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

Release 1.1.1
Issue 3
May 2016

© 2014-2016, Avaya, Inc.
All Rights Reserved.

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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 a 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 IF YOU PURCHASE A 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING 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 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

Customer acknowledges and agrees that it is responsible 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, 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 describes network architecture, deployment topologies, system capacities, and product interoperability for the following Cloud offers:

- Avaya-hosted OnAvaya™ offer.
- Business Partner-hosted Powered offer.

This document also describes the functional limitations of Cloud deployments. This document focuses on information that is unique to the Cloud environment, and does not provide detailed information about customer premise environment (CPE) deployments. For Cloud planning, deployment, and administration procedures, see *Deploying OnAvaya™ and Powered by IP Office and IP Office Contact Center for Business Partners*.

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
OnAvaya™ Release 1.0, Issue 1	July 2015	First release of this document with OnAvaya™ content only.
Powered Release 1.0, Issue 2	January 2016	Added Powered information to this document.
OnAvaya™ and Powered Release 1.1, Issue 1	March 2016	• Updated the OnAvaya™ topology diagram. • Added integration point descriptions. • Moved Resources content from the Introduction chapter into a separate chapter at the end of this document. • Listed Multichannel Agent license. • Added a “New in this release” section.
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	• Updated “New in this release” information. • 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.

Chapter 2: 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:

- OnAvaya™, where Avaya hosts the product instances in the Cloud data center. As of Release 1.1.1, 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.
- 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.

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 One Source Cloud.
- Flexibility to change your One Source Cloud 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.

Related links

New in this release on page 10
Avaya and Partner responsibilities on page 25
Business benefits on page 24

New in this release

Release 1.1.1

The following new functionality has been added to Powered and OnAvaya™ in Release 1.1.1 FP:

- With the Team Engagement OnAvaya™ offer, IP Office Contact Center is optional.
- As of June 2016, Powered and OnAvaya™ will support Avaya Contact Recorder as an optional capability with both IP Office and IP Office Contact Center.

Release 1.1

The following new functionality has been added to Powered and OnAvaya™ in Release 1.1:

- Powered supports IP Office Contact Center as an optional deployment.
- Multichannel agents, with access to voice, email, and chat functionality, are supported with IP Office Contact Center.
- The IP Office Contact Center disk size for OnAvaya™ has been increased from 200 GB to 500 GB to support the email channel.
- With OnAvaya™, the IP Office Contact Center self-signed certificate has been replaced with a single domain certificate.
- With OnAvaya™, a DNS host name has been added for a clean chat user experience.

Topologies

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.

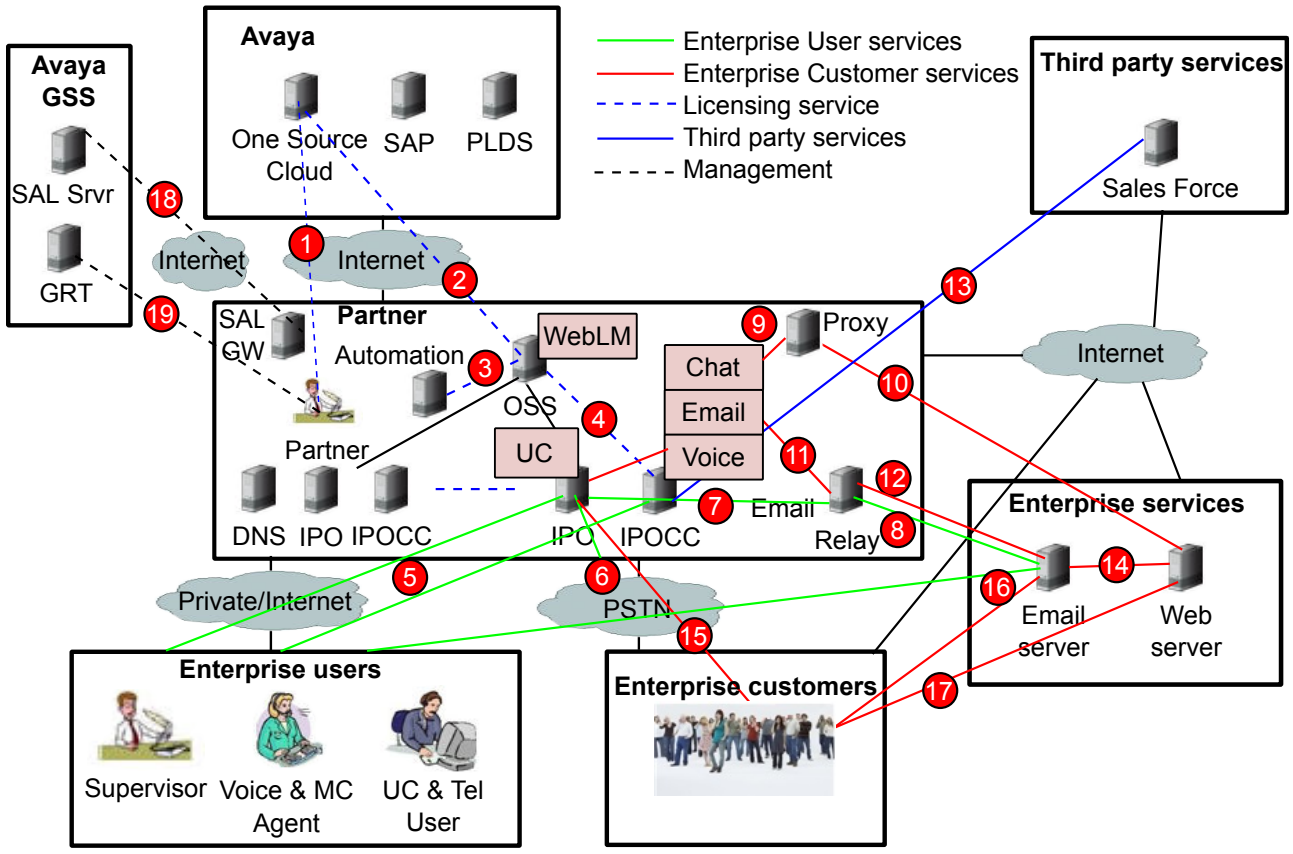

Figure 1: Powered topology

Mandatory integration points

The following sections describe the integration points shown in Powered topology on page 10.

1: Partner procurement to One Source Cloud

Partners log in to One Source Cloud using Avaya SSO credentials from a secure HTTPS browser. One Source Cloud enables Partners to request quotes, and place, change, or cancel orders.

2: Avaya Operations Support System to One Source Cloud integration

In the Powered solution, OSS is deployed in the BP network and One Source Cloud is deployed by Avaya.

The OSS connects to One Source Cloud over the public internet. The OSS in the BP management network usually has a private IP address. Communication occurs through a NATP at the edge of the BP network to the public URL in OSS.

Avaya supplies the following information for this integration:

- Protocols: HTTPS 443.
- Bandwidth.

- Certificates: Avaya uses a public third—party certificate so no One Source Cloud CA root certificates need to be installed on the OSS.
- Credentials: Avaya IT assigns a username and password to registered Partners that ordered Avaya support.

