Deploying OnAvaya™ and Powered by Avaya IP Office and IP Office Contact Center For Business Partners

Release 2.0
Issue 2
March 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document contains checklists and procedures for the Powered and OnAvaya™ planning, setup, configuration, and administration tasks that must be performed by Business Partners.

Before working with the Cloud solution, BPs must understand how to configure and administer CPE deployments of IP Office and IP Office Contact Center. BPs must also be authorized by Avaya to perform implementation.

Documentation terminology

This document uses the following terminology:

Product names

- OnAvaya™ is the product name used for the Avaya-hosted solution.
- Powered is the product name used for the BP-hosted solution.

Customers

The Cloud documentation uses the following terms.

- Enterprise: The organization that uses the IP Office and IP Office Contact Center functionality. The Cloud solution is targeted for small and medium enterprises. The documentation uses the term “enterprise” instead of “customer”.
- Business Partner or Provider: The party that sells the IP Office and IP Office Contact Center functionality to the enterprise as a service. This document also uses the acronym “BP” to refer to a Business Partner.

Change history

The following table lists key changes in this document.

Issue	Release date	Summary of changes
Powered Release 1.0	January 2016	Added Powered installation, configuration, and administration information for BPs.
Powered and OnAvaya™ Release 1.1, Issue 1	March 2016	• Updated IP Office Contact Center installation required for BPs deploying the Powered solution. • Moved Resources content from the Introduction chapter into a separate chapter at the end of this document.
OnAvaya™ and Powered Release 1.1.1, Issue 2 ✱ **Note:** This version of the document replaces the Release 1.1 document at http://support.avaya.com/.	April 2016	• Added clarification about the new Team Engagement OnAvaya™ offer, where IP Office Contact Center is optional. • Reorganized the "Components" and "Interoperability" sections in the "Overview" chapter. • Added details about CMC and third party license options in the "License packaging" section. • Added clarification about Avaya One Source Cloud Services and CMC in the "Planning" chapter. • Added a note about configuring basic user licenses for 96x1 endpoints. • Added clarification about paths for endpoint configuration. • Added additional Avaya Contact Recorder configuration information in Optional Avaya Contact Recorder configuration for IP Office and IP Office Contact Center on page 75.
Powered and OnAvaya™ Release 2.0, Issue 1	January 2017	• Removed RICS information because this option is no longer available for Cloud deployments. • Added more information about configuring endpoints without staging. • Added procedures about Hybrid Cloud configuration, which enables you to deploy an IP500 V2 expansion system in the Cloud. • Updated IP Office configuration checklist on page 43. • Added information about IP500 V2 expansion system setup. • Updated the list of related documents in Documentation on page 80.
Powered and OnAvaya™ Release 2.0, Issue 2	March 2017	• Indicated that the Application Level Gateway (ALG) must be disabled on IP Office.

Table continues…

Issue	Release date	Summary of changes
		• Listed the Avaya J129 SIP Phone as a supported endpoint in Additional IP Office endpoints supported in the Cloud on page 15.

Required skills and knowledge

As a Business Partner, you must have the following skills and knowledge before deploying and selling the OnAvaya™ and Powered Cloud solutions:

- Be authorized by Avaya to sell IP Office and IP Office Contact Center.
- Be authorized by Avaya to implement, configure, and administer customer premise environment (CPE) deployments of IP Office and IP Office Contact Center.
- For Powered, know how to deploy the Avaya Operations Support System (OSS). For more information, see *Deploying Avaya Operations Support System*.
- Understand how to use Avaya One Source Cloud Services to place, change, and delete orders.
- Understand how to use IP Office configuration tools, such as IP Office Manager and IP Office Web Manager.
- Understand how to use IP Office Contact Center provisioning and configuration tools, such as the web-based administration portal and IP Office Contact Center User Interface for Windows.

  Important:

  With the Public Network deployment, you can only access this UI with a remote desktop connection using your PartnerAdministrator account.

- Know how to deploy IP Office endpoints and applications, such as Voicemail Pro and Avaya one-X® Portal for IP Office. This document does not cover installation and configuration of endpoints and applications.

  You must configure endpoints as Remote Workers in the Public Network deployment. For information about installing and configuring H.323 and SIP endpoints as Remote Workers, see the following documents:

  - *Installing Avaya IP Office™ Platform H.323 IP Telephone*
  - “VoIP client” section in *Administering Avaya one-X® Portal for IP Office™ Platform*

Chapter 2: OnAvaya™ and Powered Cloud overview

Avaya offers the following Cloud solutions that enable BPs to sell core IP Office and IP Office Contact Center Telephony and Unified Communications (UC) features to users in small and medium enterprises:

- Powered, where you, as the Business Partner (BP), install and host the product instances in a Cloud data center at your site. IP Office Contact Center is optional with Powered.
- OnAvaya™, where Avaya hosts the product instances in the Cloud data center. Two OnAvaya™ offers are available:
    - Customer Engagement offer, which includes both IP Office and IP Office Contact Center.
    - Team Engagement offer, in which IP Office Contact Center is optional.

Key benefits of the Cloud solution include the following:

- Reduction in operational costs for the enterprise by reducing the IT complexity of equipment maintenance.
- Reduction in service delivery costs for the BP through virtualization and shared infrastructure.
- Ability to upgrade software as new versions are released.
- Programmatic interface to support license installations, configure centralized licensing, or delete a license file.
- Automated billing with Avaya One Source Cloud Services.
- Flexibility to change your Avaya One Source Cloud Services order any time. You can add or remove users anytime. With Powered and the Team Engagement OnAvaya™ offer where IP Office Contact Center is optional, you can update your order to add or remove IP Office Contact Center as needed.
- Support for IP500 V2 expansion systems at the enterprise site with Hybrid Cloud.
- Support for resiliency with High Availability (HA).

Related links

Ordering process on page 17

Topology

Powered topology

Powered supports the following deployment models:

- Public Network: This deployment model uses a public over-the-internet connection between the Cloud data center and the enterprise premises. All users connecting over the Public Network are considered Remote Workers.
- Private Network: This deployment model requires an MPLS or site-to-site VPN connection between the Cloud data center and the enterprise premises.

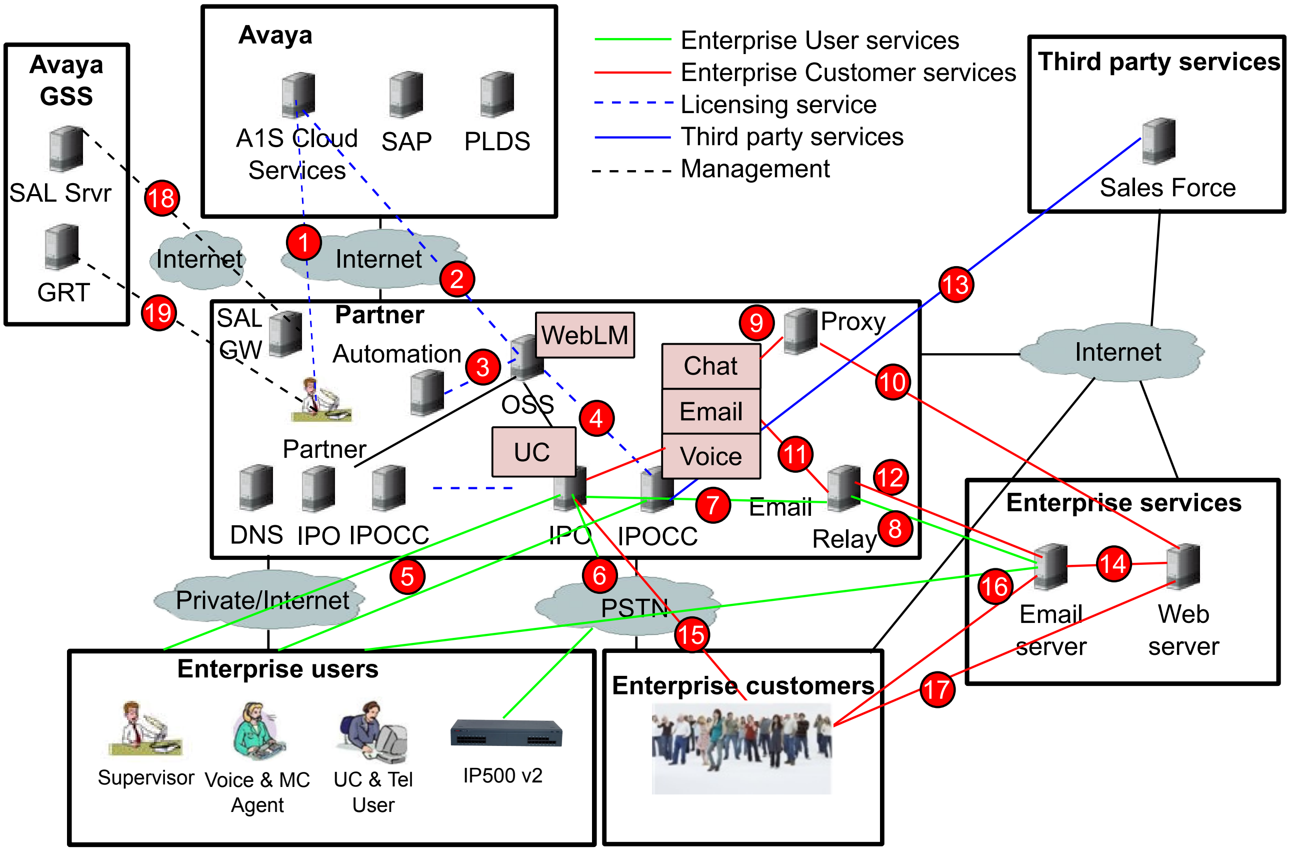


Figure 1: Powered topology

For information about OnAvaya™ integration points, see *OnAvaya™ and Powered by IP Office and IP Office Contact Center Reference Configuration for Business Partners*.

OnAvaya™ topology

OnAvaya™ supports the Public Network deployment model. This deployment model uses a public over-the-internet connection between the Cloud data center and the enterprise premises. All users connecting over the Public Network are considered Remote Workers. The solution supports a one-to-one NAT, which translates IP addresses, but not TCP or UDP ports. The solution supports any kind of NAT at the enterprise site.

As a Partner, you need the SIP Broker Trunk Service to access SIP trunks. You can optionally integrate IP Office Contact Center with third-party CRM systems, such as Salesforce.

Important:

OnAvaya™ does not currently support Private Network deployments.

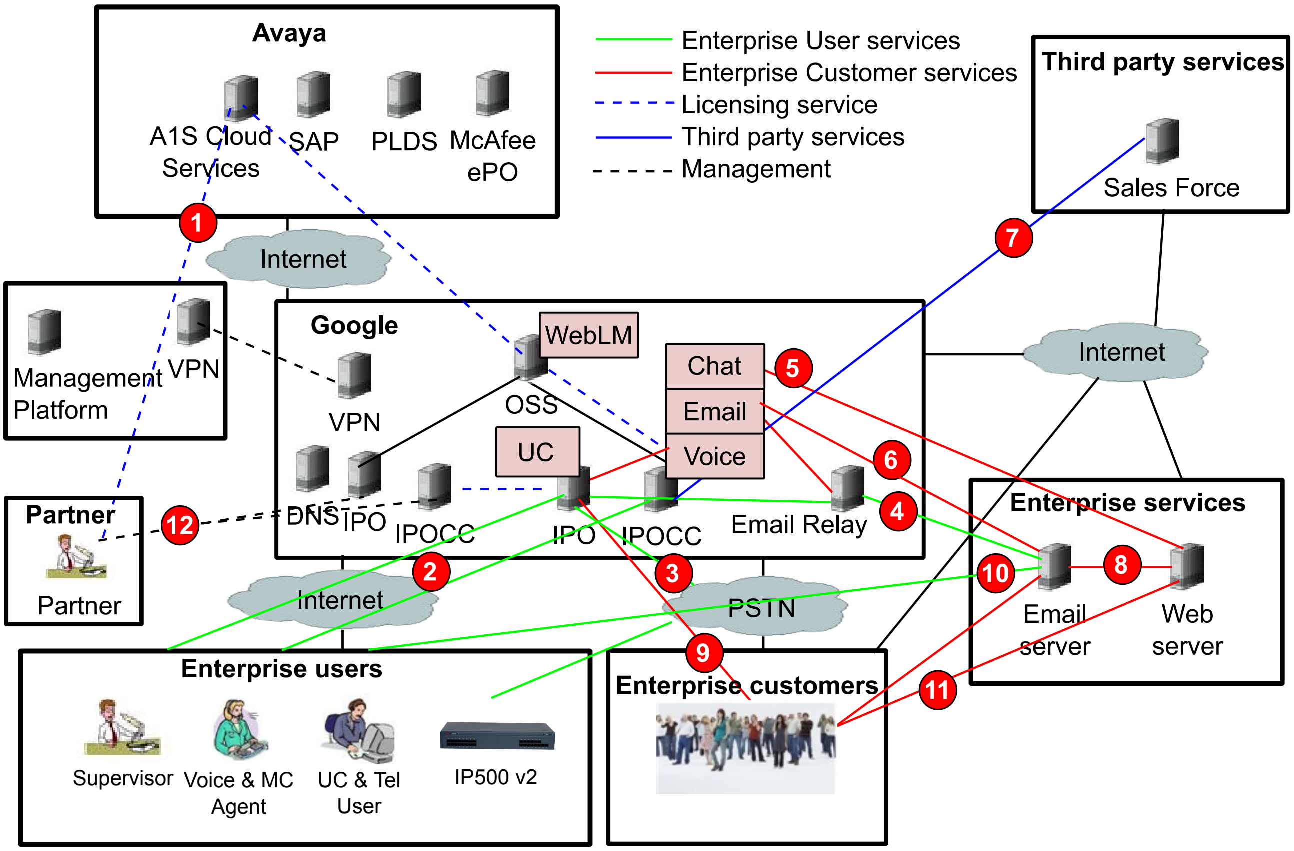


Figure 2: OnAvaya™

For information about OnAvaya™ integration points, see *OnAvaya™ and Powered by IP Office and IP Office Contact Center Reference Configuration for Business Partners*.

Related links

OnAvaya and Powered Cloud overview on page 10

Components

The following sections provide an overview of all components used in the OnAvaya™ and Powered solutions.

For general information about product interoperability, see the Avaya Support Interoperability Matrix at: http://support.avaya.com/CompatibilityMatrix/Index.aspx. Additional information about supported applications and endpoints, and their supported versions is available in the Release Notes.

Key IP Office components

The following IP Office components are used in the Cloud.

Component	Description
IP Office server	The server that provides IP Office services. This server includes the following components: • Avaya one-X® Portal and Mobility server. • Conference resources for ad-hoc and meet-me conferences. • Software download packages for various user and administration applications such as IP Office Manager, System Status Application, Voicemail Pro Client, and IP Office SoftConsole.
IP Office Manager and IP Office Web Manager	IP Office Web Manager is a web-based version of IP Office Manager, and only offers a subset of the IP Office Manager options. You must perform most management and configuration tasks in IP Office Manager. You can install and run IP Office Manager from IP Office Web Manager directly.

Key IP Office Contact Center components

The following IP Office Contact Center components are used in the Cloud. For general information about IP Office Contact Center components, applications, and endpoints, see *Avaya IP Office Contact Center Reference Configuration*.

Component	Description
IP Office Contact Center server	The server that provides IP Office Contact Center services.
IP Office Contact Center provisioning and administration tools	Business Partners must use the following tools for provisioning and administration: • Web-based administration portal to perform setup and initial administration tasks. For more information, see *Using Avaya IP Office Contact Center Web Administration Portal*. • IP Office Contact Center User Interface for Windows to perform administration tasks and assign privileges.

Table continues…

Component	Description
	Note: In the Public Network deployment, BPs can only access the IP Office Contact Center User Interface for Windows through a remote desktop protocol.
IP Office Contact Center user interface for end users	Enterprise users can use the IP Office Contact Center User Interface for Chrome Devices or the IP Office Contact Center Web User Interface. These interfaces are intended for agents and supervisors. For more information about using these interfaces, see *Using the Avaya IP Office Contact Center Chrome and Web Interfaces*.
Optional IP Office Contact Center applications and plug-ins	Enterprises and BPs can also access the following: • Wallboard application for managing statistics. For more information, see *Using Avaya IP Office Contact Center Wallboard*. • SAP or Salesforce (SFDC) CRM connectors for accessing agent telephony functionality.

Other related IP Office and IP Office Contact Center components

The following related components can be integrated with IP Office or IP Office Contact Center in the Cloud.

Component	Description
Avaya Contact Recorder	You can optionally integrate Avaya Contact Recorder with the IP Office and IP Office Contact Center Cloud systems to provide call recording functionality. BPs are responsible for Avaya Contact Recorder configuration. With Powered, BPs must also supply additional disk space if required before configuring Avaya Contact Recorder.
WebRTC	WebRTC is supported with IP Office Contact Center and is used to enable the delivery of media content through the web browser. With the WebRTC protocol, the user interface does not require a physical phone.
Extensible Messaging and Presence Protocol (XMPP) application server	The XMPP server provides chat functionality. Partners using OnAvaya™ must use the XMPP server included with Avaya one-X® Portal for IP Office. Partners using Powered can either provide their own XMPP server or use the server included with Avaya one-X® Portal for IP Office. The recommended option is to use the XMPP server included with Avaya one-X® Portal for IP Office. **Note:** For the chat server, in the Cloud, use the internal IP Office IP address rather than the public IP address. You can use the public IP address as the domain name.
Avaya Session Border Controller for Enterprise (Avaya SBCE)	Avaya SBCE is an optional component that enables Remote Workers and SIP trunking in Powered deployments. A dedicated Avaya SBCE is required for each IP Office in the enterprise.

