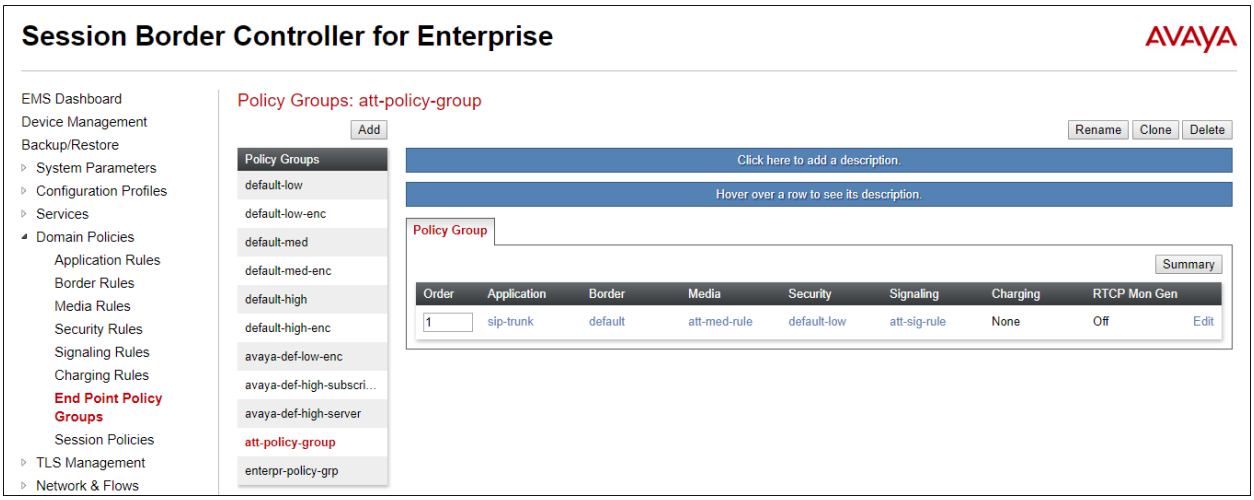
7.13. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.15**.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** as shown below. The following screen shows the **enterpr-policy-grp** created for IP Office. The details of the non-default rules chosen are shown in previous sections.



The following screen shows the **att-policy-group** created for AT&T. The details of the non-default rules chosen are shown in previous sections.

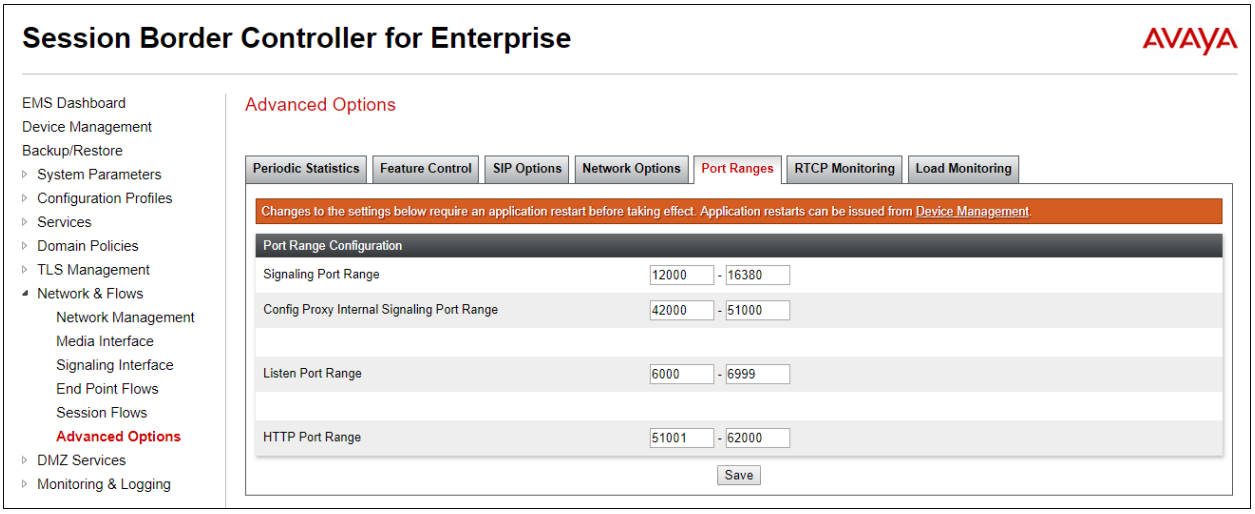


©2020 Avaya Inc. All Rights Reserved.

7.14. Advanced Options

In **Section 7.4**, the media UDP port ranges required by AT&T are configured (**16384** – **32767**). However, by default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T can be defined as shown in **Section 7.4**.

Step 1 - Select **Device Specific Settings → Advanced Options** from the menu on the left-hand side.
Step 2 - Select the **Port Ranges** tab.
Step 3 - In the **Signaling Port Range** row, change the range to **12000** – **16380**
Step 4 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000** – **51000**.
Step 5 – In the **Listen Port Range** row, change the range to **6000** – **6999**.
Step 6 – In the **HTTP Port Range** row, change the range to **51001** – **62000**.
Step 7 - Select **Save**. Note that changes to these values require an application restart (see **Section 7.1**).