3: Avaya Operations Support System to Partner automation server

In the Powered solution, BPs can optionally configure automation for Avaya Operations Support System(OSS). This integration point is only required if automation is configured.

If you are using automation, OSS is configured with a JSON-connected endpoint. OSS uses this JSON endpoint to call the configured REST API for subscription change events, including Add, Change, and Delete events.

Avaya supplies the following information for this integration:

- Protocols: HTTPS.
- Certificates: You can use OSS to install specific CA certificates for the Partner automation server if required.
- API specifications: See *Deploying Avaya Operations Support System*.

4: IP Office and IP Office Contact Center to WebLM integration

In the Powered solution, IP Office,IP Office Contact Center, and IP Office Contact Center User Interface for Windows instances retrieve their license files from the WebLM embedded in the OSS. Each application instance must be manually configured with the parameters required to connect to WebLM and retrieve a license file.

BPs can deploy IP Office, IP Office Contact Center and IP Office Contact Center User Interface for Windows instances in a separate network than the OSS. In this case, the application instances might need to traverse a NATP function to connect to the OSS and WebLM.

Avaya supplies the following information for this integration:

- Protocol: HTTPS 52233.
- Bandwidth.
- Certificates: A Java API that relies on self-signed certificates.
- Credentials: None.

5: Enterprise network to IP Office and IP Office Contact Center

As a BP, you are responsible for defining, implementing, and assuring bandwidth, capacity, and quality of service (QoS). You are also responsible for supporting the enterprise with connectivity. Network connectivity includes the following:

- Partner data center connectivity.
- Enterprise access to the data center over a Public or Private Network deployment.
- Enterprise WAN access.
- Enterprise LAN or Wifi access.

Third-party network equipment vendors supply capabilities that support enterprise access options and other identified integrations. Typically, the solution uses virtual routing and forwarding (VRF) through MPLS or IP VPNs.

Avaya supplies the following information for this integration:

- Firewall requirements for the data center, enterprise sites, and remote user sites.
- IP address management.
- NAT requirements for the data center, enterprise sites, and remote user sites.
- Network QoS requirements, such as delay, jitter, and packet loss, for stable enterprise application deployment.
- Bandwidth requirements for the:
  - Data center, including IP Office to IP Office Contact Center, and IP Office or IP Office Contact Center to WebLM.
  - Data center WAN to the enterprise and trunk provider.
  - Enterprise site WAN.
  - Remote user WAN.
- Public single site or wildcard server certificates to simplify:
  - Enterprise endpoint configuration.
  - Integration with browser clients for enterprise users.

6: IP Office to SIP trunks with regulatory support

In the Powered solution, IP Office only uses SIP trunks to connect to the PSTN. You can deploy a Session Border Controller between the IP Office and your public SIP trunk gateway.

Avaya supplies the following information for this integration:

- Protocols.
- NAT.
- Bandwidth.
- Credentials.
- Certificates.
- E911 support.

7,8: IP Office to enterprise email server directly or through outbound email relay

IP Office UC capabilities enable Partners to configure delivery of enterprise voice mail to user email accounts. IP Office is configured with an SMTP host port and credentials. BPs can deliver email directly to the enterprise email server or use an outbound email relay to reduce integration complexity for each enterprise.

Note:

Installation of root CA certificates is supported if you require direct integration to the enterprise email server.

9,10: Enterprise web server to IP Office Contact Center chat service

The IP Office Contact Center chat service uses web sockets to implement a user chat session with an agent. Avaya delivers HTML Javascript code to be included in the web server pages.

The Partner can either:

- Provide a unique public IP address for each IP Office Contact Center.
- Deploy a web socket-capable load balancer, such as NGNIX, to provide access to IP Office Contact Center.

Avaya supplies the following information for this integration:

- Javascript and installation specifications.
- Protocols: HTTPS ports.
- Bandwidth.
- Certificates: Public third-party server CA certificates are required if IP Office Contact Center is directly integrated with the enterprise through a public IP address or FQDN. Wildcard certificates use FQDN and not an IP address. If you use a load balancer, you can use self-signed certificates on IP Office Contact Center depending on the load balancer capabilities.
- Credentials: None.

11, 12: IP Office Contact Center to enterprise email server directly or through outbound email relay

The IP Office Contact Center email channel capability uses standard email client mechanisms to retrieve enterprise email requests. IP Office Contact Center can connect:

- Directly to the enterprise email server through SMTP.
- Through an outbound email relay to reduce integration complexity for each enterprise.

IP Office Contact Center can be configured with a CC option if you use the outbound email relay and the enterprise requires a copy of the replies to be stored on their email server.

Note:

Installation of root CA certificates is supported if you require direct integration to the enterprise email server.

13: IP Office Contact Center to third-party CRM connectors and plug-ins integration

Partners can integrate IP Office Contact Center with a third-party SAP CRM connector or SFDC CRM plug-in. Avaya can assist with creating CRM Partner services. For more information about IP Office Contact Center CRM support, see *Avaya IP Office Contact Center Feature Description*.

14: Enterprise web server to enterprise email server

The enterprise and Partner are responsible for determining the delivery mechanism of enterprise email requests to the enterprise email server. The options are:

- A support email address on the enterprise web server.
- A form created by the enterprise on the web server to deliver email requests to the enterprise email server.

15, 16, 17: Enterprise users to enterprise services

Enterprise users can access services on:

- IP Office:
  - PSTN calls to individual enterprise employees through Direct Inward Dialling (DID) or auto attendant.
  - Web conference.
- IP Office Contact Center: PSTN calls, emails, or web chat sessions to a multichannel contact center.

Note:

All interactions use standard integrations, such as PSTN or SIP, SMTP email, HTTPS web conference, and agent chat.

18: Secure Access Link Gateway to Secure Access Link Concentrator integration

SAL Gateway connects an SSL tunnel directly to the internet-accessible SAL Concentrator.

Avaya supplies the following information for this integration:

- SAL Concentrator IP address and port.
- Certificate: The root CA certificates for SAL Gateway.
- Credentials: SAL Gateway credentials.

Note:

Additional SAL Gateway systems might be required for scalability, high availability, or geo-redundant data centers.

19: Partner administrator to Global Registration Tool

The Global Registration Tool (GRT) enables Partners to register product instances for support from a web interface over HTTPS. Partners can access the GRT using Avaya SSO credentials.

Optional integration points

IP Office to Avaya VPN Gateway

Avaya Global Support Services (GSS) can remotely access the Cloud instances in the BP network using the Avaya VPN Gateway. The IP Office that is deployed at the BP data center must be configured with the public IP address and credentials of the Avaya VPN Gateway. This configuration creates an SSL connection between the IP Office and the Avaya VPN Gateway. For more

information about remote access with the Avaya VPN Gateway, see Global Support Services remote access connectivity on page 31.

Optional McAfee server integration

In the Powered solution, the Partner can optionally install McAfee Antivirus software on IP Office Contact Center and OSS.