Additional IP Office endpoints supported in the Cloud

Endpoint	Details	Supported for IP Office Contact Center agents and supervisors
Avaya 96x1 H.323 Phones	Supported for both Public and Private Network deployments.	✔
Avaya 16xx H.323 Phones	Supported in Private Network deployments only.	✔ For Hybrid Cloud only.
Avaya H.175 SIP Video Desk Phone	Supported for both Public and Private Network deployments.	
Avaya B179 SIP Conference Phone	Supported for both Public and Private Network deployments.	
E129 SIP Deskphone	Supported for both Public and Private Network deployments.	
Avaya E159 IP Media Station	Supported in Private Network deployments only.	
Avaya E169 IP Media Station	Supported in Private Network deployments only.	
Avaya D100 or D160 SIP Phone	Supported for both Public and Private Network deployments over TCP or RTP.	
Avaya 11xx or 12xx SIP Phone	Supported for both Public and Private Network deployments.	
Avaya J129 SIP Phone	Supported for both Public and Private Network deployments. It can be deployed on the Primary server or through IP500 V2.	
Avaya Communicator for Windows SIP	Supported directly in Public and Private Network deployments and through Avaya SBCE.	✔
Avaya Communicator for iPad SIP	Supported directly in Public and Private Network deployments and through Avaya SBCE.	
Avaya one-X® Mobile SIP for iOS	Supported directly in Public and Private Network deployments and through Avaya SBCE.	
Avaya one-X® Mobile preferred SIP for Android	Supported directly in Public and Private Network deployments and through Avaya SBCE.	
Avaya Communicator for Web (WebRTC)	Supported for both Public and Private Network deployments.	

Table continues…

Endpoint	Details	Supported for IP Office Contact Center agents and supervisors
9500 Digital Phone through IP500 V2	Supported through IP500 V2.	✔ For Hybrid Cloud only.
14xx Digital Phone through IP500 V2	Supported through IP500 V2.	✔ For Hybrid Cloud only.
Other phone models	The Hybrid Cloud deployment option enables all other supported IP Office phones to be integrated through the IP500 V2 expansion system.	Other: 96x0 H.323 Phones are supported for Hybrid Cloud only. Other IP Office endpoints that are not listed are not supported for IP Office Contact Center.

Management and subscription components

Subscription management

Component	Description
Avaya One Source Cloud Services	Avaya One Source Cloud Services handles interactions related to purchases and billing. Business Partners use Avaya One Source Cloud Services to place and change orders for Powered and OnAvaya™.
Avaya Operations Support System (OSS)	OSS handles licensing and subscription tracking of Cloud instances. OSS is configured to communicate automatically with Avaya One Source Cloud Services. **Note:** With Powered, Business Partners are responsible for deploying and managing OSS. With OnAvaya™, the Avaya service team deploys and manages OSS. Business Partners using OnAvaya™ do not work directly with OSS.
Web License Manager (WebLM)	WebLM is a licensing program that is embedded within OSS.

Google Chrome Management Console

All Chrome devices are registered under the Chrome Management Console (CMC) service. Any updates to the service are automatically downloaded to the desktop. The CMC manages the following:

- IP address information for IP Office and IP Office Contact Center.
- Certificates that CMC administrators need to install.
- The IP Office Contact Center User Interface for Chrome Devices.

Interoperability

The following sections describe compatibility requirements for the Cloud solution.

Product compatibility

The Cloud solutions interwork with IP Office and IP Office Contact Center.

For additional compatibility information for specific IP Office and IP Office Contact Center components, see the appropriate product documentation. Relevant IP Office and IP Office Contact Center documents include the following:

- For general IP Office information: *Avaya IP Office™ Platform Solution Description* and *Avaya IP Office™ Platform Feature Description*
- For general IP Office Contact Center information: *Avaya IP Office Contact Center Feature Description* and *Avaya IP Office Contact Center Reference Configuration*
- For detailed IP Office Contact Center Chrome and Web UI interoperability information: *Using the Avaya IP Office Contact Center Chrome and Web Interfaces*
- For detailed IP Office Contact Center Wallboard interoperability information: *Using Avaya IP Office Contact Center Wallboard*

Related links

Components on page 13

Ordering process

Business Partners request quotes, place orders, and retrieve billing data with the Avaya One Source Cloud Services portal. The OSS updates the IP Office and IP Office Contact Center product licenses with the associated Avaya WebLM instance.

In both solutions, BPs must perform SIP trunk configuration and enterprise-specific configuration, including station and agent administration.

Chapter 3: Planning and preconfiguration

Planning and preinstallation checklist

The following checklist describes the planning tasks you must perform before deploying the OnAvaya™ or Powered Cloud solutions. The planning tasks are the same for both solutions.

No.	Task	Notes	✔
1	Understand pre-sales engineering and determine which solution to order.	You must have an idea of enterprise requirements and the number of users within each enterprise. You must also determine whether you want to use OnAvaya™ or Powered. The questionnaire at https://sales.avaya.com/documents/1399617823596 helps you to determine if OnAvaya™ is appropriate for your enterprise. **Note:** OnAvaya™ is currently available in the US only.	
2	Set up your network infrastructure.	Ensure your network infrastructure setup allows you to connect to the: • Enterprise network • Avaya hosted Cloud data center if you are using OnAvaya™	
3	Understand key configuration details, Avaya and BP responsibilities, and required skills.	Ensure you have all required skills and knowledge for the Cloud solution. Review configuration tools and utilities.	
4	Obtain required components for your BP site and for the enterprise site.	For detailed information about components, see Components on page 13.	
5	Complete the ordering process and obtain user licenses.	Use Avaya One Source Cloud Services to place orders.	

Table continues…

No.	Task	Notes	✔
		With Powered, you must set up the Avaya Operations Support System (OSS) before placing your first trial order.	

Related links

Components on page 13

Required skills and knowledge on page 9

Avaya and Partner responsibilities

The following table compares Avaya and Business Partner responsibilities with the Avaya-hosted OnAvaya™ solution and the BP-hosted Powered solution. In both solutions, the BP is expected to have the training and skills to deliver the enterprise offer.

Task	Party responsible with OnAvaya™	Party responsible with Powered
Support to enterprises.	• BPs provide Tier 1 support. • Avaya provides Tier 2, 3, and 4 support.	• BPs provide Tier 1 and 2 support. • Avaya provides Tier 3 and 4 support
Install and manage OSS, including backups, upgrades and recovery.	With OnAvaya™, OSS is hosted by Avaya.	BPs can deploy OSS on VMware or on a physical server. **Note:** • BPs cannot deploy OSS in the Google Cloud. • Avaya deploys Avaya One Source Cloud Services. BPs can access the Avaya One Source Cloud Services interface using a web browser.
Install and manage IP Office and IP Office Contact Center instances in the Cloud data center.	Avaya is responsible.	BP is responsible.
Monitor components.	Avaya is responsible.	BP is responsible for instance monitoring including VM resources, OS resources, and application alarms.

Table continues…

Task	Party responsible with OnAvaya™	Party responsible with Powered
Backups and upgrades	Avaya is responsible. **Note:** • By default, backup jobs are scheduled at 2 AM Eastern Time. Time changes for a backup job can be done by coordinating with the Avaya service team. • Avaya coordinates any software upgrades with the BP.	BPs are responsible for: • Backups, restorations, and recovery processes. • Service Pack and Feature Pack upgrades. BPs can also upgrade existing Hosted IP Office instances to the new Powered solution.
Set up the enterprise network.	BPs are responsible for setting up their own management environment and a Public Network deployment for the enterprise.	BPs are responsible for setting up their own data center and a Public Network or Private Network deployment for the enterprise. **Note:** Avaya provides some network requirement information to BPs.
Configure instances and complete daily administrative tasks. Configuration includes setting up the following: • IP Office Contact Center agent and user privileges • Endpoints and users • Emergency services • Service calls • Service connectivity • IP Office SIP trunk providers • IP Office Contact Center Wallboards • IP Office Contact Center CRM connectors • Google Chrome Management Console (CMC)	BP is responsible in both OnAvaya™ and Powered.	

Configuration tools

The following table describes the tools BPs use to set up the Cloud solution. The table also indicates which tools apply to the Avaya-hosted OnAvaya™ solution, the BP-hosted Powered solution, or both.

Tools	Description	Used by BPs with OnAvaya™	Used by BPs with Powered
Avaya One Source Cloud Services	Use Avaya One Source Cloud Services to obtain quotes and place orders. Avaya One Source Cloud Services also enables license generation, allows you to modify or disconnect services, and to manage trials and renewals.	Yes	Yes
Avaya Operations Support System	OSS interworks with Avaya One Source Cloud Services to manage subscriptions and licenses.	No The Avaya service team deploys and manages OSS. BPs do not work with this tool directly.	Yes BPs deploy OSS at their site with Powered.
WebLM	WebLM is a licensing program that is embedded within OSS.	No BPs do not work directly with OSS or WebLM.	Yes After installing OSS, BPs must update the default WebLM password. If required, BPs can also update license information in WebLM.
IP Office Web Manager and IP Office Manager	You can use IP Office Web Manager to install and access IP Office Manager. Use IP Office Manager to configure and perform ongoing administration on IP Office.	Yes	Yes
IP Office Contact Center web administration portal	Use the web administration portal to perform initial provisioning of IP Office Contact Center in the Cloud environment. You can also choose to perform initial provisioning with a spreadsheet. For more information about using the administration portal, see *Using Avaya IP Office Contact Center Web Administration Portal*.	Yes, if IP Office Contact Center is included with the offer.	Yes, if IP Office Contact Center is included with Powered.
IP Office Contact Center User Interface for Windows	Use the Windows UI to perform administration tasks and assign privileges to agents and supervisors.		

Table continues…

Tools	Description	Used by BPs with OnAvaya™	Used by BPs with Powered
	Important: With the Public Network deployment, you can only access this UI with a remote desktop connection using your PartnerAdministrator account.		
Google Chrome Management Console (CMC)	Use the CMC to manage the following: • IP address information for IP Office and IP Office Contact Center. • Certificates that CMC administrators need to install. • The IP Office Contact Center User Interface for Chrome Devices.	Yes OnAvaya™ agents can be configured with or without Google CMC.	CMC is optional for Powered. **Note:** With Powered, you cannot order CMC through Avaya. You can purchase it directly from Google.

Key configuration information for Powered

IP Office security settings contain service users, rights groups, and password complexity rules. These security settings are stored separately from the system configuration settings.

For Powered, BPs are responsible for installing and maintaining Cloud product instances. You must implement a DHCP server for IP Office Cloud deployments. IP Office Cloud simplifies system deployment by automatically performing initial start up, ignition, and configuration. As part of the automatic system deployment, service users that are not required for Cloud are removed. The system also resets the *Administrator* and *security* service user passwords from the standard defaults. After the automatic configuration, the following service users remain in the system security settings:

- security
- Administrator
- EnhTcpaService
- IPDECTService

The new *Administrator* and *security* service user passwords are based on the LAN 1 DHCP address obtained at system launch. The new passwords contain the first four letters of the service user name followed by the LAN 1 DHCP IP address without the dots.

Example

If the LAN 1 DHCP IP address is 192.168.10.25, then the *Administrator* and *security* service user passwords are as follows:

Service user name	Service password
Administrator	Admi1921681025
security	secu1921681025

System ID

The system ID for IP Office Cloud is based on the following configuration information:

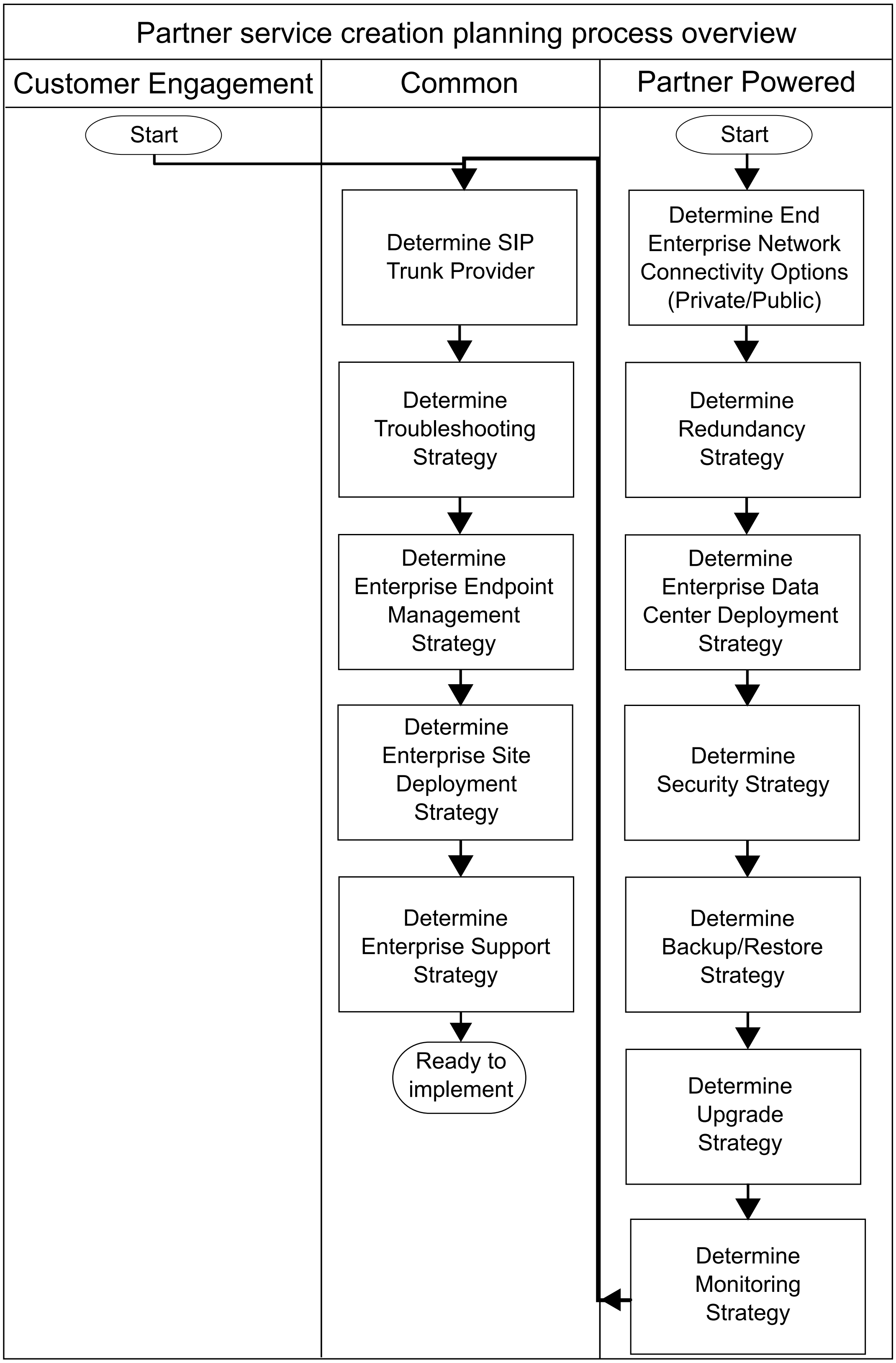
- IP Office LAN 1 IP address
- Host name
- Time zone

The system ID affects a number of system functions, including licensing. When the system ID changes, security settings are also reset, and this affects defined service users and their initial passwords.

Planning flows

The following images outline service planning, service deployment, and onboarding considerations for BPs. Each image shows OnAvaya™ tasks, Powered tasks, and common tasks for both solutions.

Service creation planning flow


Partner service creation planning process overview
Customer Engagement
Common
Partner Powered
Start
Start
Determine SIP Trunk Provider
Determine Troubleshooting Strategy
Determine Enterprise Endpoint Management Strategy
Determine Enterprise Site Deployment Strategy
Determine Enterprise Support Strategy
Ready to implement
Determine End Enterprise Network Connectivity Options (Private/Public)
Determine Redundancy Strategy
Determine Enterprise Data Center Deployment Strategy
Determine Security Strategy
Determine Backup/Restore Strategy
Determine Upgrade Strategy
Determine Monitoring Strategy

Powered task: Determine enterprise network connectivity options

The Partner is response for determining the supported network access methods for the enterprise. The options are:

- Private

  Private Network connectivity examples include IPSec VPN, MPLS, and Metro Ethernet.

