Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows

January 29, 2024

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Legal

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA LLC, 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 LLC 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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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 as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “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). End User 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”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Introduction

Purpose

This document provides planning and administration information for Avaya Workplace Client. It also describes additional setup options for Avaya Workplace Client on desktop platforms. Administrators must complete the tasks before end users can use Avaya Workplace Client.

This document includes Avaya Aura® content for Avaya Workplace Client. IP Office content for Avaya Workplace Client is covered in IP Office documentation.

Prerequisites

Before using this document, ensure that you have the following knowledge and skills:

- Know how to install and configure the Avaya products for your deployment. For example:
    - Avaya Aura® products
    - Avaya Session Border Controller
    - Avaya Equinox® Media Server
    - Avaya Multimedia Messaging

  This document includes configuration requirements specific to Avaya Workplace Client, but not general deployment instructions for all products.
- For automatic configuration, ensure that you know how to create a settings file in the settings.txt format.
- Ensure that you are familiar with the process for finding and obtaining Avaya and third-party security certificates. This document provides guidelines for certificates, but does not provide specific instructions for every certificate type that you might need.
- Ensure that you know how to open ports and firewalls. You must also be familiar with the Avaya Workplace Client Port Matrix document at https://downloads.avaya.com/css/P8/documents/101065872.

Avaya Workplace Client overview

Avaya Workplace Client is a soft phone application that provides access to Unified Communications (UC) and Over the Top (OTT) services. You can access Avaya Workplace Client on the following platforms:

- Mobile:
  - Android: From a mobile phone, tablet, or an Avaya Vantage™ device
  - iOS: From an iPad, iPhone, or iPod Touch
- Desktop:
  - Mac
  - Windows
  - Chrome: From a Google Chromebook

Based on your feature requirement, you can deploy Avaya Workplace Client in several ways. In the basic deployment type, you can have only voice calling. You can then include additional features such as directory search, contact management, presence, instant messaging, and conferencing.

With Avaya Workplace Client, you can use the following functionalities:

- Make point-to-point audio and video calls.
- Answer calls, send all calls to voice mail, and forward calls
- Extend calls to your mobile phone if EC500 is configured
- Log in to your extension and join calls with multiple devices if Multiple Device Access (MDA) is configured.
- Listen to your voice mail messages.
- View your call history.
- Access your Avaya Aura® and local contacts.
- Perform an enterprise-wide search using Avaya Aura® Device Services, Client Enablement Services, Avaya Cloud Services, ActiveSync on mobile platforms and Avaya Aura® Device Services, LDAP, or Avaya Cloud Services on desktop platforms.
- Manage your presence status and presence status message.
- Send instant messages.
- Capture photo, audio, and video files, and send generic file attachments in an IM conversation.
- Join and host conference calls with moderator controls.
- Use point-to-point and conference call control functionality. You can also add participants to a conference.
- Share a screen portion, the entire display screen, an application, or a whiteboard while on a conference call on desktop platforms.
- View a portion of the screen, the entire display screen, an application, or a whiteboard shared by another conference participant on mobile and desktop platforms.

Note:

Some Avaya Workplace Client features must be configured for your enterprise before you can use them.

Solution architecture

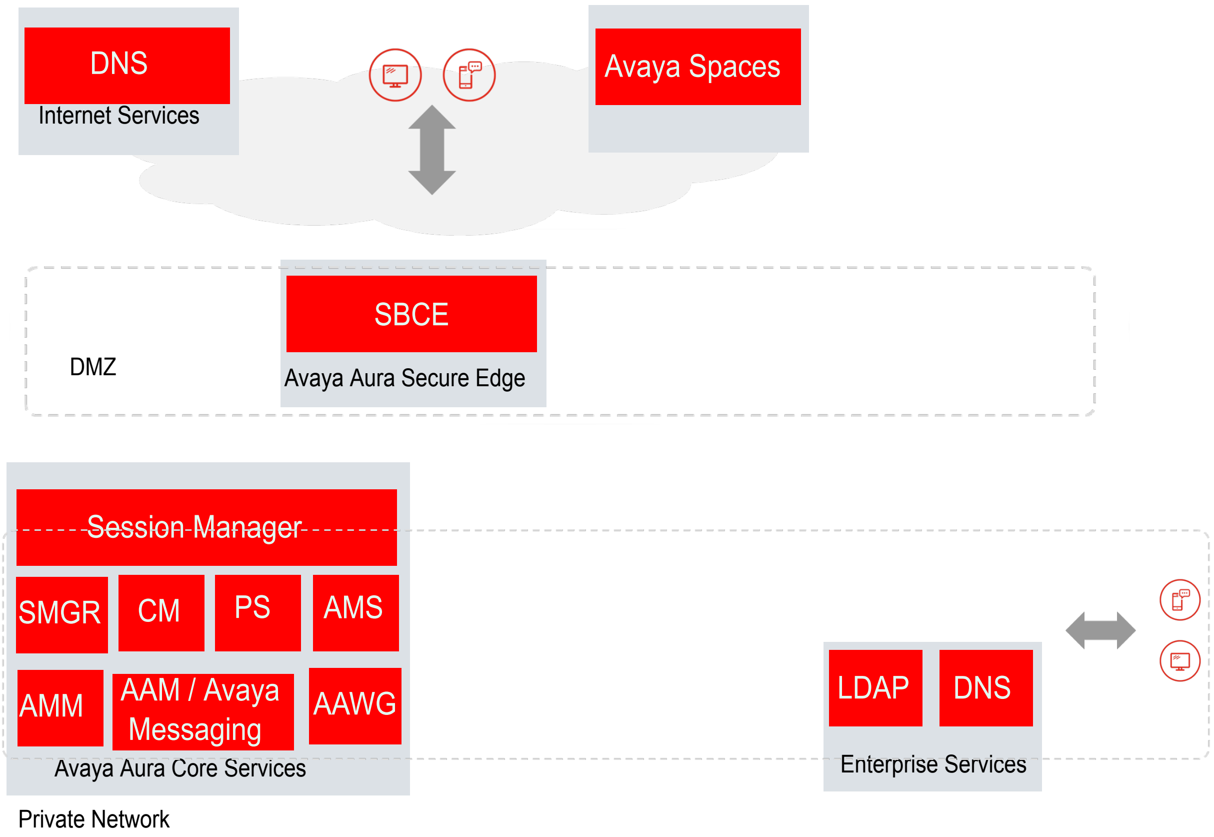
SIP Voice, Remote Worker, and Messaging

The following images provide a high-level architecture of the Avaya Workplace Client solution based on the functionality that is provided.