Avaya supplies the following information for this integration:

- OSS McAfee agent policy configuration.
- IP Office Contact Center McAfee agent policy configuration.

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.

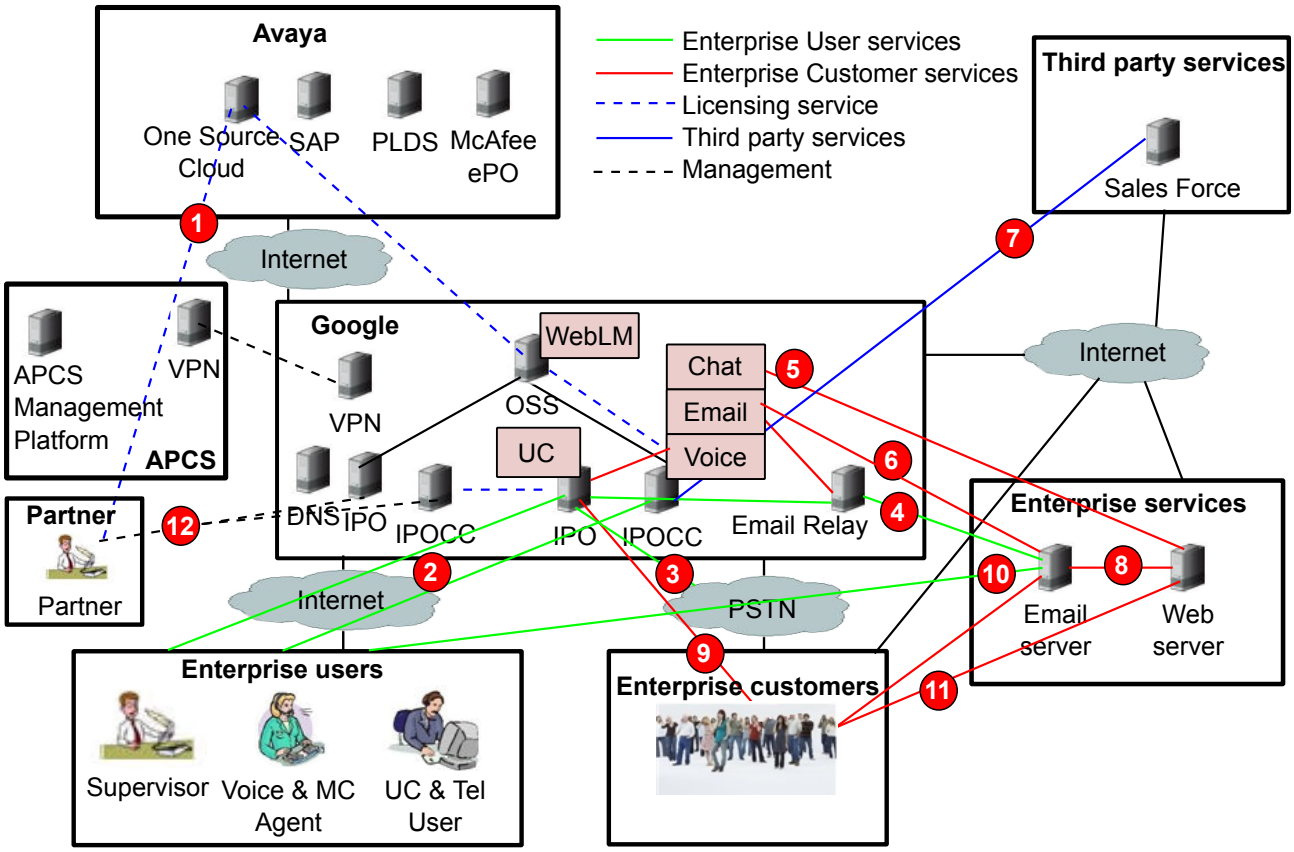

Figure 2: OnAvaya™

Related links

Caveats and limitations on page 28

1: Partner procurement to One Source Cloud

Partners log in to One Source Cloud using Avaya SSO credentials from a secure HTTPS browser. One Source Cloud enables Partners to request quotes, and place, change, or cancel orders.

2: Enterprise network to IP Office and IP Office Contact Center

OnAvaya™ only supports Internet-connected users deployed in:

- An office using LAN or Wifi.
- A home office.
- A wireless carrier network.

As a BP, you are responsible for defining, implementing, and assuring bandwidth, capacity, and quality of service (QoS). You are also responsible for supporting the enterprise with connectivity. Network connectivity includes the following:

- Internet access to the data center.
- Enterprise WAN access.

- Enterprise LAN or Wifi access.

Avaya supplies the following information for this integration:

- Firewall port requirements for enterprise sites.
- NAT requirements for enterprise sites and remote user sites.
- Network QoS requirements, such as delay, jitter, and packet loss, for stable enterprise application deployment.
- Bandwidth requirements for:
  - Enterprise site WAN.
  - Remote user WAN.
- Certificates: Avaya uses public single site and server certificates to simplify:
  - Enterprise endpoint configuration.
  - Integration with browser clients for enterprise users.

3: IP Office to SIP trunks with regulatory support

The Partner is responsible for regulatory requirements and the integration to a SIP trunk provider. To configure SIP trunks, the Partner must provision the following in IP Office:

- Protocols and ports supplied by the SIP trunk provider.
- Credentials supplied by the SIP trunk provider.

Partners might also need to install SIP trunk provider root CA certificates.

Avaya supplies the following information for this integration:

- Bandwidth.
- E911 support.

4: IP Office to enterprise email server directly or through outbound email relay

IP Office UC capabilities enable Partners to configure delivery of enterprise voice mail to user email accounts. IP Office is configured with an SMTP host port and credentials. BPs can deliver email directly to the enterprise email server or use an outbound email relay to reduce integration complexity for each enterprise.

Note:

Installation of root CA certificates is supported if you require direct integration to the enterprise email server.

5: Enterprise web server to IP Office Contact Center chat service

The IP Office Contact Center chat service uses web sockets to implement a user chat session with an agent. Avaya delivers HTML Javascript code to be included in the web server pages.

Avaya supplies the following information for this integration:

- Javascript and installation specifications.
- Protocols: HTTPS ports.
- Bandwidth.
- Certificates: Avaya installs public third party CA server certificates on IP Office Contact Center to eliminate the need for enterprise users to respond to browser certificate errors.
- Credentials: None.

6: IP Office Contact Center to enterprise email server directly or through outbound email relay

The IP Office Contact Center email channel capability uses standard email client mechanisms to retrieve enterprise email requests. IP Office Contact Center can connect:

- Directly to the enterprise email server through SMTP using ports that are not blocked by the Google Cloud environment. Blocked ports are 25, 465, and 587.
- Through the outbound email relay, which is supplied and configured by Avaya, to reduce integration complexity for each enterprise.

IP Office Contact Center can be configured with a CC option if you use the outbound email relay and the enterprise requires a copy of the replies to be stored on their email server.

Note:

Installation of root CA certificates is supported if you require direct integration to the enterprise email server.