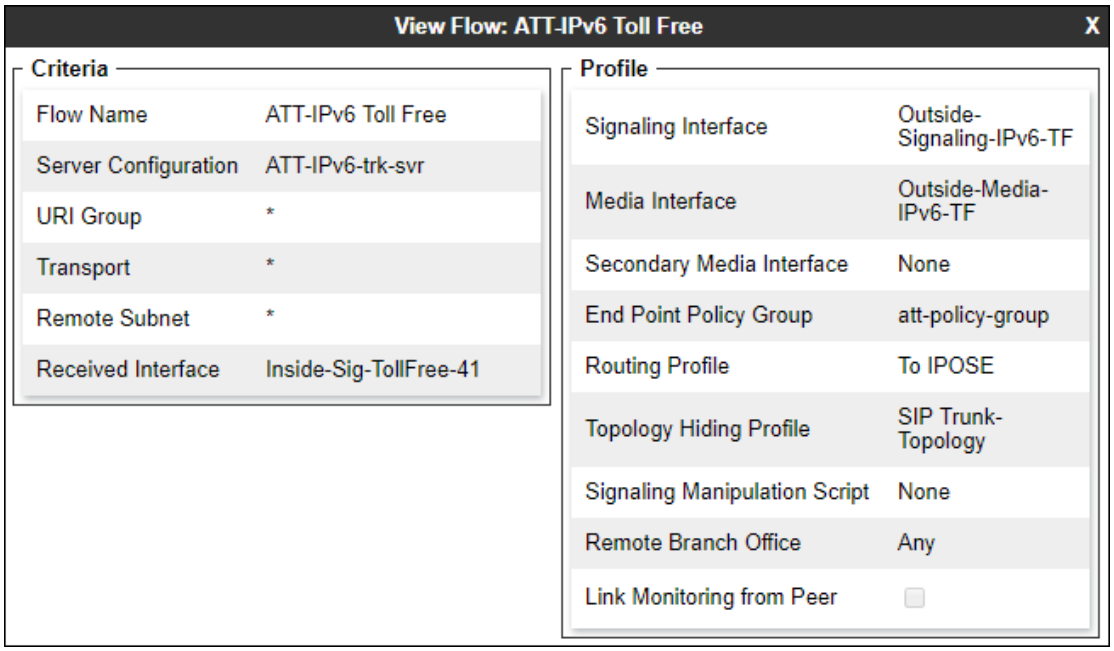
©2020 Avaya Inc. All Rights Reserved.

7.15. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow.

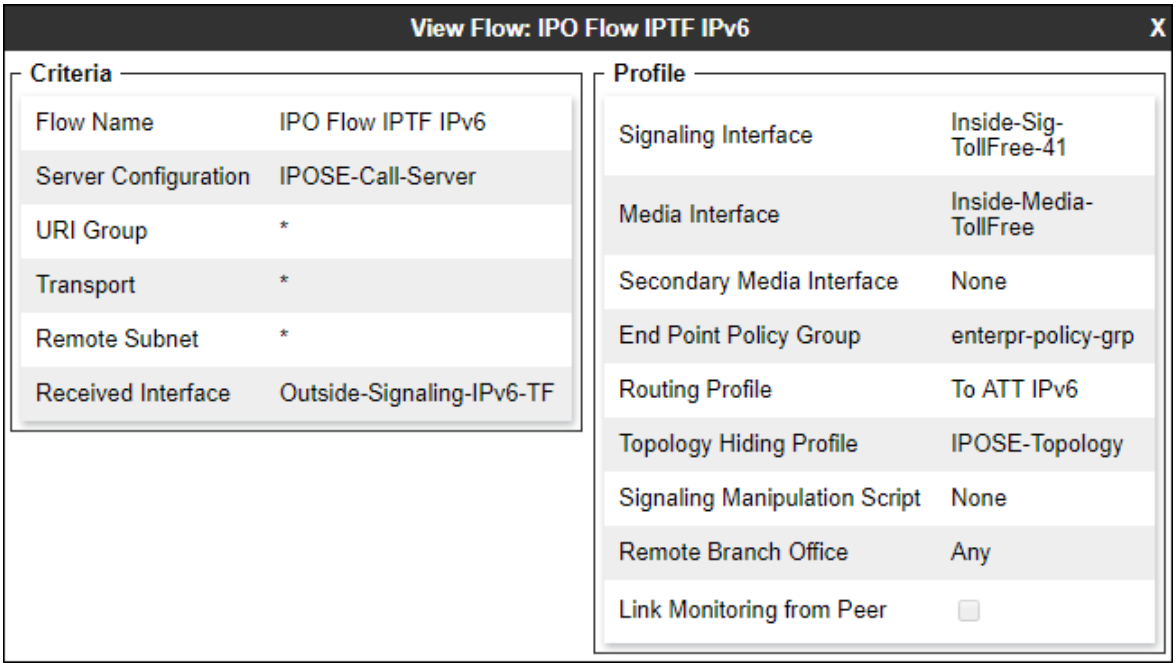
Create a Server Flow for IP Office and AT&T IPTF service. To create a Server Flow, navigate to **Networks & Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown).

The following screen shows the flow named **ATT IPTF** viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.



©2020 Avaya Inc. All Rights Reserved.

Once again, select the **Server Flows** tab and click **Add**. The following screen shows the flow named **IPO – TollFree** viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.



©2020 Avaya Inc. All Rights Reserved.