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 SBCE IP address.
- When on-premise, the internal DNS service maps the same FQDN to the Session Manager IP address.

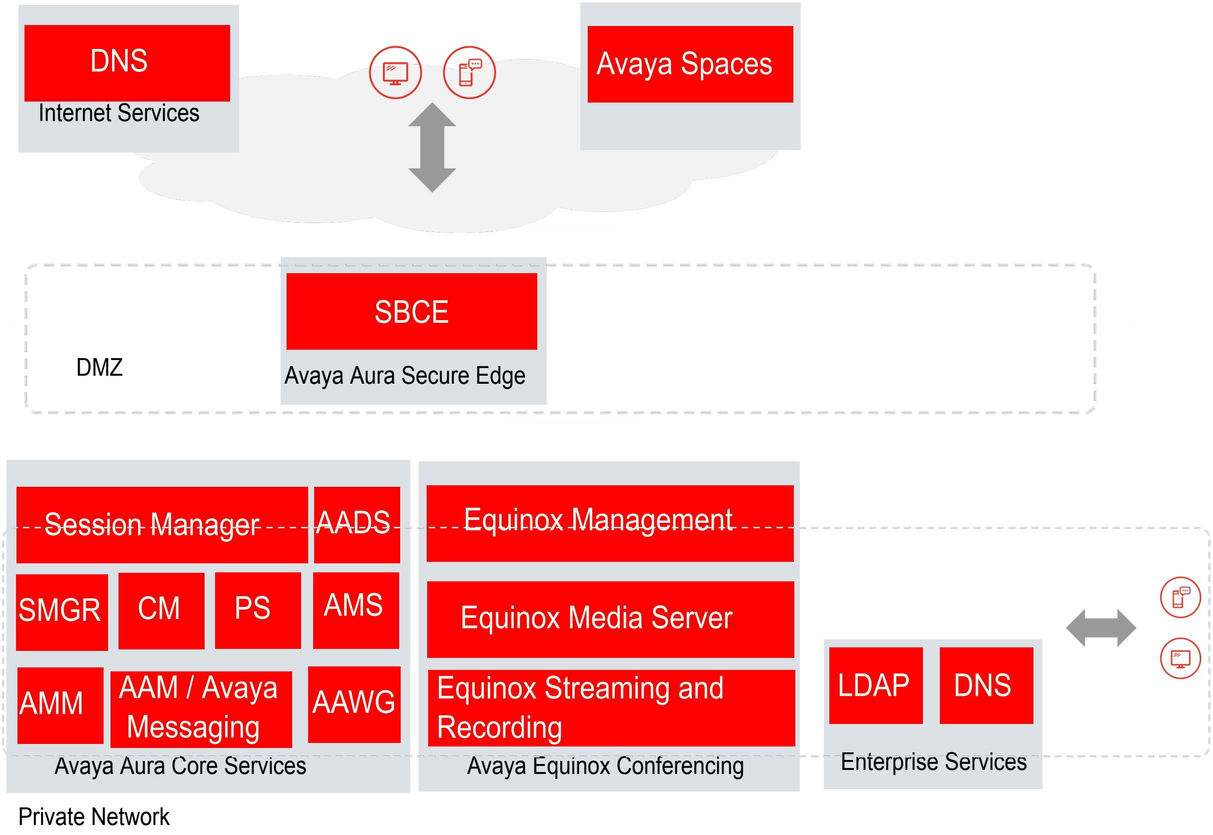
If Avaya Workplace Client connects remotely through SBCE and directly to Session Manager when on-premise, the same port must function as the internal port on Session Manager and the external port on SBCE.



Acronym	Full name
SBCE	Avaya Session Border Controller
AADS	Avaya Aura® Device Services
SMGR	Avaya Aura® System Manager
CM	Avaya Aura® Communication Manager
PS	Avaya Aura® Presence Services
AMS	Avaya Aura® Media Server
AMM	Avaya Multimedia Messaging
AAM	Avaya Aura® Messaging
AAWG	Avaya Aura® Web Gateway
CES	Client Enablement Services

Protocol	Private net destination	Service
SIP-TLS	Session Border Controller and Session Manager	SIP signaling
SRTP	Point-to-point, Media Servers, and Gateways	Audio/Video media
HTTPS	Session Manager	PPM
HTTPS	Utility Server or other Web Server	Automatic configuration
HTTPS	Avaya Multimedia Messaging	Instant messaging
DNS	Internal/External DNS	Automatic configuration service discovery resolution of internal and external services