7: IP Office Contact Center to third-party CRM connectors and plug-ins integration

Partners can integrate IP Office Contact Center with a third-party SAP CRM connector or SFDC CRM plug-in. Avaya can assist with creating CRM Partner services. For more information about IP Office Contact Center CRM support, see *Avaya IP Office Contact Center Feature Description*.

8: Enterprise web server to enterprise email server

The enterprise and Partner are responsible for determining the delivery mechanism of enterprise email requests to the enterprise email server. The options are:

- A support email address on the enterprise web server.
- A form created by the enterprise on the web server to deliver email requests to the enterprise email server.

9, 10, 11: Enterprise users to enterprise services

Enterprise users can access services on:

- IP Office:
  - PSTN calls to individual enterprise employees through Direct Inward Dialling (DID) or auto attendant.
  - Web conference.
- IP Office Contact Center: PSTN calls, emails, or web chat sessions to a multichannel contact center.

12: Partner administrator to IP Office and IP Office Contact Center instances

Avaya provides the following to enable the Partner to configure IP Office and IP Office Contact Center:

- Partner outbound firewall protocol and ports.
- Partner administrative bandwidth requirements.
- Credentials: Restricted IP Office and IP Office Contact Center user names and passwords.
- Certificates: Avaya installs public CA certificates to eliminate the need for the Partner to install root CA certificates.

Components

The following sections provide an overview of all components used in the OnAvaya™ and Powered solutions. For information about the latest supported version of components, see the Avaya Support Interoperability Matrix at: http://support.avaya.com/CompatibilityMatrix/Index.aspx.

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.

Table continues…

Component	Description
	• 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.

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. **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.
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.

Management and subscription components

Subscription management

Component	Description
One Source Cloud	One Source Cloud handles interactions related to purchases and billing. Business Partners use One Source Cloud 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 One Source Cloud. **Note:** With Powered, Business Partners are responsible for deploying and managing OSS. With OnAvaya™, APCS 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 the IP Office and IP Office Contact Center. For general information about Avaya and third-party product interoperability, see http://support.avaya.com/CompatibilityMatrix/Index.aspx.

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*

Supported endpoints and applications in the Cloud

The following is a subset of endpoints and telephony applications supported in the Cloud as Contact Center (CC) clients, Unified Communications (UC) clients, or both.

Endpoint or application	Supported as CC clients	Supported as UC Back Office clients
WebRTC, which enables a soft phone in the IP Office Contact Center User Interface for Chrome Devices	✔	
9608, 9611, 9621, and 9641 series IP desk phones (H.323)	✔	✔
one-X Mobile Preferred and Avaya Communicator (SIP)		✔
B179 SIP conference phone		✔
IP Office SoftConsole receptionist phone		✔

Business benefits

OnAvaya™ and Powered support the following business requirements:

- Reduce cost and maintenance.
- Simplify the configuration process. In the Cloud, some configuration settings are automatically populated. For a detailed comparison of deployment requirements for CPE and Cloud environments, see *Deploying OnAvaya™ and Powered by IP Office and IP Office Contact Center for Business Partners*.
- With Powered, flexibility to choose between a Public Network or Private Network deployment.
- Simplify the ordering process with One Source Cloud and Avaya Operations Support System (OSS).

Related links

Capacity and scalability on page 29

Ordering process

Business Partners request quotes, place orders, and retrieve billing data with the One Source Cloud 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.

The following images illustrates the order fulfillment process with OnAvaya™.

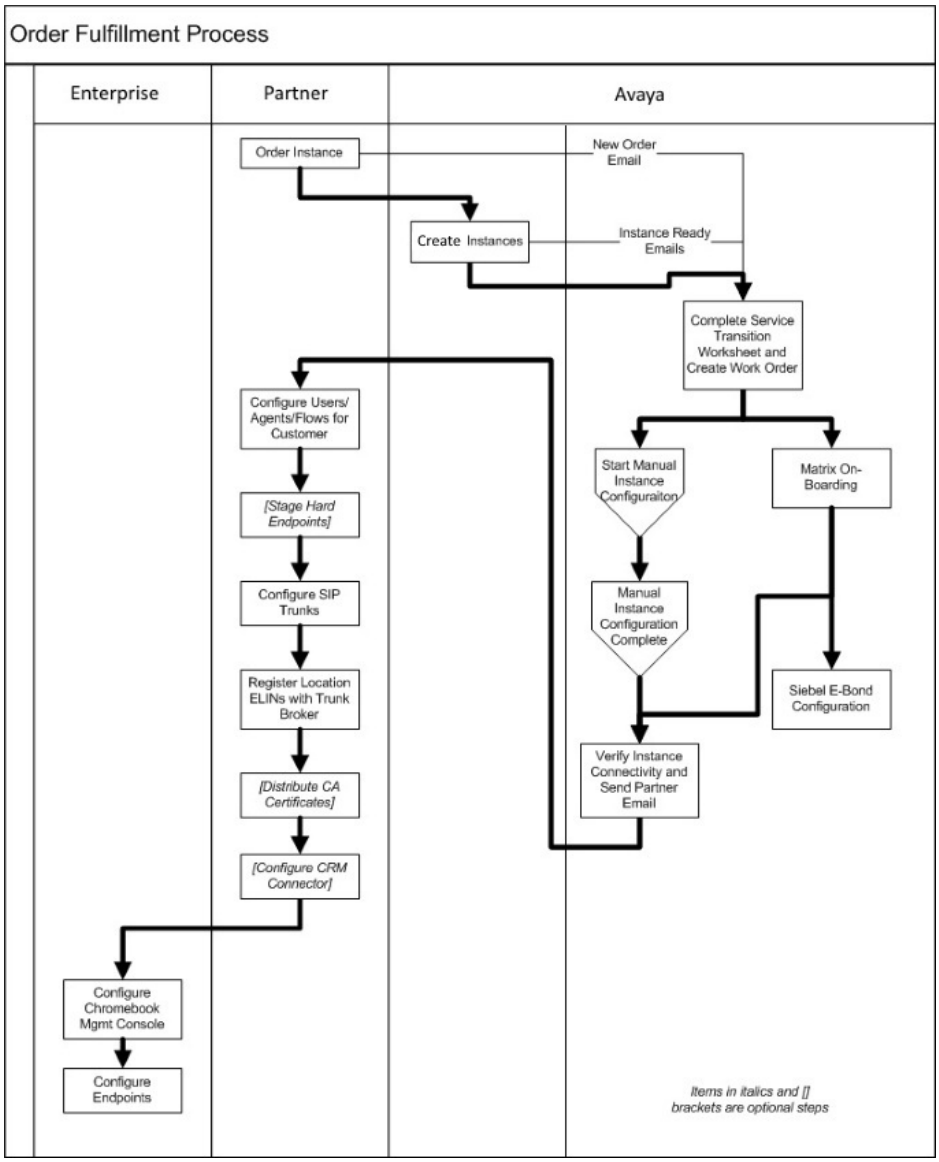

Figure 3: Ordering process flow for OnAvaya™

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.	Avaya deploys OSS in the Google Cloud.	BPs can deploy OSS on VMware or on a physical server. **Note:** • BPs cannot deploy OSS in the Google Cloud. • Avaya deploys One Source Cloud. BPs can access the One Source Cloud 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.
Backups and upgrades	Avaya is responsible. **Note:** • By default, backup jobs are scheduled at 2 AM Eastern Time. If you want to change the time for a backup job, coordinate with Avaya Private Cloud Services (APCS). • Avaya provides updated application software, upgrades, and patches. Avaya also coordinates with the BP to schedule and perform upgrades to the next release.	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.