8. AT&T IP Toll Free Service Configuration

AT&T provides the IPTF service border element IP address, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition, the AT&T IPTF features, and their associated access numbers, are also assigned by AT&T. AT&T requires that the Avaya SBCE public (B1) IP address be provided to the IPTF service, as part of the provisioning process. For more information, consult reference **[11]**.

9. Verification Steps

The following procedures may be used to verify the Avaya IP Office Release 11.0 and Avaya SBCE Release 8.0.1 with the AT&T IPTF service configuration.

9.1. AT&T IP Toll Free Service

The following scenarios may be executed to verify functionality with the AT&T IPTF service:

- Place inbound calls, answer the calls, and verify that two-way talk path exists. Verify that the calls remain stable for several minutes and disconnects properly.
- Incoming calls using the G.729A and G.711 ULAW codecs.
- Verify basic call functions such as hold, transfer, and conference.
- Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to voicemail (e.g., Voicemail Pro). Retrieve the message either locally or from PSTN.
- Using the appropriate IPTF access numbers and codes, verify the “Legacy Transfer Connect” DTMF initiated features.
- Inbound fax using T.38 or G.711. See **Section 2.2** for limitations.
- SIP OPTIONS monitoring of the health of the SIP trunk.

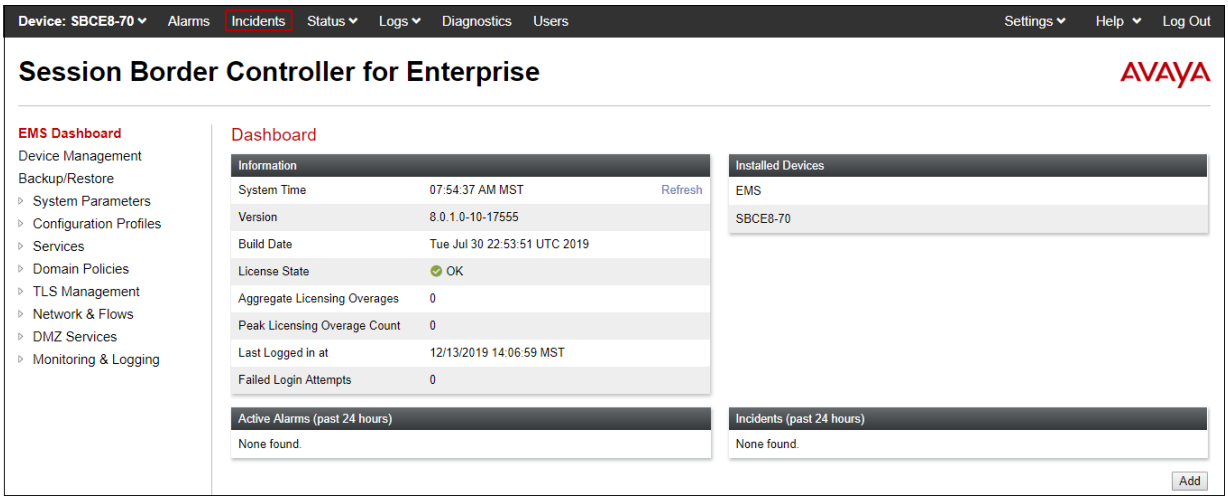
©2020 Avaya Inc. All Rights Reserved.

9.2. Avaya SBCE

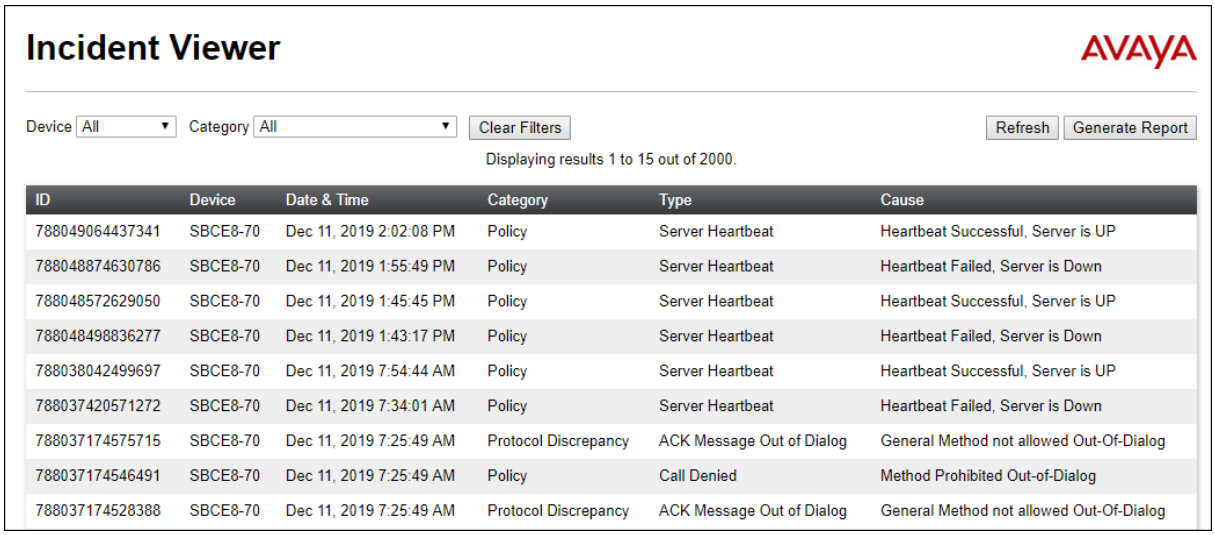
This section provides verification steps that may be performed with the Avaya SBCE.