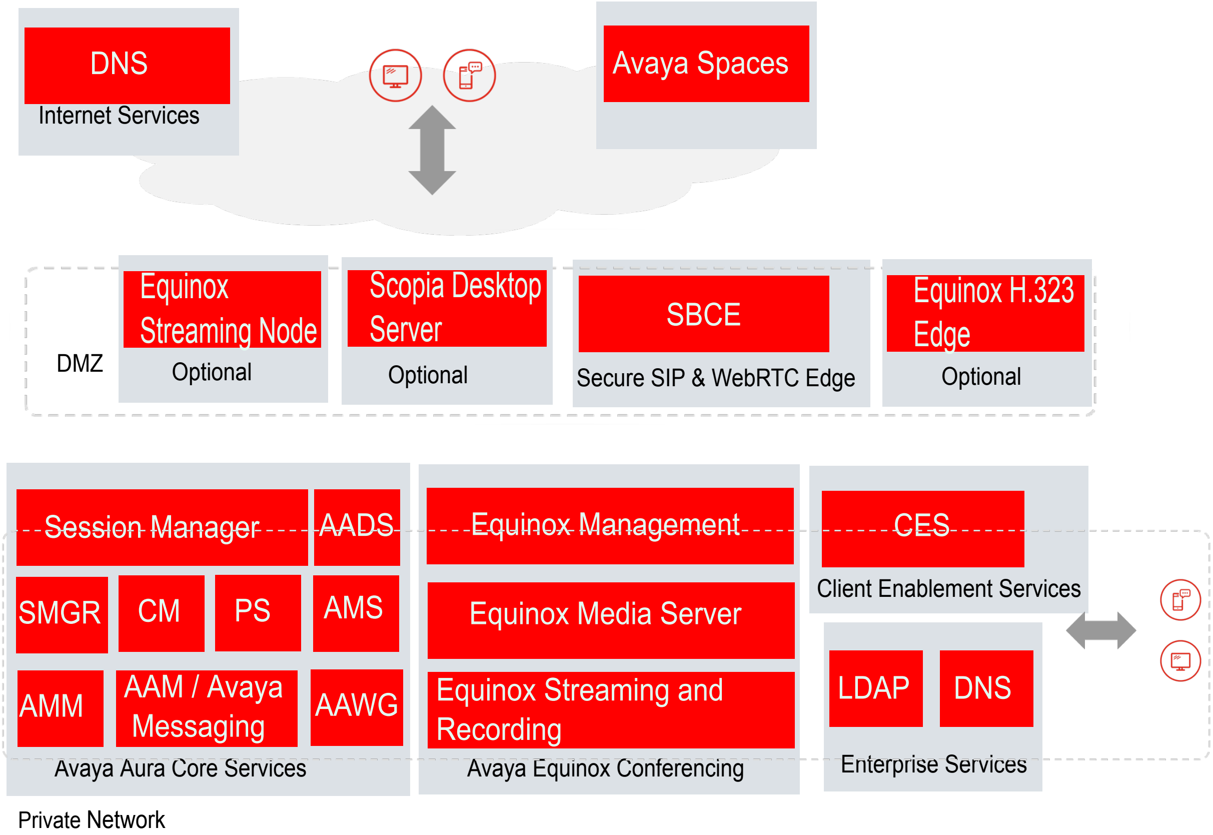
SIP Voice, Remote Worker, Messaging, Conferencing, and Device Services



Protocol	Private net destination	Service
SIP-TLS	Session Border Controller and Session Manager	SIP signaling
SRTP	Point-to-point, Media Servers, and Gateways	Audio/Video media
HTTPS	Session Manager	PPM
HTTPS	Avaya Aura® Device Services	Automatic configuration, Auto-update, Directory Service, and Contact Service
HTTPS	Avaya Multimedia Messaging	Instant messaging
HTTPS	WCS	Web Collab

Protocol	Private net destination	Service
DNS	Internal/External DNS	Automatic configuration service discovery

SIP Voice, Remote Worker, Messaging, Conferencing, Device Services, and Client Enablement Services



Protocol	Private net destination	Service
SIP-TLS	Session Border Controller and Session Manager	SIP signaling
SRTP	Point-to-point, Media Servers, and Gateways	Audio/Video media
HTTPS	Session Manager	PPM

Protocol	Private net destination	Service
HTTPS	Avaya Aura® Device Services	Automatic configuration, Auto-update, Directory Service, and Contact Service
HTTPS	Avaya Multimedia Messaging	Instant messaging
HTTPS	WCS	Web Collab
DNS	Internal/External DNS	Automatic configuration service discovery
CES	Client Enablement Services	Call logs, voice mail, and call-back

Agent

You can use the agent functionality, that is, Contact Center features, on Avaya Workplace Client. Currently, agent functionality is supported on Android, iOS, and Windows platforms.

Media Client

You can use Avaya Workplace Client for Windows as a media client for Avaya Workspaces for Call Center Elite, Avaya Oceana®, or other CTI control scenarios.

Only basic UC functionality is available in this mode.

Avaya Workplace VDI

You can use Avaya Workplace VDI in the Desk Phone mode with Avaya Workplace Client for Windows. You must deploy Avaya Workplace Client for Windows in a virtual environment.

Avaya Workplace VDI is a Virtual Desktop Infrastructure (VDI) soft client that enhances the audio and video quality of calls by processing the audio and video locally on your VDI endpoint. A VDI endpoint might be a thin client or a Windows-based personal computer. The controlling client, such as Avaya Workplace Client for Windows, is deployed on virtual desktops running in the data center and provides the user interface for unified communications.

Deployment options

Based on your feature requirement, you can deploy Avaya Workplace Client in several ways. In the basic deployment type, you can have only voice calling. You can then include additional features such as directory search, contact management, presence, instant messaging, and conferencing.