- Public Internet
- Both

Consider the following:

- For internet access, each IP Office must have a dedicated public IP address if 96x1 phones must be supported. You can use a VPN server to terminate 96x1 SSL VPN connections. Other non-96x1 endpoints can be multiplexed through a single public IP address using a Session Border Controller and reverse proxy supporting web sockets.
- IP Office and IP Office Contact Center must have one-to-one or Port NAT internet access for integration with enterprise services, such as email and web server services, or third-party Cloud CRM applications.
- IP Office, IP Office Contact Center, and the IP Office Contact Center User Interface for Windows must have access to the WebLM server in the OSS. Access can be direct, or through a one-to-one or Port NAT connection.
- IP Office must have access to SIP trunks through one of the following methods:
  - A one-to-one or Port NAT connection
  - An Avaya or third-party Session Border Controller
- The Partner must provide regulatory integration.

Powered task: Determine redundancy strategy

IP Office supports both Application HA and VMWare HA in Powered deployments. IP Office Contact Center supports VMWare HA. For geo-redundancy, the Partner must create a process that includes backup and recovery to instances in a geo-redundant data center. DNS updates can be used to direct endpoints to geo-redundant instances.

Powered task: Determine instance deployment strategy

The Partner can automate virtual machine creation or do it manually. For automation, OSS supports a Partner-supplied RESTful API server, which is called at the end of the Avaya One Source Cloud Services order fulfillment of license downloads.

Powered task: Determine security strategy

The Partner is responsible for securing their Powered service. Avaya products support third-party public certificates for secure communications. Avaya supplies the firewall rules required for the protocols that the service uses.

OSS and IP Office Contact Center support the optional installation of McAfee antivirus software.

IP Office and OSS support roles-based authorization to features and administration. IP Office Contact Center does not currently have native roles-based authorization outside of the IP Office Contact Center User Interface for Windows administration tasks. To perform administration tasks on the IP Office Contact Center User Interface for Windows, you must have access to the Windows operating system.

Powered task: Determine backup and recovery strategy

You can schedule backups for each Avaya product in the Powered service. Backups require the Partner to provide resources for the products to copy backup files. Use of virtual machine snapshots is limited because application data is stored on the same disk as the operating system data. Virtual machine recovery is limited to the most recent backup.

Powered task: Determine upgrade strategy

Avaya product upgrades affect the Powered Cloud services. To avoid service disruptions, Partners must use maintenance periods to perform upgrades.

Powered task: Determine the monitoring strategy

Avaya supports product-level SNMP trap notifications. IP Office also provides operating system resource alarms. OSS and IP Office Contact Center require the Partner to implement operating system resource monitoring mechanisms, such as Linux SSH access, CLI command line parsing, and Windows WinRM.

Common task: Determine the SIP trunk provider

IP Office supports :

- TCP, TCP and TLS, or UDP SIP signalling
- RTP or SRTP media

The OnAvaya™ and Powered services created by the Partner are regulated services. The Partner is responsible for complying with all regulatory requirements, such as E911, lawful intercept, local number portability, and regulatory taxes. Obtain legal counsel to ensure regulatory compliance.

Common task: Determine a troubleshooting strategy

The Partner is the primary point of contact for troubleshooting product and network issues. Tools are available to assist with troubleshooting tasks. Prognosis is an example of a vendor that provides tools to support voice quality monitoring.

Common task: Determine the enterprise endpoint management strategy

The Partner is responsible for support configuration, software upgrades, and security of enterprise endpoints. For 96x1 phones, the Partner must use a staging process to ensure that root CA certificates are installed securely.

Related links

Configuring endpoints with staging on page 51

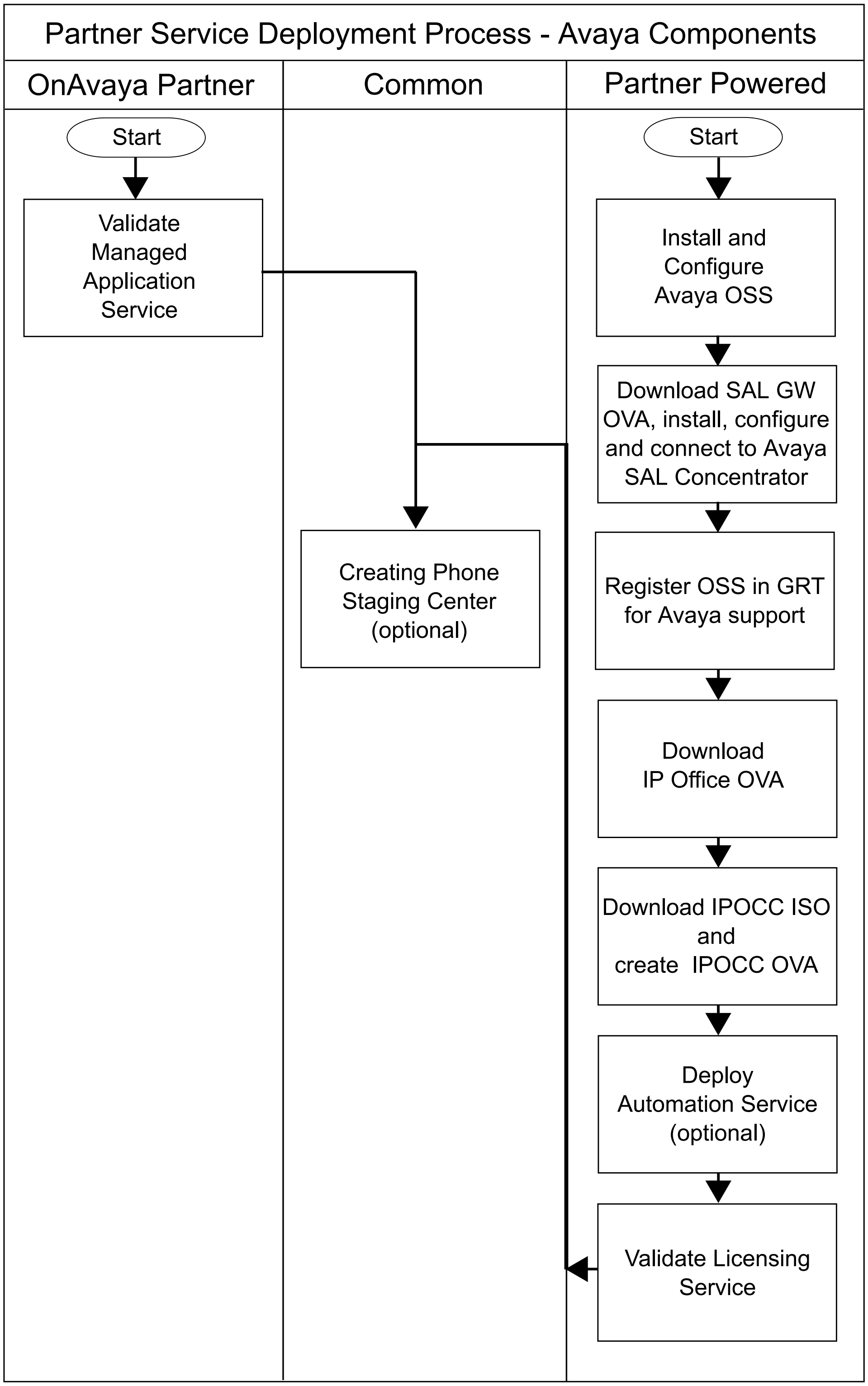
Common task: Determine enterprise site deployment strategy

The enterprise network is typically connected with WAN, LAN, or WiFi. The Partner must ensure that the enterprise network provides sufficient bidirectional bandwidth and security to integrate with Avaya products and applications. In Powered deployments, these products and applications are deployed by the Partner.

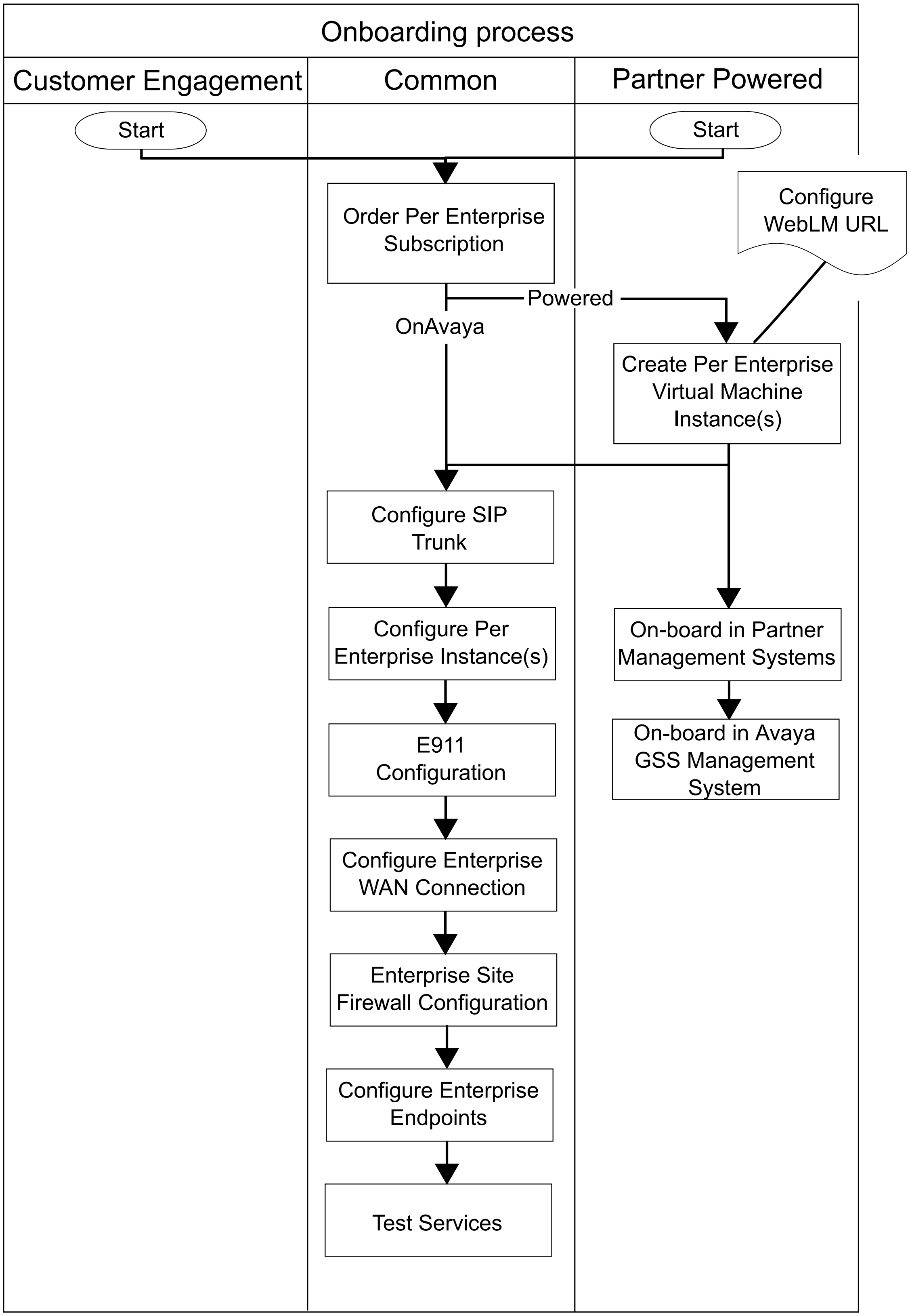
Common task: Determine an enterprise support strategy

The Partner must receive training and certifications for Avaya products and applications that are deployed within the Cloud service. The Partner must implement troubleshooting management systems to support the enterprise. In Powered, the Partner is responsible for Tier 1 and 2 support, and must escalate Tier 3 and 4 issues to Avaya.

Service deployment planning


Partner Service Deployment Process - Avaya Components
OnAvaya Partner
Common
Partner Powered
Start
Validate Managed Application Service
Start
Install and Configure Avaya OSS
Download SAL GW OVA, install, configure and connect to Avaya SAL Concentrator
Creating Phone Staging Center (optional)
Register OSS in GRT for Avaya support
Download IP Office OVA
Download IPOCC ISO and create IPOCC OVA
Deploy Automation Service (optional)
Validate Licensing Service

Onboarding process flow


Onboarding process
Customer Engagement
Common
Partner Powered
Start
Start
Order Per Enterprise Subscription
Configure WebLM URL
Powered
OnAvaya
Create Per Enterprise Virtual Machine Instance(s)
Configure SIP Trunk
Configure Per Enterprise Instance(s)
On-board in Partner Management Systems
E911 Configuration
On-board in Avaya GSS Management System
Configure Enterprise WAN Connection
Enterprise Site Firewall Configuration
Configure Enterprise Endpoints
Test Services

Ordering process

Business Partners request quotes, place orders, and retrieve billing data with the Avaya One Source Cloud Services portal. The OSS updates the IP Office and IP Office Contact Center product licenses with the associated Avaya WebLM instance.

In Powered, BPs are responsible for deploying OSS in the data center before placing their first trial order.

Understanding the Avaya Operations Support System order flow for Powered

About this task

With Powered, Partners must set up OSS before placing their first trial order. This procedure provides a high-level description of the tasks you need to perform to order OSS and place your first Cloud trial order.

Note:

This procedure does not apply to OnAvaya™. Partners using OnAvaya™ do not deploy OSS.

Procedure

1. Place the merchandise order for OSS.
2. Set up entitlements from Avaya PLDS by logging in to https://plds.avaya.com/ with your SSO credentials.

   This information is added to your Partner Sold-To installation base records, which provides Global Support Services (GSS) entitlements.
3. Obtain credentials for Avaya One Source Cloud Services.

   For more information, see Obtaining Avaya Operations Support System credentials for Avaya One Source Cloud Services on page 31.
4. Deploy OSS.

   You must also enter your Avaya One Source Cloud Services credentials in OSS. The OSS connects to Avaya One Source Cloud Services, enabling you to place orders. For more information about deploying OSS, see *Deploying Avaya Operations Support System*.
5. To use SAL or the Avaya VPN Gateway, register OSS using the Global Registration Tool.
6. Place your first trial order.

Obtaining Avaya Operations Support System credentials for Avaya One Source Cloud Services

About this task

This procedure describes how to obtain your Partner credentials for Avaya One Source Cloud Services with Powered deployments.

Procedure

1. Go to the Partner ITSS web site and do one of the following:

   Important:

   If you are an APAC Partner, do not use this web site. Email your request to appartnerhelp@avaya.com.

   - Raise a request for the “IT-AVA-ONESOURCE-CLOUD ” group.
   - Search for “Cloud”.
2. In your request for IT, specify that you are requesting an OSS password.
3. Provide the following information:
   - Company name
   - Partner Link ID
   - User first name
   - User last name
   - User full name
   - Name prefix (optional)
   - Initials (optional)
   - Email ID
   - Phone number (optional)

Result

After receiving your request, the IT support group does the following:

- Checks to make sure that you are authorized to order Powered in Avaya One Source Cloud Services.
- Creates your user ID and password. The user ID is the same as your Partner Link ID.

Next steps

Configure your Avaya One Source Cloud Services credentials in OSS. For more information, see the remaining steps in Understanding the Avaya Operations Support System order flow for Powered on page 30.

Avaya One Source Cloud Services access and navigation

Access Avaya One Source Cloud Services at https://www.avaya.com/ebizn in Canada, US, CALA, and APAC, and at www.avaya.com/ebizu in EMEA.

If you do not have access to Avaya One Source Cloud Services, log in to https://www.avaya.com/uae. From the Configuration section, request access to A1S Cloud Services. If you have a new account number, specify this in your request to ensure you have access to your new Tier 1 account in Avaya One Source Cloud Services.

The following image shows login and order processing options available in Avaya One Source Cloud Services.