9.2.1. Incidents

The Incident Viewer can be accessed from the Avaya SBCE top navigation menu as highlighted in the screenshot below.



Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.

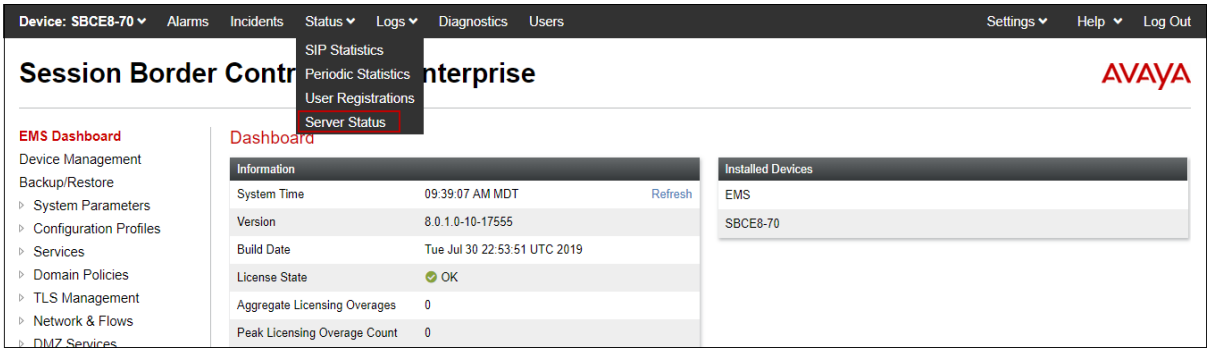


ID	Device	Date & Time	Category	Type	Cause
788049064437341	SBCE8-70	Dec 11, 2019 2:02:08 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
788048874630786	SBCE8-70	Dec 11, 2019 1:55:49 PM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
788048572629050	SBCE8-70	Dec 11, 2019 1:45:45 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
788048498836277	SBCE8-70	Dec 11, 2019 1:43:17 PM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
788038042499697	SBCE8-70	Dec 11, 2019 7:54:44 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
788037420571272	SBCE8-70	Dec 11, 2019 7:34:01 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
788037174575715	SBCE8-70	Dec 11, 2019 7:25:49 AM	Protocol Discrepancy	ACK Message Out of Dialog	General Method not allowed Out-Of-Dialog
788037174546491	SBCE8-70	Dec 11, 2019 7:25:49 AM	Policy	Call Denied	Method Prohibited Out-of-Dialog
788037174528388	SBCE8-70	Dec 11, 2019 7:25:49 AM	Protocol Discrepancy	ACK Message Out of Dialog	General Method not allowed Out-Of-Dialog

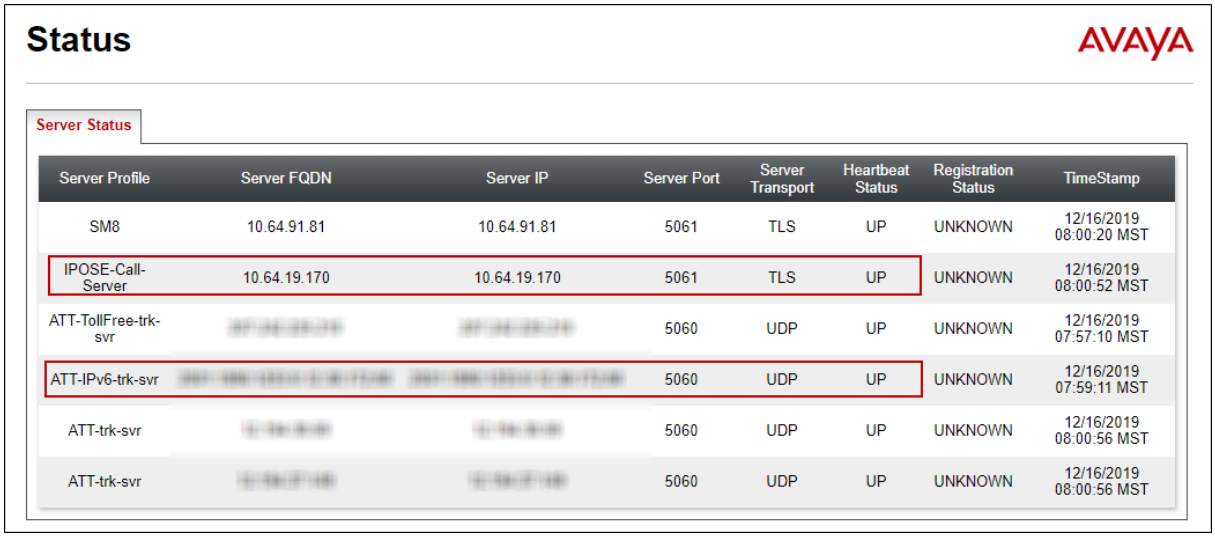
©2020 Avaya Inc. All Rights Reserved.

9.2.2. Server Status

The **Server Status** can be access from the Avaya SBCE top navigation menu by selecting the **Status** menu, and then **Server Status**.



The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Profile, as configured on **Section 7.7**.