Table continues…

Task	Party responsible with OnAvaya™	Party responsible with Powered
		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 handled by Avaya for the OnAvaya™ offer

To enable the OnAvaya™ service, Avaya configures the following:

- Email server for voice mail (SendGrid)
- DNS names
- IP Office Contact Center public certificate

Important:

Partners using OnAvaya™ must not change these settings.

For a list of pre-configured settings in IP Office and IP Office Contact Center, see Automatically configured IP Office parameters and settings with OnAvaya on page 32 and Automatically configured IP Office Contact Center settings with OnAvaya on page 38.

Chapter 3: Design and architecture considerations

Caveats and limitations

Call recording

Avaya Contact Recorder might not be able to keep up with call recordings in OnAvaya™. To prevent this issue, you must use VRLA as the recording type.

Direct media for Remote Workers

Direct media is not available for Remote Workers.

In the Cloud solution, all users connected to IP Office or IP Office Contact Center over an unsecured Public Network deployment are considered Remote Workers.

Note:

This limitation does not apply to Private Network deployments where users at the enterprise site can connect securely to the Cloud solution through MPLS or VPN.

You can also configure IP Office endpoints as remote endpoints. For more information about IP Office Remote Worker endpoints, see:

- “SIP remote worker overview” in *Administering Avaya one-X® Mobile for IP Office™ Platform*
- “Remote H.323 extensions” in *Administering Avaya IP Office™ Platform with Manager*

Endpoint support

Some endpoints, such as the IP Office IP500 and IP500V2 endpoints, are not supported in the Cloud Public or Private Network deployments.

Single data center model

The Cloud solution supports a single data center model, but not dual data centers and data center survivability.

Capacity and scalability

The Cloud solution is flexible, so features can be modified to meet the needs of small and medium enterprises. The solution supports the following general IP Office and IP Office Contact Center capacities:

- 250 IP Office Contact Center agents.
- 1250 IP Office users

IP Office Contact Center capacity limits

IP Office Contact Center Cloud deployments have the following capacity limits:

- Active agents with at least one supervisor: 250
- BHCC: 5000
- Configured agents: 1250
- Voice calls queued: 125
- Calls being recorded: 250
- Wallboards connected concurrently: 5
- Disk size for a large system: 500 GB

Tip:

Cloud enterprise users should download their email archive onto local storage at regular intervals.

Virtual machine specifications

With Powered, Business Partners install IP Office and IP Office Contact Center Cloud OVAs in a Virtualized Environment.

You can monitor virtual machines and use profiling. Profiling improves performance by allocating resources where required and optimizing the virtual infrastructure.

For supported virtual machine usage values, see the following documents:

- For IP Office, see *Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines*.
- For IP Office Contact Center, see *Avaya IP Office Contact Center Reference Configuration* and *Avaya IP Office Contact Center Installation Task Based Guide*.

Security considerations

The Cloud solution provides the following security options:

Password management

Password management is the process of resetting or updating the service access password. Business Partners manage enterprise passwords. Enterprise users can subscribe to receive notifications about security advisories by email. Perform the following password management updates to improve network security:

- On all installed systems, change the account passwords using IP Office Manager or IP Office Web Manager.
- Set the password complexity rules to *Medium*. The *Low* setting does not provide adequate security for the Cloud environment.

Firewall configuration

Firewalls provide security to the network by attempting to control the incoming and outgoing traffic using a predetermined set of rules. Filtering of traffic is based on data aspects, including protocols, ports, and application types.

Secure phone connections

The Business Partner can configure SRTP Media Encryption between IP Office and the phones. All signaling and control interactions between the SIP endpoints and IP Office can be secured with TLS. HTTPS connections from the H.323 phones to the IP Office for settings and other files can also be secured with TLS. With the Annex H mechanism, signaling between the H.323 phones and the IP Office partially secures registration, SRTP key exchange, and dialled digits.

Traffic isolation with Private Network deployments

Powered supports Private Network deployments, which can be set up using MPLS or site-to-site VPN. The Private Network deployment isolates the traffic between the enterprise site and the Cloud data center.

Chapter 4: Configuration details

Network configuration

In both Cloud solutions, BPs are responsible for configuring network connectivity at their site and at the enterprise site. The network deployment models supported vary for OnAvaya™ and Powered.

Table 1: Supported network deployments

The following table summarizes the available deployment models, and indicates which models are supported for each Cloud solution.

Deployment model	Description	Solution support
Public Network deployment	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.	Supported by both OnAvaya™ and Powered.
Private Network deployment	This deployment model requires an MPLS or site-to-site VPN connection between the Cloud data center and the enterprise premises. This deployment model is more secure than the Public Network deployment because it does not rely on an internet connection.	Supported by Powered only.

Related links

Global Support Services remote access connectivity on page 31

Global Support Services remote access connectivity

Avaya Global Support Services (GSS) provides tier 3 and tier 4 support for the Powered solution. GSS can use a connection initiated by Avaya or the BP. Connections initiated by Avaya use an SSL Gateway. Connections initiated by the BP are supported through screen sharing or the Avaya VPN Gateway.

Screen sharing does not allow remote access. The Avaya VPN Gateway is hosted by Avaya and enables remote access to the Cloud instances at the BP data center. Avaya provides the BP with firewall, NAT, bandwidth, and certificate requirements for Avaya VPN Gateway integration with IP Office.

The IP Office that is deployed at the BP data center must be configured with the public IP address and credentials of the Avaya VPN Gateway. This configuration creates an SSL connection between the IP Office and the Avaya VPN Gateway. IP Office acts as a router, enabling GSS to connect to IP Office Contact Center and the OSS. IP Office can also use an Ethernet or IP interface to enable connectivity to the OSS.

Component configuration

BPs are responsible for configuring IP Office, IP Office Contact Center, and the Google Chrome Management Console (CMC). The following sections:

- List automatically configured settings for IP Office and IP Office Contact Center.
- Describe some configuration, such as emergency calls and endpoint configuration.
- Provide information sources for CMC configuration.

For complete details about component configuration, see “Configuration” in *Deploying OnAvaya™ and Powered by IP Office and IP Office Contact Center for Business Partners*.

IP Office configuration

Business Partners are responsible for many aspects of IP Office configuration in both Cloud solutions, including SIP trunks, users, groups, extensions, emergency calls, endpoints, and voicemail. Some configuration requirements vary between OnAvaya™ and Powered Cloud. For complete details, see “IP Office configuration” in *Deploying OnAvaya™ and Powered by IP Office and IP Office Contact Center for Business Partners*.

Automatically configured IP Office parameters and settings with OnAvaya™

In OnAvaya™, Avaya does the following before sending the solution to the Business Partner for further configuration:

- Sets up the IP Office server to send event traps to the appropriate Avaya Services SNMP Client location. Using IP Office Web Manager, SNMP is enabled and a trap receiver is added.
- Uses IP Office Web Manager to take a back up of the staging server. Avaya also sets up the remote backup server and schedules backups.
- Creates the Administrator account for BPs.

The IP Office system configuration parameters listed in the following tables are automatically set in the OnAvaya™ solution.

Table 2: Metadata parameters

Parameter	Description
Hostname (required)	The host name for the instance
Timezone (required)	Based on the time zones listed in the database. For more information about time zones, see https://en.wikipedia.org/wiki/List_of_tz_database_time_zones. For example: `America/New_York`, `Europe/London`, `America/Denver`, `Asia/Calcutta`. The time zone for the IP Office instance is set to GMT by default.
NTP Server (required)	NTP server for time synchronization.
Companding (required)	One of the following companding laws: • MULaw • ALaw
Mode (required)	Only `Primary` is supported
AdminPass	Administrator platform and password provided by Avaya.
SysPass	System password for IP Office. `Sys<Private IP address without dots>` is used as the default
WebLMIP	IP address or domain name for the WebLM server.
WebLMSID	Customer ID for WebLM.
WebLMPath	Path after the IP address or FQDN to the WebLM server.
WebLMPort	WebLM server port.
LAN 1	DHCP
LAN 2	Disabled

Table 3: System configuration parameters

Parameters	Description
System > **LAN1** > **LAN Settings** > **IP Address**	Private IP Address for IP Office.
System > **LAN 1** > **Network Topology** > **Public IP Address**	Static public IP address.
System > **Voicemail** > **Voicemail IP Address**	127.0.0.1
System > **LAN 1** > **VoIP** > **Layer 4 Protocol** > **TCP/UDP port**	5056 protects against SIP attacks on port 5060. **Note:** Port 5060 is not used.
System > **LAN 1** > **VoIP** > **Layer 4 Protocol** > **TLS port**	The default port setting is 5061 and TLS is enabled.
System > **LAN 1** > **VoIP** > **SIP Trunks Enabled**	SIP trunks are enabled.

Table continues…

Parameters	Description
System > LAN 1 > VoIP > Remote Call Signalling Port	Port 1800 protects against ALG behaviors that cause port 1720, the usual value, to fail for H.323 endpoints behind NAT routers.
System > LAN 1 > VoIP > H323 Gatekeeper Enabled	H.323 sets are enabled.
System > LAN 1 > VoIP > Remote Extn Enabled	H.323 sets are enabled.
System > LAN 1 > VoIP > SIP Registrar Enabled	Communicator/Mobile/SIP sets, SIP trunks, and the SIP line between IP Office Contact Center and IP Office are enabled.
System > LAN 1 > VoIP > SIP Remote Extn Enabled	Communicator/Mobile/SIP sets are enabled.
System > LAN 1 > VoIP > Domain Name	Static IP address is set to the public IP address of the IP Office instance.
System > VoIP Security	Media Security is set to best effort.
Avaya one-X® Portal administration	XMPP Domain is set to the public IP address of the IP Office instance.

Table 4: Security settings

The following table lists advanced security settings and recommended values.

Security settings	Recommended values
Advanced > Security Settings > Security > General > Security Administrator > Minimum Password Complexity	High
Advanced > Security Settings > Security > General > Service User Details > Minimum Name Length	6
Advanced > Security Settings > Security > General > Service User Details > Minimum Password Length	8
Advanced > Security Settings > Security > General > Service User Details > Password Reject Limit	3
Advanced > Security Settings > Security > General > Service User Details > Password Reject Action	Log and Temporary Disable
Advanced > Security Settings > Security > General > Service User Details > Minimum Password Complexity	Medium
Advanced > Security Settings > Security > General > IP Office User Details > Password Enforcement	Selected
Advanced > Security Settings > Security > General > IP Office User Details > Minimum Password Length	8
Advanced > Security Settings > Security > General > IP Office User Details > Minimum Password Complexity	Medium
Add a table row for Advanced > Security Settings > Security > General > IP Office User Details > Password Reject Limit (Attempts)	5

Table continues…

Security settings	Recommended values
Advanced > **Security Settings** > **Security** > **General** > **IP Office User Details** > **Password Reject Action**	Log and Disable Account

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.

WebLM license details in IP Office

If you are using the Powered Cloud solution, you must update the WebLM URL details and client ID. You must use a `curl` command to configure the client ID in IP Office. You can configure other settings in IP Office Manager.

Emergency calls configuration

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.

To ensure the routing to the correct PSAP and the automatic identification of the caller's physical location, Business Partners must communicate the relationship between calling line IDs and physical locations to the SIP Trunk Broker. The Business Partner must do the following:

- Provide the SIP Trunk Broker with a few special phone numbers and the mapping to physical locations. These special phone numbers are referred to as Emergency Location Identification Numbers (ELINs). An ELIN can be defined for each enterprise site or, for example, for each building or floor.
- Configure IP Office to send the ELIN of the caller's location as the calling line ID in emergency calls. You can do this by configuring a location record and a respective Emergency ARS table in IP Office for each enterprise location. 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 for outgoing calls.
- Configure IP Office to identify which configured location record the calling endpoint is at. The location can be statically configured for the extension of each phone. Alternatively, if each site is defined as one location, IP Office can identify the location automatically based on the public IP address of the site that the endpoint registers from. This requires the router or NAT in the enterprise site to have a static IP address. The static IP address can be provided, for example, with the Business Internet service from some ISPs. The Business Partner must 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.

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.

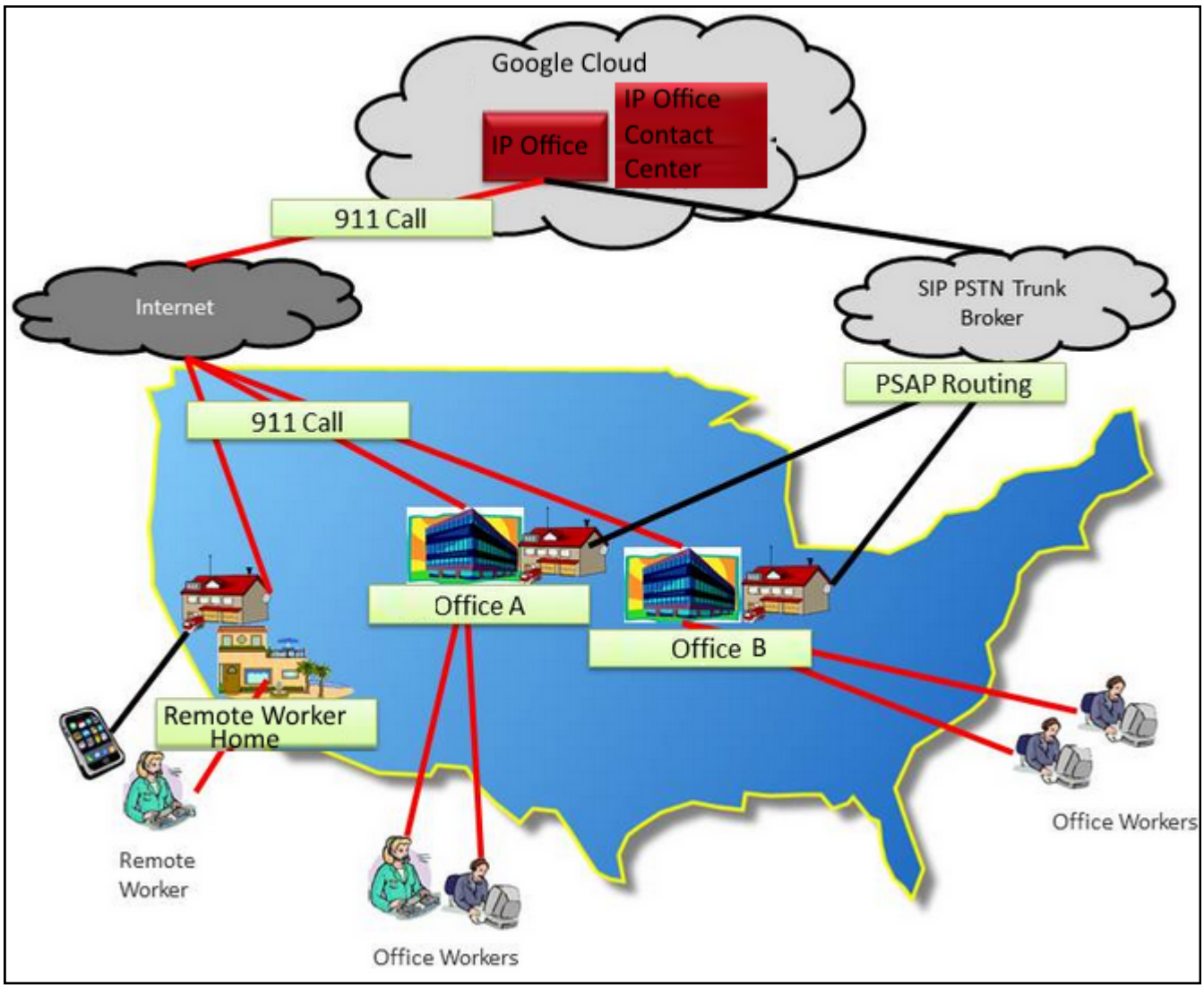

Figure 4: Emergency calls architecture

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.

IP Office Contact Center configuration

With OnAvaya™, after connecting to the IP Office Contact Center instance, a script runs. Do not attempt any manual steps or close windows on the screen. The system reboots automatically after 10 to 15 minutes. After the system reboots, operating system initialization is complete and IP Office Contact Center services start.

With Powered, Business Partners must manually create the OVA and then install and configure IP Office Contact Center.

Business Partners are responsible for completing IP Office Contact Center provisioning in both solutions. BPs are also responsible for configuring IP Office Contact Center agents, agent groups, and call flows. You can optionally configure call recording and applications, such as Wallboard and CRM connectors. Some configuration requirements vary between OnAvaya™ and Powered Cloud. For complete details, see “IP Office Contact Center configuration” in *Deploying OnAvaya™ and Powered by IP Office and IP Office Contact Center for Business Partners*.

Note:

You must perform some configuration and administration tasks in the IP Office Contact Center User Interface for Windows. In the Public Network deployment, this UI is only accessible with a remote desktop connection.

Tasks managed by Avaya with OnAvaya™

With OnAvaya™, Avaya performs the following functions:

- Creates and installs the IP Office Contact Center server certificate.
- Sets up the Windows SNMP server to send event traps.
- Sets up the backup script in the IP Office Contact Center backup scheduler.
- Creates a Business Partner account on the IP Office Contact Center server.

  You need this account to use IP Office Contact Center User Interface for Windows. In the Public Network deployment, this UI is only accessible with a remote desktop connection.

Automatically configured IP Office Contact Center settings with OnAvaya™

IP Office Contact Center automatically configures the settings described in the following sections with the OnAvaya™ solution.

Server configuration settings

- Server name
- IP address
- Windows firewall is disabled
- Time and Date setting. NTP server is set to `Google 169.254.169.254` and time zone is set to `UTC`. The BP must adjust the time zone as appropriate for the customer location.
- SNMP ports are selected
- The Windows Server login password is set

- Power settings
- Data Execution Prevention (DEP) is disabled

IP Office Contact Center Cloud image configuration settings

- Desktop icons
- Explorer options, such as **Show hidden files** and **Hide system file extensions**
- CMD tool changes
- Windows firewall is disabled
- Event tracker is disabled
- Password expiration is disabled
- Network properties, such as **Disable TCP/ IPv6**
- Unnecessary Windows services are disabled, such as, IP Helper, Portable Device Enumerator Service, and Power Print Spooler
- Hibernation is disabled with the command **- `powercfg -h off`**
- McAfee anti-virus software
- Scheduled scans
- Task Manager cleanup
- System event logs are cleared
- **Start** menu cleanup
- Automatic updates for Windows are disabled
- Databases are created
- Software is installed
- **`AdjustHostName`** is executed
- Licenses are acquired from the Avaya WebLM instance

IP Office Contact Center provisioning

You can complete initial IP Office Contact Center provisioning using one of the following options:

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

If you use the Configuration Wizard for provisioning, many values are automatically populated in the System Configuration screen. With OnAvaya™, the following IP Office information is automatically populated:

- IP Office IP Address
- IP Office Service Password
- IP Office System Password

You must complete the blank fields in all tabs. By default, the signaling port number is set to 5056 with OnAvaya™, and 5060 with Powered and CPE deployments.

If you use the spreadsheet for provisioning, you can gather IP Office information, such as the IP address or SIP port, from the IP Office Contact Center web-based administration portal.

WebLM license details for IP Office Contact Center with Powered

If you are using the Powered Cloud solution, you must update the WebLM URL details and client ID. You can update WebLM details in the IP Office Contact Center web-based administration portal using the **System** > **License** menu.

Google Chrome Management Console configuration

BPs are responsible for Google Chrome Management Console (CMC) configuration. For CMC configuration steps, see *Deploying OnAvaya™ and Powered by IP Office and IP Office Contact Center for Business Partners*.

Additional information

For more information about CMC configuration, see the following links:

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

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 with the Powered offer and the Team Engagement OnAvaya™ offer. You can update your order in One Source Cloud 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 5: IP Office licensing

Cloud subscriptions	IP Office license mapping	Quantity
System bundle	Server Edition Virtualized	1
	SIP Trunks	1024
	Receptionist	10
	VM Ports	350
	CTI Link Pro	1
	Third Party Endpoints (available until June 2016) [1]	5
Telephony User	Avaya IP Endpoint License	1
	Third Party IP Endpoint License (available in June 2016) [2]	1
UC User	Avaya IP Endpoint License	1
	Third Party IP Endpoint License (available in June 2016) [3]	1
	Power User License	1
	Web Collaboration User	1

Table 6: 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

[1] As of June 2016, this license will no longer be available. At this time, a Third Party IP Endpoint license will be available for Third Party Telephony and UC Users.

[2] This license will be available as of June 2016 for Third Party Telephony Users. It will include Avaya Contact Recorder as an optional capability.

[3] This license will be available as of June 2016 for Third Party UC Users. It will include Avaya Contact Recorder as an optional capability.

Port assignments

The enterprise premise firewall must allow traffic to flow outbound from the premise to IP Office and IP Office Contact Center Cloud. Normally, the enterprise premise router or firewall only blocks inbound traffic and not outbound traffic. If the enterprise premise router or firewall is configured to block outbound traffic, the ports for the needed traffic listed in the following tables must be opened.

Related links

Ports at the enterprise premise on page 42
Ports at the Business Partner premise on page 43

Ports at the enterprise premise

Table 7: IP Office ports at the Enterprise premise

Ports	Direction	Protocol	Description
411	Out	TCP	96x1 H.323 Settings.
443	Out	TCP	Backup and restore, HTTPS for provisioning Avaya soft phone and file transfer.
1718	Out	TCP	H.323 Discovery Use this port for remote H.323 client support.
1719	Out	UDP	H.323 Status Use this port for remote H.323 client support.
1800	Out	TCP	H.323 Signaling Use this port for remote H.323 client support.
5005	Out	UDP	RTCP Monitor - If IP session performance information is being monitored.
5056	Out	TCP or UDP	SIP Signaling. This is the Cloud setting for the TCP/UDP SIP Port. Only needed for unsecured SIP devices.
5061	Out	TCP	SIP TLS Signaling.
5222	Out	TCP	One-x Mobility and Avaya Communicator.
7070	Out	TCP	IP Office Solution Web Manager (preferences must have SE Central Access selected), WebRTC Signaling.
7071	Out	TCP	IP Office Solution Web Control.
8063	Out	TCP	Secure web socket-based delivery for Avaya Communicator.
8411	Out	TCP	96x1 H.323 firmware download.

Table continues…

Ports	Direction	Protocol	Description
8443	Out	TCP	Web Services.
8444	Out	TCP	Mobility and Avaya Communicator.
9443	Out	TCP	Secure access to Avaya one-X® Portal – Management and User.
9444	Out	TCP	Contact Recorder.
40750-50750	Out	UDP	The RTP or RTCP ports used for SIP or H.323 media.
50791	Out	TCP	Centralized Voicemail Pro Client.
50802	Out	TCP	TCP Discovery – IP Office Manager. IP Office Manager preferences must be modified to use TCP Discovery.
50809	Out	TCP	System Status Application (Secured).
50813	Out	TCP	IP Office Manager secure configuration.
56000-58000	Out	UDP	WebRTC gateway media ports.

Table 8: IP Office Contact Center ports at the Enterprise premise

Ports	Direction	Protocol	Description
28443	Out	TCP	Wallboard module
28443	Out	TCP	IP Office Contact Center User Interface for Chrome Devices

Related links

Port assignments on page 42

Ports at the Business Partner premise

Table 9: IP Office ports at the Partner premise

Ports	Direction	Protocol	Description
7070	Out	TCP	IP Office Solution Web Manager with SE Central Access selected, and WebRTC Signaling.
7071	Out	TCP	IP Office Solution Web Control.
9443	Out	TCP	Secure access to Avaya one-X® Portal – Management and User.
9444	Out	TCP	Contact Recorder.
50791	Out	TCP	Centralized Voicemail Pro Client.
50802	Out	TCP	TCP Discovery – IP Office Manager. IP Office Manager preferences must be modified to use TCP Discovery.
50809	Out	TCP	System Status Application Secured.
50813	Out	TCP	IP Office Manager secure configuration.

Table 10: IP Office Contact Center ports at the Partner premise

Ports	Direction	Protocol	Description
3389	Out	TCP	Remote desktop connection
28443	Out	TCP	Wallboard module
28443	Out	TCP	Web-based administration portal
28443	Out	TCP	IP Office Contact Center User Interface for Chrome Devices

Related links

Port assignments on page 42

Traffic and Quality of Service

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 11: 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

Table continues…

Requirements	Description
	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.

Traffic and bandwidth guidelines

The BP must ensure that the connection at the enterprise site provides adequate service quality. The enterprise network must have enough bandwidth to accommodate the traffic that will be generated. With the Public Network deployment, enterprises are connected over the internet. With the Private Network deployment, the enterprise is connected though MPLS or a site-to-site VPN.

Important:

Avaya is not responsible for inadequate voice quality caused by underlying network problems at the enterprise site.

For Powered, the Business Partner must also ensure that their data center has sufficient bandwidth to handle traffic.

For a bandwidth calculation tool, see https://support.avaya.com/ext/index?page=content&id=FAQ110655. Separate tabs are available to help you calculate general enterprise bandwidth and Partner data center bandwidth requirements.

IP Office and IP Office Contact Center bandwidth guidelines

The Internet Service Provider (ISP) connection must have sufficient bi-directional bandwidth to support IP Office and IP Office Contact Center along with existing business bandwidth requirements.

The following table provides IP Office Contact Center bandwidth guidelines for the enterprise site.

Traffic	Minimum bandwidth	Description of connection
IP Office Contact Center agents	50 kbit/second for the IP Office Contact Center User Interface for Chrome Devices client.	Connection between the IP Office Contact Center User Interface for Chrome Devices, phone, IP Office Contact Center server, and IP Office server.
	Additional 100 kbit/second for a WebRTC or H.323 phone connection.	

The following bandwidth requirements exist:

- Agents and supervisors for voice and the Chrome UI application
- Wallboards
- Voice users for voice services
- UC users for voice, IM and presence, web conferencing, and Avaya Communicator for Windows point-to-point video

For a general IP Office bandwidth calculator for voice traffic, see http://marketingtools.avaya.com/knowledgebase/businesspartner/ and then navigate to **Tools** > **Bandwidth**.

Chapter 5: 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
How to order Avaya RICS	Order the optional Remote Installation and Configuration Support (RICS) service.	Business Partners
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 • 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

Table continues…

Title	Use this document to:	Audience
		• 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.	Agents and supervisors.
Using Avaya IP Office Contact Center Wallboard	Use Wallboard functionality.	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
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

General information about the OnAvaya™ solution is available at https://sales.avaya.com/en/onavaya. 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. You can contact Avaya using the following methods:

- Call the Avaya Service Desk at 1-866-282-9267
- Visit the APCS Web Portal at https://www.aosportal.com/

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. Enter the product in **The InSite Knowledge Base** text box.
4. Click the red arrow to obtain the Search Results.
5. Select relevant articles.

Glossary

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

M

N

O

P

Q

R

S

T

V

W