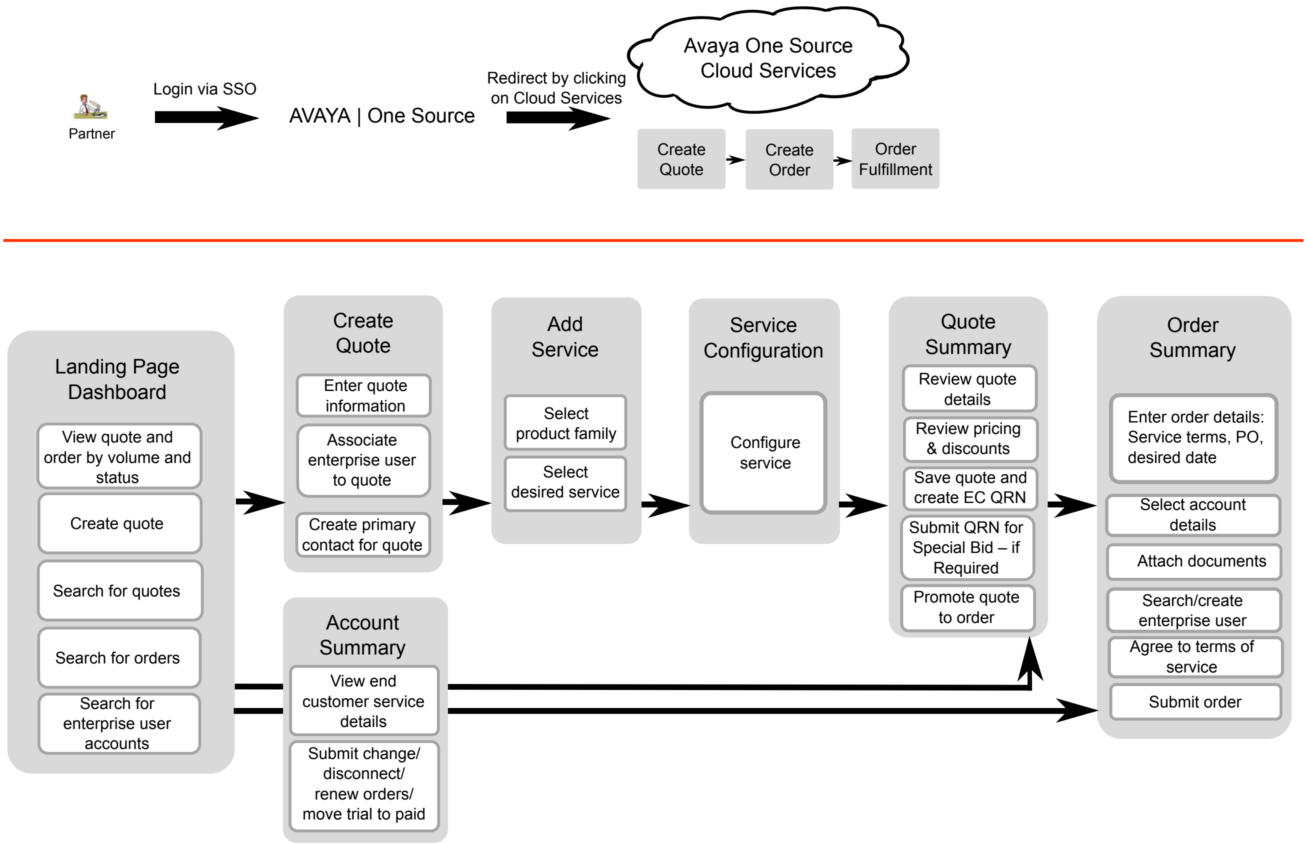

Partner
Login via SSO
AVAYA | One Source
Redirect by clicking on Cloud Services
Avaya One Source Cloud Services
Create Quote
Create Order
Order Fulfillment
Landing Page Dashboard
View quote and order by volume and status
Create quote
Search for quotes
Search for orders
Search for enterprise user accounts
Create Quote
Enter quote information
Associate enterprise user to quote
Create primary contact for quote
Add Service
Select product family
Select desired service
Service Configuration
Configure service
Quote Summary
Review quote details
Review pricing & discounts
Save quote and create EC QRN
Submit QRN for Special Bid – if Required
Promote quote to order
Order Summary
Enter order details: Service terms, PO, desired date
Select account details
Attach documents
Search/create enterprise user
Agree to terms of service
Submit order
Account Summary
View end customer service details
Submit change/ disconnect/ renew orders/ move trial to paid

Figure 3: Avaya One Source Cloud Services navigation

License packaging

The Cloud solution is sold based on a user subscription model. The BP places an order for each enterprise subscription. The subscriptions are based on the following user counts:

- Telephony User
- UC User
- Agent (voice or multichannel)
- Supervisor Agent

Each enterprise subscription includes IP Office system bundles, or IP Office and IP Office Contact Center system bundles.

Note:

IP Office Contact Center is optional for Powered. You can update your order in Avaya One Source Cloud Services anytime to add or remove IP Office Contact Center.

System bundle licenses are fixed and cannot be changed. Product feature license counts are set to enable IP Office and IP Office Contact Center features.

The following tables show the product license counts allocated to each bundle.

Table 1: IP Office licensing

Cloud subscriptions	IP Office license mapping	Quantity
System bundle	Server Edition Virtualized	Maximum
	SIP Trunks	Maximum
	Receptionist	10
	VM Ports	Maximum
	CTI Link Pro	Maximum
	PRI channels	Maximum
Telephony User	Avaya IP Endpoint License	1
Third Party Telephony User	Third Party IP Endpoint License	1
UC User	Avaya IP Endpoint License	1
	Power User License	1
	Web Collaboration User	1
Third Party UC User	Third Party IP Endpoint License	1
	Power User License	1
	Web Collaboration User	1
IP500 Digital or Analog User	IP500 Digital/Analog User License	1
IP500 UC Digital or Analog User	IP500 Digital/Analog User License	1
	Power User License	1

Table continues…

Cloud subscriptions	IP Office license mapping	Quantity
Avaya Contact Recorder system based license	Avaya Contact Recorder. This system add-on license is optional for IP Office only. IP Office Contact Center Release 10.0.x includes Avaya Contact Recorder in the system bundle.	1

Table 2: IP Office Contact Center licensing

Cloud subscriptions	IP Office Contact Center license mapping	Quantity
System bundle	IP Office Contact Center Base License	1
	IP Office Contact Center Wallboard	5
	Avaya Contact Recorder	1
	Avaya IP Endpoint License	1
Agent An agent can either be a voice-only agent or a multichannel agent. Any agent can be configured as a multichannel agent with access to telephony, email, and chat.	Voice Agent	1
	Multichannel Agent	1
Supervisor Agent	Supervisor Agent	1

Chapter 4: Initial setup and connectivity

Initial setup and connectivity checklist

The following checklist outlines installation and network connectivity tasks for BPs to perform in the Cloud environment.

No.	Task	Required by BPs with OnAvaya™	Required by BPs with Powered	✔
1	Understand the differences between CPE and Cloud deployments. The deployment tasks you perform with Powered are very similar to the tasks for CPE. However, OnAvaya™ and CPE have a lot of differences.	✔		
2	Install the IP Office and IP Office Contact Center Cloud instances in the virtual infrastructure.		✔	
3	Set up connectivity between your network and the enterprise network. You must also help the enterprise to set up endpoints.	✔	✔	

Deployment comparison worksheet for OnAvaya™

The following worksheet compares deployment tasks required in the OnAvaya™ Cloud environment and in a standard IP Office Contact Center customer premise environment (CPE). Deployment instructions for CPEs are in the IP Office Contact Center task based guides (TBGs).

The Powered solution is very similar to standard IP Office and IP Office Contact Center CPE deployments.

Requirement	Environment		Installation and Maintenance TBG sections	Notes
	CPE	OnAvaya™		
Physical components are available.	Yes	Partial	Site preparation checklist	IP Office and IP Office Contact Center servers are not required. The customer is responsible for the CRM server if CRM integration is required.
Additional hard disk drive (HDD) on IP Office or the Applications Server for Avaya Contact Recorder.	Yes	No	Site preparation checklist	Pre-installed in the Cloud.
Applications Server requirements.	Yes	No	Site preparation checklist	The Cloud environment uses IP Office Server Edition.
Telephone and internet services are in place.	Yes	Yes	Site preparation checklist	
Download documents.	Yes	Yes	Planning checklist	
Plan endpoint deployment.	Yes	Yes	Planning checklist	
IP Office Contact Center hardware requirements.	Yes	No	IP Office Contact Center requirements	The Cloud image supports up to 250 agents (N1–Standard-16).
Network and QoS requirements.	Yes	Yes	IP Office Contact Center requirements	Does not include Public Internet delays.
IP Office Contact Center User Interface for Windows computer requirements.	Yes	No	IP Office Contact Center requirements	IP Office Contact Center User Interface for Windows is not supported on premise in the Cloud environment.
Telephone requirements.	Yes	Yes	IP Office Contact Center requirements	Digital phones are not supported in the Cloud environment.
Trunk requirements.	Yes	Yes	IP Office Contact Center requirements	Digital trunks are not supported in the Cloud environment.

Table continues…

Requirement	Environment		Installation and Maintenance TBG sections	Notes
	CPE	OnAvaya™		
Virus scan specifications.	Yes	No	IP Office Contact Center requirements	Anti-virus is preinstalled and maintained by Avaya in the Cloud environment.
Required information for IP Office Contact Center.	Yes	Partial	IP Office Contact Center requirements	Some information is pre-populated or emailed to the BP from Avaya.
Server name required.	Yes	No	Server preparation	The server name is pre-assigned in the Cloud and should never be changed. Do not use `AdjustHostName.exe` .
Windows firewall required.	Yes	No	Server preparation	Disabled in the Cloud because the Cloud environment uses Google facilities.
Time and date settings required.	Yes	Partial	Server preparation	The BP must set the time zone in the Cloud. The time and date settings use the Google NTP Server, and cannot be configured in the Cloud.
SNMP.	No	No	Server preparation	The Cloud environment uses SNMP. BPs should not modify SNMP.
Server user name and password required.	Yes	No	Server preparation	The Administrator account is reserved for the Avaya service team. Avaya creates a PartnerAdministrator account and emails the credentials to the BP.
IP address required.	Yes	No	Server preparation	Public and private IP addresses are set and should not be modified in the Cloud.
Power settings required.	Yes	No	Server preparation	Preset for Cloud.
Disable DEP.	Yes	No	Server preparation	Preset for Cloud.
Install Windows.	Yes	No	IP Office Contact Center installation	Windows 2008 R2 is pre-installed for Cloud.
Install IP Office Contact Center software.	Yes	No	IP Office Contact Center installation	Software is pre-installed in the Cloud instance. The database password is `Administrator`.

Table continues…

Requirement	Environment		Installation and Maintenance TBG sections	Notes
	CPE	OnAvaya™		
Licensing	Yes	No	Licensing	Licenses are pre-installed in the Cloud based on ordering data.
Create certificates for the IP Office Contact Center server.	Yes	No	Certificates	Certificates are created and uploaded to the IP Office Contact Center server before the instance is provided to the BP.
Import the Root CA certificate to your browsers.	Yes	Yes	Certificates	Use the IP Office Root CA certificate for deployment.
Enable TAPI communication	Yes	No	Enabling TAPI	Preset for Cloud.
Back up the database.	Yes	No	Provisioning	Backup of the basic database is available from Avaya if required to recover from a provisioning failure.
Configuration Wizard.	Yes	Yes	Provisioning	Some information is preset for Cloud.
Excel Spreadsheet.	Yes	Yes	Provisioning	Avaya emails some IP Office information in the spreadsheet to the BP.
Configure IP Office.	Yes	Yes	Provisioning	With automatic synchronization, minimal configuration is required in CPEs and the Cloud.
Text to speech.	Yes	Yes	Provisioning	TTS licensing is pre-applied for Cloud.
Create automatic synchronization service account.	Yes	Yes	Provisioning	
WebRTC configuration.	Yes	Yes	Post-provisioning	WebRTC is mandatory in the Cloud. **Note:** IP Office is delivered with the WebRTC configuration already performed.
Install IP Office Contact Center	Yes	No	Post-provisioning	IP Office Contact Center User Interface for Windows is pre-configured on the IP Office

Table continues…

Requirement	Environment		Installation and Maintenance TBG sections	Notes
	CPE	OnAvaya™		
User Interface for Windows.				Contact Center instance in the Cloud. You can use the PartnerAdministrator account with RDP to configure and administer the system.
Default task flows.	Yes	Yes	Post-provisioning	The default call flows are automatically enabled when you use the Configuration Wizard.
Install the IP Office Contact Center User Interface for Chrome Devices or the IP Office Contact Center Web User Interface.	Yes	Yes	Post-provisioning	Cloud users can use the IP Office Contact Center Chrome or Web UI.
Upload agent pictures.	Yes	Yes	Post-provisioning	
Configure agents in the UI.	Yes	Yes	Post-provisioning	
Install and configure the SAP connector.	Yes	Yes	CRM	
Install and configure SalesForce CRM plug-in.	Yes	Yes	CRM	
Set up regular backups.	Yes	No	Maintenance	With OnAvaya™, the service team can schedule backups before delivering the Cloud instance to the BP. The BP must inform the service team if the schedule (time of day and frequency) needs to be changed.
Upgrades.	Yes	No	Maintenance	With OnAvaya™, Avaya handles patches, Service Packs, and major upgrades.

Installing Cloud product instances with Powered

About this task

In Powered, BPs are responsible for installing IP Office and IP Office Contact Center Cloud instances.

Before you begin

- You must have a DHCP server in your network.
- Set up a virtual machine (VM). For information about VM requirements in:
  - IP Office, see *Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines*.
  - IP Office Contact Center, see *Avaya IP Office Contact Center Reference Configuration*.

Procedure

1. Deploy the required Cloud OVA files for IP Office and IP Office Contact Center.

   Note:

   For IP Office Contact Center, Business Partners must create the OVA file first and then deploy it.

   For information about deploying the OVAs, see the following documents:

   - For IP Office, *Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines*.
   - For IP Office Contact Center, *Avaya IP Office Contact Center OVA Installation for Powered*.

2. Install the IP Office and IP Office Contact Center Cloud instance.

   You can also set up IP500 V2 expansion systems with IP Office.

Next steps

Set up access to management tools and set up network connectivity for the enterprise.

Setting up network connectivity and components

About this task

The following procedure provides guidelines for setting up network connectivity between the provider network and the enterprise site. With OnAvaya™ and Powered, you must ensure you have access to management components and help the enterprise set up required endpoints.

Before you begin

With Powered, install the Cloud product instances.

Procedure

1. Ensure you have access to the following management tools:
    - IP Office Web Manager and IP Office Manager.
    - IP Office Contact Center web administration portal.
    - IP Office Contact Center User Interface for Windows, which you can only access with a remote desktop connection in the Public Network deployment.
2. Connect the enterprise network to the Cloud data center.

    Specify the external, public IP address that the enterprise uses to connect to the Cloud server.

    With Powered, you can use a Public or Private Network connection.

    OnAvaya™ includes the basic IP Office and IP Office Contact Center Cloud Google Engine image. All users are connected to OnAvaya™ using remote endpoints through secure connections.
3. Ensure your network and the enterprise network are able to support good audio quality.

    For detailed information about quality of service and bandwidth requirements, see *OnAvaya™ and Powered by IP Office and IP Office Contact Center Reference Configuration for Business Partners*.
4. Work with the enterprise to set up endpoints.

    Note:

    - IP Office leverages standard signaling protocols, such as SIP and H.323. Some routers can manipulate SIP and H.323 through the Application Level Gateway (ALG). IP Office requires that any ALG for SIP or H.323 be disabled to ensure proper operation.
    - If you configure a basic user license for a 96x1 endpoint, you must set the **Remote Worker** option, because the service is over the internet. Otherwise, the phone will not login or register correctly.

Related links

Quality of service requirements on page 41

Quality of service requirements

To achieve good voice quality, the enterprise network must meet certain requirements. The terms used to describe acceptable voice quality are toll quality and business communication quality. Optimal voice quality is toll quality, but business communication quality is well suited for most enterprises. Business communication quality is not as high as toll quality, but is still much better than cell phone quality.

The following table provides guidelines for network delay, jitter, and packet loss. Even if the enterprise network meets these requirements, other factors might still negatively impact voice quality.

Table 3: Quality of Service (QoS) requirements

Requirements	Description
Network delay	Voice quality: • To obtain toll quality, the delay cannot exceed 80 millseconds (ms). • To obtain business communication quality, the delay must be between 80 to 180 ms. Business communication quality is suitable for most enterprises. • Delays exceeding 180 ms provide a lower quality than business communication quality, but this might still be acceptable for some enterprises.
Network jitter	To achieve optimal voice quality, the average jitter must be less than half the network packet payload. This value can vary depending on the type of service the jitter buffer has in relation to other buffers and to the packet size used. Assuming the packet size is 20 ms, to prevent problems with voice quality, the network jitter must not exceed 20 ms.
Network packet loss	Voice quality: • To obtain toll quality, the packet loss cannot exceed 1%. • To obtain business communication quality, the packet loss cannot exceed 3%. • Packet losses exceeding 3% might result in signalling interferences.

When transporting voice over low speed links, normal data packets can prevent or delay voice packets from getting across the link. This voice transportation can result in unacceptable speech quality. To ensure low speech latency and help maintain sufficient voice quality, you can implement another Quality of Service (QoS) mechanism, such as a QoS router, on the traffic routers and switches in the network.

Related links

Setting up network connectivity and components on page 40

Chapter 5: Configuration

The following sections provide configuration information for Cloud deployments. You must perform configuration tasks in IP Office, IP Office Contact Center, and the Chrome Management Console.

Important:

This chapter does not provide comprehensive information about standard configuration options available in CPE deployments.

IP Office configuration

In the Cloud environment, many IP Office settings are configured automatically. You can perform most other IP Office configuration and administration tasks using IP Office Manager. You can install and launch IP Office Manager from IP Office Web Manager. This document does not describe how to use IP Office tools and how to configure IP Office in a CPE deployment.

For a list of IP Office settings that are configured automatically, see *OnAvaya™ and Powered by IP Office and IP Office Contact Center Reference Configuration for Business Partners*.

For information about using IP Office Manager and IP Office Web Manager, see the following documents:

- *Administering Avaya IP Office™ Platform with Manager*
- *IP Office Web Manager for Server Edition and Standard Mode*

IP Office configuration checklist

The following checklist outlines the configuration tasks you must perform on IP Office. Many of these configuration tasks are the same as the configuration tasks you must perform for CPE deployments.