Deployment type	Function
Basic UC deployment	Use this deployment option to perform voice calling in your enterprise. The Avaya Aura® environment includes Communication Manager, Session Manager, and System Manager.
UC deployment without conferencing	Use this deployment option to access UC functionality without conferencing in your enterprise. The Avaya Aura® environment includes Session Manager, Communication Manager, System Manager, and Presence Services. Avaya Aura® environment provides UC services such as voice and video calls, and presence. You can optionally integrate Avaya Workplace Client with the following components: • Avaya Multimedia Messaging: For instant messages • Avaya Session Border Controller • Client Enablement Services: Only on mobile clients
Unified Communications (UC) deployment Also known as the Team Engagement (TE) deployment	Use this deployment option to access complete UC functionality in your enterprise. The Avaya Aura® environment includes Session Manager, Communication Manager, System Manager, Presence Services, and Avaya Aura® Device Services. Avaya Aura® environment provides UC services to an enterprise. The UC services include voice and video calls, audio and video conferences, directory search, contact management, and presence. You can optionally integrate Avaya Workplace Client with the following components: • Avaya Equinox® Conferencing Release 9.0 or later

Deployment type	Function
	• Avaya Multimedia Messaging: For instant messages • Avaya Spaces: For instant messages and meetings • Avaya Session Border Controller • Unified Portal • Avaya Aura® Web Gateway • Client Enablement Services: Only on mobile clients
Over the Top (OTT) deployment Also known as the Meet-Me deployment	Use this deployment option to access only the conferencing functionality in your enterprise. You can deploy Avaya Equinox® Conferencing Release 9.0 or later in an environment with a non-Avaya voice solution, such as Cisco CUCM or Siemens. You can assign some users a virtual room for audio, video, and data conferencing. In an OTT deployment, clients join the conference by using HTTP-based protocols, not SIP. For OTT deployments that use third-party SIP servers, Avaya Workplace Client signs in to Avaya Equinox® Management or LDAP directory for user validation and authentication. You can optionally integrate Avaya Workplace Client with the following components: • Avaya Spaces • Avaya Session Border Controller • Unified Portal • Avaya Aura® Web Gateway
Media client deployment	Use this deployment option to access Avaya Workplace Client for Windows as a media client for Avaya Workspaces for Call Center Elite, Avaya Oceana®, or other CTI control scenarios. Basic UC functionality is available in this mode.

Deployment type	Function
Contact Center client deployment	Use this deployment option to access the agent functionality, that is, Contact Center features, on Avaya Workplace Client. Currently, agent functionality is supported on Android, iOS, and Windows platforms. Agent functionality includes enabling the work mode, configuring the Ready, Not Ready, and ACW states, configuring the call work code, updating the skill set, and so on.

User types

User type	Definition
Basic UC with voice only	These users use Avaya Workplace Client for voice calls.
UC without conferencing	These users use Avaya Workplace Client as a primary UC client for voice and video calls, instant messaging, and presence.
UC	These users use Avaya Workplace Client as a primary UC client for voice and video calls, audio and video conferences, directory search, contact management, instant messaging, and presence. A UC user can be a host or guest at any conference.
OTT Named or OTT Signed in	These users do not use Avaya Workplace Client as a primary UC client but need to host conferences with audio and video and present content. These users have a virtual room and associated features such as recording resources. In an OTT

User type	Definition
	deployment, clients join the conference by using HTTP-based protocols, not SIP.
OTT Guest	These users do not use Avaya Workplace Client as a primary UC client but need to join conferences with audio and video as guests. These users might need to present by using screen sharing. In an OTT deployment, clients join the conference by using HTTP-based protocols, not SIP.
Outbound Guest	An outbound guest is a user of the Avaya UC or OTT deployment who joins an Avaya Workplace Client conference hosted by an external party. For example, an Avaya Workplace Client user of XYZ Corp joins an Avaya Equinox® Conferencing 9.0 conference hosted by a user at ABC Corp.
Inbound Guest	An inbound guest is a user from an external company, such as a partner, supplier, customer, or a prospect who joins a conference hosted by a user of the Avaya UC or OTT deployment.
Media client	These users use Avaya Workplace Client for Windows as a media client for Avaya Workspaces for Call Center Elite, Avaya Oceana®, or other CTI control scenarios. Basic UC functionality is available in this mode.
Agent	These users use the agent functionality, that is, Contact Center features, on Avaya Workplace Client. Currently, agent functionality is supported on Android, iOS, and Windows platforms. Agent functionality includes enabling the work mode, configuring the Ready, Not Ready, and ACW states,

User type	Definition
	configuring the call work code, updating the skill set, and so on.

Feature support

Voice features

Feature	Android	iOS	Windows	Mac	Desk Phone mode	Other Phone mode
Make and receive audio calls	Yes	Yes	Yes	Yes	Yes	Yes
Consultative Transfer	Yes	Yes	Yes	Yes	Yes	Yes
CM-based Consultative Conference (6-party)	Yes	Yes	Yes	Yes	Yes	Yes (Tested up to 3-party)
Local Call History	Yes	Yes	Yes	Yes	Yes	Yes
Centralized Call History	Yes	Yes	Yes	Yes	Yes	Yes
Desk Phone mode	N.A.	N.A.	Yes	Yes	Yes	N.A.
Simultaneous Ring (EC500)	Yes	Yes	Yes	Yes	Yes	N.A.
Extend Call to Cellular	Yes	Yes	Yes	Yes	Yes	N.A.

Feature	Android	iOS	Windows	Mac	Desk Phone mode	Other Phone mode
Call Forward All	Yes	Yes	Yes	Yes	Yes	Yes
Call Forward Busy / No Answer	Yes	Yes	Yes	Yes	Yes	Yes
Call Forward Enhanced	Yes	Yes	Yes	Yes	Yes	Yes
Send All Calls	Yes	Yes	Yes	Yes	Yes	Yes
Exclusion	Yes	Yes	Yes	Yes	Yes	Yes
Auto Callback	Yes	Yes	Yes	Yes	Yes	No
EC500 FNE auto-dialer	Yes	Yes	N.A.	N.A.	N.A.	N.A.
Call Back (CES)	Yes	Yes	N.A.	N.A.	N.A.	N.A.
Ring Phone Group (CES)	Yes	Yes	N.A.	N.A.	N.A.	N.A.
Call Handoff (Cell<>VoIP)	Yes	Yes	N.A.	N.A.	N.A.	N.A.
VoIP Call Recovery between networks	Yes	Yes	N.A.	N.A.	N.A.	N.A.
Secure Call Indicator	Yes	Yes	Yes	Yes	N.A.	N.A.

Advanced Voice features

Feature	Android	iOS	Windows (Feature Manager + Button Module)	Mac	Desk Phone mode	Other Phone mode
Auto Dial	No	No	Yes	Yes	Yes	No
Auto Callback Cancel	Yes	Yes	Yes	No	Yes	No
Team Button	Yes	Yes	Yes	No	Yes	No
Hunt Group Busy	Yes	Yes	Yes	Yes	Yes	Yes
Limit Number of Concurrent Calls	Yes	Yes	Yes (Button Module only)	No	Yes	Yes
Extended Call Pickup	No	No	Yes	Yes	Yes	No
Directed Call Pickup	No	No	Yes	Yes	Yes	No
Bridge Line Appearances (Admin)	Yes	Yes	Yes	Yes	Yes	No
Message Waiting 3rd-party	No	No	Yes (Button Module only)	No	Yes	Yes
Busy Indicator	No	No	Yes	Yes	Yes	Yes
Call Park / Unpark	Yes	Yes	Yes	Yes	Yes	No
Call Pickup	Yes	Yes	Yes	Yes	Yes	No

Feature	Android	iOS	Windows (Feature Manager + Button Module)	Mac	Desk Phone mode	Other Phone mode
Calling Party Number Block / Unblock	Yes	Yes	Yes (Button Module only)	Yes	No	No
Malicious Call Trace	No	No	Yes (Button Module only)	No	Yes	
No Hold Conference	No	No	Yes (Button Module only)	No	Yes	Yes
Send All Calls (Other Extension)	Yes	Yes	Yes	Yes	Yes	Yes
Call Forward (Other Extension)	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced Call Forward (Other Extension)	Yes	Yes	Yes (Button Module only)	Yes	Yes	Yes
Service Observe	No	No	Yes (Button Module only)	No	Yes*	Yes

Note:

You can use the Service Observe feature in the Desk Phone mode with J1xx and 96x1 SIP phones. However, Avaya Workplace VDI does not support the Service Observe feature. Hence, you cannot use the Service Observe feature in the Desk Phone mode with Avaya Workplace VDI.

Contact Center features

Feature	Android	iOS	Windows (Button Module + Agent bar)	Mac	Desk Phone mode	Other Phone mode
Agent Login	Yes	Yes	Yes	No	Yes	Yes
Auto/Manual In	Yes	Yes	Yes	No	Yes	Yes
After Call Work	Yes	Yes	Yes	No	Yes	Yes
Not Ready	Yes	Yes	Yes	No	Yes	Yes
Call Work Code	Yes	Yes	Yes	No	Yes	Yes
Change Agent Skill	Yes	Yes	Yes	No	Yes	No
Button LED states	N.A.	N.A.	Yes (Button Module only)	No	Yes	Yes
Change Agent States	Yes	Yes	Yes	No	Yes	Yes
No Hold Conference	No	No	Yes (Button Module only)	No	No	Yes
Forced Logout Override	No	No	Yes (Button Module only)	No	Yes	Yes
ASAI UUI	No	No	Yes	No	Yes	Yes
Supervisor Assist	No	No	Yes	No	Yes	No
Q-Stats	No	No	Yes	No	Yes	Yes

Feature	Android	iOS	Windows (Button Module + Agent bar)	Mac	Desk Phone mode	Other Phone mode
Service Observe	No	No	Yes (Button Module only)	No	Yes	Yes
Agent Greetings	No	No	Yes	No	No	No

Note:

If you are using Avaya Workplace Client in the Other Phone mode, do not use the functionality with the CTI or 3PCC client, which controls Avaya Workplace Client in the Other Phone mode.

FIPS support

Federal Information Processing Standards (FIPS) is a cryptographic security standard.

FIPS 201 is a United States federal government standard that specifies Personal Identity Verification (PIV) requirements for federal employees and contractors. FIPS 201 specifies that an identity credential must be stored on a smart card. Avaya Workplace Client provides smart card support with both FIPS and non-FIPS clients.

FIPS installation is only supported for new installations. You can download and install the FIPS and non-FIPS versions of Avaya Workplace Client from https://support.avaya.com/downloads/. You cannot upgrade any version of a non-FIPS client to a FIPS client.

To enable FIPS on a non-FIPS version or disable FIPS on a FIPS version, uninstall Avaya Workplace Client first and then install the FIPS or non-FIPS version of Avaya Workplace Client. Avaya Workplace Client works in the FIPS version, where the OpenSSL API and OpenSSL FIPS Object Module are used.

The following are the approved FIPS-compliant cryptography algorithms:

- RSA
- DSA
- 3DES in CBC, (CFB1), CFB8, CFB64, ECB, OFB mode
- DH
- AES in CBC, (CFB1), CFB8, CFB128, ECB, OFB mode with 128/192/256 bit keys
- SHA-1, SHA-2
- HMAC

Note:

All other non-FIPS-approved algorithms are disabled in the FIPS version.

Configuration differences between FIPS and non-FIPS clients

The following table lists the configuration differences between the FIPS and non-FIPS version of Avaya Workplace Client:

Configuration	FIPS	Non-FIPS
Supported protocols	Only secure protocols. For example, HTTPs, SIP TLS, LDAPs	Both non-secure and secure protocols
Minimum supported TLS version	1.3	1.0
Minimum certificate key length	2048	1024
Joint Interoperability Test Command (JITC) feature set support	• DSCPAUD_PRIORITY • DSCPAUD_IMMEDIATE • DSCPAUD_FLASH • DSCPAUD_FLASHOVERRIDE • DSCPVID_PRIORITY • DSCPVID_IMMEDIATE • DSCPVID_FLASH • DSCPVID_FLASHOVERRIDE	Limited support
Avaya QoS (DSCP) driver	Mandatory	Optional

Components overview

During the planning phase, you must configure Avaya Workplace Client components and their associated security certificates in your network. The required components vary depending on the deployment type and the functionality that you choose to configure. For information about the available UI functionality and advanced functionality options, see the “Planning for deployment” chapter in this document.

For more information about interoperability with other components, see http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Solution component to feature map

The components you require depend on the feature set you need. For new deployments and the best experience for any implementation, you must include the Avaya Aura® core components including Avaya Aura® Presence Services and Avaya Aura® Device Services.

The following table provides a mapping of solution components to Avaya Workplace Client features:

Solution component	Feature
Core Avaya Aura® components including: • Avaya Aura® System Manager • Avaya Aura® Session Manager • Avaya Aura® Communication Manager	• Audio and video calling • Voice and advanced voice features • 6-party adhoc audio conference • Multiple Device Access • Centralized Workplace Contacts for Mac and Windows • Centralized call logs • VoIP Push Notifications for: • Android with Session Manager Release 10.1 and later • iOS with Session Manager Release 8.1.3.3 and later **Important:** Avaya recommends the use of Session Manager for push notifications on Android and iOS devices.
Avaya Aura® Presence Services	• Persistent multimedia messaging • Presence • Instant messaging and presence federation

Solution component	Feature
	• Microsoft Exchange and Office 365 Calendar integration
Avaya Aura® Device Services	• Directory search and advanced search • Contact favorites and contact grouping • Centralized Workplace Contacts for Android, iOS, Mac, and Windows • Advanced automatic configuration • Unified Login with enterprise credentials • Automatic update of Mac and Windows clients • OAuth or SAML authentication and SSO
Avaya Aura® Web Gateway	VoIP Push Notifications for iOS ❗ **Important:** Avaya recommends the use of Session Manager for push notifications on Android and iOS devices.
Avaya Session Border Controller (SBCE)	Remote worker support without VPN
Avaya IX Meetings	On-premise or private cloud audio, video, or web conferencing
Microsoft Exchange or Office 365	Top of Mind calendar support
Avaya Cloud Services	• Avaya Spaces Direct Messaging • Open Avaya Spaces dashboard • Alternative service discovery option for automatic configuration

Components needed for UC deployments

Component	Platform	Function
Core Avaya Aura® components	All Avaya Workplace Client platforms	Configure the following components in your network: • Avaya Aura® System Manager • Avaya Aura® Session Manager • Avaya Aura® Communication Manager Use these components to perform voice calling in your enterprise.
Avaya Aura® Device Services	All Avaya Workplace Client platforms	This component provides a common place in the Avaya Aura® architecture for client and endpoint devices to store and retrieve contact data. Contact data includes enterprise contacts and Avaya Aura® PPM contacts. Users can view contact data on any of their devices. Contact groups are only available with Avaya Aura® Device Services Release 7.1.6 and later. Avaya Aura® Device Services is also used for the automatic configuration of Avaya Workplace Client. **Note:** Call logs are not a part of Avaya Aura® Device Services. This component is mandatory for Avaya Equinox® Conferencing.
Avaya Aura® Web Gateway	All Avaya Workplace Client platforms	This component acts as a gateway to Avaya Aura® clients and

Component	Platform	Function
		applications utilizing WebRTC signaling and media. This component also provides the telephony and messaging events for the VoIP push notification solution. This component is mandatory for Avaya Equinox® Conferencing.
Avaya Equinox® Conferencing	All Avaya Workplace Client platforms	Use this component to access advanced conferencing functionality, such as audio and video conferencing, and web collaboration. **Note:** For basic conferencing functionality, you only need Avaya Aura® Communication Manager.
Avaya Aura® Presence Services and Avaya Multimedia Messaging	All Avaya Workplace Client platforms	Use these components for the presence and instant messaging functionalities. • Avaya Aura® Presence Services provides presence functionality. • Avaya Multimedia Messaging provides IM functionality. Avaya Multimedia Messaging provides access to additional capabilities, such as: • Sending attachments over IM • Capturing video and audio from

Component	Platform	Function
		Avaya Workplace Client **Note:** Presence Services Release 8.0.1 integrates Avaya Multimedia Messaging with the current Presence Services platform creating one streamlined solution for the users. With IM and rich presence functionalities, Presence Services is a powerful communication tool.
Avaya Spaces	All Avaya Workplace Client platforms	Use this component with Avaya Workplace Client : • To exchange instant messages with other users using Avaya Spaces Direct Messaging. • To join a Spaces meeting. • To open your Spaces dashboard.
Avaya Session Border Controller (SBCE)	All Avaya Workplace Client platforms	Use this component if your enterprise requires support for remote workers. Besides configuring SBCE, you must also perform other tasks for remote workers to use all Avaya Workplace Client functionalities.
Client Enablement Services	Avaya Workplace Client for Android and iOS platform	Use Client Enablement Services to access the visual voice mail service. New customers can use most of the Avaya Workplace Client

Component	Platform	Function
		functionality without using Client Enablement Services. Avaya Workplace Client on Avaya Vantage™ does not support Client Enablement Services. **Note:** If you enable the Offline Call Journaling feature on Avaya Aura® Communication Manager, the user cannot view the Client Enablement Services logs, including voice mail.
Unified Portal	All Avaya Workplace Client platforms	Use this component to manage your meetings. You can plan meetings, customize meeting properties, and send meeting details to participants.

Components needed for Over the Top deployments

Component	Platform	Function
Avaya Equinox® Conferencing	All Avaya Workplace Client platforms	Use this component to access audio and video conferencing, and web collaboration.
Avaya Aura® Web Gateway	All Avaya Workplace Client platforms	This component acts as a gateway to Avaya Aura® clients and applications utilizing WebRTC signaling and media.

Component	Platform	Function
Avaya Session Border Controller (SBCE)	All Avaya Workplace Client platforms	Use this component if your enterprise requires support for remote workers. Besides configuring SBCE, you must also perform other tasks for remote workers to use all Avaya Workplace Client functionalities.
Unified Portal	All Avaya Workplace Client platforms	Use this component to manage your meetings. You can plan meetings, customize meeting properties, and send meeting details to participants.
Avaya Equinox® Media Server	All Avaya Workplace Client platforms	This component provides HD video transcoding Multipoint Control Unit (MCU) and high-scale audio engine derived from Avaya Media Server and Web Collaboration Engine. Besides the traditional Scopia MCU functionalities, Avaya Equinox® Media Server includes WebRTC and Web Collaboration features in the same virtualized application.
Avaya Spaces	All Avaya Workplace Client platforms	Use this component with Avaya Workplace Client : • To exchange instant messages with other users using Avaya Spaces Direct Messaging. • To join a Spaces meeting.

Component	Platform	Function
		- To open your Spaces dashboard.

End-user components

Component	Platform	Description
Avaya Workplace Client interface for your device	You can use Avaya Workplace Client with the following operating systems: - Android - iOS - Mac - Windows	After planning and configuring Avaya Workplace Client, end users can install and use the Avaya Workplace Client interface. If you configure MDA, end users can use Avaya Workplace Client on different devices simultaneously.
Deskphone (optional)	You can use this component with: - Desk Phone mode on an Avaya Workplace Client on desktop platforms. - Dual registration on all platforms. You can use an H.323 phone with Avaya Workplace Client. - MDA in My Computer mode on an Avaya Workplace Client on desktop platforms.	With Desk Phone mode, you can optionally use an Avaya Workplace Client on desktop platforms to control your SIP deskphone. The list of SIP proxy controllers on the deskphone and Avaya Workplace Client on desktop platforms must match. Desk Phone mode requires MDA and TLS. You can use the following deskphone models in the Desk Phone mode with SIP software release 7.0 or later versions: - 9601 - 9608 - 9608G - 9611G - 9621G

Component	Platform	Description
		• 9641G • 9641GS • H175 • J100 Series (J129, J139, J159, J169, J179, and J189) For the complete list of supported deskphone models, see http://support.avaya.com/CompatibilityMatrix/Index.aspx. If you configure dual registration, users can use an H.323 deskphone with any Avaya Workplace Client for making and receiving calls. Dual Registration functionality works similar to MDA functionality. Dual Registration and Desk Phone mode are different features.
Avaya Workplace VDI (optional)	You can use this component with Desk Phone mode on Avaya Workplace Client for Windows. You must deploy Avaya Workplace Client for Windows in a virtual environment.	Avaya Workplace VDI is a Virtual Desktop Infrastructure (VDI) soft client that enhances the audio and video quality of calls by processing the audio and video locally on your VDI endpoint. A VDI endpoint might be a thin client or a Windows-based personal computer. The controlling client, such as Avaya Workplace Client for Windows, is deployed on virtual desktops running in the data center and provides the user interface for unified communications.

System requirements and interoperability

For the latest and most accurate compatibility information for Avaya Workplace Client, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Note:

Microsoft does not support Windows 7, Windows 8, Windows 8.1, Windows Server 2008, and Windows Server 2008 R2. Hence, Avaya Workplace Client for Windows does not support these operating systems from Release 3.13. From Release 3.13, the click-to-call browser extension is not provided for the Internet Explorer web browser.

Ensure that your mobile device or desktop system includes the latest OS updates. Your system must have the latest vendor-supplied drivers, specifically for:

- Headsets
- Cameras
- Display adapters

Avaya does not maintain a list of supported USB headsets for Avaya Workplace Client as vendors continue to release new products frequently. You can use any headset compatible with your personal computer or device for audio.

For complete integration, including call control with USB headsets, vendors such as Poly, Jabra, and EPOS have integrated Avaya Workplace Client with a desktop companion software. You can download this software from the headset vendor site. Avaya also provides integrated support for headset call controls, without requiring additional software, for the following headsets on the Windows and Mac platforms:

- Avaya L100 series
- Jabra
- Poly

Updating Windows display adapter drivers

About this task

Use this procedure on Windows 10 computers. If you are using a computer with a different Windows OS, the procedure varies slightly.

Procedure

1. Open Windows Control Panel.
2. Select **Device Manager**.
3. Expand **Display adapters**.

4. For each display adapter, right-click the adapter name and select **Update Driver Software**.
5. Select **Search automatically for updated driver software**.
6. **Optional** If updated drivers are available, select **Search for updated drivers on Windows update**.

Planning for deployment

Deployment process

You need to perform the following steps to deploy Avaya Workplace Client:

1. Obtain components and licenses for the planning phase.
2. Choose configuration options for the planning phase.
3. Complete configuration and setup tasks for the planning phase.
4. Install the client.

   End users can install Avaya Workplace Client on mobile and desktop platforms. You can install Avaya Workplace Client on desktop platforms using a command line option. Command line installation only works with administrative privileges.

   If the enterprise is using a Mobile Device Management (MDM) system with the mobile devices enrolled in it, you can push the application installs to the Android and iOS devices.
5. Configure client settings manually or with automatic configuration.

After you complete the planning, installation, and configuration, end users can use Avaya Workplace Client. For setup and usage information for end users, see *Using Avaya Workplace Client for Android, iOS, Mac, and Windows*.

Checklist for Unified Communications deployment

Use this checklist if you are deploying Avaya Workplace Client in a UC environment.

Task	Description	Reference	✔
Obtain and install the required components.	Determine which components are appropriate for your enterprise.	For a list of supported components, see Components needed for UC deployments.	

Task	Description	Reference	✔
	The components that you must install and configure vary depending on the functionality you choose.		
Obtain the required licenses.	Determine which licenses are appropriate for your enterprise. Suite licenses include all the required licenses. The licenses you need vary depending on the functionality that you plan to use.	For more information about license options, see Licensing requirements.	
Prepare the site.	Understand the following: • Network considerations and diagnostics for Avaya Workplace Client • Supported codecs and DSCP configuration • Wi-Fi best practices Configure the Wi-Fi infrastructure and learn about changes in the device functionality based on access point changes.	For more information, see the following topics in the chapter on Site preparation: • Network considerations and diagnostics • Supported codecs • DSCP values • Configuring DSCP values on the network • Wi-Fi best practices	
Understand the security and certificate requirements.	Understand the following: • Security requirements for Avaya Workplace Client	For more information, see the following topics in the chapter on Security and certificate configuration: • Security requirements	

Task	Description	Reference	✔
	- Password storage encryption methods - Security recommendations for desktop and mobile platforms - Client identity and server certificates - Guidelines to determine whether you need certificates - Procedures for obtaining Avaya product certificates - Guidelines and implications to support antivirus and malware scanning software - Supported cipher suites and limitations of blacklisting cipher suites	- Password storage - Desktop platform security recommendations - Mobile device security recommendations - Client identity certificates - Server certificates - Guidelines to determine whether you need certificates - Obtaining the Avaya SIP Product CA certificate - Obtaining the Avaya Aura System Manager CA certificate - Antivirus and malware scanning support - Supported cipher suites - Limitations of blacklisting cipher suites	

Task	Description	Reference	✔
Set up and configure core Avaya Aura® components.	Configure the core Avaya Aura® components. Review the checklist, which outlines the high-level setup and configuration tasks for core Avaya Aura® components.	For more information, see Checklist for configuring Unified Communications infrastructure.	
Configure Avaya Aura® Device Services.	This component provides a common place in the Avaya Aura® architecture for client and endpoint devices to store and retrieve contact data that users want to view. Contact groups are only available with Avaya Aura® Device Services Release 7.1.6 and later. You can use Avaya Aura® Device Services for automatic configuration of Avaya Workplace Client.	For more information, see the chapter on Avaya Aura Device Services configuration.	
Set up and configure Avaya Workplace Client functionality.	Determine which Avaya Workplace Client functionality is appropriate for your enterprise. Configure the functionality according to your requirement. Review the checklist, which outlines the high-level setup and configuration tasks for Avaya Workplace Client functionality.	For more information, see Checklist for configuring Avaya Workplace Client functionality for Unified Communications.	
Set up and configure Avaya Equinox® Conferencing functionality.	Determine which Avaya Equinox® Conferencing functionality is appropriate for your enterprise. Configure the	For more information, see Checklist for configuring Avaya Equinox Conferencing functionality.	

Task	Description	Reference	✔
	functionality according to your requirement. Review the checklist, which outlines the high-level setup and configuration tasks for Avaya Equinox® Conferencing functionality.		
Set up and configure remote worker functionality.	The remote worker functionality enables users that are not connected to the enterprise network to access Avaya Workplace Client. Determine which remote worker functionality is appropriate for your enterprise. Configure the functionality according to your requirement. Use the worksheet to determine how to provide the remote workers with access to available functionality.	For more information, see Remote worker configuration worksheet.	
Install the client.	If you use the command line and silent installation options on desktop platforms, then end users do not need to install Avaya Workplace Client manually. If the enterprise is using a Mobile Device Management (MDM) system with the mobile devices enrolled in it, you can push the application installation to the Android and iOS devices. MDM is a deployment of a combination of on-device applications and	For additional setup options on desktop platforms, see the chapter on Additional setup options for Avaya Workplace Client for Windows and Mac platforms.	

Task	Description	Reference	✔
	configurations, corporate policies and certificates, and backend infrastructure. Use MDM to simplify and enhance the IT management of end user devices.		
Set up automatic configuration.	Set up automatic configuration so that users do not have to manually configure Avaya Workplace Client.	For more information, see Automatic configuration.	
Set up Avaya Workplace Client add-in for Microsoft Outlook	Avaya Workplace Client provides an Outlook add-in for desktop platforms. The add-in enables you to: • Add meeting details to an appointment. • Start and join conferences from your calendar. • Start a call from within Outlook to a contact by using Avaya Workplace Client for Windows.	For more information, see the chapter on Avaya Workplace Client add-in for Microsoft Outlook.	

Checklist for Over the Top deployment

Use this checklist if you are deploying Avaya Workplace Client in an OTT environment. If you do not have Avaya Aura®, you must use this deployment option.

Task	Description	Reference	✓
Obtain and install the required components.	Determine which components are appropriate for your enterprise. The components that you must install and configure vary depending on the functionality you choose.	For a list of supported components, see Components needed for Over the Top deployments.	
Obtain the required licenses.	Determine which licenses are appropriate for your enterprise. Suite licenses include all the required licenses. The licenses you need vary depending on the functionality that you plan to use.	For more information about license options, see Licensing requirements.	
Prepare the site.	Understand the following: • Network considerations and diagnostics for Avaya Workplace Client • Supported codecs and DSCP configuration • Wi-Fi best practices Configure the Wi-Fi infrastructure and learn about changes in the device functionality based on access point changes.	For more information, see the following topics in the chapter on Site preparation: • