Administering Avaya Communicator for Android, iPad, iPhone, and Windows

Release 2.1
Issue 5
September 2015

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: http://support.avaya.com 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 types

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 the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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

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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://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 the administration tasks that apply to the solution components and network infrastructure required to support Avaya Communicator on Android, iPad, iPhone, and Windows. Avaya Communicator is a common Unified Communications (UC) experience for use on Android, iPad, iPhone, and Windows. Each operating system has its own application and installation process.

Intended audience

This document is intended for administrators who deploy, support, maintain, and troubleshoot Avaya Communicator on Android, iPad, iPhone, and Windows.

Related resources

Documentation

See the following documents in the Avaya Communicator portfolio at http://support.avaya.com.

Document number	Title	Use this document to:	Audience
Overview			
—	*Avaya Communicator Overview and Specification for Android, iPad, iPhone, and Windows*	Understand high-level product functionality, performance specifications, security, and licensing.	Customers and sales, services, and support personnel
Using			
—	*Using Avaya Communicator for Android*	Understand overview, installation, and feature usage information.	Enterprise users

Table continues…

Document number	Title	Use this document to:	Audience
18-603943	*Using Avaya Communicator for iPad*		
—	*Using Avaya Communicator for iPhone*		
18-604158	*Using Avaya Communicator for Windows*		

Other product documentation:

- *Deploying Avaya Aura® Communication Manager on System Platform*
- *Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment*
- *Administering Avaya Aura® Communication Manager*
- *Deploying Avaya Aura® Session Manager*
- *Administering Avaya Aura® Session Manager*
- *Deploying Avaya Aura® Presence Services*
- *Deploying Avaya Aura® Presence Services on VMware® in Virtualized Environment*
- *Administering Avaya Aura® Presence Services*
- *Avaya Identity Engines Ignition Server Administration*
- *Avaya Identity Engines Ignition CASE Administration*
- *Avaya Identity Engines Ignition Access Portal Administration*
- *Deploying Avaya Multimedia Messaging*
- *Avaya Multimedia Messaging Overview and Specification*
- *Avaya one-X® Client Enablement Services Overview and Specification*
- *Implementing Avaya one-X® Client Enablement Services*
- *Administering Avaya one-X® Client Enablement Services*
- *Deploying Avaya Aura® Conferencing*
- *Administering Avaya Aura® Conferencing*

You can also download the latest copies of these product documents related to Avaya Communicator administration from the Avaya Support website at http://support.avaya.com.

You can also see *Updating server certificates to improve end-user security and client user experience* at https://downloads.avaya.com/css/P8/documents/100180626.

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.

Document changes since last issue

The document includes the following changes since the last issue:

- Included the Avaya Communicator for iPhone administration content as 2.1 is the first release of Avaya Communicator for iPhone.
- Included the administration content specific to Avaya Communicator for Android 2.1 and Avaya Communicator for Windows 2.1.

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. Click **Documents**.
4. In the **Enter Your Product Here** search box, type the product name and then select the product from the drop-down list.

5. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
6. 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.
7. Click **Enter**.

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.

Send us your comments

Avaya appreciates any comments or suggestions that you might have about this product documentation. Send your comments to infodev@avaya.com.

Chapter 2: Avaya Communicator overview

Avaya Communicator provides enterprise users with simple access to all communication tools in a single interface. Use Avaya Communicator to log in to your enterprise Avaya Aura® server and make and receive calls from the telephone extension using your mobile device or computer.

Using Avaya Communicator, you can also:

- Send instant messages.
- Access your call history.
- Access your Avaya Aura® and local contacts.
- Perform an enterprise search.
- Manage your presence status.

Avaya Communicator is available on the following platforms:

- Mobile platforms: Avaya Communicator for Android, iPad, and iPhone
- Desktop platform: Avaya Communicator for Windows

Use Avaya Communicator to perform entry-level configurations to achieve mass adoption of the application through deployment into older infrastructure environments.

Avaya Communicator provides high impact unified communications (UC) and Collaboration features for customers in SIP environments.

Avaya Communicator can interwork with the following services:

- Extension to Cellular (EC500)
- Client Enablement Services
- VoIP
- Avaya Multimedia Messaging

Each Avaya Communicator product provides some or all of the services. For more information, see the using guide for that product.

Solution architecture

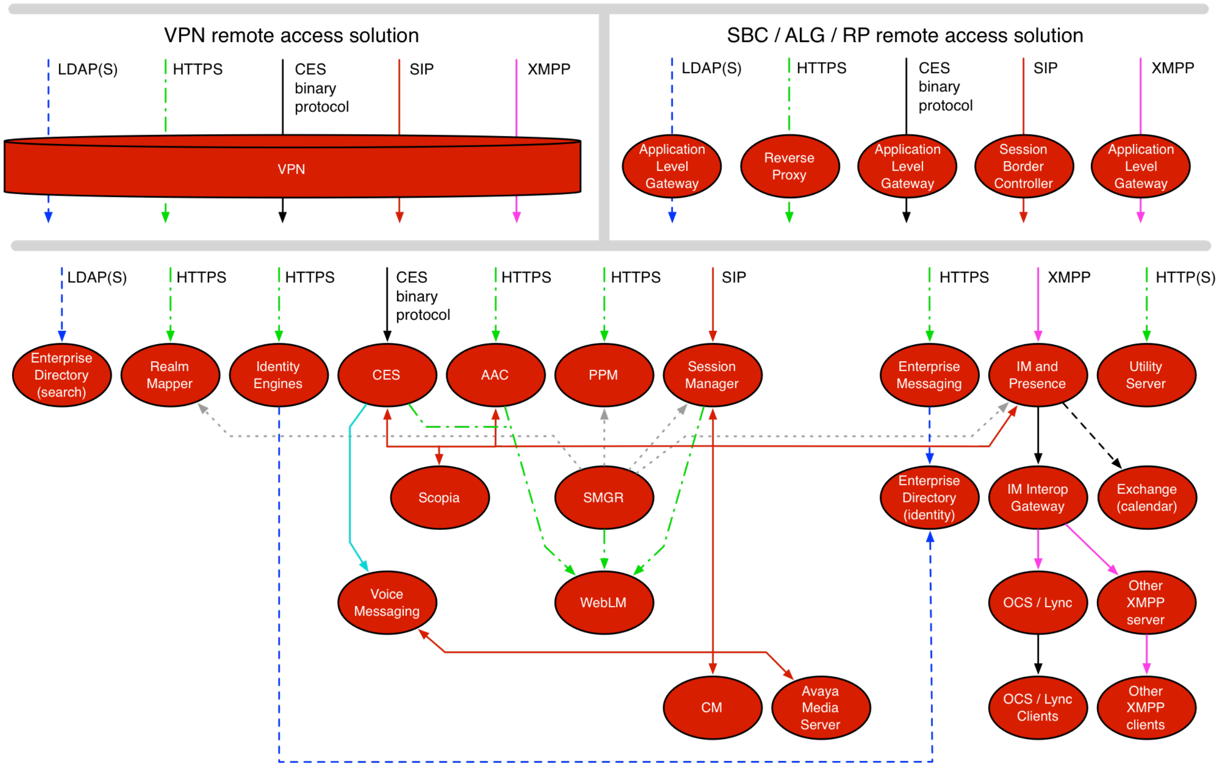

Figure 1: Solution architecture of Avaya Communicator

	Android	iPhone	iPad	Windows
Avaya Aura® Session Manager / SIP	Yes[1]	Yes[1]	Yes	Yes
Avaya one-X® Client Enablement Services	Yes[1]	Yes[1]	No	No
EC500	Yes[1]	Yes[1]	No	No
Avaya Aura® Presence Services (Presence)	Yes with Client Enablement Services	Yes with Client Enablement Services	Yes	Yes
Avaya Aura® Presence Services (XMPP IM)	No	No	Yes	No

Table continues…

[1] SIP, Client Enablement Services, and EC500 are optional for Avaya Communicator for Android and iPhone. At a minimum, one service must be provisioned and any multi-configuration option is supported.

	Android	iPhone	iPad	Windows
Avaya Multimedia Messaging	Yes	Yes	Yes	Yes
Avaya Aura® Conferencing	No	No	Yes	Yes
Scopia	No	No	Yes	No
Avaya Identity Engines	No	No	Yes	No
LDAP	Yes with Client Enablement Services	Yes with Client Enablement Services	Yes	Yes

Users can gain access to the application using any of the following methods:

- Direct: For on-premise Wi-Fi access and wired access.
- VPN and Non-VPN: For off-premise remote access.

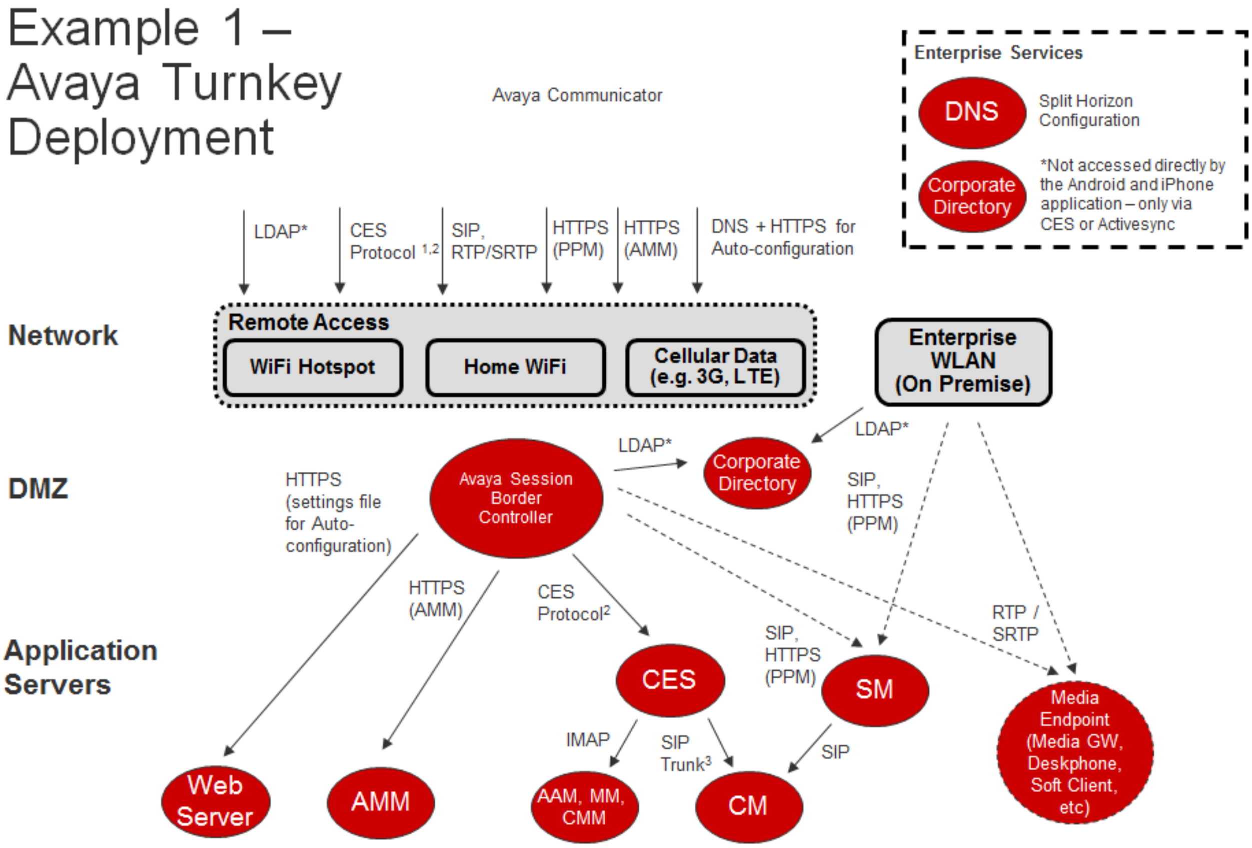
Example 1 – Avaya Turnkey Deployment
Avaya Communicator
Enterprise Services
DNS
Split Horizon Configuration
Corporate Directory
*Not accessed directly by the Android and iPhone application – only via CES or Activesync
LDAP*
CES Protocol 1,2
SIP, RTP/SRTP
HTTPS (PPM)
HTTPS (AMM)
DNS + HTTPS for Auto-configuration
Network
Remote Access
WiFi Hotspot
Home WiFi
Cellular Data (e.g. 3G, LTE)
Enterprise WLAN (On Premise)
DMZ
HTTPS (settings file for Auto-configuration)
Avaya Session Border Controller
LDAP*
Corporate Directory
LDAP*
SIP, HTTPS (PPM)
Application Servers
HTTPS (AMM)
CES Protocol2
SIP, HTTPS (PPM)
RTP / SRTP
CES
SM
Media Endpoint (Media GW, Deskphone, Soft Client, etc)
IMAP
SIP Trunk3
SIP
Web Server
AMM
AAM, MM, CMM
CM

Figure 2: Different deployment scenarios: Avaya turnkey deployment

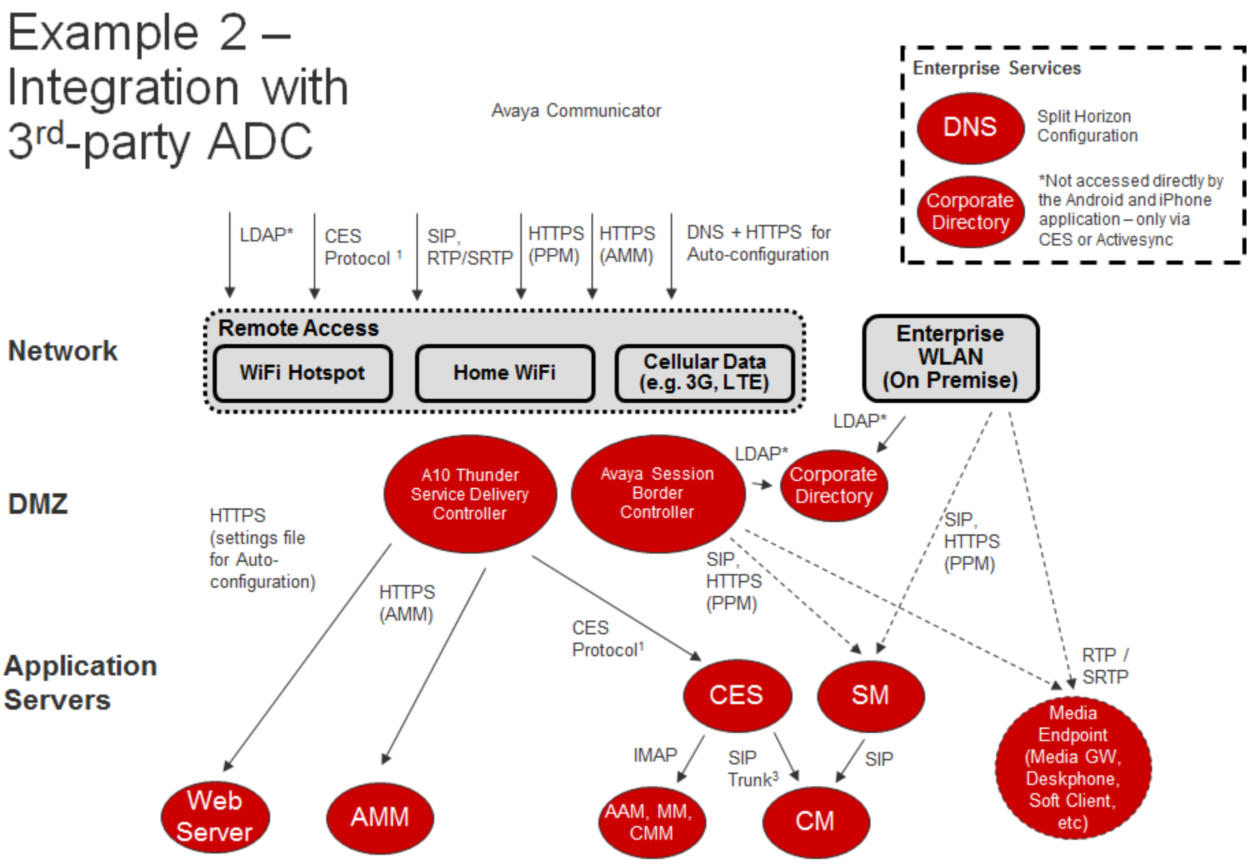
Example 2 – Integration with 3rd-party ADC
Avaya Communicator
Enterprise Services
DNS
Split Horizon Configuration
Corporate Directory
*Not accessed directly by the Android and iPhone application – only via CES or Activesync
LDAP*
CES Protocol 1
SIP, RTP/SRTP
HTTPS (PPM)
HTTPS (AMM)
DNS + HTTPS for Auto-configuration
Network
Remote Access
WiFi Hotspot
Home WiFi
Cellular Data (e.g. 3G, LTE)
Enterprise WLAN (On Premise)
DMZ
LDAP*
LDAP*
A10 Thunder Service Delivery Controller
Avaya Session Border Controller
Corporate Directory
HTTPS (settings file for Auto-configuration)
HTTPS (AMM)
CES Protocol1
SIP, HTTPS (PPM)
SIP, HTTPS (PPM)
RTP / SRTP
Application Servers
CES
SM
Media Endpoint (Media GW, Deskphone, Soft Client, etc)
IMAP
SIP Trunk3
SIP
Web Server
AMM
AAM, MM, CMM
CM

Figure 3: Different deployment scenarios: Integration with 3rd party ADC

In the Split-Horizon Domain Name System (DNS) scenario:

- When remote, the external DNS service maps a single fully qualified domain name (FQDN) to the SBC IP address.
- When on-premise, the internal DNS service maps the same FQDN to the Session Manager IP address.

If the application connects remotely through the SBC and directly to Session Manager when on-premise, the same port must function as the internal port on Session Manager and the external port on SBC.

For Avaya Communicator for Android and iPhone, the Avaya one-X® Client Enablement Services traffic always routes through Handset Server in the DMZ to simplify the deployment and use a consistent access method. The Client Enablement Services traffic does not benefit from a Split-Horizon DNS configuration. The reason is the low overhead of the traffic and 1-1 mapping between the Client Enablement Services server and Handset Server.

Avaya Communicator for Android and iPhone can accommodate single-configuration and multi-configuration deployments:

- Single-configuration deployment options:
  - Client Enablement Services only: You might choose this option if Avaya Communicator is replacing Avaya one-X® Mobile clients that were provisioned as Client Enablement Services

clients. Avaya Communicator is designed to use your existing Client Enablement Services server.

  - EC500 only: You might choose this option if Avaya Communicator is replacing Avaya one-X® Mobile clients that were provisioned in Lite mode. Avaya Communicator is designed to use your existing EC500 interface.
  - VoIP (SIP) only: Mobile SIP softphone functionality is enabled by Avaya Aura® and requires users to have a SIP account and *Mobile SIP* license.

- Multi-configuration deployment options:
  - Client Enablement Services + VoIP (SIP): This is the most common deployment configuration that delivers the most functionality and flexibility for mobile users.
  - EC500 + VoIP (SIP): This is a suitable configuration when the primary requirement is mobile VoIP. However, users require some basic cellular voice integration as well.

You can add Avaya Multimedia Messaging whenever Client Enablement Services or VoIP (SIP) is configured.

The deployment models of Client Enablement Services for remote access are unchanged for Avaya Communicator. For more information about the deployment models of Client Enablement Services, see *Avaya one-X® Client Enablement Services Overview and Specification*.

Remote access overview

Avaya mobility clients such as Avaya Communicator can operate as remote workers with the help of the Remote Worker feature. Users of such mobility clients can now seamlessly roam between the inside and outside the corporate network.

The design of Avaya Communicator is such that users can use client applications both onsite and offsite. When offsite, users might use devices with:

- Cellular data service
- Internet connectivity through a home Internet provider
- Public Wi-Fi hotspot

To support enterprise services in these cases, Avaya Communicator requires access to Avaya Aura® enterprise services from the public Internet. One means to provide this access is by using a VPN. You can also use another option to provide IP connectivity for each service required by the client using the enterprise DMZ.

Avaya Communicator supports both remote access models. The decision to choose either VPN or IP connectivity through the DMZ for remote access is a per customer design choice. To access enterprise services in these scenarios, the choice might be driven by factors such as existing remote access investments and security policy or requirements.

Split-Horizon DNS

If the Avaya Communicator client is communicating with Avaya Session Border Controller for Enterprise (Avaya SBCE), you must provision DNS entries for Avaya Aura® Session Manager, Presence Server, and the Enterprise Search (LDAP) server that:

- Resolve to the internal service IP addresses for internal DNS clients
- Resolve to the Avaya SBCE IP address for external DNS clients

By doing this, you do not need to perform any configuration change for users that use the client both inside and outside your corporate network. This scenario is known as Split-Horizon Domain Name System (DNS) scenario.

For information about installing Avaya SBCE, see *Installing Avaya Session Border Controller for Enterprise*. For information about configuring Avaya SBCE, see *Administering Avaya Session Border Controller for Enterprise*.

EC500 service overview

The EC500 feature provides users with the capability to have one administered telephone that supports Communication Manager features for both an office telephone and up to four outside telephones. An office telephone is a telephone that is directly under the control of Communication Manager, such as a deskphone in an office. EC500 works with any type of wireless or cellular service.

With EC500, users can receive and make official calls anywhere, anytime, even if the users are not in the office. In addition, users can also access Communication Manager features through the mobile phone. Users can enable and disable EC500 so that the mobile phone does not always receive office telephone calls. Users can also change between the mobile phone and office telephone during an ongoing EC500 telephone call.

With EC500, the application provides the Simultaneous Ring feature. You can continue to connect to the enterprise with a single telephone number and use voice mail capabilities. You can also forward calls to any other telephone number or send all calls to the corporate voice mail number.

The tariff rates of the service provider are applicable when you make calls using the EC500 service. The application does not affect how you receive personal calls on the device.

If the user enables Client Enablement Services and EC500, then pressing the EC500 button has no effect on endpoints that the application manages using the Ring Phones feature of Client Enablement Services. Hence, for Client Enablement Services users, you must remove the EC500 button on Communication Manager.

EC500 Call Suppression

EC500 Call Suppression is a Communication Manager feature that supports the deployment of dual-mode device applications with Avaya Aura® 6.2 Feature Pack 2 and later versions. The feature ensures that users of dual-mode client applications such as Avaya Communicator receive only a single incoming call on the device for that particular extension. EC500 Call Suppression ensures that users receive an alert either by a VoIP call or a cellular call, but never both.

You must configure the **Extend Call** button on Communication Manager for EC500 Call Suppression to function properly. Additionally, you must enable the EC500 status for the station regardless of whether the user has EC500 mapping or ONE-X mapping.

The high-level implementation on Communication Manager is as follows:

- For each incoming call to a dual-mode device application, that is, EC500 + VoIP, Communication Manager configures an interval of 4 seconds before starting an EC500 cellular call. You can change the default interval of 4 seconds on Communication Manager.
- When Communication Manager starts an incoming call, Communication Manager pauses for a response from the VoIP interface of the dual-mode device application. If the server establishes that the VoIP application has received an incoming call alert, the server suppresses the EC500 call to the device.
- If the server cannot determine if the VoIP application received an alert after an interval of 4 seconds, then Communication Manager initiates an EC500 cellular call to the device.

The Communication Manager logic is optimized for applications that are not registered with VoIP device clients on Session Manager. In such cases, Communication Manager initiates the EC500 calls immediately.

Note:

- EC500 Call Suppression is available only when the server installation is Avaya Aura® 6.2 FP2 or later. Users administered on previous versions might need to disable the EC500 service in the application when users are within the Wi-Fi range and when users are connected to the VoIP service.
- EC500 Call Suppression logic is applicable for calls that you make using Client Enablement Services only with Communication Manager 6.3 FP6 and later versions.

Avaya one-X® Client Enablement Services overview - Avaya Communicator for Android and iPhone

The application connects to the Client Enablement Services server to provide multiple Avaya Unified Communications (UC) capabilities, such as telephony and presence.

Use the Client Enablement Services features on your device to gain access to your enterprise telephone system. You can use your device as your deskphone extension to:

- Make and receive calls.
- Review voice mails.
- Search the corporate directory.

If the user enables Client Enablement Services and EC500, then pressing the EC500 button has no effect on endpoints that the application manages using the Ring Phones feature of Client Enablement Services. Hence, for Client Enablement Services users, you must remove the EC500 button on Communication Manager.

VoIP service overview

Use Avaya Communicator as a VoIP softphone for SIP calling over enterprise or public Wi-Fi networks and also cellular data networks. With Avaya Communicator, you can take advantage of the Avaya Aura® SIP environment and use VoIP connectivity from the device.

VoIP connectivity provides the following capabilities:

- Support for inbound and outbound calls
- Active call features
- Support for multiple active calls
- Multiple Device Access (MDA)
- Consultative conference and transfer

The Avaya Communicator VoIP service implements call preservation for VoIP calls. If you are on a VoIP call in an area where access to the network is impaired, that is, weak Wi-Fi signal strength, you might have a situation where the application disables the midcall features on your VoIP call. Instead of dropping the call in such an environment, Avaya Communicator allows the audio for the call to continue if possible subject to the limitations of the underlying network.

Avaya Multimedia Messaging service overview

Use Avaya Communicator to connect to the Avaya Multimedia Messaging service to:

- Exchange text-based instant messages with other users using Avaya Multimedia Messaging. You can also add multiple participants to a conversation.
- Receive image, audio, video, and generic attachments in an Instant Messaging (IM) conversation.

For Avaya Communicator for Windows and iPad, all users can send generic attachments. However, only users with enhanced privileges can use the built-in recording feature of the application to attach audio, video, or image files.

For Avaya Communicator for Android and iPhone, only users with enhanced privileges can send generic attachments and use the built-in recording feature of the application to attach audio, video, or image files.

- Search for archived or inactive conversations.

You must log out and log in to the application to recognize a newly assigned rich content entitlement. If your entitlement is removed when you are logged into the application, you can continue to access the rich-media privileges until the application restarts or you need to relogin.

You must add the messaging domains on the Avaya Multimedia Messaging server. The messaging domain list provides an indication to the Avaya Multimedia Messaging clients as to which domains are reachable by the Avaya Multimedia Messaging server. For more information, see *Deploying Avaya Multimedia Messaging*.

Chapter 3: Requirements

Server requirements

To support Avaya Communicator, you need the following main Avaya Aura® server elements. For more information about products that interwork with Avaya Communicator, see http://support.avaya.com/CompatibilityMatrix/Index.aspx.

- Avaya Aura® Session Manager Release 6.2 or 6.3.
- One of the following Avaya Aura® Communication Manager servers:
  - Avaya Aura® Communication Manager Feature or Evolution Server Release 6.3.1 (FP2, SP1) for encrypted audio and unencrypted video.
  - Avaya Aura® Communication Manager Feature or Evolution Server Release 6.3.2 (FP3) for encrypted audio and encrypted video.
- Avaya Aura® System Manager Release 6.2 or 6.3.
- Core Avaya Aura® network must be at FP4 or later to support audio and video SRTP interoperability with Avaya Scopia®.
- Avaya Aura® Conferencing Release 7.2 or later if you want to use the Conference (audio and video) and Web Collaboration features.
- Avaya Aura® Presence Services Release 6.1 SP2 or later if you want to use the presence and instant messaging features. To use the unified login feature, you must have Avaya Aura® Presence Services Release 6.2.2 FP3 with SASL authentication configured and also Avaya Identity Engines.

  Important:

  Avaya Communicator for Android, iPhone, and Windows do not support unified login.

If you configure Avaya Communicator for iPad and Windows to use Presence Services for the Messaging service, then users can send and receive instant messages with Microsoft Office Communicator 2007 R2 users and Microsoft Lync users. For more information about using Presence and IM with users of these Microsoft clients, see *Integrating Avaya Aura® Presence Services with Microsoft OCS*.

You can optionally use the Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2 or later to provide a secure connection for the following Avaya Communicator settings when users are working remotely and do not connect to the enterprise network.

Avaya SBCE provides the following features:

- SIP-TLS to Avaya Aura® Session Manager and Avaya Aura® Presence Services for Presence functionality
- XMPP or HTTP relay to Avaya Aura® Presence Services or Avaya Multimedia Messaging for instant messaging functionality
- PPM over HTTPS to Avaya Aura® Session Manager
- LDAPS to LDAP server

Related links

Conference requirements on page 22
Port utilization on page 72

Multiple Device Access requirements

Avaya Communicator supports Multiple Device Access (MDA) to provide the capability to:

- Log on to the same extension from multiple devices.
- Answer a call from multiple devices.
- Join a call from other logged in devices.
- Simultaneously ring all logged in devices when you receive a call on your extension.

The number of devices that can log in simultaneously depends on the Avaya Aura® configuration for an extension.

Block New Registration When Maximum Registrations Active is an Avaya Aura® feature. If you select the **Block New Registration When Maximum Registrations Active** check box and an endpoint attempts to register after the number of registration requests exceed the administered limit, the system denies any new request. The system sends a warning message and stops SIP service to the endpoint.

When the user reaches the maximum simultaneous device limit, the Avaya Aura® configuration determines whether the first or the last logged in device is denied access.

Avaya Communicator supports the **Block New Registration When Maximum Registrations Active** feature only with Session Manager 6.3.3, that is, Avaya Aura® 6.2 FP2 SP1 or later. If you are using Avaya Communicator with an earlier version of Session Manager, you must disable the **Block New Registration When Maximum Registrations Active** feature.

MDA requires the use of TLS endpoints. Users can log in to their extension with a TCP device. However, a new incoming call does not ring on the TCP device and the user cannot join the call from that device.

Some MDA limitations exist for IM and Presence between Avaya Communicator and other applications. For more information, see *Multiple Device Access White Paper*.

For more information about other MDA user limitations, see:

- *Using Avaya Communicator for Android*
- *Using Avaya Communicator for iPad* (18-603943)

- *Using Avaya Communicator for iPhone*
- *Using Avaya Communicator for Windows* (18–604158)

Simultaneous registration

You can configure more than one Session Manager server. If you have more than one Session Manager server, the first Session Manager server is known as the primary server and the additional Session Manager server is known as secondary server.

If the primary server fails or if Avaya Communicator cannot connect to the primary Session Manager server, Avaya Communicator automatically fails over to the secondary Session Manager server to ensure service continuity for users. If failover occurs while on an active call, the application preserves the speech path when possible.

Failover and failback occur as quickly as possible without user intervention. Failover is possible because of the Simultaneous Registration feature.

Avaya Communicator supports the following configurations:

- Registration to a single Session Manager server, that is, nonredundant configuration.
- Registration to multiple Session Manager servers as a redundancy mechanism, that is, simultaneous registration.
- Registration to multiple Session Manager servers with potential failover to a Branch Session Manager, that is, simultaneous registration with failover to a branch.

Conference requirements

The following sections describe requirements for conferences, including the requirements for setting up Avaya Scopia®.

Requirements for mixed conference environment with Avaya Communicator

In a mixed conference environment with MX and Avaya Aura® Conferencing, you must enable the `isFocus` parameter for the MX conference system if possible. If you cannot enable the `isFocus` parameter, the conference call might freeze when you try to open Collaboration. You cannot resume the conference call for approximately 30 seconds.

Requirements for Avaya Scopia®

For detailed Avaya Scopia® administration information, see:

- *Administrator Guide for Avaya Scopia® Management*
- *Administrator Guide for Avaya Scopia® Management for Avaya Aura® Collaboration Suite*
- *Administrator Guide for Avaya Scopia® Elite 6000 Series MCU*
- *Administrator Guide for Avaya Scopia® Elite 6000 Series MCU for Avaya Aura® Collaboration Suite*

You must complete the following configuration to join or host Avaya Scopia® conferences from Avaya Communicator.

- Configure interoperability for video calls between Avaya Communicator and Avaya Scopia®. The following table describes supported configuration options for different calls.

  Avaya Communicator for iPad supports a maximum resolution and frame rate of 352 x 288 pixels @ 30 fps. Avaya Communicator for Windows supports a maximum resolution and frame rate of 1280 x 720 pixels @ 30 fps.

  ⚠ **Warning:**

  The TLS and SRTP configuration and VIVR dialing options described in the following table have not been fully tested on all Avaya Communicator platforms, and might not work as expected.

  Note:

  To have video when dialing through Avaya Scopia® VIVR, users must initially dial the video call to the VIVR number. Users cannot dial in with audio only and then escalate to video.

  Table 1: Avaya Scopia® configuration options

Video call type	Supported configuration methods	Supported features
Point-to-point video calls between Avaya Communicator and Avaya Scopia®	Connect Avaya Scopia® to Avaya Aura® Communication Manager through H.323 signaling (Not recommended)	- H.264 baseline profile HD video - Mid-call control, including mute, pause, and hold
	Connect Avaya Scopia® to Avaya Aura® Session Manager through TCP SIP signaling (Recommended)	- H.264 baseline profile HD video - Mid-call control, including mute, pause, and hold - Escalate and de-escalate video
	Connect Avaya Scopia® to Avaya Aura® Session Manager through TLS SIP signaling **Note:** With this configuration method, you might encounter a limitation where Avaya Scopia® cannot connect to TCP endpoints	Same as TCP SIP signaling, with the option of SRTP connections.
Multipoint video calls between Avaya Communicator and a federated Avaya Aura® Conferencing	Connect Avaya Scopia® iView to Avaya Aura® Session Manager through TCP SIP signaling	- H.264 baseline profile HD video - Mid-call control, including mute, pause, and hold - Escalate and de-escalate video

Table continues…

Video call type	Supported configuration methods	Supported features
with Avaya Scopia® bridge **Note:** Avaya Communicator connects directly to Avaya Aura® Conferencing and not to Avaya Scopia® MCU.		- All standard Avaya Aura® Conferencing features supported on Avaya Communicator. Avaya Communicator for Android does not support video with Avaya Aura® Conferencing. You can access Avaya Aura® Conferencing web collaboration, roster indication, and moderator controls when: - Avaya Communicator for Android connects to Avaya Aura® Conferencing over SIP. - You have also installed the Avaya Web Collaboration application available in the Google Play Store. Avaya Communicator for iPad support with Avaya Aura® Conferencing includes single video stream, video SRTP, built-in web collaboration, roster indication, and moderator controls. Avaya Communicator for iPhone does not support video with Avaya Aura® Conferencing. You can access Avaya Aura® Conferencing web collaboration, roster indication, and moderator controls when: - Avaya Communicator for iPhone connects to Avaya Aura® Conferencing over SIP. - You have also installed the Avaya Web Collaboration application available in the Apple App Store. Avaya Communicator for Windows support with Avaya Aura® Conferencing includes continuous presence, video SRTP, built-in web collaboration, roster indication, and moderator controls.
Multipoint video calls with direct connection between Avaya Communicator and Avaya Scopia®	Connect Avaya Scopia® iView to Avaya Aura® Session Manager through TCP SIP signaling	- H.264 baseline profile HD video - Mid-call control, including mute, pause, and hold - Escalate and de-escalate video

Table continues…

Video call type	Supported configuration methods	Supported features
		- Avaya Scopia® content sharing as part of the gallery video stream and moderator controls **Note:** Avaya Scopia® MCU5000 does not support content sharing mixed with video stream. Avaya Communicator for Windows users cannot share content or join the Scopia conference as moderators from the client user interface. Some controls are accessible through DTMF digits, but these controls might not work as expected. A known limitation is that the Lecture functionality might disable video. - Avaya Scopia® roster name display - Access to some controls through DTMF - Directly dialing into an MCU virtual room or dialing in through a VIVR autoattendant
	Connect Avaya Scopia® iView to Avaya Aura® Session Manager through TLS SIP signaling	Same as TCP SIP signaling, with the option of SRTP connections.

- Complete all other required administration tasks in Avaya Scopia®.
  - Add new users and configure virtual meeting rooms for users in Avaya Scopia® under the **Users** menu.
  - Configure meeting types in Avaya Scopia® under **Settings** > **Meetings** > **Meeting Types**.
  - Enable autoattendant numbers in Avaya Scopia® under **Settings** > **Meetings** > **Auto-Attendant**.
  - Configure required endpoints for point-to-point calls in Avaya Scopia® under the **Endpoints** menu.
  - Configure routing of autoattendant numbers and meeting room ranges between Avaya Aura® and Avaya Scopia®. The meeting room prefix used in Avaya Scopia® must be a number that you can route between Avaya Aura® Session Manager and Avaya Scopia® over the SIP trunk.

Supported codecs

Avaya Communicator supports the following audio codecs:

Codec	Avaya Communicator for Android	Avaya Communicator for iPad	Avaya Communicator for iPhone	Avaya Communicator for Windows
G.711 A-law (PCM-A)	Yes	Yes	Yes	Yes
G.711 U-law (PCM-U)	Yes	Yes	Yes	Yes
G.722	Yes	Yes	Yes	Yes
G.726	Yes	No	No	Yes
G.729A	Yes	Yes	Yes	Yes
G.729B (G.729A with annex B silence suppression)	Yes	No	Yes	No
iSAC	No	Yes	Yes	Yes

Avaya Communicator supports the following video codecs:

Codec	Avaya Communicator for Android	Avaya Communicator for iPad	Avaya Communicator for iPhone	Avaya Communicator for Windows
H.263 (SD)	No	No	No	Yes
H.264 Advanced Video Coding (AVC)	No	Yes	No	Yes
H.264 Scalable Video Coding (SVC)	No	No	No	Yes

For information on bandwidth requirement for different codecs, see the *Codec Selection* section in *Avaya IP Voice Quality Network Requirements* on the Avaya website at http://support.avaya.com.

DSCP values

The Avaya Communicator client uses the following default Differentiated Services Code Point (DSCP) values to mark packets to support network quality of service mechanisms:

- Audio: 46
- Video: 26

DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. You can override the default values for Avaya Communicator for Windows and iPad using the linked procedure.

Related links

Configuring the audio and video quality of service settings on page 31

Supported LDAP directories

Supported LDAP directories for Avaya Communicator for Android

Avaya Communicator for Android does not connect to any LDAP directories directly. Avaya Communicator for Android supports integration with LDAP directories using Client Enablement Services.

If the user configures Microsoft ActiveSync on the Android device, Avaya Communicator for Android searches the Exchange server for contacts.

Supported LDAP directories for Avaya Communicator for iPad

Avaya Communicator for iPad supports LDAPv3, that is, both LDAP and secure LDAP, with Microsoft® Active Directory 2003 and 2008. You must set up the LDAP server using an FQDN and not an IP address.

During an LDAP search, Avaya Communicator for iPad searches the following attributes:

- sn: Surname or family name
- givenName
- cn: Common name

The search results also return the thumbnailPhoto and jpegPhoto attributes for the contact. Thumbnail photo is in JPEG format.

After the search, Avaya Communicator for iPad constructs the name using the sn and givenName attributes.

If a user adds a contact to the Communicator contacts and that contact is already an enterprise contact, the system overwrites the name with the last name and first name on Avaya Aura® 6.2 FP3 and later. If a user adds a contact from an enterprise search, the system uses the mail and telephone number attributes to determine whether the contact is added to Enterprise or Private in the Communicator contacts. The Avaya Communicator for iPad client displays the homephone, mobile, and mail attributes for the contact that the user adds in the Contacts fan.

Supported LDAP directories for Avaya Communicator for iPhone

Avaya Communicator for iPhone does not connect to any LDAP directories directly. Avaya Communicator for iPhone supports integration with LDAP directories only using Client Enablement Services.

Supported LDAP directories for Avaya Communicator for Windows

Avaya Communicator for Windows supports LDAPv3, that is, both LDAP and secure LDAP, with the following directories:

- Microsoft® Active Directory 2003, 2008, and 2012
- Novell® eDirectory
- IBM® Lotus® Domino®

You must set up the LDAP server using an FQDN and not an IP address. During an LDAP search, Avaya Communicator for Windows searches the following attributes:

- cn
- sn: Surname or family name
- givenName
- displayName

The search results also return the thumbnailPhoto and jpegPhoto attributes for the contact. Thumbnail photo is in JPEG format.

After the search, Avaya Communicator for Windows constructs the name using the sn and givenName attributes.

If a user adds a contact to the Communicator contacts and that contact is already an enterprise contact, the system overwrites the name with the localized display name on Avaya Aura® System Manager. If a user adds the contact from an enterprise search, the system uses the mail attribute to determine whether the contact is combined or aggregated with a Microsoft Outlook contact. The Avaya Communicator for Windows client displays the homephone, work, mobile, and chat attributes for the contact that the user adds in the Contacts fan.

Chapter 4: Network configuration

The Avaya Communicator network configuration affects the quality of audio and video services. Use the following information to obtain optimal quality with Avaya Communicator.

Network diagnostics and system configuration for Avaya Communicator

Media quality on a consumer device is influenced heavily by the network in which the device is deployed and also the deployed Avaya Aura® system configuration. The way in which the device is connected to the wireless network can also influence media quality. For example, a cellular data connection with a virtual private network.

The Avaya Communicator client video encoders adjust to fit within the bandwidth *envelope* that the network provides. However, the amount of bandwidth available influences the resulting video quality. If more bandwidth is available, the resulting video quality for the user is better.

Network diagnostics

Avaya Communicator provides a call quality indicator to help you diagnose some of the issues that occur in wireless networks. By tapping and holding the call duration timer box for an active call, you can view the audio and video statistics for the current session. You can use these statistics to determine the network conditions that might be affecting the session.

Note:

On Avaya Communicator for Windows, to view the call statistics, you must use the drop-down menu on the *Name* field and select **Call Statistics**. The Quality attribute in Audio Statistics represents the network link quality and not the local PC related items.

Packet loss

As you approach 1% packet loss, you might see visual artifacts or hear audible artifacts. For example, see broken images. As you approach 2 to 3% packet loss, you might see consistent visual artifacts and hear audible artifacts.

Note:

Packet loss characteristics influence the occurrence of visual and audible artifacts. For example, a burst of lost packets affects the media quality differently than an even distribution of lost packets.

Jitter

Jitter is caused when the packets that make up a media stream are not delivered at regular intervals to the endpoint. For the most part, buffering cancels the effects of jitter. However, buffering causes delay. Delay or latency has a noticeable effect on lip synchronization between the audio and video feed for the user. Lip synchronization issues occur when the delay exceeds 100 ms.

Generally speaking, network and network engineering issues influence the statistics described above. If you find the values of the impairments exceeding the limits listed above, you might need to contact your network administrator for more diagnostic information to solve any network implementation issues.

Avaya Aura® configuration

The Avaya Aura® solution enables the administrator to configure the maximum bandwidth permitted on a per-user basis. Network engineers must also confirm that the appropriate classes of service for the network are defined and that the correct DSCP mark is set for media in the Avaya Aura® configuration.

For Avaya Aura® Conferencing 7.0 Service Pack 2 or later, each user is assigned a specific profile for video, which enables different classes of resolution. These profiles can be provisioned to be 180p or 360p, but the profiles can be provisioned only at the conferencing server, not at the client device.

If you have good quality video, but you are dissatisfied with the resolution, you must check the provisioning at your endpoint to confirm that adequate bandwidth and the correct profile have been assigned to your endpoint. To determine the resolution you are receiving on the Avaya Communicator client, check the call statistics for the resolution as well as the frames per second provided.

Virtual Private Networks (VPNs)

Virtual private networks provide a significant challenge to high-quality video because as a security measure the VPN assigns video packets the same priority it does to all other packets. This method prevents malicious users from differentiating certain classes of traffic that could lead to targeted attacks on clients. VPNs effectively negate network engineering for differentiated service and also introduce additional delay, which can be problematic for media packets that depend on timely receipt of all video packets for subjectively good quality.

Troubleshooting Logs

When troubleshooting issues, it might become necessary to report logs to your support organization. Logging for the Avaya Communicator client includes media quality statistics that record information about network performance for analysis by support teams. To enable these logs, you must enable the **Verbose Logging** option in the Settings dialog box. These logs can assist support teams in diagnosing media issues due to network performance.

To send log files, in **Settings**, select **Support Information** > **Report a problem** or tap **Support** > **Report a Problem** > **Send Logs**.

Configuring the audio and video quality of service settings

About this task

Use the Avaya Aura® System Manager administration interface to configure the audio and video quality of service (QoS) settings. For more information, see *Installing and Configuring Avaya Aura® Session Manager* on the Avaya website at http://support.avaya.com.

Note:

Avaya Communicator for Android and iPhone do not support configuring quality of service settings.

Procedure

1. Log in to Avaya Aura® System Manager.
2. Select **Elements** > **Session Manager**.
3. In the navigation pane, select **Device and Location Configuration** > **Device Settings Groups**.
4. On the Device Settings Groups page, select the appropriate group and click **Edit**.

   For example, the group might be a default group, a terminal group, or a location group.
5. On the Device Settings Group page, click the right-arrow for **DIFFSERV/QOS Parameters**.
6. Configure the PHB values.
7. Click **Save**.
8. In the navigation pane, select **Device and Location Configuration** > **Location Settings**.
9. On the Location Settings page, select the device settings group you modified in Steps 4 through 6 from the **Device Setting Group** field for each appropriate location.
10. Click **Save**.

Wi-Fi best practices

While performing the bandwidth planning calculation, you must think about the codec to use in each call scenario based on your deployment configuration. For more information about media bandwidth planning calculation, see *Avaya Aura® Solution Design Considerations and Guidelines, Release 6.2*.

When you use Avaya Communicator as a VoIP client on a Wi-Fi network, various factors ensure best performance, security, and reliability. You must know the limitations of the Wi-Fi implementation.

Prior to operational deployment, test Avaya Communicator within your environment to ensure that the function and performance capabilities meet your requirements. Due to the variability of Wi-Fi and Cellular 3G or 4G data connections, the stability and voice quality of the application can vary widely.

The following points discuss the parameters of the Wi-Fi network and supporting infrastructure, which you can set up to optimize performance and security.

- For a home Wi-Fi router, use the latest firmware for the device in accordance with the instructions of the manufacturer.
- For an enterprise-class Wi-Fi security switch, ensure that the switch uses the latest software release.
- If you change the configuration, you must remove the Wi-Fi settings from your network for any device that connects to your Wi-Fi router. When you remove the Wi-Fi settings, you prevent the device from trying to connect to your network with the old configuration. After you apply the new settings, you can reconnect the device to your network.
- For applications that use a Wi-Fi security switch or router, establish a VLAN for traffic use on your new SSID. Configure the new VLAN with dedicated bandwidth control to Session Manager.
- For applications that use a Wi-Fi security switch or router, configure the switch or the router so that all inbound traffic to the new SSID gets higher traffic priority. This feature might be unavailable on some Wi-Fi switch or routers.
- Disable hidden networks. Hidden networks do not broadcast the SSID. Hence, devices face difficulties while detecting the hidden network resulting in increased connection time and reduced reliability of autoconnection.
- Certain devices might be adversely affected by enabling TSPEC, which is an 802.11 Traffic Specification configuration, on the wireless network. This might cause significant delays in the actions that the user performs or packet loss. By disabling TSPEC, you might be able to resolve issues with these devices.
- Set security to WPA2, known as AES. AES is the strongest form of security that Wi-Fi products offer. When you enable WPA2, select a strong password based on the enterprise guidelines. If your device does not support WPA2, opt for the WPA/WPA2 mode, known as the WPA mixed mode. In the WPA mixed mode, the new devices use the stronger WPA2 AES encryption, while the older devices connect to the old WPA TKIP-level encryption. If your Wi-Fi router does not support the WPA/WPA2 mode, then you can choose the WPA (TKIP) mode.
- Connecting from the client application to Session Manager through Network Address Translation (NAT) causes connection problems with SIP signaling. The client application connects, but does not operate correctly. Hence, do not connect to Session Manager through NAT. To address problems with NAT, you can use a VPN client or Session Border Controller for remote endpoint deployments.
- When you travel with a device, the device might try connecting to Access Points (APs) that are part of a different subnetwork or SSID. In this case, the device functions differently depending on whether you are on a call or not.

  The following table describes the impact of changing SSID and subnetwork conditions. Many of these combinations of subnetworks and SSIDs require manual intervention. Hence, you must use a single SSID for devices throughout the enterprise and a single subnetwork for a geographic location. If you are using a device from the home network through a VPN, you might have to manually select the correct SSID after you return to your workplace. Manual selection might be necessary as the device does not always connect to the last SSID that was in use at a location.

Condition	1	2	3	4	5
SSID	Same	Different	Same	Different	Same Separate WLAN
Subnetwork	Same	Same	Different	Different	Same Separate WLAN
Call Maintenance	Yes	No	No	No	No
Automatic client registration		Yes	No	Yes	Yes
Manual client registration			N/A		
Client restart	No	No	Yes	No	No
Manually select the SSID	No	Yes**	No	Yes**	No
Renew the DHCP	No	No	Yes	No	No

Note:

For Condition 5, the APs are not part of the same security switched network.

Yes** applies to a new SSID, which was previously not associated.

- Design the Wi-Fi AP distribution based on the best practices for designing VoIP Wi-Fi networks instead of straight data. Areas of weak signal cause voice quality issues and, at times, dropped calls. A signal strength and bandwidth that supports degraded data transmission might cause VoIP calls to drop or be of poor quality.
- Design the density and placement of the Wi-Fi AP according to the device Wi-Fi density. Adjust AP density accordingly in the denser areas, employing load-balancing among APs where appropriate. The device Wi-Fi capability is not as good as a laptop or of a dedicated Wi-Fi device. A Wi-Fi network that works for dedicated Wi-Fi handsets does not imply that the Wi-Fi network is acceptable for VoIP phones or other smart phones.
- Disable 40 MHz in the 2.4 GHz settings on the Wi-Fi router to reduce interference issues.
- Disable the 802.11b band to increase VoIP capacity for each AP.
- Disable the lower speeds, such as, 1, 2, and 5.5 Mbps. Change 6 Mbps to mandatory and the beacon rate to 6 Mbps, and set multicast to *automatic*. Set all other rates to *supported*. However, this setting might not be possible on a home Wi-Fi router.

If you need any help in designing the Wi-Fi service, contact Avaya Professional Services.

Related links

Supported codecs on page 26

Remote worker requirements

With Avaya Communicator, users can use the Remote Worker feature to connect to the Avaya Communicator client. Users can also access servers that you configure with Avaya Communicator, such as Presence or Avaya Multimedia Messaging, remotely when users do not connect to the enterprise network.

For more information about Avaya Multimedia Messaging features, see *Avaya Multimedia Messaging Overview and Specification*.

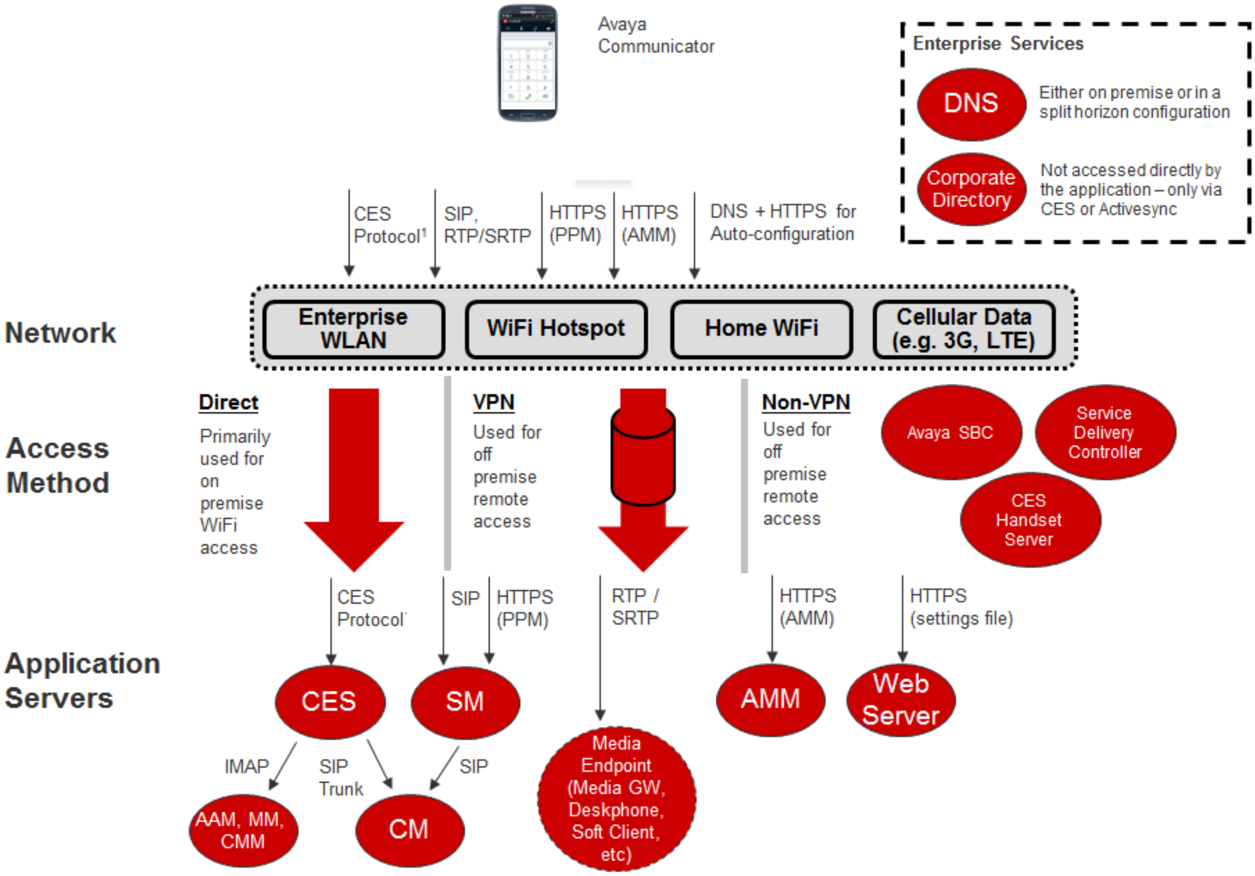
Avaya Communicator
Enterprise Services
DNS
Either on premise or in a split horizon configuration
Corporate Directory
Not accessed directly by the application – only via CES or Activesync
CES Protocol[1]
SIP, RTP/SRTP
HTTPS (PPM)
HTTPS (AMM)
DNS + HTTPS for Auto-configuration
Network
Enterprise WLAN
WiFi Hotspot
Home WiFi
Cellular Data (e.g. 3G, LTE)
Access Method
Direct
Primarily used for on premise WiFi access
VPN
Used for off premise remote access
Non-VPN
Used for off premise remote access
Avaya SBC
Service Delivery Controller
CES Handset Server
CES Protocol
SIP
HTTPS (PPM)
RTP / SRTP
HTTPS (AMM)
HTTPS (settings file)
Application Servers
CES
SM
AMM
Web Server
IMAP
SIP Trunk
SIP
AAM, MM, CMM
CM
Media Endpoint (Media GW, Deskphone, Soft Client, etc)

Figure 4: Architecture of Avaya Communicator with SBC Remote Worker functionality

To take advantage of the Remote Worker functionality, you must use the Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides the following functionality to Avaya Communicator:

- SIP-TLS to Avaya Aura® Session Manager and Avaya Aura® Presence Services for Presence functionality
- XMPP or HTTP relay to Avaya Aura® Presence Services or Avaya Multimedia Messaging for instant messaging functionality
- PPM over HTTPS to Avaya Aura® Session Manager
- LDAPS to LDAP server

Perform the following tasks to take advantage of the Remote Worker features.

Feature	Remote Worker configuration task	Documentation link
Avaya Multimedia Messaging	Configuring HTTP relay for Remote Worker functionality topic	*Administering Avaya Session Border Controller for Enterprise* at https://downloads.avaya.com/css/P8/documents/100168982 *Deploying Avaya Multimedia Messaging*
Avaya Aura® Presence Services	Creating an Avaya presence server profile topic	*Administering Avaya Session Border Controller for Enterprise* at https://downloads.avaya.com/css/P8/documents/100168982.
VoIP	Installing an Avaya SBCE device topic	*Administering Avaya Session Border Controller for Enterprise* at https://downloads.avaya.com/css/P8/documents/100168982.
Avaya Aura® Conferencing	Secure Access Link Gateway chapter	*Deploying Avaya Aura® Conferencing* at https://downloads.avaya.com/css/P8/documents/100172035
XMPP	Configuring application relay for file download topic Configuring application relay for IM topic	*Administering Avaya Session Border Controller for Enterprise* at https://downloads.avaya.com/css/P8/documents/100168982.
LDAP	Additional port assignments topic	*Avaya Session Border Controller for Enterprise Overview and Specification* at https://downloads.avaya.com/css/P8/documents/100168980

Related links

Solution architecture on page 12

SBCE deployment scenarios for failover

Avaya SBCE high availability

Enterprises might deploy the Avaya Session Border Controller for Enterprise (SBCE) in high availability (HA) mode to ensure media preservation in the event of failover of the Session Manager server. The Avaya SBCE HA pairs are deployed within the enterprise in a parallel mode configuration. The active Avaya SBCE (SBCE-A) is the primary SBC server through which all signaling packets are routed. The interface ports on the standby Avaya SBCE (SBCE-S) do not process any traffic. When a failure is detected on the active Avaya SBCE by the Avaya Element Management System (EMS), the active Avaya SBCE network interface ports are automatically disabled and the network interface ports of the standby Avaya SBCE are enabled. Failure detection and operational transfer occur without dropping packets or adding any significant amount of latency into the data paths.

Multiple Session Manager with SBCE in high availability mode

If multiple Session Manager servers are present, failover is supported by a single Avaya SBCE deployed in HA mode. The active Avaya SBCE maintains connectivity to all endpoints registered on multiple Session Manager servers. In the event of a failover of the active Avaya SBCE, the standby Avaya SBCE ensures that all media sessions of active calls are preserved appropriately.

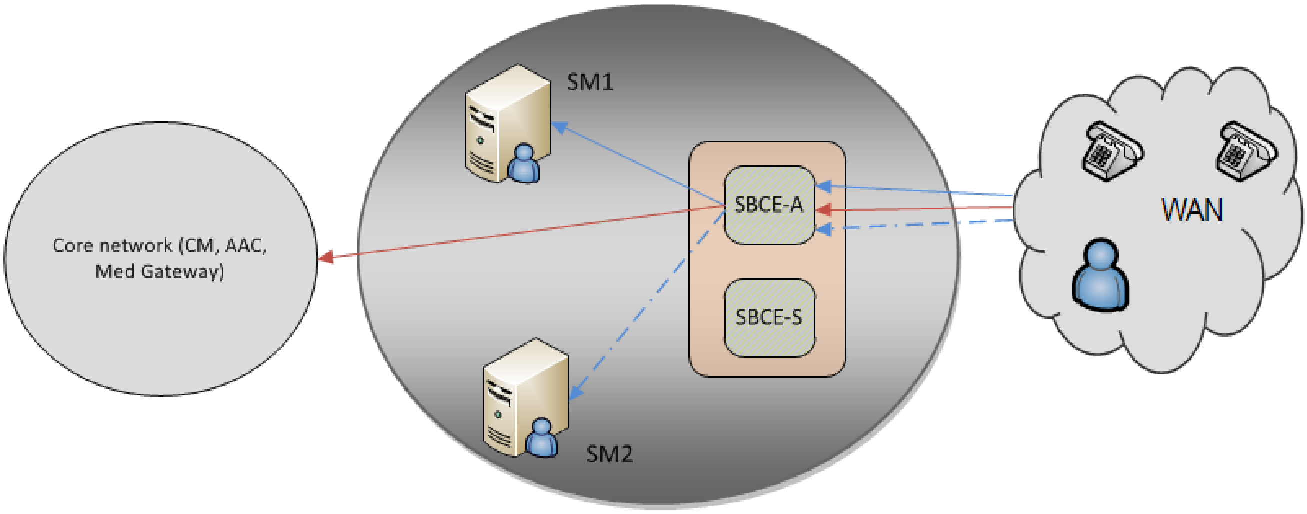

Figure 5: Deployment model: Single SBCE in high availability mode

In the deployment model, the bounding box represents the SBCE high availability solution: Avaya SBCE-A and Avaya SBCE-S are distinct hardware devices.

Scenario 1: Link failure between the endpoints and the active SBCE:

- Signaling traffic from the endpoints:
  - When the server connectivity is lost owing to a link failure on the active SBCE, the network fails over to the standby SBCE.
  - In the event of a network failure, for example, because of a router malfunction, the endpoints lose the service.
  - The trigger initiated at the endpoint to detect the unreachable SBCE is the same as detecting the unreachable Session Manager, when it is not routed through Avaya SBCE.
- Media traffic:
  - In case of a link failure on SBCE-A, the network fails over to SBCE-S, and all media sessions of active calls are preserved over the standby SBCE.
  - In case of a network failure between the endpoints and the active SBCE, all media sessions of active calls are lost.

Scenario 2: Active SBCE is down:

- Signaling traffic from the endpoints:
  - When the active SBCE is down, the network fails over to the standby SBCE.
  - The endpoints receive a *link bounce* signal and attempt to register onto SBCE-S. This is followed by new subscriptions if the primary Session Manager is still serviceable on SBCE-S and a successful sanity check is initiated in all future failover events.
  - The trigger initiated at the endpoint to detect the unreachable SBCE is the same as detecting the unreachable Session Manager, when it is not routed through the Avaya SBCE.
- Media traffic:
  - Media sessions of active calls are preserved over the standby SBCE-S.
  - All SIP dialogs are preserved and any subsequent SIP traffic is routed through SBCE-S. However, any transactions in progress will fail.

Scenario 3: Link failure between the SBCE-A and primary Session Manager (or) primary Session Manager is down:

- In the case of a socket error between SBCE-A and the primary Session Manager, all socket connections from the endpoints to the SBCE-A are ended.
- In case of SIP failure detection, the OPTIONS ping towards the primary Session Manager fails, and SBCE-A determines that the primary Session Manager is down.
- A loss of connectivity causes the endpoints to initiate a sanity check and failover to the backup Session Manager if available and reachable.

Chapter 5: Obtaining the application

Installing the application

You can obtain:

- Avaya Communicator for Android from Google Play
- Avaya Communicator for iPad and iPhone from the Apple App Store
- Avaya Communicator for Windows from the Avaya website

PLDS

Product Licensing and Delivery System (PLDS) is an Avaya application for downloading software, generating and managing software licenses, and performing paid and prepaid upgrades. The service agreement or software warranty includes the details about entitlements to licenses and software downloads. PLDS is available to authorized Avaya BusinessPartners, customers, and Avaya associates.

Avaya Communicator is accessible through PLDS download to registered users of the PLDS service. For information on downloading the application from PLDS, see *Getting Started with Avaya PLDS* from the Avaya Support website at http://support.avaya.com.

Chapter 6: Configuring Avaya Aura® Communication Manager settings

Use the Avaya Aura® System Manager administration interface to change the Avaya Aura® Communication Manager settings. For information about configuring Avaya Aura® Communication Manager, see *Administering Avaya Aura® Communication Manager* (03-300509).

Perform the following steps:

- For the Communication Manager signaling group associated with Avaya Aura® Session Manager, under IP network regions, set:
  - **Transport Method** to **tls**.
  - **Enforce SIPS URI for SRTP** to **y**.
  - **Initial IP-IP Direct Media** to **y**.
  - **DTMF over IP** to **rtp-payload**.

    rtp-payload enables Communication Manager to send DTMF tones using RFC 2833.

    Note:

    Avaya Communicator for Android and iPhone do not support sending tones using in-band or out-of-band DTMF.
- For trunk signaling with the PRI line, under Trunk Parameters, set **Disconnect Supervision - Out** to **y**. If you do not set this field, some point-to-point call transfers do not work correctly.
- On page 19 of System Parameters – Features, set **SIP Endpoint Managed Transfer** to **y**.
- To support secure calls, set the following additional parameters:
  - Under System Parameters – Features, set **Initial INVITE with SDP for secure calls?** to **y**.
  - Under System Parameters – IP-Options, set **Override ip-codec-set for SIP direct-media connections** to **n**.
  - Under System Parameters – Customer Options, set **Media Encryption Over IP?** to **y**.
  - Under IP Codec Set, in the Media Encryption area, set 1 to **1-srtp-aescm128-hmac80**, 2 to **2-srtp-aescm128-hmac32**, and 3 to **none**.
- For SIP and H.323 dual registration, configure the off-pbx-telephone station-mapping.

- If you have configured dual registration, that is, H.323 and SIP, for users that use Avaya Aura® Conferencing, set the **Fast Connect on Origination** field in the CONFIGURATION SET section to `n`.

  You can perform this by using the **`change off-pbx-telephone configuration-set n`** command, where n is a configuration set number.
- Configure FNEs and FNUs for Avaya Communicator for Android and iPhone.
- Assign and configure a station security code.
- Configure settings for SRTP support.
- Configure the barge-in tone alert for a user extension.
- Configure the Automatic Exclusion feature.

You must also configure Avaya Aura® endpoints for Avaya Communicator. The following list describes the minimum configuration you must perform on the Endpoints page to use Avaya Communicator features:

- Enable **IP SoftPhone**.
- Enable **IP Video SoftPhone**. For video calls, Avaya Communicator for iPad supports a maximum resolution and frame rate of 352 x 288 pixels @ 30 fps and Avaya Communicator for Windows supports a maximum resolution and frame rate of 1280 x 720 pixels @ 30 fps.
- If a bridged line appearance is configured for the extension, enable **Bridged Call Alerting** to alert the Avaya Communicator client when a call arrives at the main extension to which the Avaya Communicator client is bridged.
- Configure eight call appearances to provide support for merging active calls.

Depending on your system configuration, you might need to perform additional configuration steps on the Avaya Aura® Communication Manager Endpoints page.

Chapter 7: Configuring Avaya Session Border Controller for Enterprise settings

Sending DTMF tones using RFC 2833

Avaya Communicator for Android and iPhone do not support sending tones using in-band or out-of-band DTMF. Hence, you must configure Avaya SBCE to use RTP-Payload, which enables sending of DTMF tones using RFC 2833.

The default configuration of the Avaya SBCE is to pass DTMF unchanged from Avaya Communicator. Hence, if you are using the default configuration, you do not need to perform anything.

However, if you select the **Codec Prioritization** and **Allow Preferred Codecs Only** check boxes in the Audio Codec area of the **Domain Policies** > **Session Polices** > **Codec Prioritization** screen in Avaya SBCE, then you must add **Dynamic (120)** (RFC2833),which is a DTMF payload type, as one of the preferred codecs in the list.

Call restoration of an active call

While on an active call, it is possible that the underlying OS might decide that a change of network is required. For example, network changes between Wi-Fi and cellular data. The OS determines the network change and in many cases is unavoidable as a result of the loss of the current network in use when walking out of coverage.

In cases where both networks are external to the enterprise and require SBC access, you must set the value of the **Include End Point IP for Context Lookup** attribute in **Global Profiles** > **Phone Interworking** > **<concerned Interworking Profile>** > **Advanced** as **NO**. By setting this value, active calls are preserved and restored correctly so that the speech path is recovered and the call can continue automatically.

- If you set the value as YES, the system applies dialog matching based on the to-tag, from-tag, and the Call-ID including the endpoint IP address. However, the call fails as the to-tag, from-tag, and Call-ID are identical, but client IP changes. This results in the call-restoration issue. The client cannot restore the call and might also lead to one-way or no-way speech-path.
- If you set the value as NO, the system applies dialog matching based on only the to-tag, from-tag, and the Call-ID ignoring the endpoint IP address. The call succeeds as the to-tag, from-tag, and Call-ID are identical.

Chapter 8: Configuring user accounts in Avaya Aura® Session Manager

Use the Avaya Aura® System Manager administration interface to gain access to Avaya Aura® Session Manager. You can add or change user profiles through Avaya Aura® Session Manager. For more information about user profiles, see *Administering Avaya Aura® Session Manager*.

Avaya Communicator supports SIP with Multiple Device Access (MDA) and SIP/H.323 Dual Registration.

Avaya Communicator supports only SIP endpoints, not H.323 endpoints. For each Avaya Communicator extension, set the following on the User Profile page:

- Set an **Avaya SIP** communication address. If you have E.164 numbers in your enterprise directory, you must also set an **Avaya E.164** communication address for the extension.
- Set **Origination Application Sequence** to the Communication Manager server.
- Set **Termination Application Sequence** to the Communication Manager server.
- If the setup involves only a SIP implementation, you need a 96x1 SIP template. If you are enabling SIP and H.323 Dual registration, you need a 96x1 H.323 template.
- In the **Max. Simultaneous Devices** and **Block New Registration When Maximum Registrations Active?** fields, specify the requirement for simultaneous device registrations.

  This is required for MDA to work properly.
- Disable the TLS Endpoint Certification Validation parameter in an Avaya Aura® FP2 environment.
- Configure the **Extend Call** feature by assigning the **extnd-call** feature button to the SIP user.

  You must configure the **Extend Call** feature for the EC500 Call Suppression feature to remain active for the user. EC500 Call Suppression is a Communication Manager feature that supports the deployment of dual-mode mobile clients with Avaya Aura®. This feature ensures that users of dual-mode client applications such as Avaya Communicator receive only a single incoming call on the mobile phone for that particular extension. Users receive an alert either by a VoIP call or a cellular call, but never both.

  EC500 Call Suppression is available only when the server installation is Avaya Aura® 6.2 FP2 or later. Users administered on previous versions might need to disable the EC500 service in the application when users are within the Wi-Fi range and when users are connected to the VoIP service.
- Set **Clear Subscription on Notification Failure** to **yes**.

- Enable capability negotiation within a media rule to support the Direct Media functionality and enhance the SIP Secure Real-Time Transport Protocol (SRTP) capability on Communication Manager.
- Enable **Conferencing Profile** and configure the settings for the Avaya Aura® Conferencing profile of the user. See *Deploying Avaya Aura® Conferencing* for information about configuring Avaya Aura® Conferencing. You must configure Avaya Aura® Conferencing to use the conferencing feature in Avaya Communicator.
- To use Avaya Scopia®, administer a SIP trunk between Avaya Aura® Session Manager and Scopia Management through Avaya Aura® System Manager. Additional requirements for using Avaya Scopia® with Avaya Communicator are described in Requirements for Avaya Scopia on page 22.

Related links

Conference requirements on page 22

Chapter 9: Configuring Avaya Aura® Session Manager to support Avaya Aura® Presence Services

Procedure

1. Administer the DNS server that Session Manager uses to resolve the FQDN of the Presence Services server.
2. Administer the Local Host Name Resolution (LHNR) on Session Manager with an entry that represents the FQDN of the Presence Services server.
3. Administer a Regular Expression SRE route on Session Manager that points to the Presence Services server.

   The pattern is `.*@ps-fqdn`. For more information, see *Administering Avaya Aura® Session Manager*.

Chapter 10: Using automatic configuration

The following sections describe how to set up automatic configuration on each Avaya Communicator operating system. The automatic configuration process automatically configures the Avaya Communicator client settings when users open the client for the first time after installation.

Automatic configuration

Users can automatically configure Avaya Communicator using a settings file that you store on a central server or a settings service that you provide. On Android and iOS, you can provide the settings file URL to your users or set up DNS records for your domain. On Windows, you can trigger autoconfiguration by creating a Windows registry entry. The settings file URL or DNS records that you create must be secure.

- If you use DNS, the user must enter the email address in the appropriate screen of the application to determine the search domain for autoconfiguration. You must configure a number of records on your DNS server.
- If you use a settings file URL, you must send the URL to your users. Tell the users to enter the URL in the appropriate screen of the application.
- If you use Windows registry entries, you must configure a Windows Group Policy Object to distribute the registry entry to managed PCs.

Manual configuration versus Automatic configuration

To manually configure the settings in the application, the user must navigate to the **Settings** menu and enter the details on the different screens.

The automatic configuration process automatically populates the application settings with the details that you include as part of the configuration file.

Avaya recommends the automatic configuration process as the automatic configuration process is simple and user friendly.

Checklist: Using automatic configuration for Avaya Communicator

The following checklist describes the tasks that you must perform to use automatic configuration for the enterprise on the various Avaya Communicator clients.

Task	Create a configuration file with the settings information for the enterprise.	Configure your DNS server with three DNS records.	Update the Windows registry with the appropriate URL.
Avaya Communicator for Android	Yes	Yes	No
Avaya Communicator for iPad	Yes	Yes	No
Avaya Communicator for iPhone	Yes	Yes	No
Avaya Communicator for Windows	Yes	No	Yes
Notes	Save your configuration file to an enterprise web server. If the web server for your enterprise uses a secure *https* connection, ensure that a security certificate is available for users to install on the device.	The DNS server setup varies for each enterprise. However, you must create three standard DNS records to link the enterprise DNS server to the configuration file. **Note:** You require a DNS setup only if the user uses an email address for automatic configuration. If the user uses a standard web address, you do not require a DNS setup.	Set the HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE registry entry value to the URL where you store the configuration file.
✔			

Related links

Modifying registry entries for automatic configuration on page 66

Setting up the DNS server on page 63

Configuration file parameters on page 47

Configuration file requirements

Users can either configure the application settings manually or use a configuration file to automatically configure the settings. Using a configuration file simplifies the telephony settings configuration process and minimizes the chance of error. As an administrator, you must create a configuration file and share the file with users. You must send an email to users with instructions and a link to download and install the application. After installing the application, users can click the autoconfiguration link to configure the application.

The configuration file has the telephony settings and FNE codes for various application settings. When you create a configuration file, remember the following points:

- The configuration file must be a 46xxsettings.txt file.
- You can store all settings on the same 46xxsettings.txt file for all endpoints, that is, 46xx, 96xx, and Avaya Communicator.
- The configuration file structure can include information about the SIP settings, EC500 settings, and dialing rules.
- The FNE values must include only numbers and must be in the E.164 international format. For example, +<country code><national number>.

  The application does not apply any dialing rules translation to these numbers. Use the E.164 international format to ensure that the number can be dialed regardless of the location or network in use by the device.
- You can use a blank string to clear the existing value for a setting.
- Each configuration file must only contain a single dial plan configuration. If you have users with different dial plan settings, create multiple files. Ensure that the process you use to deliver the link to each user, for example, email, contains a link to the appropriate autoconfiguration file for the region.

  For configuring multiple sets of FNEs with extension to cellular, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Configuration file parameters

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
No	No	Yes	No	SSOUSERID	The account user ID.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
No	No	Yes	No	SSOPASSWORD	The account password.
No	No	Yes	No	SSOENABLED	The option that indicates whether unified login is enabled. Type 1 to indicate that unified login is enabled, and type 0 to indicate that unified login is disabled.
No	No	Yes	No	SSOREALMMAPPERADDRESS	The link to the Realm Mapper service.
No	No	Yes	No	SIPSSO	The option that indicates whether unified login is being used. Type 1 to indicate that unified login is enabled, and type 0 to indicate that unified login is disabled.
Yes	No	Yes	Yes	SIPENABLED	The option that indicates whether VoIP is enabled. Type 1 to indicate that VoIP is enabled, and type 0 to indicate that VoIP is disabled.
Yes	No	Yes	Yes	SIPUSERNAME	The SIP account name.
Yes	No	Yes	Yes	SIPPASSWORD	The SIP account password.
Yes	No	Yes	Yes	SIPPROXYSRVR	The IP address or the fully qualified domain name (FQDN) of the VoIP server. An example of an IP address is `135.20.246.20`. An example of a FQDN is `sip.gsc.avaya.com`.
Yes	No	Yes	Yes	SIPPORT	The port number of the VoIP server. The default port numbers are 5060 for TCP and 5061 for TLS.
Yes	Yes	Yes	Yes	SIPDOMAIN	The domain for transmitting VoIP data. An example is `example.com`.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
Yes	No	Yes	Yes	SIPSECURE	The option that indicates whether TLS is enabled for SIP signalling. Type 1 to indicate that TLS is enabled, and type 0 to indicate that TLS is disabled.
Yes	No	No	Yes	ENABLE_MDA_JOIN	On Communication Manager 6.3.7 and earlier versions, there is an issue that causes Communication Manager to reset if a user attempts to bridge into an active call from their MDA extension. Hence, by default, the remote line appearance Join button is disabled. Use this setting to enable the MDA Join feature if the deployment includes Communication Manager 6.3.8 or later versions. Type 1 to enable the MDA Join button, and type 0 to disable the MDA Join button.
Yes	No	No	Yes	VOIPCALLINGENABLED	The option that indicates whether VoIP calling is enabled. Type 0 to indicate that VoIP calling is disabled, type 1 to indicate that VoIP calling is always enabled, and type 2 to indicate that VoIP calling is enabled only on Wi-Fi.
No	Yes	No	No	SIP_CONTROLLER_LIST	SIP_CONTROLLER_LIST specifies a list of SIP controller designators, separated by commas without any intervening spaces, where each controller designator has the following format: host[:port][;transport=xxx]

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					An example is proxy1:5060;transport=tls,proxy2:5060;transport=tls.
Yes	No	No	Yes	CESENABLED	The option that indicates whether Client Enablement Services is enabled. Type 1 to indicate that Client Enablement Services is enabled, and type 0 to indicate that Client Enablement Services is disabled.
Yes	No	No	Yes	CESUSERNAME	The Client Enablement Services account name.
Yes	No	No	Yes	CESPASSWORD	The Client Enablement Services password.
Yes	No	No	Yes	CESSRVR	The IP address or the FQDN of the Client Enablement Services server. An example of an IP address is `135.20.246.21`. An example of a FQDN is `ces.gsc.avaya.com`.
Yes	No	No	Yes	CESPORT	The port number of the Client Enablement Services server.
Yes	No	No	No	CESSECURE	The option that indicates whether TLS is enabled. Type 1 to indicate that TLS is enabled, and type 0 to indicate that TLS is disabled.
Yes	Yes	Yes	Yes	ESMENABLED	The option that indicates whether Messaging is enabled. Type 1 to indicate that Messaging is enabled, and type 0 to indicate that Messaging is disabled.
No	Yes	Yes	Yes	ESM_ALLOW_PREVALIDATION	The option that indicates if a user can enable sending of contact email addresses to the server for validation.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					Type 1 to indicate that the option is enabled, and type 0 to indicate that the option is disabled.
No	No	Yes	No	ESMSSO	The option that indicates whether unified login is being used by Messaging. Type 1 to indicate that unified login is enabled, and type 0 to indicate that unified login is disabled.
Yes	Yes	Yes	Yes	ESMUSERNAME	The Messaging account user name.
Yes	Yes	Yes	Yes	ESMPASSWORD	The Messaging account password.
Yes	Yes	Yes	Yes	ESMSRVR	The IP address or the fully qualified domain name (FQDN) of the Messaging server. An example of an IP address is `135.20.246.95`. An example of a FQDN is `amm.example.com`.
Yes	Yes	Yes	Yes	ESMPORT	The port number of the Messaging server. The default port number is 8443.
Yes	No	Yes	Yes	ESMREFRESH	The Messaging refresh interval in minutes.
No	No	Yes	No	CONFERENCEENABLED	The option that indicates whether Conferencing is enabled. Type 1 to indicate that Conferencing is enabled, and type 0 to indicate that Conferencing is disabled.
No	Yes	Yes	No	CONFERENCE_FACTORY_URI	The Adhoc conference URL. For example, `60397@example.com`.
Yes	No	No	Yes	LOCKED_PREFERENCES	The list of locked preferences.

Table continues…

Supported on Android	**Supported on Windows**	**Supported on iPad**	**Supported on iPhone**	**Avaya settings text file value name**	**Description**
					For example, SET LOCKED_PREFERENCES "CESSRVR" , "CESPORT" , "CESENABLED". The user cannot modify the values of the locked preferences in the application as locked preferences appear as read-only. To reset locked preferences, use SET LOCKED_PREFERENCES "". **Note:** You must lock or unlock the Secure Connection option and the Port option together. If you lock the dialing rules check box, the application disables all dialing rules.
Yes	No	No	No	ECHO_CANCELLATION	The option to configure the echo cancellation setting. The options are aecm, aec, and off.
Yes	No	Yes	Yes	SUPPORTEMAIL	The default email address to send diagnostic logs.
No	No	Yes	No	SUPPORTURL	The default URL to get support.
No	No	Yes	Yes	PRESENCEENABLED	The option that indicates whether Presence is enabled. Type 1 to indicate that Presence is enabled, and type 0 to indicate that Presence is disabled.
No	Yes	Yes	Yes	PRESENCE_SERVER	The IP address or the fully qualified domain name (FQDN) of the Presence server. An example of an IP address is `135.20.246.11`. An example of a FQDN is `presence.example.com`.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
No	No	Yes	Yes	ENABLE_AUTO_AWAY	The option that determines if presence status automatically changes to Away when idle. Type 1 to enable this option, and type 0 to disable this option.
No	No	Yes	Yes	AUTO_AWAY_TIME	The idle time in minutes after which the presence status automatically changes to Away. The value is normalized to one of: 10, 15, 30, 60, 90, and 120.
No	Yes	Yes	No	VIDEOENABLED	The option that indicates whether video is enabled. Type 1 to indicate that video is enabled, and type 0 to indicate that video is disabled.
Yes	Yes	Yes	Yes	ENHDIALSTAT	The option that indicates whether dialing rules are enabled. Type 1 to indicate that dialing rules are enabled, and type 0 to indicate that dialing rules are disabled.
Yes	Yes	Yes	Yes	PHNOL	The number to dial to access an external line. If you do not configure a value, the application sets the value 9 by default.
Yes	Yes	Yes	Yes	PHNCC	The country code that the application uses when you make a call within your home country.
Yes	Yes	Yes	Yes	SP_AC	The area code that the application uses when you make a call within your home country.
No	Yes	No	No	DIALPLANAREACODE	Same as SP_AC. This element is supported by Avaya one-X® Communicator.
Yes	Yes	Yes	Yes	PHNPBXMAINPREFIX	The PBX main prefix for your telephone number.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					For example, 538.
No	Yes	No	No	DIALPLANPBXPREFIX	Same as PHNPBXMAINPREFIX. This element is supported by Avaya one-X® Communicator.
Yes	Yes	Yes	Yes	PHNLD	The number to dial when you make a long distance call within the same country.
Yes	Yes	Yes	Yes	PHNIC	The number to dial when you make an international call.
Yes	Yes	Yes	Yes	PHNDPLENGTH	The number of digits in an extension number within your corporate directory. For example, 7.
No	Yes	No	No	DIALPLANEXTENSIONLENGTHLIST	The internal extension length list. The list of commas separated integers. Basically a collection of PHNDPLENGTH values. If PHNDPLENGTH is also present, DIALPLANEXTENSIONLENGTHLIST takes precedence, that is, PHNDPLENGTH is ignored. This element is supported by Avaya one-X® Communicator. For example, “5, 7”.
Yes	Yes	Yes	Yes	PHNLDLENGTH	The length of phone numbers within the country, that is, national phone numbers. For example, 10.
No	Yes	No	No	DIALPLANNATIONALPHONENUMLENGTHLIST	The national number length list. The list of comma separated integers. Basically a collection of PHNLDLENGTH values. If PHNLDLENGTH is also present, DIALPLANNATIONALPHONENUMLENGTHLIST takes

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					precedence, that is, PHNLDLENGTH is ignored. This element is supported by Avaya one-X® Communicator. For example, “9, 10”.
Yes	No	Yes	Yes	PHNREMOVEAREACODE	The option that indicates whether the area code must be removed for local calls. Type 1 for true, and type 0 for false.
No	Yes	No	No	DIALPLANLOCALCALLPREFIX	The option that indicates whether the area code must be removed for local calls. If you set the value as DIAL_AS_IS, the parameter is check-marked. If you set the value as AC, the parameter is not check-marked. This element behaves like LOCAL_CALL_PREFIX, which is supported by Avaya one-X® Communicator. For Avaya one-X® Communicator compatibility: • If you set the value as *areacode* - SP_AC, the parameter is not check-marked. • If you set the value to anything other than *areacode* - SP_AC, the parameter is check-marked.
Yes	No	Yes	Yes	ANALYTICSENABLED	The option that indicates whether Google analytics is enabled. Type 1 for true, and type 0 for false.
Yes	No	No	Yes	STATION_SECURITY_ENABLED	The option that indicates whether station security code is enabled. The station security

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					code reduces the risk of toll fraud. Type 1 for true, and type 0 for false.
Yes	No	No	Yes	EC500ENABLED	The option that indicates whether EC500 is enabled. Type 1 for true, and type 0 for false.
Yes	No	No	Yes	FNUIDLEAPPEARANCESELECT	The FNE that you must dial to identify an idle line on your extension when you make a call. This EC500 parameter maps to the Idle Appearance Select FNE on Communication Manager.
Yes	No	No	Yes	FNUOFFPBXCALLENABLE	The FNE that you must dial so that your mobile phone rings when you receive a call on your deskphone. This EC500 parameter maps to the Off-Pbx Call Enable FNE on Communication Manager.
Yes	No	No	Yes	FNUOFFPBXCALLDISABLE	The FNE that you must dial to disable your mobile phone from ringing when you receive a call on your deskphone. This EC500 parameter maps to the Off-Pbx Call Disable FNE on Communication Manager.
Yes	No	No	Yes	FNUCFWDALL	The FNE that you must dial to activate call forwarding for all calls. This EC500 parameter maps to the Call Forward All FNE on Communication Manager.
Yes	No	No	No	FNUCFWDBUSY	The FNE that you must dial to activate call forwarding for busy calls. This EC500 parameter maps to the Call Forward Busy/No

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					Answer FNE on Communication Manager.
Yes	No	No	Yes	FNUCFWDCANCEL	The FNE that you must dial to disable call forwarding. This EC500 parameter maps to the Call Forward Cancel FNE on Communication Manager.
Yes	No	No	Yes	FNUACTIVEAPPEARANCESELECT	The FNE that you must dial to join an active call on your deskphone using your mobile phone. This EC500 parameter maps to the Active Appearance Select FNE on Communication Manager.
No	No	No	No	FNUHELDAPPEARANCESELECT	The FNE that you must dial to hold an active call on your deskphone using your mobile phone. This EC500 parameter maps to the Held Appearance Select FNE on Communication Manager.
Yes	No	No	Yes	FNUSAC	The FNE that you must dial to send all calls to a predefined number set on the server. This EC500 parameter maps to the Send All Calls FNE on Communication Manager.
Yes	No	No	Yes	FNUSACCANCEL	The FNE that you must dial to disable the sending of all calls to a predefined number set on the server. This EC500 parameter maps to the Send All Calls Cancel FNE on Communication Manager.
No	No	No	No	FNUCONFERENCEONANSWER	The FNE to dial for conference on answer. This EC500 parameter maps to the Conference on Answer FNE on Communication Manager.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
No	No	No	No	FNUTRANSFERONHANGUP	The FNE to dial for transfer on hangup. This EC500 parameter maps to the Transfer On Hang-Up FNE on Communication Manager.
No	No	No	No	FNUDROPLASTADDEDPARTY	The FNE to dial for dropping last added party. This EC500 parameter maps to the Drop Last Added Party FNE on Communication Manager.
No	No	No	No	FNUEXCLUSION	The FNE to dial for exclusion. This EC500 parameter maps to the Exclusion (Toggle On/Off) FNE on Communication Manager.
No	No	No	Yes	FNE_SETUP_DELAY	The delay in seconds inserted between the EC500 call being placed and the transmission of the digits for EC500. The value can be 3, 6, 9, 12 or 15.
No	No	Yes	No	DIRENABLED	The option that indicates whether LDAP is enabled. Type 1 to enable, and type 0 to disable.
No	No	Yes	No	DIRSSO	The option that indicates whether unified login is being used. Type 1 to indicate that unified login is enabled, and type 0 to indicate that unified login is disabled.
No	Yes	Yes	No	DIRSRVR	The IP address or the fully qualified domain name (FQDN) of the LDAP server. An example of an IP address is `135.20.246.111`. An example of a FQDN is `ldap.gsc.avaya.com`.
No	Yes	No	No	SP_DIRSRVR	Same as DIRSRVR.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
No	No	Yes	No	DIRLDAPPORT	The port number of the LDAP server.
No	Yes	No	No	DIRSRVRPRT DIRSRVRPORT SP_DIRSRVRPORT	Same as DIRLDAPPORT. This element is supported by Avaya one-X® Communicator.
No	Yes	Yes	No	DIRUSERNAME	The LDAP authentication user name.
No	Yes	Yes	No	DIRPASSWORD	The LDAP authentication password.
No	Yes	Yes	No	DIRTOPDN	The LDAP search root. An example is `ou=global users,dc=global,dc=example,dc=com`.
No	Yes	No	No	SP_DIRTOPDN	Same as DIRTOPDN.
No	No	Yes	No	DIRSECURE	The option that indicates whether TLS is enabled. Type 1 to indicate that TLS is enabled, and type 0 to indicate that TLS is disabled.
No	Yes	Yes	No	DIRIMATTRIBUTE	The application provides access to enterprise directory search using a direct LDAP connection. While processing the results, the application can process the attribute specified in DIRIMATTRIBUTE as an instant messaging address. For example, telephoneNumber, as often the administrator provisions users with Presence Server instant messaging addresses that correspond to the telephone number of the user.
No	Yes	Yes	No	DIRUSEIMDOMAIN	The DIRUSEIMDOMAIN setting controls whether the application should perform a mapping to the IM domain.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					Type 1 to enable this option, and type 0 to disable this option. In the DIRIMATTRIBUTE attribute example, the telephone number of the user is mapped into the IM domain, that is, 16135551212 becomes 16135551212@presence.example.com if the IM domain is presence.example.com. This would also potentially be used if an email address field was used, that is, alice@example.com becomes alice@presence.example.com. The DIRUSEIMDOMAIN setting must only be enabled in single-domain deployments. Customers must not use domain mapping if any form of messaging federation is in place and must instead ensure that the correct IM address is stored in an LDAP attribute.
No	Yes	No	No	DIRTYPE	The type of directory. The options are: • ACTIVEDIRECTORY • DOMINO • NOVELL
No	Yes	No	No	ENABLEGSSBIND	The option that indicates whether the GSS bind is enabled. When the GSS bind is enabled, the Windows credentials are used for LDAP connection. Type 1 for enabled, and type 0 for disabled.
No	Yes	No	No	TCP_KEEP_ALIVE_STATUS	The option that specifies whether the telephone sends TCP keep alive messages.

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					The options are: • 0: The telephone does not send TCP keep alive messages. • 1: The telephone sends TCP keep alive messages.
No	Yes	No	No	TCP_KEEP_ALIVE_TIME	The option that specifies the number of seconds that the telephone will wait before sending out a TCP keep-alive (TCP ACK) message. Valid values are 10 through 3600. The default value is 60.
No	Yes	No	No	TCP_KEEP_ALIVE_INTERVAL	The option that specifies the number of seconds that the telephone will wait before retransmitting a TCP keep-alive (TCP ACK) message. Valid values are 5 through 60. The default value is 10.
No	No	Yes	Yes	DND_SAC_LINK	Type 1 to enable the setting, and type 0 to disable the setting.
No	No	Yes	Yes	ALLOW_DND_SAC_LINK_CHANGE	Type 1 to allow, and type 0 to disallow.
No	No	No	Yes	ALLOW_CREATE_LOCAL_CONTACTS	The option to allow call history records to be used to create new device-local contacts. By default, this option is enabled. Type 1 to allow, and type 0 to disallow.
Yes	No	No	No	TRUSTCERTS	The list of URLs, absolute or relative, to CA certificates that will be stored in the application trust store and used to validate certificates of the various servers. For example, `SET TRUSTCERTS "http://300815isac.global.avaya.com/pki/AvayaITrootCA.crt","../../certs/avaya-sip-`

Table continues…

Supported on Android	Supported on Windows	Supported on iPad	Supported on iPhone	Avaya settings text file value name	Description
					`ca.crt","../../certs/gsc-lab-smgr.crt"` . To clear the private trust store, you must reset TRUSTCERTS to an empty value ("") or the user must clear the application data.
Yes	No	No	No	TLSSRVRID	The option that specifies whether the hostname verification failures are fatal. • If you specify the value as 0, the application logs the hostname verification failures. However, failures are not fatal, that is, the user can log in to the application. • If you specify the value as 1, the hostname verification failures are fatal and the user cannot continue with the login process.

VoIP calls logic

You can configure the following values for the VOIPCALLINGENABLED attribute in the auto-configuration file:

- 0: Never
- 1: Always
- 2: Only over WiFi

The application maintains an internal variable to represent user preference for the **Use VoIP For Calls** setting:

- 0: Never
- 1: Always
- 2: Only over WiFi

The application logic depends on both the administrative setting in the auto-configuration file and the user preference in the application.

	Use VoIP for calls = Never	**Use VoIP for calls = Always**	**Use VoIP for calls = Only over WiFi**
VOIPCALLINGENABLED = 0	The application displays this option as selected by you. However, the user cannot edit the setting in the application.	The user cannot select this option in the application.	The user cannot select this option in the application.
VOIPCALLINGENABLED = 1	The user can select this option in the application. The application logic depends on the user setting.	The user can select this option in the application. The application logic depends on the user setting. This value is the default value for a new installation.	The user can select this option in the application. The application logic depends on the user setting.
VOIPCALLINGENABLED = 2	The user can select this option in the application. The application logic depends on the user setting.	The user cannot select this option in the application.	The user can select this option in the application. The application logic depends on the user setting. This value is the default value for a new installation.

Setting up the DNS server

Note:

The content in this topic is only applicable for Avaya Communicator for Android, iPad, and iPhone.

Before you begin

- Create the configuration file.
- Configure a web server and save the configuration file to that web server. You must know the URL to the file on the web server.
- Set the following information based on your DNS server policy:
  - SRV and TXT record time-to-live period in seconds. For example, 300.
  - During this time, the client or intermediate servers might cache the retrieved record. Usually, the SRV and TXT record time-to-live periods share the same value.
  - Web server port number. Use 0 to have the client use the default port number for the protocol used.
  - SRV record priority. For example, 0.
  - SRV record weight. For example, 0.

About this task

You require the DNS setup only if the user uses an email address for automatic configuration. You do not need the DNS setup if the user uses a standard web address.

For users to use automatic configuration, you must create records on the DNS server of the enterprise to link your DNS server to the configuration file. Use split-horizon DNS and the same FQDN for Session Border Controller and Session Manager. Then users do not have to reconfigure the application on moving out of the enterprise network.

Note:

You might need to discuss with your DNS provider if your level of service is sufficient to provide support for DNS Service Discovery (DNS-SD). For more information, see DNS-Based Service Discovery. Avaya Communicator uses DNS PTR records consistent with the DNS-SD RFC, which in some cases might require an additional level of service from your DNS provider.

Procedure

1. Create a PTR record that links the descriptive name of your configuration file to the domain of the enterprise.

   a. Ensure that you name the PTR record as `_avaya-ep-config._tcp.`*`<domain>`*.

   b. Use the descriptive name for the configuration file as the target of the PTR record: *`<Descriptive name>`*`._avaya-ep-config._tcp.`*`<domain>`*.

   The following is an example of a PTR record: `_avaya-ep-config._tcp.`*`example.com`*`. IN PTR East._avaya-ep-config._tcp.`*`example.com`*.

2. Create an SRV record linking the descriptive name of your configuration file to the web server where the file resides.

   If the URL to the configuration file is `https://server.example.com/East_settings.txt`, then the server name is `server.example.com`.

   An SRV record also includes the following information:

   - SRV *time to live* period in seconds during which the client or intermediate servers might cache the retrieved record.

   The following is an example of an SRV record: *`East`*`._avaya-ep-config._tcp.`*`example.com`*`. `*`300`*` IN SRV `*`0 0 443 server.example.com`*.

   In this example:

   - 300 is the time-to-live period
   - The first zero is the priority, the second zero is the weight, and 443 is the port number.

3. Create a TXT record linking the descriptive name of your configuration file to the remaining URL information.

   TXT records are provisioned differently depending on the DNS server. However, all TXT records must have the following parameters:

   - *txtvers*: The text version of the TXT record. This value indicates the structure version of the record. You must always set the value to 1.

- *path*: The path to the configuration file. An example value is `path=/East_settings.txt`.
- *proto*: The web server access scheme. This value is usually http or https.

The following is an example of a TXT record: `East._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/East_settings.txt"`

In this example, 300 is the time-to-live period.

Sample DNS SRV records configuration

Note:

The content in this topic is only applicable for Avaya Communicator for Android, iPad, and iPhone.

To support automatic configuration, you must configure the PTR, SRV, and TXT records in your DNS server configuration. For more information, see the documentation for your DNS server.

PTR records

Provides a list of configurations with multiple PTR records.

Format: `_avaya-ep-config._tcp.<domain>. IN PTR <Descriptive name>._avaya-ep-config._tcp.<domain>`

Examples:

- `_avaya-ep-config._tcp.example.com. IN PTR East._avaya-ep-config._tcp.example.com`
- `_avaya-ep-config._tcp.example.com. IN PTR West._avaya-ep-config._tcp.example.com`

SRV records

Provides a link from the descriptive name to the web server where you stored the file.

Format: `<Descriptive name>._avaya-ep-config._tcp.<domain>. <TTL> IN SRV <priority> <weight> <port number> <web server FQDN>`

Examples:

- `East._avaya-ep-config._tcp.example.com. 300 IN SRV 0 0 443 server.example.com`
- `West._avaya-ep-config._tcp.example.com. 300 IN SRV 0 0 443 server.example.com`

TXT records

Provides a link from the descriptive name to the URL information, protocol, and path.

Format: `<Descriptive name>._avaya-ep-config._tcp.<domain>. <TTL> IN TXT "txtvers=1" "proto=<http or https>" "path=<file path>"`

Examples:

- `East._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1‟ "proto=https" "path=/East_settings.txt”`
- `West._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1‟ "proto=https" "path=/West_settings.txt”`

Modifying registry entries for automatic configuration

Note:

The content in this topic is only applicable for Avaya Communicator for Windows.

About this task

You must modify registry entry values under the appropriate Windows Group Policy Object (GPO) for the user.

Procedure

Modify the registry entry at one of the following locations:

- HKEY_CURRENT_USER\SOFTWARE\Avaya\Avaya Communicator\SettingsFileURL
- HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\Avaya Communicator\SettingsFileURL
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avaya\Avaya Communicator\Settings

The registry entry value must be the URL where you store the configuration file for automatic configuration.

See Microsoft help documentation for more information about configuring a registry item.

Configuration file template for Avaya Communicator

Avaya settings text file format

The following example shows the common configuration file in the Avaya settings text file format, that is, 46xxsettings.txt. The settings that are applicable for a particular platform are covered in the *Configuration file parameters* topic.

```
## SSO
SET SSOUSERID ""
SET SSOPASSWORD ""
SET SSOENABLED "1"
SET SSOREALMMAPPERADDRESS "ide.example.com/getCredentials"

## SIGNALING
SET SIPSSO "1"
SET SIPENABLED "1"
SET SIPUSERNAME "5551212"
SET SIPPASSWORD ""
SET SIPPROXYSRVR "sipserver.example.com"
SET SIPPORT "5061"
SET SIPDOMAIN "example.com"
SET SIPSECURE "1"
SET ENABLE_MDA_JOIN "1"
SET VOIPCALLINGENABLED "1"
SET SIP_CONTROLLER_LIST "135.9.28.76:5061;transport=TLS"

## CES
SET CESENABLED "1"
SET CESUSERNAME "5551212"
SET CESPASSWORD ""
SET CESSRVR "ces.example.com"
SET CESPORT "7777"
SET CESSECURE "1"

## MESSAGING
SET ESMENABLED "1"
SET ESM_ALLOW_PREVALIDATION "1"
SET ESMSSO ""
SET ESMUSERNAME ""
SET ESMPASSWORD ""
SET ESMSRVR "amm.example.com"
SET ESMPORT "8443"
SET ESMREFRESH "15"

## CONFERENCE
SET CONFERENCEENABLED "1"
SET CONFERENCE_FACTORY_URI "22111@example.com"

SET LOCKED_PREFERENCES "CESSRVR" , "CESPORT", "CESENABLED"

## ADVANCED SETTINGS
SET ECHO_CANCELLATION "aecm"

## SUPPORT
SET SUPPORTEMAIL "support@example.com"
SET SUPPORTURL "example.com/support"

## PRESENCE
SET PRESENCEENABLED "1"
SET PRESENCE_SERVER "presence.example.com"
SET ENABLE_AUTO_AWAY "1"
SET AUTO_AWAY_TIME "30"

## VIDEO
SET VIDEOENABLED "1"

## DIALING RULES
SET ENHDIALSTAT "1"
SET PHNOL "9"
SET PHNCC "1"
SET SP_AC "613"
SET PHNPBXMAINPREFIX "538"
SET PHNLD "1"
SET PHNIC "011"
SET PHNDPLENGTH "7"
SET DIALPLANEXTENSIONLENGTHLIST "5, 7"
SET PHNLDLENGTH "10"
SET DIALPLANNATIONALPHONENUMLENGTHLIST "9, 10"
SET PHNREMOVEAREACODE "1"
SET DIALPLANLOCALCALLPREFIX "0"

## ANALYTICS
SET ANALYTICSENABLED "1"
```

```
## STATION SECURITY
SET STATION_SECURITY_ENABLED "1"

## TELEPHONY SETTINGS
SET EC500ENABLED "1"
SET FNUIDLEAPPEARANCESELECT "12345678901"
SET FNUOFFPBXCALLENABLE "12345678902"
SET FNUOFFPBXCALLDISABLE "12345678903"
SET FNUCFWDALL "12345678904"
SET FNUCFWDBUSY "12345678905"
SET FNUCFWDCANCEL "12345678906"
SET FNUACTIVEAPPEARANCESELECT "12345678907"
SET FNUSAC "12345678909"
SET FNUSACCANCEL "12345678910"

## LDAP
SET DIRENABLED "1"
SET DIRSSO "1"
SET DIRSRVR "ldapserver.example.com"
SET DIRLDAPPORT "389"
SET DIRSRVRPRT "636"
SET DIRUSERNAME "johndoe"
SET DIRPASSWORD ""
SET DIRTOPDN "dc=global,dc=example,dc=com"
SET DIRSECURE "1"
SET DIRIMATTRIBUTE "telephoneNumber"
SET DIRUSEIMDOMAIN "1"
SET DIRTYPE "ACTIVEDIRECTORY"
SET ENABLEGSSBIND "1"

## SIP FAILOVER
SET TCP_KEEP_ALIVE_STATUS "0"
SET TCP_KEEP_ALIVE_TIME "45"
SET TCP_KEEP_ALIVE_INTERVAL "15"

## FEATURES
SET DND_SAC_LINK "1"
SET ALLOW_DND_SAC_LINK_CHANGE "1"
SET ALLOW_CREATE_LOCAL_CONTACTS "1"
SET TRUSTCERTS "http://300815isac.global.avaya.com/pki/AvayaITrootCA.crt","../../certs/
avaya-sip-ca.crt","../../certs/gsc-lab-smgr.crt"
SET TLSSRVRID "1"
```

Chapter 11: Security

Security specification

Connections through a VPN or internal LAN

Avaya Communicator supports connections through a VPN or internal LAN.

Secure server connections

Avaya Communicator requires TLS. Install a secure server certificate obtained from a certificate authority. Users can then connect to Avaya Communicator without any security concerns.

For more information about installing secure server certificates, see the corresponding documentation for Session Manager and Client Enablement Services. If the server certificates are not signed by one of the certificate authorities included by default in the operating system, you must install the corresponding root certificates on the device.

You can also see *Updating server certificates to improve end-user security and client user experience* at https://downloads.avaya.com/css/P8/documents/100180626.

Security requirements

To maintain a secure environment for Avaya Communicator:

- Use role assignments and assign security groups for operations.
- For accountability, ensure that each user has a unique login ID. Instruct users not to share the user login ID and password.
- Periodically review and update the list of administered users, roles, and permissions.
- Review administration logs regularly to ensure that the system is operating correctly.
- Review audit logs regularly to ensure that the system is operating correctly.
- Review security logs and alarms regularly to monitor possible security events.

Additional security information

For more information about additional security for Avaya Communicator and related Avaya components, see the Avaya Support website at http://support.avaya.com/security. For example, you can find information about the following:

- Avaya Product Security Vulnerability Response Policy
- Avaya Security Vulnerability Classification
- Avaya Product Security Support Flow
- Security advisories for Avaya products
- Software patches for security issues

- Reporting a vulnerability for any security issues
- Automatic email notifications of security advisories

You can also find more information about security practices on the National Security Agency website at http://www.nsa.gov.

Mobile device security recommendations

Use the Avaya Communicator applications on standard-issue hardware running original versions of vendor-approved software. To ensure protection of user data, you must secure devices using a passcode and enable full-disk encryption on Android. Full-disk encryption is the default behavior on iOS devices.

For more information about the built-in security features of:

- iOS, see iOS Security.
- Android, see Android Security Overview.

Remote attacks

The Avaya Communicator applications are hardened against remote attacks, specifically against attacks actively directed towards the client by an external entity. The Avaya Communicator applications do not have any listening ports. All connections are made outbound from the client.

Jailbroken devices

The Avaya Communicator applications implement techniques for detecting jailbroken devices. If Client Enablement Services is in use, administrators have a mechanism to disable use of the application on a device that was detected as jailbroken. However, jailbreak technology evolves quickly and Avaya cannot guarantee that the techniques will effectively detect all jailbroken devices always. Jailbreaking a device compromises the built-in security mechanisms and no guarantees of security can be made if the user has jail broken the device.

Android:

The use of full-disk encryption ensures that the user passcode protects data on the device. The owner of the device might be able to restore any backed-up data to the device after jailbreaking. Also, all data will be cryptographically inaccessible to an attacker.

iOS:

Jailbreaking an iOS device has the effect of wiping any data that was previously present on the device. The owner of the device might be able to restore any backed-up data to the device after jailbreaking. Also, all data will be cryptographically inaccessible to an attacker.

Server identity validation

Avaya Communicator for Android includes implementation of server identity validation on all secure connections.

If the user uses the application to connect to the VoIP, PPM, Client Enablement Services, XMPP, LDAP, Avaya Multimedia Messaging, Auto-configuration, Web Collaboration, or SSO server, Avaya Communicator for Android performs hostname verification to ensure communication with the correct server.

If the user uses the application to connect over https to Client Enablement Services, for example, as a fully qualified domain name, that is, ces.avaya.com or as an IP address, that is, 135.20.246.169, you must ensure that the certificate on the Client Enablement Services server has a Common Name or a Subject Alternative Name that matches the fully qualified domain name or IP address. Avaya Communicator for Android ensures communication with the correct server if you meet the certificate requirement. The same logic applies to the other services listed above.

For VoIP, the application logic varies slightly. Avaya Communicator for Android can communicate with multiple Session Manager servers. If the Session Manager server certificate has the appropriate information about the SIP domain, Avaya Communicator for Android accepts the server identity validation.

If Avaya Communicator for Android detects a hostname validation failure, the logs include the security certificate or hostname validation details. The hostname validation failure is fatal, that is, the user cannot continue with the login process if both of the following conditions are met:

- If the server is signed by a CA certificate that is not the Avaya SIP Product Certificate Authority.
- If you set TLSSRVRID to a value of 1.

If you do not set TLSSRVRID or set TLSSRVRID to a value of 0, the hostname validation failure is not fatal, that is, the user can continue with the login process.

Note:

The application does not display the TLSSRVRID value. Only the application logs include the TLSSRVRID value.

Remote Wipe overview - Avaya Communicator for Android and iPhone

When a user reports a lost or stolen mobile phone, go to the Client Enablement Services administration website. Select the **Lost or Stolen Device** check box for that user.

When you select this check box, the Client Enablement Services server notifies the application to:

- Remove all locally stored data, such as downloaded voice mails.
- Clear the account information.
- Force the user to login again to gain access to the application.

The user is then unable to use the application on any mobile phone until you clear the **Lost or Stolen Device** check box.

Note:

The Client Enablement Services server has the administration interface to support the Lost or Stolen Device feature. Hence, the Lost or Stolen Device feature is unavailable if you did not configure Client Enablement Services for a user.

You might configure Client Enablement Services for a user. However, if the user does not set up the application to connect to Client Enablement Services or the person who finds the device disables Client Enablement Services on the device, remote wipe does not occur.

Port utilization

To provide a secure communication channel for voice and instant messaging sessions, Avaya Communicator requires TLS. Avaya Communicator also supports SRTP for both video and audio with Avaya Aura® dependencies.

Note:

- Avaya Communicator does not support audio or video with Polycom SRTP devices.
- In Avaya Aura® Conferencing, ensure that the Encrypt RTCP parameter is *not* selected to maintain SRTP on a conference call. If you select this parameter, the SRTP call becomes an RTP call when the moderator adds participants into the conference.

To see the ports and protocols that Avaya Communicator uses, see the port matrix document at http://support.avaya.com/security.

Log in to the Avaya Support website using valid Support site credentials.

Certificate distribution and management

Before you deploy Avaya Communicator, determine whether the servers in the UC infrastructure use certificates signed by a certificate authority that the device operating system trusts. If the servers are using trusted certificates, you do not need to take further action.

Security alert:

Avaya Communicator for Android does not support certificate revocation checks. Hence, users of Avaya Communicator for Android are potentially vulnerable to certain forms of certificate abuse. To reduce the risk of abuse, Avaya recommends that customers use certificates issued by a secure private certificate authority in combination with the private trust store feature.

Follow the standard operating system procedures for distributing and managing certificates. You can also refer to the *Updating server certificates to improve end-user security and client user experience* document at https://downloads.avaya.com/css/P8/documents/100180626. Upload the certificates to a location, usually a website, from where the user can download and install the certificates. Avaya is not responsible for distribution of certificates to the device.

Note:

Recent versions of Android display a warning message if the user installs additional trusted certificates on the device.

Avaya Communicator validates the server identity certificate during the TLS connection establishment process. If the application cannot establish a TLS connection because of an inability of the device to validate the certificate, the application displays an error message.

You must check for certificate requirements on the following servers as applicable:

- Avaya Aura® Session Manager
- Avaya Session Border Controller for Enterprise
- Client Enablement Services for Avaya Communicator for Android and iPhone
- HTTP, which you use to host the settings file for automatic configuration
- LDAP
- Avaya Aura® Conferencing
- Avaya Identity Engines
- Avaya Aura® Presence Services
- Avaya Multimedia Messaging

Note:

Avaya Communicator does not support self-signed certificates for any connection. All servers must have certificates that the trusted certificate authorities issues.

Third-party certificates

Deploy third-party certificates in the network to enhance the security of the enterprise. For instructions on installing third-party certificates, see *Application Notes for Supporting Third-party Certificates in Avaya Aura® System Manager*. For information on managing certificates, see *Administering Avaya Aura® System Manager*.

Certificate requirements

VoIP

If Session Manager and optional systems such as Session Border Controller use:

- A commercial certificate and the CA certificates are already available on the device OS, you can continue to use Avaya Communicator.
- An enterprise server certificate and if you already deployed the matching CA certificate to devices, you can continue to use Avaya Communicator.

- A demonstration Avaya Certificate, you must distribute the matching Avaya demonstration CA certificate to each device.

Client Enablement Services - Avaya Communicator for Android and iPhone

If the Client Enablement Services server uses:

- A commercial certificate and the CA certificates are already available on the device OS, you can continue to use Avaya Communicator.
- An enterprise server certificate and if you already deployed the matching CA certificate to devices, you can continue to use Avaya Communicator.
- The default certificate, perform one of the following:
    - Install an enterprise server certificate on the Client Enablement Services server and deploy the matching CA certificate to devices.
    - Install a commercial certificate on the Client Enablement Services server to take advantage of the CA certificates on the device OS.

You can also refer to the *Updating server certificates to improve end-user security and client user experience* document at https://downloads.avaya.com/css/P8/documents/100180626.

Obtaining the Avaya SIP Product CA certificate

Procedure

1. On System Manager Web Console, click **Services** > **inventory** > **Manage Elements**.

   The system displays the Manage Elements screen.
2. Select the Session Manager instance from the list.
3. In the **More Actions** field, select **Configure Trusted Certificates**.

   The system displays the Trusted Certificates screen.
4. Select an Avaya SIP Product CA certificate from the list.

   For example, `trust-cert.pem`.
5. Click **Export**.
6. Save the file to a location on your system.
7. **(Optional)** For Avaya Communicator for Android and Windows, change the certificate extension from `PEM` to `CRT`.

   iOS recognizes a certificate file with the `PEM` extension.
8. Perform one of the following:
    - Upload the CA Certificate to a website and send your users a link.
    - Send the CA certificate through email as an attachment.

Obtaining the Avaya Aura® System Manager CA certificate

About this task

If you have a server with a certificate issued by Avaya Aura® System Manager, you must either:

- Replace the certificate as described in the *Updating server certificates to improve end-user security and client user experience* document at https://downloads.avaya.com/css/P8/documents/100180626.
- Distribute the Avaya Aura® System Manager CA certificate to the device of the users.

Procedure

1. On the home page of System Manager Web Console, under **Services**, click **Security** > **Certificates** > **Authority**.
2. On the main page, click **Download pem file**.
3. Save the file to a location on your system.
4. **(Optional)** For Avaya Communicator for Android and Windows, change the certificate extension from `PEM` to `CRT`.

   iOS recognizes a certificate file with the `PEM` extension.
5. Perform one of the following:
   - Upload the CA Certificate to a website and send your users a link.
   - Send the CA certificate through email as an attachment.

Chapter 12: Licensing requirements

Avaya Communicator does not require licenses for each client application. However, to gain access to other services, the licensing model is consistent with other Avaya client applications:

- EC500 features require EC500 licenses.
- Client Enablement Services features require Client Enablement Services licenses.
- VoIP features require Mobile SIP licenses.
- Avaya Multimedia Messaging features require Avaya Multimedia Messaging licenses. The following licenses exist for Avaya Multimedia Messaging:
    - Avaya Multimedia Messaging server software: Sold per instance and by major release number. You require this license to access Avaya Multimedia Messaging services.
    - Enhanced Avaya Multimedia Messaging services: Sold on a per user basis. You must enforce the Rich Content license restrictions by disabling the Rich Content feature when there is no license for a user. You must identify which users have access to Enhanced privileges in the web-based administration portal. You can change user privileges in the web-based administration portal any time.
- For all video communications, that is, point-to-point video and video conferencing, you need Communication Manager licenses. For only video conferencing, you need Avaya Aura® Conferencing licenses.

Chapter 13: Troubleshooting and interoperability limitations

Video window does not get closed from Avaya Communicator

If a user de-escalates or stops a video from the Avaya one-X® Communicator - H.323 endpoint, the video window does not get closed from Avaya Communicator.

For a simple P2P video call between Avaya Communicator and Avaya one-X® Communicator, Avaya Communicator has a different behavior regarding the window state of the video, that is, close or open.

- If Avaya one-X® Communicator - SIP drops the video, CM reINVITE AC user with port = 0 in the mline. Because of this, Avaya Communicator closes the video window.
- If Avaya one-X® Communicator - H.323 drops the video, CM reINVITE AC user with a=inactive in the mline. Because of this, Avaya Communicator keeps the video window open with a black display.

Proposed solution

Procedure

Close the video window manually.

Avaya Communicator for Windows stops transmitting video after 15 minutes

Condition

Avaya Communicator for Windows using services of Avaya Aura® Conferencing 7.2 or previous releases of Avaya Aura® Conferencing stops transmitting video after 15 minutes.

Cause

The **VideoAuditTimer** parameter is set as *15* by default in Avaya Aura® Conferencing 7.2 and previous releases.

Solution

Change the **VideoAuditTimer** parameter to *0* if you are using Avaya Aura® Conferencing 7.2 or if you upgraded from Avaya Aura® Conferencing 7.2 to 8.0.

User cannot access local contacts with Avaya Communicator for iPad and iPhone

Avaya Communicator for iPad and iPhone users do not receive a prompt to allow access to local contacts. The device does not show local contacts.

Cause

When initially logging in to Avaya Communicator for iPad and iPhone, the user did not allow access to local contacts from iOS.

Solution

Under **Settings**, set **Privacy** > **Contacts** to **On**.

One-way speech issue in Avaya Communicator for iPhone

Condition

Avaya Communicator for iPhone user can hear the voice of the person at the other end. However, the person at the other end cannot hear the voice of the Avaya Communicator for iPhone user.

Cause

Avaya Communicator for iPhone user did not enable the microphone setting on the iOS device.

Solution

In iOS settings, enable **Avaya Communicator** > **Microphone**.

Call is not restored correctly during a network change

Condition

While on an active call, if the network changes between Wi-Fi and cellular data networks, the call is not restored properly.

Cause

The issue occurs if both networks are external to the enterprise and require SBC access and you set the value for the **Include End Point IP for Context Lookup** attribute on Avaya Session Border

Controller for Enterprise as **YES**. The **Include End Point IP for Context Lookup** attribute is located in **Global Profiles** > **Phone Interworking** > **<concerned Interworking Profile>** > **Advanced**.

- If you set the value as YES, the system applies dialog matching based on the to-tag, from-tag, and the Call-ID including the endpoint IP address. However, the call fails as the to-tag, from-tag, and Call-ID are identical, but client IP changes. This results in the call-restoration issue. The client cannot restore the call and might also lead to one-way or no-way speech-path.
- If you set the value as NO, the system applies dialog matching based on only the to-tag, from-tag, and the Call-ID ignoring the endpoint IP address. The call succeeds as the to-tag, from-tag, and Call-ID are identical.

Solution

Set the value for the **Include End Point IP for Context Lookup** attribute as **NO**.

Connecting to a protocol sniffer

About this task

Avaya Communicator connects with and supports a protocol sniffing tool such as Wireshark. Use such tools to capture network traces associated with the VoIP service on Avaya Communicator for Android, iPad, and iPhone.

For more information about protocol sniffers, see the developer tools guide for your device operating system.

Procedure

1. Set up your personal computer as an access point.
2. Install a protocol sniffing tool such as Wireshark on your computer.
3. Connect your device to the access point on your computer.
4. Capture the trace on the bridged adapter.

Troubleshooting voice quality issues - Avaya Communicator for Android

Avaya Communicator generates log entries at the beginning and end of each VoIP call. The log entries exist in the application log files, which the application includes in the .zip archive as part of the Report a Problem feature.

All these log entries only apply to VoIP calls.

After you receive the log files, you must look for the following entries.

Call Start Log Entry

At the beginning of each VoIP call, the application generates a log entry similar to the following:

```
2013-05-02 10:38:12,122 INFO [main] - [logCallStarted] > VoIP Call Start (outgoing,
sessionID=1)
```

The application displays this entry in the log files even when the user disables verbose logging.

For an outgoing call, Call Start occurs when the user presses the Call button. For an incoming call, Call Start occurs after the application receives the incoming call notification from the network.

Use the session ID to correlate the log entries related to the same call. The IDs come from the signaling engine and start at 1 every time the application opens.

Mid-call QoS Statistics Entries

Every 5 seconds during an active call, the application generates a log entry similar to the following:

```
2013-05-02 10:38:32,261 DEBUG [VoIP QoS Logging] - [logAudioDetails] > Session 1 media:
Xmit 509p/81440b Recv 519p/83040b Lost(Loc=0 Rem=3) RTT=35ms Jitter(Loc=10ms Rem=165ms)
Codec=G722/20ms LocalAddr=135.55.85.181:5000 RemoteAddr=135.55.85.222:5006  Encryption=NO
ENCRYPTION
```

The application displays this entry in the log files only when the user enables verbose logging. Use the session ID to correlate the log entries related to this entry.

The application displays these log entries only after the user answers the call.

Call End Log Entry

When you end a call, the application generates a log entry similar to the following:

```
2013-05-02 10:38:45,480 INFO [main] - [logCallEnded] > VoIP Call End (sessionID=1,
duration=41s, callStats={Xmit 1508p/241280b Recv 1514p/242240b Lost(Loc=0 Rem=2) RTT=10ms
Jitter(Loc=12ms Rem=200ms) Codec=G722/20ms LocalAddr=135.55.85.181:5000
RemoteAddr=135.55.85.222:5020 Encryption=AES 128 HMAC SHA1 80})
```

The application displays this entry in the log files even when the user disables verbose logging.

This entry includes the QoS statistics from the end of the call and uses the same session ID as for the rest of the call.

Interpreting results

QoS Stats:

The following is a brief summary of the QoS statistics from RTCP captured in the mid-call and end-call log entries, in the order in which the statistics appear in the log entries:

- Transmitted media: The number of media packets transmitted from the device to the network, followed by the number of data bytes represented in those packets.
- Received media: The number of media packets received on the device from the network, followed by the number of data bytes represented in those packets.
- Lost packets: The fraction of packets detected as lost locally or at remote locations.
- Round-Trip-Time: The average time in milliseconds to send a packet and to receive the response.
- Jitter: The delay in milliseconds applied to media packets by network jitter, locally and at remote locations.

- Codec and Packetization Time: The standard identifier for the media codec in use, and the length of time for a single media packet.
- Local media address: The IP address and port on the device that the media traffic is using.
- Remote media address: The IP address and port of the remote peer with which the application exchanges media traffic.
- Encryption: The encryption algorithm, if any, which is being applied to the media traffic.

The QoS statistics are cumulative from the beginning of that media session. If the user puts the call on hold, the current media session ends. If the user resumes the call, the collection of statistics restarts from zero.

Evidence of no media:

If no media is exchanged while on the call, either because of a network problem or because the call is on hold, the statistics display a zero.

One-way media is indicated when one of the Transmitted or Remote media has a zero value, but the other one has a non-zero value.

Evidence of calls that ended abnormally:

If the call ends because the application ended abnormally, the log shows a call started log entry with no corresponding call ended entry. Abnormal ending of a call might indicate:

- A failure.
- That the user ended the application using the task manager.
- The operating system ended the application.

Evidence of network issues:

If the voice quality is poor because of network issues, the call log shows unusually large numbers for lost packets and jitter.

Known interoperability limitations

The following sections describe known interoperability limitations between Avaya Communicator and other products.

Avaya Aura® Conferencing behaviors

Avaya Aura® Conferencing behaviors can affect Avaya Communicator conference calls. For information about Avaya Aura® Conferencing behaviors and limitations, see:

- *Deploying Avaya Aura® Conferencing*
- *Administering Avaya Aura® Conferencing*

Examples of interoperability limitations with Avaya one-X® Mobile

The following are examples of limitations that occur when you use Avaya one-X® Mobile and Avaya Communicator. Similar limitations might also exist between Avaya Communicator and other products.

- Call logs are inconsistent between Avaya one-X® Mobile and Avaya Communicator.

- When you add contacts in Avaya one-X® Mobile, the contacts do not appear in Avaya Communicator.

Interoperability and limitations with voice mail privacy enforcement

The Client Enablement Services server and the Avaya Communicator applications have a limitation with respect to private voice mail.

The Client Enablement Services server and the Avaya Communicator applications do not support email style privacy. Hence, if the audio attachment for a message is marked as private, the user can continue to download and play the audio attachment using Avaya Communicator.

- If the administrator configures the Messaging service for voice mail style privacy, the voice mail messages do not contain the voice mail attachment. Hence, the user cannot play the audio for the voice mail message using Avaya Communicator.
- If the administrator configures the Messaging service for email style privacy, the Client Enablement Services server and the Avaya Communicator applications do not respect this setting. Hence, the user can download and play the audio attachment using Avaya Communicator as if the administrator did not enable privacy at all.

Appendix A: Emergency calls

Do not use Avaya Communicator to make emergency calls. Avaya recommends that you check the product documentation that accompanies your mobile device to learn about the emergency calling features available on your device.

Avaya Communicator for Android Release 2.0 includes a feature to allow the administrator to provide a list of emergency numbers to be sent to the cellular network. This feature has been removed from the current release.

If you have any questions or concerns, contact your support team.

Appendix B: Presence behavior

Access Control List:

Avaya Communicator does not provide an interface to directly manage the presence Access Control List (ACL) requests. The Client Enablement Services server delivers the presence information to Avaya Communicator for Android and iPhone. Check the Client Enablement Services product documentation for guidance on using the presence ACL requests with Client Enablement Services.

AES configured	User client configuration	Automatic	Result
No	Single client: 1XCES	Yes	Client always displays the presence status as Offline.
No	Single client: 1XCES	No: User sets presence manually	Client always displays whatever presence state the user sets manually.
No	Multiple clients: 1XCES and other presence-enabled clients such as Avaya Communicator	Yes	Client always displays whatever presence state the other client such as Avaya Communicator publishes.
No	Multiple clients: 1XCES and other presence-enabled clients such as Avaya Communicator	User sets presence manually on 1XCES	1XCES pushes the manual presence update to Presence Services. Presence Services then updates the self-presence state of the user. All clients of that user, based on that update, display the same manual presence that the user sets manually.
Yes	Single client: 1XCES	Yes	Client always displays the presence status as Available. If the user is on a call, the status is Busy. **Note:** This result is true and valid until Avaya Aura® FP3, at which point if 1XCES is the only client, then the client always displays the presence status as Offline. If the user is on a call, the status is Busy.

Table continues…

AES configured	User client configuration	Automatic	Result
Yes	Single client: 1XCES	No: User sets presence manually	Client always displays whatever presence state the user sets manually.
Yes	Multiple clients: 1XCES and other presence-enabled clients such as Avaya Communicator	Yes	The resultant presence state between AES and the other presence-enabled client is determined by the Presence Services aggregation logic. For example, AES publishes the status as Available and the Avaya Communicator client logs out and goes offline. Then the presence state of the user always displays as Available. **Note:** This result is true and valid until Avaya Aura® FP3. Else, for Avaya Aura® FP3, AES publishes the status as Available if an H.323 device is registered, otherwise AES publishes the status as Offline.
Yes	Multiple clients: 1XCES and other presence-enabled clients such as Avaya Communicator	User sets presence manually on 1XCES	1XCES pushes the manual presence update to Presence Services. Presence Services then updates the self-presence state of the user. All clients of that user, based on that update, display the same manual presence that the user sets manually.

Limitations:

- Client Enablement Services supports only a single Presence Server.
- Avaya Communicator for Android and iPhone clients using Client Enablement Services for presence do not support the Do Not Disturb (DND) presence status. Hence, DND users continue to receive audio and visual notifications for new messages.
- If the enterprise directory that you are using with Client Enablement Services is Microsoft Active Directory Application Mode (ADAM), then Client Enablement Services does not support presence.
- In a multi-domain configuration, you can configure presence for users only in one domain.
- If the user selects the **Automatic** option, Avaya Communicator does not influence presence in any way. Hence, if the user uses Avaya Communicator, then the user might still appear as offline if the other devices are offline.
- If you enable the **mod_dnd** parameter, which is only available on Presence Services FP4 and if the presence status is set to Unavailable in Avaya Communicator, users do not receive IMs right away.

Examples:

If a user uses only a single Client Enablement Services client and you deploy Client Enablement Services without AES, then:

- If the user selects the **Automatic** option, the availability status of the user is always *Offline*.
- In the manual mode, the availability status displays the presence that the user selects manually.

If a user uses only a single Client Enablement Services client and you deploy Client Enablement Services with AES, then:

- If the user selects the **Automatic** option, the availability status of the user is always *Available* unless the user is on a call in which case the availability status appears as *Busy*.

  Note:

  You can optionally configure the AES collector timers that automatically set the presence of a user to *Unavailable* or *Out of Office* after a period of time since the last call was made. This feature is made available in Avaya Aura® FP3.

- In the manual mode, the availability status displays the presence that the user selects manually.

If the Client Enablement Services user has more than one client that supports presence, that is, Avaya one-X® Communicator, Avaya Communicator, etc., then self-presence is subject to the aggregation rules on Presence Services.

- Without AES, Client Enablement Services does not publish presence. Hence, the availability status of the user displays the presence that is available on the other client.
- With AES, self-presence is subject to the aggregation rules on Presence Services.

Appendix C: Messaging behavior

You can configure Avaya Communicator for iPad and Windows to use the Instant Messaging capabilities of either Presence Services or Avaya Multimedia Messaging.

- You can configure Avaya Communicator for iPad and Windows for only Presence Services messaging when you do not have Avaya Multimedia Messaging deployed in the solution.
- You must configure Avaya Communicator for iPad and Windows to use Avaya Multimedia Messaging for messaging when you deploy Avaya Multimedia Messaging in the solution, even if Presence Services continues to provide messaging for other endpoints.

If you have configured Avaya Communicator for iPad and Windows clients for Presence Services messaging, you must reconfigure to use Avaya Multimedia Messaging for messaging. Presence Services continues to provide Self and Buddy Presence for Avaya Communicator for iPad and Windows clients after you reconfigure Avaya Multimedia Messaging for instant messaging.

Appendix D: Supported deployment configurations and limitations with Avaya Communicator for Android and iPhone

Configuration	Configuration details	Call origination	FNE support	Simring for incoming calls
EC500 only	Communication Manager Off PBX Mapping = EC500	FNE = Idle Appearance Select	Supported	Depends on the EC500 mobile number configuration on Communication Manager and whether EC500 on Communication Manager is on/off.
Client Enablement Services only	Communication Manager Off PBX Mapping = ONE-X	Client Enablement Services Call Back	Supported. For example, Join Active Call.	Users use Ring My Phones to turn on/off calls to the device.
VoIP only	Standard SIP endpoint configuration	VoIP	Not supported	When registered with Session Manager, users receive SIP calls.
EC500 + Client Enablement Services	Communication Manager Off PBX Mapping = ONE-X	Call Origination menu selection (EC500 or Client Enablement Services)	Supported	Users use Ring My Phones to turn on/off calls to the device.
EC500 + VoIP	Communication Manager Off PBX Mapping = EC500, Standard SIP	Call Origination menu selection (EC500 or VoIP)	Supported	EC500 Call Suppression logic on Communication Manager determines where

Table continues…

Configuration	Configuration details	Call origination	FNE support	Simring for incoming calls
	endpoint configuration			the system delivers the incoming calls.
Client Enablement Services + VoIP	Communication Manager Off PBX Mapping = ONE-X, Standard SIP endpoint configuration	Call Origination menu selection (Client Enablement Services or VoIP)	Supported. For example, Join Active Call.	Users use Ring My Phones to turn on/off calls to the device. EC500 Call Suppression logic is not supported in this configuration.
EC500 + VoIP + Client Enablement Services	Communication Manager Off PBX Mapping = ONE-X, Standard SIP endpoint configuration	Call Origination menu selection (EC500 or Client Enablement Services or VoIP)	Supported	Users use Ring My Phones to turn on/off calls to the device. EC500 Call Suppression logic is not supported in this configuration.

✱ **Note:**

EC500 Call Suppression logic is applicable for calls that you make using Client Enablement Services only with Communication Manager 6.3 FP6 and later versions.

Appendix E: Avaya Communicator for iPhone support for URL schemes

avaya-onex-call

Applications can access the call features of Avaya Communicator for iPhone using the avaya-onex-call url scheme:

```
avaya-onex-call://<phone number>
avaya-onex-call://<phone number>?<parameters>
```

Supported Parameters

phone number	You can use the following characters in <phone number>: [0-9] + * , ; and %23 (url encoded #). If you use any other character, the application removes the same. "," (pause) inserts a 3 second wait before sending the subsequent digits. ";" (wait) is currently implemented as a double pause. All other characters in <phone number> (e.g. '#', '*') are passed to the SIP dialer. **Note:** The first , or ; ends the phone number and the application sends the remaining digits after the called party answers the call.
callbackURL	<url>, where <url> is a valid url to be opened when the application ends the SIP call.

Examples	`avaya-onex-call://9254877934`
	`avaya-onex-call://+19254877934,12345%23`
	`avaya-onex-call://+19254877934,12345%23?`
	`avaya-onex-call://7934?&callbackURL=http://www.google.com`

Limitations	The first character of a <phone number> must be a digit. - , and ; are not legal first characters.

avaya-onex

Users can log in and log out of Avaya Communicator for iPhone using the avaya-onex url scheme:

```
avaya-onex://login
avaya-onex://login?username=<name>&password=<pw>&transaction_id=<id>
avaya-onex://login?username=<name>&password=<pw>&callbackURL=<url>&transaction_id=<id>

avaya-onex://logout?username=>name>&transaction_id=<id>&callbackURL=<url>
```

Login:

Supported Parameters

username	This parameter is optional. The Session Manager username, that is, extension.
password	This parameter is optional. The Session Manager password.
callbackURL	This parameter is optional. Any URL that contains 1 parameter: • transaction_id = (mandatory) An integer that is echoed back to the caller to allow the caller to associate a response to request. • A *result* parameter is added to the callback request to indicate the result of the request: - 0 = success - 1 = login failed - 2 = syntax error - 3 = permission denied - 4 = SIP not configured Provide the URL in the format <scheme>://<host>/path>
Example	`avaya-onex://login?username=11111&password=22222&callbackURL=scheme://host/path&transaction_id=12345` In the example, the one-x client attempts to log in with username, 11111, and password, 22222. After the login attempt, assuming the login was successful, the one-x client invokes the callback response: `scheme://host/path?transaction_id=12345&result=0`.

Logout:

Supported Parameters:

username	This parameter is mandatory. The Session Manager username, that is, extension.
callbackURL	This parameter is mandatory. Any URL that contains 1 parameter: • transaction_id = (mandatory) An integer that is echoed back to the caller to allow the caller to associate a response to request. • A *result* parameter is added to the callback request to indicate the result of the request: - 0 = success - 1 = logout failed - 2 = syntax error - 3 = permission denied - 4 = SIP not configured - 5 = logged into a different extension

Table continues…

Example	`avaya-onex://logout?username=11111&callbackURL=scheme://host/path&transaction_id=12345` In the example, the one-x client attempts to log out with username, 11111. After the logout attempt, assuming the logout was successful, the one-x client invokes the callback response: `scheme://host/path?transaction_id=12345&result=0`.

Glossary

Apple App Store
A digital distribution platform for applications for iOS operated by Apple Inc.

Communication Manager
A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.

Feature name extension
An extension assigned to a feature within Communication Manager. The system administrator administers Feature name extension (FNE) to correspond to a feature access code that activates the feature.

FQDN
The fully qualified domain name (FQDN) is the complete domain name. For example, if the local host name of SBC is *myhost* and the parent domain name is *avaya.com*, the FQDN is *myhost.avaya.com*.

Google Play
A digital distribution platform for applications for the Android operating system and an online digital media and electronics store, operated by Google.

Session Border Controller
A component that delivers security to a SIP-based Unified Communications network.

Session Manager
A SIP routing and integration tool that is the core component within the Avaya Aura® solution.

System Manager
A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity.

Index