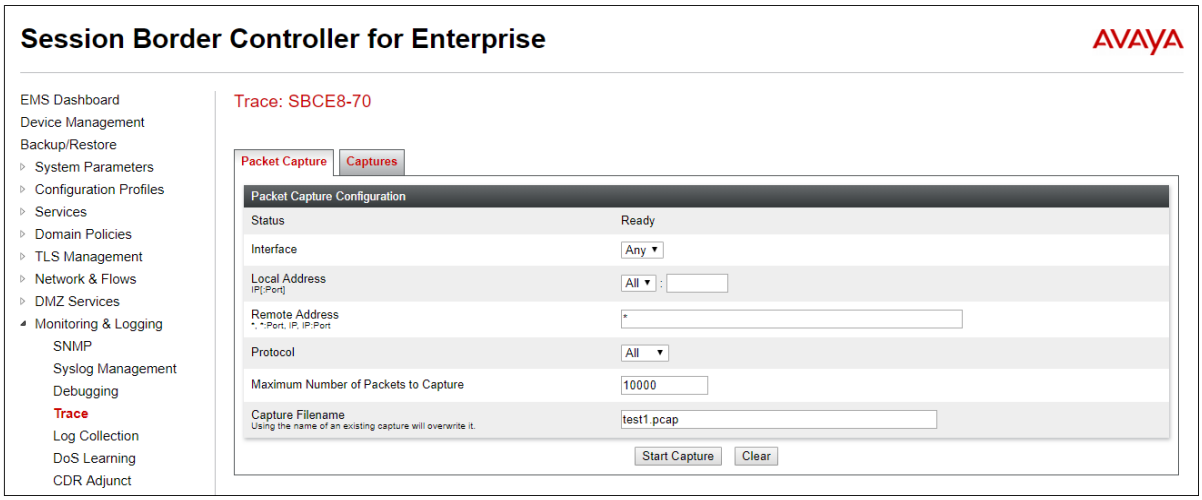


Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
SM8	10.64.91.81	10.64.91.81	5061	TLS	UP	UNKNOWN	12/16/2019 08:00:20 MST
IPOSE-Call-Server	10.64.19.170	10.64.19.170	5061	TLS	UP	UNKNOWN	12/16/2019 08:00:52 MST
ATT-TollFree-trk-svr	[redacted]	[redacted]	5060	UDP	UP	UNKNOWN	12/16/2019 07:57:10 MST
ATT-IPv6-trk-svr	[redacted]	[redacted]	5060	UDP	UP	UNKNOWN	12/16/2019 07:59:11 MST
ATT-trk-svr	[redacted]	[redacted]	5060	UDP	UP	UNKNOWN	12/16/2019 08:00:56 MST
ATT-trk-svr	[redacted]	[redacted]	5060	UDP	UP	UNKNOWN	12/16/2019 08:00:56 MST

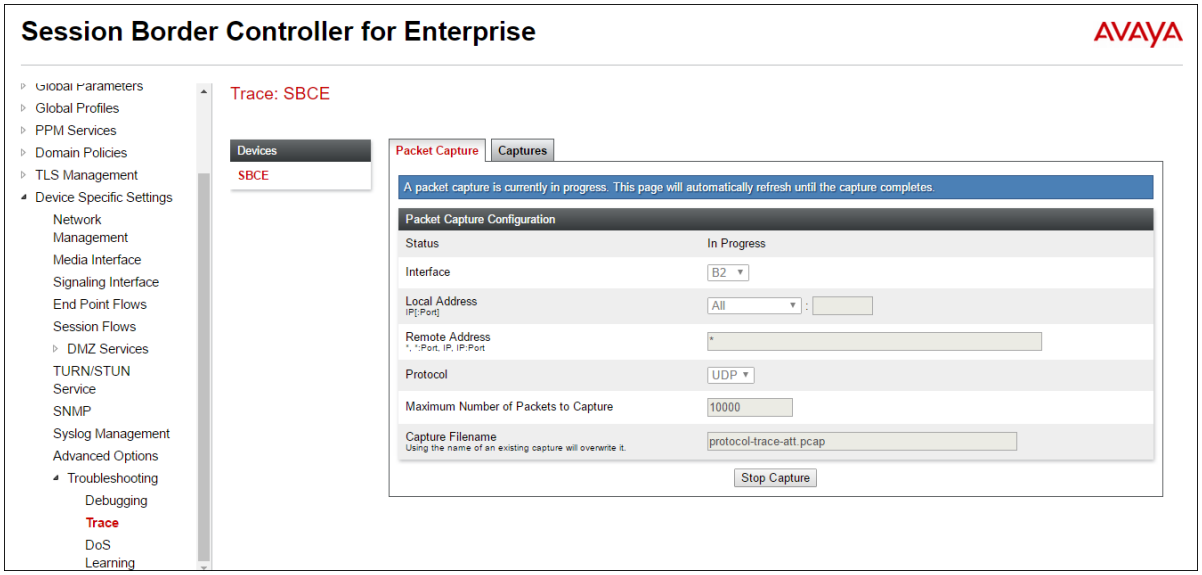
©2020 Avaya Inc. All Rights Reserved.

9.2.3. Protocol Traces

To take a call trace, navigate to **Monitoring & Logging → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.

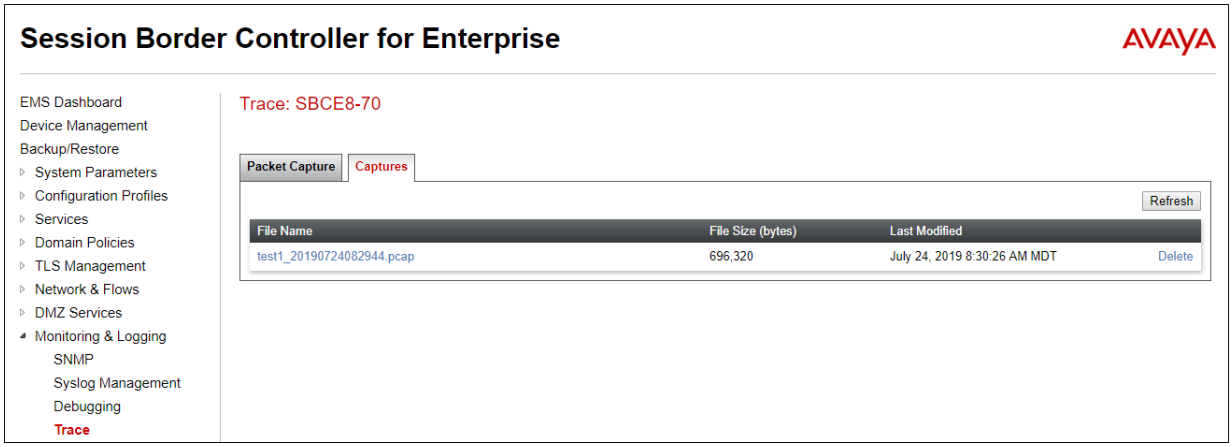


When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.



©2020 Avaya Inc. All Rights Reserved.

Select the **Captures** tab to view the files created during the packet capture.



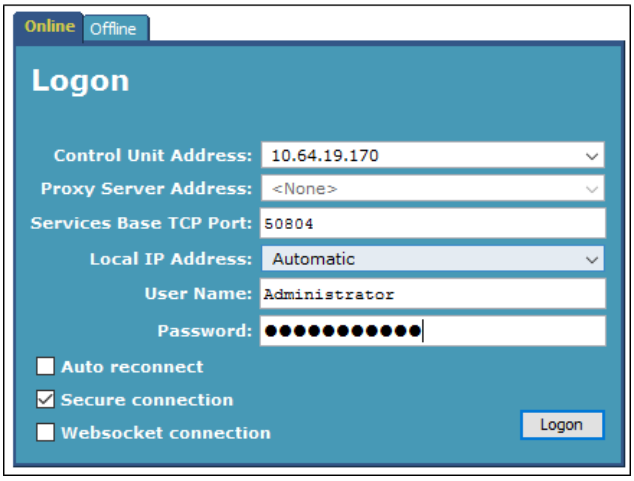
The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like Wireshark.

9.3. Avaya IP Office

The following items may be used to analyze/troubleshoot Avaya IP Office operations.

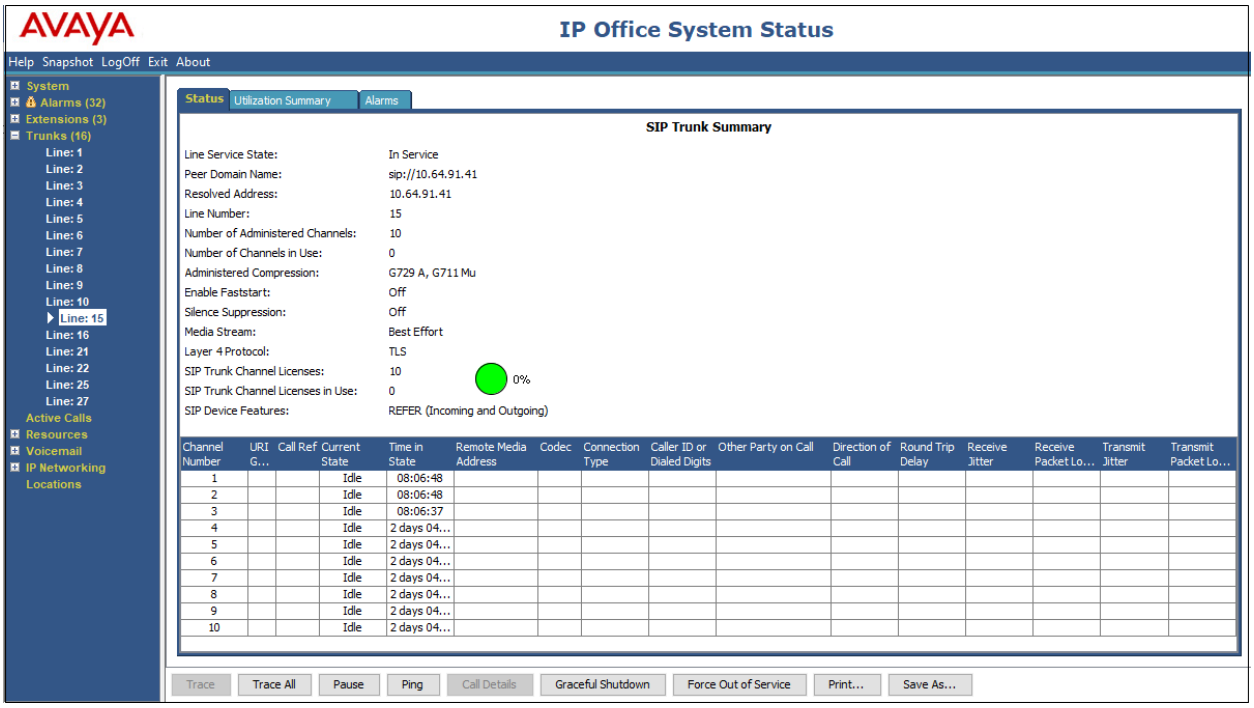
9.3.1. System Status Application

The Avaya IP Office System Status application can be used to verify the service state of the SIP line. From the IP Office Manager application, select **File → Advanced → System Status**. Under **Control Unit IP Address** select the IP address of the IP Office system under verification. Log in using the appropriate credentials.

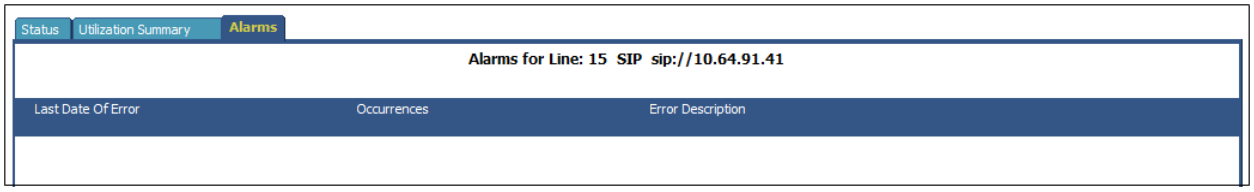


©2020 Avaya Inc. All Rights Reserved.

After logging in, select **Trunks → Line: 15** from the left navigation menu. (SIP Line 15 is configured in **Section 5.5**). A screen such as the one shown below is displayed. In the lower left, the **Trace All** button may be pressed to display tracing information as calls are made using this SIP Line. The **Ping** button can be used to ping the other end of the SIP trunk (e.g., the Avaya SBCE).



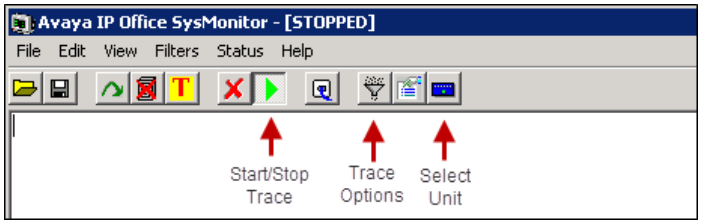
S**elec**t the **Alarms** tab and verify that no alarms are active on the SIP line.



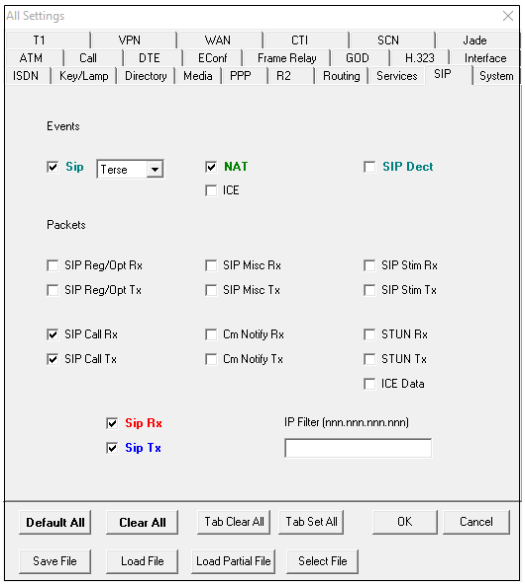
©2020 Avaya Inc. All Rights Reserved.

9.3.2. System Monitor Application

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.



Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting to the desired color.



©2020 Avaya Inc. All Rights Reserved.

10. Conclusion

As illustrated in these Application Notes, Avaya IP Office Release 11.0 and the Avaya Session Border Controller for Enterprise Release 8.0.1 can be configured to interoperate successfully with the AT&T IP Toll Free service using IPv6 and **AVPN** or **MIS/PNT** transport connections, utilizing service features listed in **Section 2.1**, and within the limitations described in **Section 2.2**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

11. Additional References

Avaya:

Avaya product documentation is available at http://support.avaya.com. Additional Avaya IP Office information can be found at: http://marketingtools.avaya.com/knowledgebase/

[1] *Deploying IP Office Platform Server Edition Solution*, Release 11.0, May 2018

[2] *IP Office Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, April 2019

[3] *IP Office Platform 11.0, Deploying Avaya IP Office Essential Edition (IP500 V2)*, January 2020.

[4] *Administering Avaya IP Office Platform with Manager, Release 11.0*, February 2019.

[5] *Administering Avaya IP Office Platform with Web Manager, Release 11.0 FP4*, February 2019.

[6] *IP Office Platform 11.0, Administering Avaya IP Office Platform Voicemail Pro*, December 2019.

[7] *IP Office Platform 11, IP Office SIP Phones with ASBCE, Issue 03f*, April 2019

[8] *Deploying Avaya Session Border Controller in Virtualized Environment*. Release 8.0.x, Issue 4, August 2019.

[9] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0.x, Issue 4, August 2019.

[10] *RFC 3261 SIP: Session Initiation Protocol*. https://www.ietf.org/rfc/rfc3261.txt

AT&T IPTF Service:

[11] AT&T IP Toll Free Service description - https://www.business.att.com/products/ip-toll-free.html

©2020 Avaya Inc. All Rights Reserved.

©2020 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.

IP Productos y Servicios S.A. de C.V.

TRANSFORMACIONES TECNOLÓGICAS
RFC: IPS0703142W1

FORMATO A
PRESENTACIÓN DE LA PROPUESTA ECONÓMICA

Estado de México a 22 de agosto de 2025

COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA
P r e s e n t e

De conformidad con lo establecido en la Convocatoria de Invitación a Cuando Menos Tres Personas de Carácter Nacional Electrónica No. **IA-11-L5X-011L5X001-N-44-2025**, para la contratación del "**SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP"**, manifiesto bajo protesta de decir verdad que:

Oferto los servicios objeto del procedimiento con los precios siguientes:

Servicio a partir de un día posterior a la notificación de fallo y hasta el 31 de diciembre de 2025.

Tipo	Partida Contrato Marco	Descripción TIPO de Servicio	Cantidad	Precio unitario (MXN sin IVA) Si su cotización no tiene diferencia por Estado y puede abastecer a nivel Nacional, cotice aquí	Ciudad de México	Oaxaca
Equipo TIPO 2 / FXO / IP con capacidad de manejo de hasta 1,000 extensiones	1	Equipo de procesamiento de llamadas IP	1	$ 122,334.18		
	3	Gateway para troncales	3	$ 21,227.63		
	12	Servicio de Tarificación Telefónica (No. de extensiones a tarificar)	1	$ 26,670.00		

DESGLOSE DE LA PROPUESTA

Tipo	Partida Contrato Marco	Descripción TIPO de Servicio	Cantidad	Precio unitario Si su cotización no tiene diferencia por Estado y puede abastecer a nivel Nacional, cotice aquí	Precio Mensual Si su cotización no tiene diferencia por Estado y puede abastecer a nivel Nacional, cotice aquí	Ciudad de México	Oaxaca
Equipo TIPO 2 / FXO / IP con capacidad de manejo de hasta 1,000 extensiones	1	Equipo de procesamiento de llamadas IP	1	$ 122,334.18	$ 122,334.18		
	3	Gateway para troncales	3	$ 21,227.63	$ 63,682.89		
	12	Servicio de Tarificación Telefónica (No. de extensiones a tarificar)	1	$ 26,670.00	$ 26,670.00		
					Subtotal Mensual	$ 212,687.07		
					Número de meses	4		
					Subtotal por el periodo	$ 850,748.28		
					I.V.A.	$ 136,119.72		
					Total con IVA	$ 986,868.00		

Conforme a la Junta de Aclaraciones respuesta 871839: IP Productos y Servicios, S.A. de C.V. considera en su propuesta incluir en el formato A (Formato para la presentación de la Propuesta Económica) los campos de subtotal sin IVA, el IVA y el Precio total ya incluyendo el IVA.

Con el propósito de evaluar en igualdad de condiciones, la proposición económica que IP Productos y Servicios, S.A. de C.V. envía o presenta (oferta económica), es de acuerdo con lo siguiente: (Se cotizan todos los conceptos solicitados)

Se señala el importe con letra del total de su oferta:
(Novecientos Ochenta y Seis Mil Ochocientos Sesenta y Ocho Pesos 00/100 M.N.) IVA Incluido.

IP Productos y Servicios S.A. de C.V.

NOTA: Se anota en el presente cuadro lo siguiente:

- Condiciones de Pago: DE CONFORMIDAD CON LA CONVOCATORIA.
- Condiciones de Precio: EL PRECIO SERÁ FIJO DURANTE LA VIGENCIA DEL CONTRATO
- Lugar de ejecución del servicio: DE CONFORMIDAD CON LA CONVOCATORIA.
- Tiempo y lugar de ejecución del servicio: DE CONFORMIDAD CO LA CONVOCATORIA.
- Moneda en que cotiza: PESOS MEXICANOS

El precio contenido en la oferta económica estará vigente durante el procedimiento de contratación.

El precio se cotiza en moneda nacional separando el importe que corresponda por el impuesto al valor agregado.

1) IP Productos y Servicios, S.A. de C.V. acepta los términos y condiciones de pago que se establecen en la convocatoria, que mis precios ofertados permanecerán fijos durante el procedimiento de contratación y hasta la emisión del fallo respectivo y, en caso de resultar adjudicado, mantendré dichos precios fijos y vigentes hasta la terminación del contrato correspondiente.

2) IP Productos y Servicios, S.A. de C.V. esta consciente de que el precio unitario será el único valor que se tomará en cuenta para efectos de evaluación y adjudicación.

3) IP Productos y Servicios, S.A. de C.V. manifiesta que los equipos que se cotizan son nuevos, conforme al Anexo No. 1 "Descripción Técnica del Servicio" y a los formatos que se acompañan

IP Productos y Servicios, S.A. de C.V., manifiesta bajo protesta de decir verdad que el servicio que oferta en esta proposición cumple debidamente con las especificaciones establecidas en la convocatoria de referencia y que, en el evento de ser adjudicado, cumplirá cabalmente con las obligaciones a mi cargo que deriven del fallo correspondiente en los términos y condiciones estipulados en la Convocatoria de Invitación a Cuando Menos Tres Personas Pública Nacional Electrónica No. IA-11-L5X-011L5X001-N-44-2025, para la contratación del "SERVICIO DE ARRENDAMIENTO DE EQUIPO TELEFÓNICO IP"

A T E N T A M E N T E

Rubén Plaza Aguilar
Representante Legal
IP Productos y Servicios S.A. de C.V.