No.	Task	Required by BPs with OnAvaya™	Required by BPs with Powered	✔
1	To enable IP Office Cloud integration with IP Office Contact	✔	✔	

Table continues…

No.	Task	Required by BPs with OnAvaya™	Required by BPs with Powered	✔
	Center, you must do the following: • Configure agent extensions • Reserve global licenses • Set the contact center type • Configure the NTP server			
2	Configure the WebLM client ID and URL. WebLM is embedded within OSS. For information about configuring OSS and the embedded WebLM, see *Deploying Avaya Operations Support System*.		✔	
3	Configure SIP trunks in IP Office Manager. The exact configuration process can vary slightly depending on your SIP trunk provider. **Important:** With OnAvaya™, Google firewall rules must be configured to allow bidirectional SIP trunk traffic with the SIP trunk service provider.	✔	✔	
4	You must configure users on IP Office. You can also associate an extension with a user, or add users to groups or hunt groups. Use IP Office Manager in Configuration mode to configure users, extensions, hunt groups, and other types of user groups. For more information, see *Administering Avaya IP Office™ Platform with Manager*.	✔	✔	
5	Configure IP Office endpoints or stations for each user.	✔	✔	
6	Configure emergency call handling in IP Office.	✔	✔	

Table continues…

No.	Task	Required by BPs with OnAvaya™	Required by BPs with Powered	✔
	Important: Do not use soft clients to make emergency calls. The users of soft clients must use a hard phone, such as a desk phone, or a mobile phone to make an emergency call directly through the PSTN, if required.			
7	Configure Voicemail Pro for users by logging in with your Administrator account and password. For OnAvaya™, you must specify the public IP address of the IP Office. The IP address might vary for Powered deployments. You must configure the voicemail system for each user in IP Office Manager. For more information, see *Administering Avaya IP Office™ Platform with Manager*.	✔	✔	
8	Optionally configure Hybrid Cloud, which enables you to deploy an IP500 V2 expansion system in the Cloud.	✔	✔	

Launching IP Office Manager

Before you begin

- Log in to IP Office Web Manager with your administrator credentials. You can access IP Office Web Manager with the URL `https://<IP Office public IP address>:7070`.
- Install the latest Java Runtime Environment (JRE) Oracle version.u

Procedure

In the Web Manager menu bar, click **Applications** and then **IP Office Manager**.

The system automatically loads the IP Office configuration file from the primary server. To load an alternate IP Office configuration file, select the appropriate server.

Result

The system checks if Manager is installed. The system also checks for the version of Manager that is installed.

The system prompts you to download and install the latest version of Manager in the following situations:

- If the version of Manager is not the latest.
- If Manager is not installed.

Next steps

Do one of the following:

- Click **OK**, to open the current version of Manager that the system has detected.
- Download and install the latest version of Manager. Then restart your browser.
- Select **Start** > **Programs** > **IP Office** > **Manager** to open Manager directly from the computer.

Verifying IP Office Manager preferences

Before you begin

Launch IP Office Manager.

Procedure

1. In IP Office Manager, navigate to **File** > **Preferences**.
2. Confirm that the **SE Central Access** check box is selected.
3. Ensure that the following four check boxes are not selected:
    - **Set Simplified View as Default**
    - **Default to Standard Mode**
    - **Use Remote Access**
    - **Consolidate Solution to Primary Settings**
4. If you make any changes, click **OK**.

IP Office Contact Center configuration in IP Office

You must use IP Office Manager to complete initial IP Office Contact Center setup required to integrate IP Office and IP Office Contact Center in the Cloud environment.

Configuring agent extensions

Before you begin

- Have the starting extension and extension range. An example of an extension range is 2100 to 2109.

Procedure

1. In IP Office Manager, navigate to the Configuration page.
2. For each extension beginning with the starting extension, do the following:
    a. Right-click **Extension**, and select **New** > **H.323 Extension**.
    b. In **Base Extension**, enter the extension number.
    c. Click **OK**.

Reserving global licenses

Procedure

1. In IP Office Manager, navigate to the License page.
2. Click the **Remote Server** tab.
3. In the Reserved Licenses section, locate the following fields and change the quantities as follows from the default of zero:
    a. **Voicemail Pro Ports** to 20.
    b. **VMPro Recording Administrators** to 1.
    c. **VMPro TTS Professional** to 1.
    d. **CTI Link Pro** to 1.
4. Click **OK**.

Setting the contact center type

Procedure

1. In IP Office Manager, navigate to **Contact Center** on the System page.
2. In **Contact Center**, from the **Contact Center Application** drop-down menu, select **Avaya IP Office Contact Center**.
3. Click **OK**.
4. Click **File** > **Save Configuration** to save all changes to the IP Office server.

   Although warnings regarding insufficient passwords can be ignored, Avaya recommends that you review the warnings and perform appropriate configuration corrections before concluding installation.

Configuring the time zone and NTP server

Procedure

1. In a browser, enter the Web Control URL `https://<Public IP Office IP Address>:7071`.
2. Log in with your PartnerAdministrator credentials.
3. Click **Settings** and then click **System** at the top of the page.

4. Navigate to the Date and Time section, and select the proper time zone from the **Timezone** drop-down menu.
5. Confirm that the NTP Servers dialog box displays the correct information for your deployment.

   For OnAvaya™, the NTP server values must be `0.pool.ntp.org` and `metadata.google.internal`. The NTP settings vary for Powered deployments.
6. If either of these servers is missing, add the required server to the list.
7. Click **Save**.
8. Accept the server reboot warning.

   Allow several minutes for the reboot to finish.
9. Launch the IP Office System Status application (SSA) from **Start** > **All Programs** > **IP Office** > **System Status**.
10. Confirm that the correct time of day displays in the lower right corner.

    If you recently changed the time zone configuration, allow 5 to 10 minutes for the IP Office clock to sync with the NTP server.

Configuring WebLM settings in IP Office Manager

About this task

Use IP Office Manager to configure WebLM settings in IP Office for Powered deployments.

Before you begin

Log in to IP Office Manager.

Procedure

1. In IP Office Manager, navigate to **License** > **Remote Server**.

   For more information about the settings in IP Office Manager, see “License | Remote Server” in *Administering Avaya IP Office™ Platform with Manager*.
2. Select the **Enable Remote Server** checkbox.
3. In **Domain Name (URL)**, enter `https://` followed by the DNS name or IP address of the OSS server.

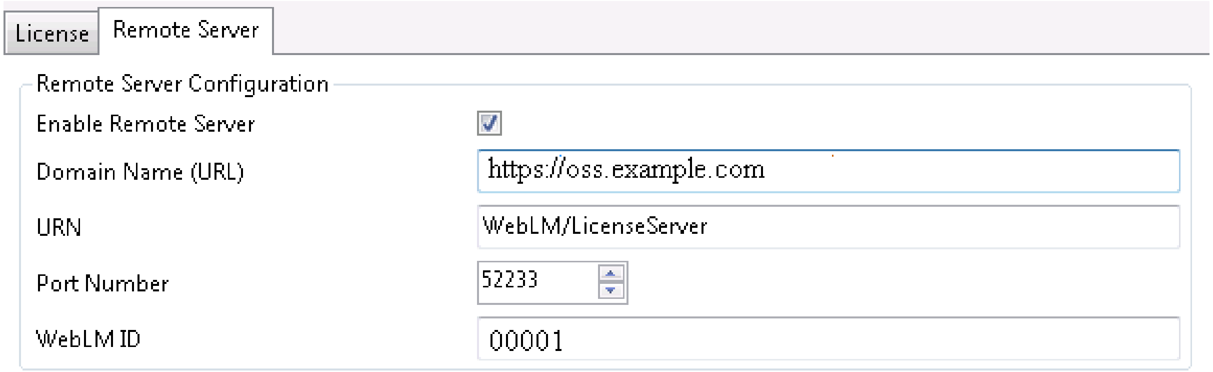
   Note:

   Do not use the loopback address 127.0.0.1.
4. In **URN**, enter the last part of the WebLM URL that comes after the port number.

   For example, `/WebLM/LicenseServer`.

After you complete the steps above, the complete WebLM URL appears in **WebLM address**. For the given examples, the complete URL would be `https://oss.example.com:52233/WebLM/LicenseServer`.

5. **(Optional)** If required, change the port number.
6. Enter the WebLM ID generated by OSS.



Remote Server Configuration

Enable Remote Server ☑

Domain Name (URL): https://oss.example.com

URN: WebLM/LicenseServer

Port Number: 52233

WebLM ID: 00001

Figure 4: WebLM settings in IP Office Manager

7. Restart IP Office after you update any WebLM settings.

Result

The system should be in WebLM Normal mode. If it is not, check the System Status Application alarms for licensing issues.

Configuring SIP trunks

About this task

The following procedure provides guidelines for configuring SIP trunks in IP Office Manager. The exact configuration process might vary depending on your SIP trunk provider.

Before you begin

- You must know the IP address of both ends of the trunk.
- Ensure that **Maximum SIP Sessions** in **System** > **Telephony** is set to a value higher than zero. The **Maximum SIP Sessions** setting determines the number of SIP Trunk Channel licenses reserved for concurrent SIP sessions on any SIP trunks provided by the server.

Procedure

1. In the Manager navigation pane, right click **Line** and select **New** > **SIP Line**.
2. Record the **Line Number** value that appears on the SIP Line page for use later.
3. In the **ITSP Domain Name** field, enter the far end's **ITSP Proxy Address**.
4. Use the default values for the remaining fields.
5. Select the **Transport** tab.

6. In the **ITSP Proxy Address** field, enter the IP Address of the far end.
7. If the Layer 4 protocol is TCP or UDP, change the value in **Send Port** and **Listen Port** to `5056`.
8. Select the **SIP URI** tab.
9. Click **Add**.
10. Enter values for the **Incoming Group** and **Outgoing Group** fields.

    You can use the **Line Number** from the **SIP Line** tab for both values.
11. In the Manager navigation page, select **Incoming Call Route**.
12. On the **Standard** tab, in the **Line Group ID** field, enter the **Line Number** from the **SIP Line** tab.
13. Select the **Destinations** tab.
14. In the **Destination** column, replace the value with a period (“.”).
15. In the Manager navigation pane, select **Short Code**.
16. Add a short code to dial the trunk you have just added.
17. Save the configuration to IP Office.

Result

One end of the trunk is now configured.

Next steps

Provide the configured SIP trunk parameters to the SIP trunk broker to use when configuring the far end of the trunk.

Configuring emergency calls

About this task

Emergency call handling is based on mapping a set of phone numbers to a physical street address. The mapping is maintained by the SIP trunk provider.

When the enterprise places an emergency call, the trunk provider routes the call based on the calling line ID. The call routes to the Public Safety Answering Point (PSAP) that handles emergency calls in the geographic area of the caller.

Important:

Do not use soft clients to make emergency calls. The users of soft clients must use a hard phone, such as a desk phone, or a mobile phone to make an emergency call directly through the PSTN, if required.

Procedure

1. Provide the SIP trunk broker with a set of Emergency Location Identification Numbers (ELINs) and their mapping to physical locations.

ELINs are special phone numbers that can be defined for each enterprise site or for each building or floor.

2. Configure IP Office to send the ELIN of the caller’s location as the calling line ID in emergency calls.

   For each enterprise location, you must configure a Location record and a respective Emergency ARS table in IP Office.

   Each Emergency ARS points to a Line Group ID of a SIP URI Channel on the SIP trunk.

   Each SIP URI Channel is dedicated to a particular enterprise location and specifies its respective ELIN as the calling line ID to set on outgoing calls.

3. Configure each site as one Location and configure IP Office to identify at which configured Location the calling endpoint is. Do one of the following:

   - Configure the Extension record of each phone statically to belong to the respective Location.
   - Configure IP Office to identify the Location automatically based on the public IP address of the site that the endpoint registers from.

     The router or NAT in the enterprise site must have a static IP address. The static IP address can be provided with the Business Internet service from some ISPs. Configure the static public IP address in the IP Office Location record for the site as the subnet address with a mask of 255.255.255.255.

Endpoint configuration

BPs must work with the enterprise to configure endpoints and telephony applications. You can configure endpoints with or without staging. The staging process is the most secure.

In the less secure configuration alternative without staging, the phone does not authenticate the server with the initial HTTPS connection. If the initial phone connection to HTTPS is hijacked to an attacker’s file server, the fraudulent file server can become trusted by the phone, and provide a misleading settings file to the phone. This could result in the phone registering to a fraudulent call server, which would comprise the integrity and confidentiality of user calls. This type of attack would require a lot of technical knowledge and would also require access to the local network of the user to hijack the initial HTTPS connection. Therefore, the risk is low and might be acceptable for some deployments. If the enterprise has higher security requirements where this risk is unacceptable, then you must stage the phones in a controlled environment.

Configuring endpoints with staging

About this task

For secure network interactions, stage the 96x1 H.323 phones with a staging file server in a secure environment before installation. The staging file server can be an IP Office or another HTTP server.

Procedure

1. Obtain the files for phone firmware version 6.6 and the `96x1Hupgrade.txt` file, which is included with IP Office.
2. Obtain the root CA certificate used to sign the IP Office identity certificate.
   - If the trust policy selected for the IP Office uses a well-known public CA, download the PEM-encoded root CA certificate from the CA's web site.
   - If the trust policy selected for the IP Office uses the internal CA, download the PEM-encoded root CA certificate from IP Office. In IP Office Web Manager, navigate to **Settings** > **General** > **Certificates** > **CA Certificate** > **Download (PEM-encoded)**.
3. Record the file name of the root CA certificate.

   By default, the file name is assumed to be `root-ca.pem`. If the file name is different, you can rename the file.
4. Obtain and edit the phone settings file.
   a. Get the automatically generated settings file from the IP Office Cloud by opening a web browser and navigating to one of the following addresses:
   b. Open a text editor such as Notepad and copy the text from the settings file.
   c. Add the following settings to the file under `SETTINGS 96X1`.

Table 4: Staging file settings

Settings to add to staging file with example value	Description
SET NVTLSSRVR ipo-001.example.com	The example `ipo-001.example.com` must be replaced with the FQDN of the Cloud IP Office. If the IP Office is using an identity certificate issued by its own internal CA, and if the IP Office does not have an FQDN that is resolvable in DNS, then replace `ipo-001.example.com` with the public IP address of the Cloud IP Office.
SET NVHTTPSRVR ipo-001.example.com	The example `ipo-001.example.com` must be replaced with the FQDN of the Cloud IP Office. If the IP Office is using an identity certificate issued by its own internal CA, and if the IP Office does not have an FQDN that is resolvable in DNS, then replace `ipo-001.example.com` with the public IP address of the Cloud IP Office.
SET NVMCIPADD ipo-001.example.com	The example `ipo-001.example.com` must be replaced with the FQDN of the Cloud IP Office. If the IP Office is using an identity certificate issued by its own internal CA, and if the IP Office does not have an

Table continues…

Settings to add to staging file with example value	Description
	FQDN that is resolvable in DNS, then replace `ipo-001.example.com` with the public IP address of the Cloud IP Office.
SET TRUSTCERTS root-ca.pem	The filename of the root CA certificate. **Note:** Depending on the file server type, additional configuration might be required for the file server to store files with the `.pem` extension. You can rename the file with the `.txt` extension.
SET TLSSRVRVERIFYID 1	When set to 1, the phone verifies that the IP address of the contacted server, as set in NVTLSSRVR, matches the Cloud identity certificate.
SET HTTPPORT “80”	TCP port number used for downloading HTTP files from a staging file server. Automatically generated settings files from IP Office Cloud point telephones to use HTTP port 8411 for downloads. Adding this line under `SETTINGS 96X1` in the staging file instructs phones to use the standard HTTP port 80 during the staging process.

d. Save the `46xxsettings.txt` file.

5. Place all the files you obtained on the staging file server.
6. Connect the phone to the secure network.

   You can use DHCP option 242 or static programming to initially point the phones to the staging file server IP address. For more information, see *Administering Avaya IP Deskphone 9608/9608G/9611G/9621G/9641G/9641GS H.323* at http://support.avaya.com.

   The phone contacts the staging file server using HTTP, gets the upgrade file, the staging settings file, and the trusted root CA certificate. If the phone is not already at version 6.6, the phone downloads version 6.6 firmware from the staging server.

Result

After staging, the phone is shipped to the enterprise site. The phone connects securely to IP Office through HTTPS over TLS using the NVTLSSRVR IP address and port 411. The phone gets the `96x1Hupgrade.txt` file and the auto-generated `46xxsettings.txt` file. The auto-generated `46xxsettings.txt` specifies the HTTP port 8411 settings.

When a new firmware version is available, the phone downloads the firmware files through HTTP on port 8411.

Endpoint configuration without staging

You can choose to configure endpoints without staging using one of the following procedures. This approach is less secure than the staging approach.

Using an internal Certificate Authority or a third party Certificate Authority

About this task

If you are using the IP Office internal CA, you need to generate the IP Office identity certificate so that it includes the IP Office public IP address in a Subject-Alt-Name entry. The identity certificates issued by third-party certificate authorities include only the IP Office FQDN or a wild-card FQDN. Public CAs do not usually support IP addresses. To ensure success in configuring endpoints when using third-party certificates, the phones can be provisioned with the IP Office FDQN either by staging or through the manually-edited settings file as specified in this procedure.

Procedure

1. If you have an identity certificate issued by a third party CA, install the certificate on IP Office before installing phones.

   The identity certificate must include the IP Office FQDN.

   ⚠ **Warning:**

   If phones have previously been installed and provisioned to trust the IP Office internal CA, and you later install an identity certificate issued by a different CA, the phones can get locked out. If this situation occurs, the configuration of the phones must be cleared.

   Important:

   You do not need to perform this step if you want to use an identity certificate generated by the IP Office internal CA.

2. Obtain the PEM-encoded root CA certificate of the CA that issued the IP Office identity certificate.

   - If the trust policy selected for the IP Office uses a well-known public CA, download the PEM-encoded root CA certificate from the CA's web site.
   - If the trust policy selected for the IP Office uses the internal CA, download the PEM-encoded root CA certificate from IP Office. In IP Office Web Manager, navigate to **Settings** > **General** > **Certificates** > **CA Certificate** > **Download (PEM-encoded)**.

3. Record the file name of the root CA certificate.

   By default, the file name is assumed to be `root-ca.pem`. If the file name is different, you can rename the file.

4. Place the file of the root CA certificate on the IP Office.

   - If you are using the File Manager, which is accessible from the **Applications** menu in Web Manager, then navigate to the Folders list and place the file at `Disk/system/primary/`.
   - If you are using Embedded File Management in IP Office Manager, then place the file at `/opt/ipoffice/system/primary/`.

5. Get the automatically generated settings file from the IP Office Cloud by opening a web browser and navigating to one of the following addresses:

   - `https://<FQDN of IP Office Cloud>/46xxsettings.txt` for the third-party CA.

- https://<Public IP Address of IP Office Cloud>/46xxsettings.txt for the internal CA.

6. Open a text editor such as Notepad and copy the text from the settings file.
7. Add the following lines in the 96x1 settings area of the file under SETTINGS 96X1:
    - If the IP Office is using its internal root CA certificate:

      ```
      ## The following two lines were manually added
      SET TRUSTCERTS root-ca.pem
      SET TLSSRVRVERIFYID 1
      ```

    - If the IP Office is using an identity certificate issued by a third-party:

      ```
      ## The following five lines were manually added
      SET TRUSTCERTS root-ca.pem
      SET TLSSRVRVERIFYID 1
      SET NVTLSSRVR ipo-001.example.com
      SET NVHTTPSRVR ipo-001.example.com
      SET NVMCIPADD ipo-001.example.com
      ```

      You must replace ipo-001.example.com with the FQDN of the IP Office instance.
8. If required, modify the text root-ca.pem on the TRUSTCERTS line to match the name of the root CA certificate file you placed on IP Office in step 4 on page 54.
9. Save the manually edited 46xxsettings.txt file and place the file on IP Office at the paths described in step 4 on page 54.
10. When you are ready to set up the phones, use the CRAFT menu on each phone to set the HTTPS Server IP Address parameter to the public IP address of IP Office.

    If the IP Office is using its internal root CA certificate, set the following additional parameters to the public IP address of IP Office:

    - HTTP Server IP Address
    - Call Server IP Address
11. Reboot the phone.

    The phone displays error messages and might automatically reboot again after approximately 20 seconds.
12. If the phone does not reboot automatically, reboot the phone again manually.

    After the second reboot, the phone will connect to IP Office successfully.

Using DHCP option 242

About this task

If you can set up DHCP Scope options on the DHCP server at the local site where the phones are being installed, you can use the following variant of the above procedure. This variant delivers the server’s FQDN to the phone through DHCP option 242, so you do not need to provide the FQDN from the settings file or enter the server IP address on the phone's CRAFT menu.

Procedure

1. In the Scope options for the DHCP server, enter the following line to configure option 242:

   ```
   TLSSRVR=ipo-001.example.com,HTTPSRVR=ipo-001.example.com,MCIPADD=ipo-001.example.co
   m
   ```

   You must replace `ipo-001.example.com` with the FQDN of the IP Office instance.
2. Follow steps 1 on page 54 to 6 on page 55 in the previous procedure.
3. Add the following lines in the 96x1 settings area of the file under `SETTINGS 96X1`:

   ```
   SET TRUSTCERTS root-ca.pem
   SET TLSSRVRVERIFYID 1
   ```
4. Follow steps 8 on page 55 and 9 on page 55 in the previous procedure.

Result

When you install a new phone or use the CRAFT menu to clear an existing phone, the phone will get the server FQDN from the DHCP and will successfully connect to the server.

Hybrid Cloud configuration

The following sections describe how to configure Hybrid Cloud functionality, which allows you to deploy IP500 V2 expansion systems in the Cloud.

Configuring the IP500 V2 expansion system

Before you begin

- The IP500 V2 expansion system must be in the private IP address subnet and the IP Office primary server must be in the public IP address subnet.
- IP500 V2 must be on the same load as the primary IP Office server.

Procedure

1. Upgrade the IP500 V2 system to the Cloud load on the IP Office server.
2. Run the IP Office Initial Configuration Utility (ICU) and complete the following details:
   a. For **System Type**, select **Server Edition Expansion**.

   b. Select the **Activate IP Office Select Mode** check box.

   c. If an old connection needs to be retained, select the **Retain Configuration Data** check box.

   d. Select the **Hosted Deployment** check box for Powered deployments.

   e. Complete the **System Name** field.

   You can use a mixture of numeric or alphabetic characters.

   f. Complete the **Web Socket Password** field to establish an SCN line with the primary IP Office server.

   g. From **Locale**, select the geographical region.

   h. Select the appropriate LAN interface, and enter the appropriate IP address details.

      This information is used to select Network Interface Cards (NICs) on IP Office.

   i. Enter the IP address for the primary IP Office in **Server Edition Primary**.

   j. Enter the IP address for the secondary IP Office in **Server Edition Secondary**.

   k. Enter the DNS IP Address in **DNS Server**

   l. Ensure **DHCP Mode** is set to **Disabled**.

3. To make and answer calls, configure the following settings in **LAN1** > **VoIP**:

   a. Select the **H.323 Gatekeeper Enable** check box.

   b. Select the **H.323 Remote Extension Enable** check box.

   c. Select the **SIP Trunks Enable** check box.

   d. Select the **SIP Registrar Enable** check box.

   e. In **SIP Domain Name** and **SIP Registrar FQDN**, enter the same values that are used for the primary IP Office server.

4. In **LAN1** > **Network Topology**, configure the following settings:

   a. In **Pubic IP Address**, enter the public NAT for the private IP500 V2 expansion system on IP Office.

   b. In **Firewall/Nat Type**, select **Unknown**.

   c. Leave the other settings at their default values.

Result

After the configuration is complete:

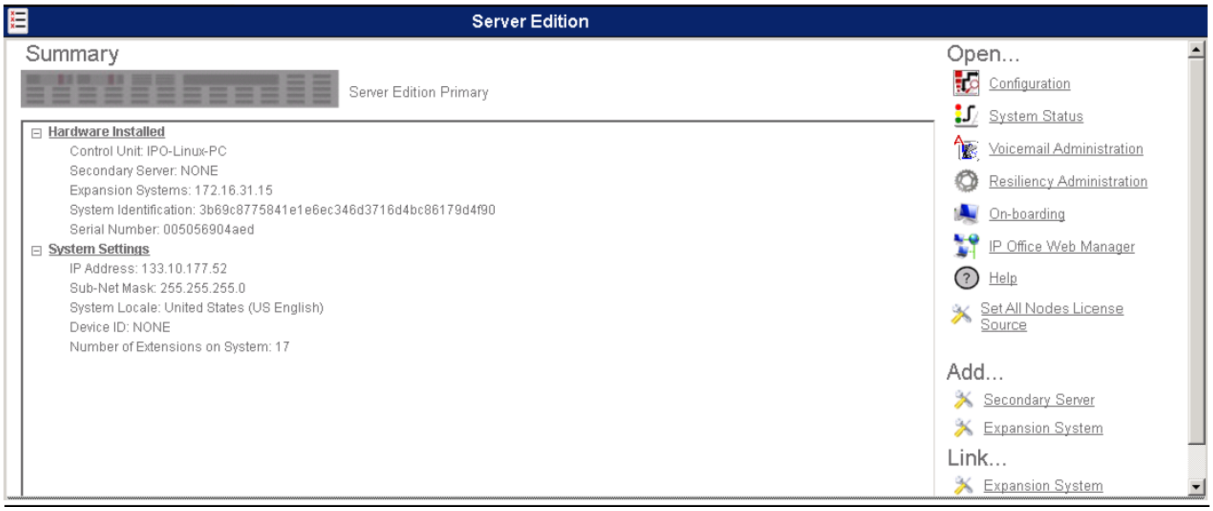
- The SCN trunk is created for the IP500 V2 expansion system.
- In **License** > **Remote Server**, the details are automatically populated based on the data entered when you ran the ICU.

Configuring the primary IP Office server

Procedure

1. Use the public address location to access the primary IP Office server.

   The following is an example of the view you see:



Server Edition

Summary

Server Edition Primary

⊟ Hardware Installed
Control Unit: IPO-Linux-PC
Secondary Server: NONE
Expansion Systems: 172.16.31.15
System Identification: 3b69c8775841e1e6ec346d3716d4bc86179d4f90
Serial Number: 005056904aed

⊟ System Settings
IP Address: 133.10.177.52
Sub-Net Mask: 255.255.255.0
System Locale: United States (US English)
Device ID: NONE
Number of Extensions on System: 17

2. Select **Add** > **Expansion System** and do the following:

    a. Enter the public IP address of the IP500 V2 expansion system.

    b. Click 🔍 and click **OK**.

    After the synchronization is complete, the public IP address automatically becomes the IP address of the internal IP500 V2 expansion system.

3. For resiliency, select **SCN Resiliency Options** on the SCN trunk.

IP Office Contact Center configuration

In the Cloud environment, many IP Office Contact Center settings are configured automatically. For a list of IP Office Contact Center settings that are configured automatically, see *OnAvaya™ and Powered by IP Office and IP Office Contact Center Reference Configuration for Business Partners*.

As a BP, you must complete initial provisioning for IP Office Contact Center. You can perform additional configuration tasks, such as configuring agents and agent groups, from the Administration tab in the IP Office Contact Center User Interface for Windows.

Important:

In the Public Network deployment, you can only access the IP Office Contact Center User Interface for Windows through a remote desktop protocol (RDP) session to perform administration tasks and assign privileges. With the Private network deployment, you can deploy IP Office Contact Center User Interface for Windows at your site.

Use the following sections in combination with *Avaya IP Office Contact Center Installation Task Based Guide* to configure IP Office Contact Center.

IP Office Contact Center configuration checklist

Initial configuration

The following checklist outlines the configuration tasks you must perform in IP Office Contact Center before you can make a call. These initial configuration tasks must be performed in order.

No.	Task	Required by BPs with OnAvaya™	Required by BPs with Powered	✔
1	Complete initial IP Office Contact Center provisioning. You can provision IP Office Contact Center using one of the following options: • Configuration zip file • Configuration Wizard screen in the web-based administration portal	✔	✔	
2	Configure automatic synchronization. Once provisioning is complete, you must confirm that automatic synchronization succeeded and create an IP Office Contact Center synchronization account.	✔	✔	
3	Configure agents as power users. You can set up agents as power users in IP Office Manager after automatic synchronization is complete.	✔	✔	
4	Configure the WebLM client ID and URL. WebLM is embedded within OSS. For information about configuring OSS and the embedded WebLM, see *Deploying Avaya Operations Support System*.		✔	
5	Configure additional agents and agent groups. You can set up IP Office Contact Center agents, groups, and profiles as part of the initial IP Office Contact Center provisioning. When setting up users, you can define privileges. You can also create and edit agents and agent groups using the Configuration tab in the IP Office Contact Center User Interface for Windows.	✔	✔	

Table continues…

No.	Task	Required by BPs with OnAvaya™	Required by BPs with Powered	✔
	Important: In the Public Network deployment, you can only access the IP Office Contact Center User Interface for Windows through a remote desktop protocol (RDP) session to perform administration tasks and assign privileges. With the Private network deployment, you can deploy IP Office Contact Center User Interface for Windows at your site.			
6	Configure call flows. The initial provisioning configures the initial default call flow automatically. To further refine and enhance call flows, you can configure IVR Editor and Task Flow Editor scripts to define IP Office Contact Center telephony and dialer options in the IP Office Contact Center User Interface for Windows. For more information, see *Administering Avaya IP Office Contact Center IVR Editor* and *Administering Avaya IP Office Contact Center Task Flow Editor* .	✔	✔	

Additional configuration settings

The following checklist outlines additional configuration you can perform in IP Office Contact Center. The order in which you perform these additional configuration tasks is not important.

Task	Applies to BPs with OnAvaya™	Applies to BPs with Powered	✔
Configure call recording. You can optionally integrate IP Office Contact Center with Avaya Contact Recorder. Calls are recorded with Voicemail Pro and the details of the complete recording are stored in the Avaya Contact Recorder database. You can search for and manage recordings using a web browser. For information about Avaya Contact Recorder configuration, see Optional Avaya Contact Recorder configuration for IP Office and IP Office Contact Center on page 75.	✔	✔	

Table continues…

Task	Applies to BPs with OnAvaya™	Applies to BPs with Powered	✔
Configure additional web components and plug-ins. You can configure Wallboard, and SAP or Salesforce (SFDC) CRM connectors. For more information, see the following: • *Using Avaya IP Office Contact Center Wallboard* for information about setting up and using Wallboard. The Wallboard component enables you to view and modify statistics. • *Avaya IP Office Contact Center Installation Task Based Guide* for information about setting up CRM connectors that you can use to access agent telephony functionality.	✔	✔	
With the Powered deployment, customize the branding for the IP Office Contact Center User Interface for Chrome Devices and the IP Office Contact Center Web User Interface. This customization is optional.		✔	

IP Office Contact Center provisioning

Choose carefully the appropriate provisioning method for IP Office Contact Center from the following:

- Configuration spreadsheet
- Configuration Wizard in the web-based administration portal

Provisioning IP Office Contact Center with a configuration spreadsheet

About this task

Use the following procedure to provision IP Office Contact Center using configuration files instead of the Configuration Wizard in the administration portal. With this provisioning method, a Configuration workbook spreadsheet in Excel is used to generate configuration files on a Windows computer. The workbook creates the following files:

- `DataImport.zip`: A zip archive containing `.sql` and `summary.txt` database files.
- `DataImport.exe`: A Windows executable that populates the IP Office Contact Center database.
- `Configuration.csv`: A table structured data file that configures the IP Office integration for IP Office Contact Center.

For more information about using the Excel workbook method, see the Excel spreadsheet configuration data detailed instructions in *Avaya IP Office Contact Center Installation Task Based Guide*.

Procedure

1. Download the blank Excel workbook from the IP Office Contact Center server to your computer.

   Using this version of the workbook guarantees compatibility between the workbook and the IP Office Contact Center that you are configuring.

2. Edit the workbook on your computer and complete all required fields.

   a. Use the values from your deployment planning.

   b. Enter the values as instructed with the Cloud-specific exceptions described in Configuring Cloud settings in the Excel workbook on page 62.

3. Activate **Create Data Import** to create the three configuration files.

4. Open an RDP session, and back up the current IP Office Contact Center database using the information in *Avaya IP Office Contact Center Maintenance Task Based Guide*.

5. Use the IP Office Contact Center web-based administration portal to upload and execute `DataImport.zip` and `DataImport.exe` to the IP Office Contact Center server.

6. Use IP Office Manager to import `Configuration.csv` to IP Office.

7. Restart the system for your changes to take effect.

Next steps

After the system reboot is complete, perform configuration for automatic synchronization. Verify that the synchronization succeeds and then configure agents as power users.

Related links

Verifying automatic synchronization configuration on page 68

Configuring Cloud settings in the Excel workbook

About this task

The following procedure describes the Cloud-specific settings you must configure if you are using the Excel workbook to provision IP Office Contact Center.

Before you begin

Ensure you have the Excel workbook open.

Procedure

1. In the **Base Data** tab, do the following:

   a. On the PBX panel, click the red “Change Me” cell, and enter the IP Office Contact Center server hostname.

   b. Change the IP Office service port from `8443` to `7070`.

   c. To use email and chat, enter the required email and chat server settings.

   For more information about populating email and chat server settings, see *Avaya IP Office Contact Center Email and Chat Services Task Based Guide*.

> **Note:**
>
> For the chat server, in the Cloud, use the internal IP Office IP address rather than the public IP address. You can use the public IP address as the domain name.

2. In the **Chap** tab, do the following:
    a. In **Local IP Address**, enter the IP Office Contact Center private IP address.
    b. In **PBX IP Address**, enter the IP Office private IP address.
    c. In **SIP Domain**, enter the IP Office server public IP address.
    d. In **DNS Server IP**, enter the IP Office server private IP address.
    e. Change **PBX Signal Port** from `5060` to `5056`.
3. In the **Agent Groups** tab, do the following:
    a. In the Email section, remove the three `X` values in the **Task Type Email** fields.
    b. In the Email section, remove the three `0` values in the **Sign Off Prevention** fields.
4. In the **Profiles** tab, leave all fields blank.
5. In the following tabs, clear all fields in the Email section:
    - **Agents**
    - **Topics**
    - **Topic — AG Assignment**
6. In the **Job Codes** and **Time Off** tabs, do not modify any settings.

Provisioning IP Office Contact Center with the administration portal

About this task

Use the following procedure to provision IP Office Contact Center using the Configuration Wizard in the web-based administration portal. Some configuration data is automatically populated in the Configuration Wizard. For detailed information, see the following documents:

- *Using Avaya IP Office Contact Center Web Administration Portal*
- Administration Page content in *Avaya IP Office Contact Center Installation Task Based Guide*

Procedure

1. Log in to the web-based administration portal.

    The URL of the administration portal has the following format: `https://<IPOCC Public IP Address>:28443/Administration`.

    The default username is `Administrator` and the default password is `Administrator`.
2. Open the Configuration Wizard.

    On first access, the Configuration Wizard starts automatically.
3. Complete the information in all sections and then preview your changes as described in the subsequent procedures.

4. Submit your changes and restart the system.

Next steps

After the system reboot is complete, perform configuration for automatic synchronization. Verify that the synchronization succeeds and then configure agents as power users.

Performing system configuration

About this task

In the Cloud environment, some information is pre-populated in the Configuration Wizard. For detailed information about the fields in the IP Office Contact Center administration portal, see *Using Avaya IP Office Contact Center Web Administration Portal*.

✱ **Note:**

The default signaling port number is set to `5056`.

Procedure

1. In the Configuration Wizard, open the System screen.
2. **(Optional)** Review the pre-populated information in the **IP Office Data** tab.

   The following values are automatically populated:

   - IP Office IP Address
   - IP Office Service Password
   - IP Office System Password
3. In **IP Office Contact Center SIP Connection Setup (CHAP Configuration)**, do the following:

   a. **(Optional)** Change the pre-populated local IP address, local signaling portal, and DNS server IP address values.

   b. **(Optional)** Change the pre-populated IP Office signaling port and SIP extension.

   c. In **SIP Password**, type the password for the SIP extension assigned to IP Office Contact Center in IP Office.

      This password is numeric only.

   d. In **SIP Domain**, type the domain name, which should be the same as the domain name in IP Office.

      In the Cloud environment, the SIP domain must be the public IP address for the IP Office instance.
4. To proceed to the next screen, click **Next**.

Next steps

Complete the fields in the Group and Profile screen.

Configuring groups and profiles

About this task

Use the following procedure to configure agent group assignments and privileges. You can configure agent groups consisting of agents and agent profiles.

Note:

Topic and agent group mapping must match the mapping in the task flow for the telephony, email, and chat channels. For example, if you create a new topic with telephony, chat, and email enabled, this topic must be mapped to a specific agent group. You must also enable the appropriate channels (in this case, telephony, chat, and email) in the agent group. The task flow of all channels for the topic must map to this agent group only.

Before you begin

If you want to enable email and chat for your groups, you must complete the information in the Email and Chat screen.

Procedure

1. To add a new group, click **Add Group** and then do the following:
    a. Enter a name for the new group.

       By default, the group name displays as `Group X`, where X is the number of the group.

    b. Enter a topic name.

    c. To enable telephony, select the **Enable Telephony** check box.

       The Configuration Wizard assigns a read-only topic ID to each group. The short code that IP Office uses to direct incoming calls to the agent group must match the topic ID.

    d. To enable email, select the **Enable Mailbox** check box and then enter an email or mailbox address, user name, and password for the group.

    e. To enable chat, select the **Enable Chat** check box and then enter a chat address for the group.

2. To add a new profile, click **Add Profile** and then do the following:
    a. Enter a name for the new profile.

    b. From **Privileges**, select **Agent** or **Supervisor**.

    c. In **Group**, enter the group to which you want to associate the profile.

3. **(Optional)** To delete a row, click 🗑.

4. **(Optional)** To view the previous screen, click **Previous**.

5. To proceed to the next screen, click **Next**.

Next steps

Complete the fields in the User screen.

Configuring users

About this task

Use the User screen to configure IP Office Contact Center users.

Procedure

1. In **Number of Users**, type the required number of users, which must not exceed the number of licenses ordered.
2. In **Profile Name**, select a profile.

   The available profiles are based on what you created in the Group and Profile screen.
3. In **Start Extension Number**, type a phone extension number.

   The starting extension number must be consistent with the IP Office dial plan. The Configuration Wizard creates a range of sequential extensions for all users starting with this extension, and those extensions must not already be assigned for other purposes in IP Office.
4. To add the users, click **Add User**.
5. For each user, provide the following information:
   1. In the **Name** column, type a name that you can use to identify each user.

      You can choose to keep the name generated by the Configuration Wizard, and then change the name later.

      ⚠ **Warning:**

      The name cannot exceed 15 characters, or it will be truncated, causing IP Office and IP Office Contact Center name mismatches.
   2. If telephony is enabled for the user, enter an extension.
   3. If email is enabled for the user, enter a Reply-To and From address.
   4. To change the profile assigned to a specific user, select the appropriate profile from the **Profile Name** column.

      For example, you can assign a supervisor profile to some users and keep the standard agent profile assigned to other users.

      ❗ **Important:**

      Do not exceed the number of agent or supervisor licenses ordered.
6. **(Optional)** To delete a row, click 🗑.
7. **(Optional)** To delete all existing users, click **Delete All Users**.

   The **Number of Users** and **Start Extension Number** fields become blank and the generated list of users is cleared.
8. **(Optional)** To view the previous screen, click **Previous**.
9. To proceed to the next screen, click **Next**.

Next steps

Complete the fields in the Time Off screen.

Configuring time off

About this task

You can configure breaks and break repetitions in IP Office Contact Center.

Procedure

1. To add a new time off period, click **Add Time Off**.
2. Enter the name of each holiday or vacation period.
3. Select any one of the following recurrences:
   - None
   - Daily
   - Weekly
   - Yearly
4. If the recurrence is weekly, do the following:
   a. In **Begin Week**, click a start day, such as Monday.
   b. In **End Week**, click an end day, such as Friday.
5. If the recurrence is yearly, do the following:
   a. In **Begin Date**, click a start date.
   b. In **End Date**, click an end date.
6. In **Begin Time**, enter a start time.
7. In **End Time**, enter an end time.
8. **(Optional)** To delete a row, click 🗑.
9. **(Optional)** To view the previous screen, click **Previous**.
10. To proceed to the next screen, click **Next**.

Next steps

Review your configuration changes in the Preview screen.

Previewing configuration changes

About this task

The Preview screen displays the configuration changes in a read-only format. After you save the configuration, a background service moves the configured data into IP Office.

Procedure

1. Review your changes.

2. **(Optional)** Click **Download Configuration PDF** to download a PDF with your configuration data.
3. Do one of the following:
    - To make a change, go back to the appropriate screen and edit the information. You can also use the **Previous** button to return to the previous screen.
    - To accept and save your changes, click **Save**.
4. After you save your changes, in the Confirmation dialog box, click one of the following: .
    - **Yes**: Save your data in the IP Office Contact Center database and restart your system.
    - **No**: Prevent the system from restarting.

Related links

Configuring agents as power users on page 69

Verifying automatic synchronization configuration

About this task

Use the following procedure to confirm that automatic synchronization succeeded.

Before you begin

Complete IP Office Contact Center provisioning with the web administration portal Configuration Wizard or the configuration spreadsheet.

Procedure

1. Log in to IP Office Manager.
2. Select **Configuration** > **User**.

    Confirm that all agent users configured in IP Office Contact Center are also created in IP Office by automatic synchronization.
3. Select **Short code**.
    a. Confirm that the IP Office Contact Center short code is available.

    This short code is the dialled number that redirects incoming contact center calls to the IP Office Contact Center SIP extension.

    b. Confirm that the values in **Code** and **Telephone Number** match the values that you provided when provisioning IP Office Contact Center.
4. Select **Extension**.
    a. Select the extension used for the IP Office Contact Center SIP line.

    b. Confirm that **Device type** on the **Extn** tab is set to “IP Office Contact Center”.

Note:

If the display shows `Unknown SIP Device` instead, then IP Office Contact Center has not successfully registered its SIP extension with IP Office. You will not be able to make incoming calls with IP Office Contact Center until the registration is complete.

Next steps

Create the IP Office Contact Center synchronization account using the detailed procedure about creating new accounts for automatic synchronization in *Avaya IP Office Contact Center Installation Task Based Guide*.

Configuring agents as power users

Procedure

1. Log in to IP Office Manager using your PartnerAdministrator credentials.
2. Select **Configuration**.
3. Navigate to **User** in the **Configuration** column.
4. For each configured agent user, select **Power User** in the **Profile** field, and click **OK**.
5. Click **File** > **Save Configuration** to download the changes to the IP Office server.

   Although warnings regarding insufficient passwords can be ignored, Avaya recommends that you review the warnings and perform appropriate configuration corrections before concluding installation.

Result

Initial configuration is now complete. Agent and back office user can generate test calls by dialing the IP Office Contact Center short code. They can also call each other by dialing assigned extensions. External Contact Center calls can be tested once the IP Office SIP trunk to the ITSP is configured.

Configuring WebLM information in IP Office Contact Center for Powered

About this task

You can track and edit WebLM license details in the administration portal. You can also see a list of deployed IP Office Contact Center licenses for the Powered environment.

Procedure

1. Click **Settings** > **License**.

   The License Manager screen is displayed.

2. In **WebLM address**, enter the first part of the WebLM URL or location that comes before the port number.

   For example, `https://oss.example.com`.

3. In **Port Number**, enter `52233`.

   This is the WebLM port number.

4. In **URN**, enter the last part of the WebLM URL that comes after the port number.

   For example, `/WebLM/LicenseServer`.

   After you complete the steps above, the complete WebLM URL appears in **WebLM address**. For the given examples, the complete URL would be `https://oss.example.com:52233/WebLM/LicenseServer`.

5. Enter the WebLM CLID generated by OSS.

   For example, `00001`.

6. Click **Save**.

Creating agents and agent groups

About this task

You created initial agents and agent groups when provisioning IP Office Contact Center. Use this procedure to create additional agents and agent groups in theIP Office Contact Center User Interface for Windows.

Important:

With the Public Network deployment, you must access IP Office Contact Center User Interface for Windows through a remote desktop connection with your PartnerAdministrator credentials.

Procedure

1. In the IP Office Contact Center User Interface for Windows, click **Configuration**.

   You can access **Configuration** from the **Administration** tab or the **Go to** menu.

2. Configure a telephone extension for the agent you plan to add.

   a. In the **Telephone** tab, click **Create**.

   b. If prompted, select a PBX line for the telephone.

   c. On the Create window, in **Start no.**, enter the new telephone extension for the agent.

   d. Click **OK**.

3. To create agents, perform the following actions:

   a. In the **Agent** tab, click **Create**.

   b. Enter a system name.

   c. Enter a login name for the agent.

   d. Enter the last name for the agent.

   e. Select the **Telephony** check box.

   f. Click the **Password** button, and provide the password for the agent extension.

   g. Select the **Telephony** tab.

   h. In **Number**, enter the extension of the agent configured in step 2 on page 70.

   i. In **Group assignment**, add, move, or delete the telephony groups to which the agent is assigned if required.

   j. Click **OK** when you finish creating the agent.

   For information about the agent configuration settings, see *Administering Avaya IP Office Contact Center Configuration Module*, chapters *Configuring agents* and *Adding agent profiles*.

4. To create agent groups, perform the following actions:

   a. In the **Agent groups** tab, click **Create**.

   b. Enter the required settings.

   c. Click **OK**.

   For information about the agent group configuration settings, see *Administering Avaya IP Office Contact Center Configuration Module*, chapters *Configuring agents* and *Adding agent profiles*.

5. To create a virtual agent group, perform the following actions:

   a. In the **Agent groups** tab, click **Create virtual AG**.

   b. In the **Name** field, type `ChromeAppAG` as the name for the agent group.

   c. Click **OK**.

Next steps

Assign all applicable agent groups to the virtual agent group *ChromeAppAG*.

Integrating IP Office Contact Center with CRM systems

About this task

The following procedure provides guidelines for configuring IP Office Contact Center integration with the SAP CRM connector or Salesforce (SFDC) CRM plug-in. For detailed CRM installation and configuration instructions, see *Avaya IP Office Contact Center Installation Task Based Guide*.

Procedure

1. Open the CRM folder in the IP Office Contact Center installation package.

2. To set up the SAP connector, do the following:

   a. Run the `Contact Center ICI Connector` installer and follow the instructions to complete the installation.

   b. Add the SAP connector to IP Office Contact Center Watchdog if you want the SAP connector to automatically start with IP Office Contact Center.

   c. Configure the SAP connector and verify IP Office Contact Center settings.

3. To set up the SFDC plug-in, do the following:

   a. Stop IP Office Contact Center Watchdog.

   b. Run the `CRMConnector` installer and follow the instructions to complete the installation.

   c. Configure the `CRMConnector` properties file.

   d. Restart IP Office Contact Center Watchdog.

   e. Install the SFDC web application from https://appexchange.salesforce.com/ or http://www.salesforce.com/.

   f. Add your custom logo to the SFDC plug-in.

   g. Configure IP Office Contact Center server details in SFDC.

   h. Configure the soft phone layout for agents. For more information, see http://help.salesforce.com/htviewhelpdoc?id=cti_admin_phonelayoutscreate.htm.

Customizing the user interface branding

About this task

With the Powered deployment, Business Partners can customize the default application branding and logo on the Login and Home screens of the Chrome and Web UIs.

Before you begin

Ensure that you are familiar with the application branding and logo specifications.

Procedure

1. Create a custom branding directory on the server at:

   ```
   C:\Program Files (x86)\Avaya\IP Office Contact Center\Tomcat WWW
   \webapps\branding
   ```

2. Add the new branding and Powered logo images into the directory.

   Your new images must meet the specifications described in Application branding and logo specifications on page 73.

3. In the Chrome or Web UI, do the following:

   a. Open the UI and accept security certificates if prompted.

      The UI displays the default branding and logo images.

   b. Close and reopen the UI to see the new custom images you added to the branding directory.

Note:

If you are using the IP Office Contact Center Web User Interface, clear your browser cache so the latest application branding and logo images appear in the UI.

Application branding and logo specifications

When you customize the application branding and logo, your new images must meet the same specifications as the default images.

Application branding specifications

Image format	PNG
Image name	• For the Login screen: `brandname_login_image.png` • For the Home screen: `brandname_home_image.png`
Size	• For the Login screen: 256*97 pixels • For the Home screen: 292*28 pixels

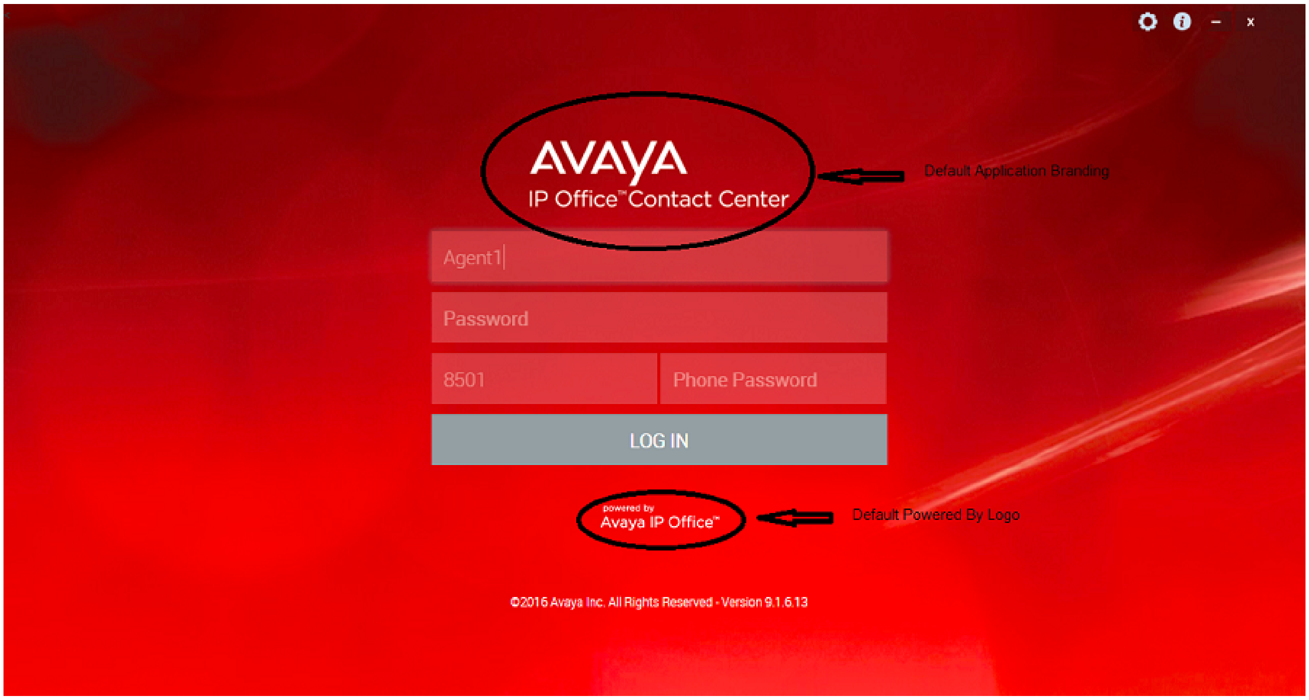
Powered logo specifications

Image format	PNG
Image name	`poweredby_login_image.png` for both screens
Size	118*96 pixels

Default branding in the user interface

The following images show the default application branding and Powered logo on the Login and Home screens of the Chrome and Web UIs.

Default Login screen application branding and logo



Default Application Branding

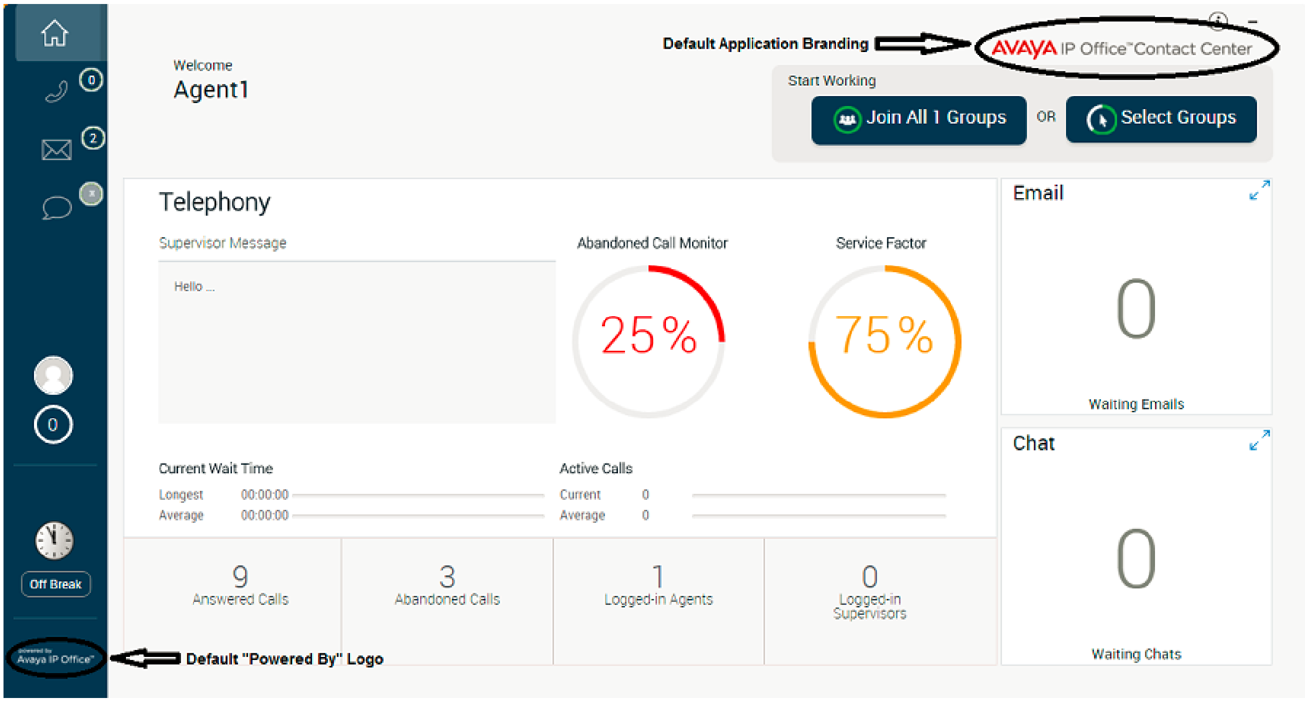
Default Powered By Logo

Agent1

8501

©2016 Avaya Inc. All Rights Reserved - Version 9.1.6.13

Default Home screen application branding and logo



Default Application Branding

Default "Powered By" Logo

Welcome

Agent1

Supervisor Message

Hello ...

Abandoned Call Monitor

25%

Service Factor

75%

Current Wait Time

Longest 00:00:00

Average 00:00:00

Active Calls

Current 0

Average 0

9 Answered Calls

3 Abandoned Calls

1 Logged-in Agents

0 Logged-in Supervisors

Email

0

Waiting Emails

Chat

0

Waiting Chats

Optional Avaya Contact Recorder configuration for IP Office and IP Office Contact Center

Partners can set up Avaya Contact Recorder with IP Office, and then integrate Avaya Contact Recorder with IP Office Contact Center to enable call recording functionality. For more information, see the following documents:

- *Installing Avaya IP Office™ Platform Contact Recorder* to set up Avaya Contact Recorder with IP Office.
- *Avaya IP Office Contact Center Contact Recorder Configuration Task Based Guide* to configure integration between Avaya Contact Recorder and IP Office Contact Center.

Important:

When integrating Avaya Contact Recorder with IP Office Contact Center, you require an additional hard disk drive (HDD) for Avaya Contact Recorder. When setting up the additional HDD, ensure you verify the mount points on the Avaya Contact Recorder server and the web-based management console.

Call storage path for OnAvaya™

When you configure the call storage path for Avaya Contact Recorder, you must have the instance name, which is provided in the initial email you receive from Avaya. The call storage path must also be followed by `partition1`, where “1” is the number of partitions on the drive. For OnAvaya™, this number is always “1”.

For example, the call storage path setting might be `/additional-hdd/ipo-00022-secondary/partition1`.

Google Chrome Management Console

Business Partners are responsible for Chrome Management Console (CMC) and Chrome UI configuration. The CMC tracks all user devices, and service updates are automatically distributed to users.

For more information about working with the CMC, see the following online resources:

Topic	Link
Getting started with the Administration console	https://support.google.com/a/answer/55955?hl=en
Console feature map administration	https://support.google.com/a/answer/3035631?hl=en
Application and extension management	https://support.google.com/chrome/a/answer/1375694?hl=en
Certificate and network management	https://support.google.com/chrome/a/answer/2634553?hl=en&ref_topic=4386934

Configuring the Chrome Management Console

About this task

Use the guidelines in the following procedure to configure the CMC and the Chrome UI for end users.

Note:

CMC is optional for Powered.

Before you begin

- Complete IP Office and IP Office Contact Center configuration.
- Know how many end users will need extensions and access to the Chrome UI application.

Procedure

1. Sign up for the Administration console.
2. Set up IP Office Contact Center User Interface for Chrome Devices applications for end users.
3. Set up user extensions.
4. Set up device restrictions if needed.
5. Upload certificates to the Administration console so the user devices can get the certificates.
6. Register users and managed devices.

Chapter 6: Administration

BPs are responsible for administration tasks in the Powered solution. You must perform administration separately for IP Office, IP Office Contact Center, and Avaya Operations Support System (OSS). The process for administering IP Office and IP Office Contact Center Cloud instances is the same as for CPE deployments.

Administration tasks

BPs are responsible for administration tasks in the Powered solution. The following table describes key administration tasks that you can perform:

Task	Description		
	IP Office	IP Office Contact Center	OSS
Update settings and user information.	Use IP Office Manager to update settings and perform configuration.	Use the Administration tab in the IP Office Contact Center User Interface for Windows. **! Important:** With the Public Network deployment, you must access IP Office Contact Center User Interface for Windows through a remote desktop connection with your PartnerAdministrator credentials.	Use the OSS interface to update your configuration settings, add and edit users, and change your password.
Monitor components	Use the System Status Application to check the status of IP Office components. You can also view information on system resources, alarms, and call details.	You can use the Watchdog service to monitor components. You can also use the Watchdog to start and stop IP Office Contact Center applications.	You can check alerts and the status of your subscriptions in the OSS interface. You can also choose to receive emails about OSS

Table continues…

Task	Description		
	IP Office	IP Office Contact Center	OSS
			alarms in the OSS configuration settings.
Run system diagnostics and troubleshooting	Use IP Office System Monitor to assist you in performing a diagnosis of system issues.	You can use TTrace to assist you in performing a diagnosis of system issues.	You can view logs and alarms in the OSS interface.
Backup and restore	Use IP Office Web Manager to back up files and servers. Use the backup versions to restore IP Office.	You must back up and restore IP Office Contact Center databases individually. You can perform backups manually, or you can set automatic database backups.	You choose a backup location when you configure OSS. You can use the latest backup to restore OSS.
Upgrade	You can perform upgrades in IP Office Web Manager. You must download an ISO file before you can upgrade.	You can upgrade directly from a previous IP Office Contact Center release. Before performing an upgrade, you must back up your current databases. You can also upgrade your server capacity when you upgrade IP Office Contact Center.	You can configure automatic updates or run a command to upgrade OSS manually.

Reference documents for administration

Product	Documents
IP Office	• For information about monitoring with the System Status application, see *Using Avaya IP Office™ Platform System Status Application*. • For information about backing up IP Office servers and restoring them from Web Manager, see *Administering Avaya IP Office™ Platform with Web Manager*. • For general configuration and administration options available with IP Office Manager see *Administering Avaya IP Office™ Platform with Manager*.

Table continues…

Product	Documents
IP Office Contact Center	• For a brief description of IP Office Contact Center administration options, see *Avaya IP Office Contact Center Feature Description*. • For a description of migrations and upgrades, see "Migration roadmap and limitations" in *Avaya IP Office Contact Center Reference Configuration*. • For detailed maintenance and troubleshooting information, see *Avaya IP Office Contact Center Maintenance Task Based Guide*.
OSS	All OSS deployment and administration details are in *Deploying Avaya Operations Support System*.

Chapter 7: Resources

Documentation

The following table lists related documents. Download the documents from the Avaya Support website at support.avaya.com. Most documents are available in PDF format.

Title	Use this document to:	Audience
Planning		
OnAvaya™ and Powered by IP Office and IP Office Contact Center Reference Configuration for Business Partners	Understand system architecture and network engineering requirements for the Cloud environment.	• Sales engineers • Business Partners
Avaya IP Office Contact Center Reference Configuration	Understand IP Office Contact Center deployment topologies, network architecture, system capacities, product interoperability, and functional limitations of specific configurations.	• Sales and support personnel • Architects • Implementation engineers
Implementing		
Deploying OnAvaya™ and Powered by IP Office and IP Office Contact Center for Business Partners	Understand the Cloud environment deployment tasks that Business Partners perform.	• Implementation engineers • Business Partners
Avaya IP Office Contact Center OVA Installation for Powered	Deploy the IP Office Contact Center OVA for Powered. This document is in a ZIP file.	• Implementation engineers • Business Partners
Avaya IP Office Contact Center Installation Task Based Guide	Install IP Office Contact Center software.	• Support personnel • Implementation engineers
Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines	Understand how to install IP Office in a Virtualized Environment.	• Support personnel • Implementation engineers
Configuring and Administering		
Chrome Management Console for Customer Engagement OnAvaya	Configure the Google Chrome Management Console (CMC).	• Implementation engineers

Table continues…

Title	Use this document to:	Audience
		• Business Partners
Administering Avaya IP Office™ Platform with Manager	Understand administration tasks performed on IP Office Manager for IP Office Standard Mode and Server Edition.	• Architects • System administrators
Administering Avaya IP Office™ Platform Voicemail Pro	Understand Voicemail Pro administration tasks.	• Architects • System administrators
Using Avaya IP Office Contact Center Web Administration Portal	Use the web-based administration portal to set up IP Office Contact Center.	• Support personnel • Administrators
Supporting		
Avaya IP Office Contact Center Maintenance Task Based Guide	Perform maintenance and upgrade tasks.	• Support personnel • Implementation engineers • Administrators
Using		
Using the Avaya IP Office Contact Center Chrome and Web Interfaces	Use the IP Office Contact Center User Interface for Chrome Devices and the IP Office Contact Center Web User Interface.	Agents and supervisors.
Using Avaya IP Office Contact Center Wallboard	Use Wallboard functionality.	All interface users, including agents, supervisors, and administrators.
Using Avaya IP Office Contact Center for Windows	Use the IP Office Contact Center User Interface for Windows.	All interface users, including agents, supervisors, and administrators.

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.

6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Training

Before deploying the Cloud solution, ensure you are familiar with the courses and certification credentials for CPE deployments.

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging in to the website, click **Learning & Certification**. In the **Catalog Search** menu, use the **Curriculum / Credential** or **Course Code** field to search for a course.

✱ **Note:**

If you cannot find a course using in the **Course Code** field, locate the course title in the **Curriculum / Credential** field.

OnAvaya™ sales authorization credentials and courses

Before selling OnAvaya™, Partners must obtain the APSS-4710: OnAvaya™- Google Cloud Platform Credential. This credential includes the following courses and tests:

Code	Title
4721W	Selling OnAvaya™- Google Cloud Platform Overview
4722W	OnAvaya™- Google Cloud Platform Components
4720T	OnAvaya™- Google Cloud Platform Online Test

Partner co-delivery training

Code	Title
ACSS: IP Office Contact Center training and credential	
0S00010E	Knowledge Collection Access: Avaya Midmarket Implementation and Support - Virtual Instructor Led
2252C	Avaya IP Office Contact Center Expanded Configuration and Administration
3003	Avaya IP Office Contact Center Credential Exam
AIPS: IP Office training	
10S00005I or 10S00005E	Avaya IP Office™ Platform Technical Basic Implementation Workshop – Instructor or Virtual Lead

Table continues…

Code	Title
Avaya IP Office Platform Implementation Assessment Test	
4001	Avaya IP Office™ Platform Implementation Assessment Test

General Cloud courses

Course code	Course title
4700W	Avaya Contact Center Solutions for Avaya IP Office Platform Overview
4701W	Selling Avaya Contact Center Solutions for Avaya IP Office Platform

Additional OnAvaya™ resources

The following table lists key materials available to OnAvaya™ Partners.

Title	Link
OnAvaya™ - Google Cloud Platform Sales Awareness Training	https://sales.avaya.com/documents/1399616546379
OnAvaya™ Partner Value Document	https://sales.avaya.com/documents/1399585705350
OnAvaya™ - Google Cloud Platform Fact Sheet	https://sales.avaya.com/documents/1399581317308
OnAvaya™ Partner Recruitment Deck	https://sales.avaya.com/documents/1399616657486

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  Note:

  Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Google Chrome Management Console support

Google provides direct technical support to the enterprise administrator in accordance with the Technical Support Service (TSS) guidelines at http://support.google.com/enterprise/terms and the license agreement at http://www.google.com/apps/intl/en/terms/chrome_terms.html. Contact Google for support in the following situations:

- You do not have active Avaya licenses
- You have a problem with your Chrome OS device or Chrome Management Console (CMC)

For information about Google support and other Google resources, see the following websites:

- http://support.google.com/chrome/a/?hl=en#topic=4386908
- http://toolbox.googleapps.com/apps/main/
- http://support.google.com/chromebook

For interoperability issues between the Cloud solution and Google CMC, Business Partners act as the first level of support and engage Avaya using the standard support process.

Important:

When requesting support, ensure you have the PIN for the enterprise. The enterprise administrator can find the PIN in the Administration console under **Support**.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya User ID and password.

   The Support page appears.
3. Under **Support by Product**, click **Product-specific support**.
4. Enter the product in **Enter Product Name** text box and press Enter.
5. Select the product from the drop down list and choose the relevant release.
6. Select the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Glossary

Avaya One Source Cloud Services
A web-based application that is used to manage licenses and billing.

direct media
A method that enables voice to travel directly between two endpoints. When direct media is unavailable, voice and other media elements are anchored through IP Office.

Emergency Location Information Number
An emergency contact number. Emergency Location Information Number (ELIN) must be used when the user is unreachable at the main number.

hunt group
A group of users who are accessible through a single directory number. An incoming caller calls the single directory number, but the call can be answered by any available member of the hunt group.

Infrastructure as a Service
A Cloud computing service model. With Infrastructure as a Service (IaaS), the provider outsources the required equipment. The equipment belongs to the provider who stores, maintains, and runs the equipment and bills the enterprise based on usage.

Network Address Translation
A network routing technique to access systems on the same subnet as the server. Network Address Translation (NAT) works like a firewall to protect the internal IP address and differentiate this address from the external IP address

Port NAT
Also known as NATP. For packets from multiple source devices, NATP changes source addresses and the source protocol port to the external router address and the router’s unique port. When packets are returned, the NATP router substitutes back the original values.

Private Network
The Private Network deployment model uses an MPLS or VPN network connection between the provider data center and the enterprise premises.

Public Network
A deployment model that uses an unsecured, over-the-Internet connection between the provider data center and the enterprise premises.

Public Safety Answering Point routing
A routing method that routes calls made to an emergency telephone number to the call center that is responsible for answering such calls.

Remote Worker

Users and endpoints in the Cloud solution. Users are connected to IP Officeover an unsecured Public Network. Endpoints are configured as remote entities over a Public Network deployment.

Simple Mail Transfer Protocol (SMTP)

A TCP/IP protocol used for sending and receiving e-mail. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another and to send messages from an e-mail client to an e-mail server.

Web License Manager

A product that provides support for installing licenses, configuring centralized licenses, or deleting license files. Also known as WebLM.

Index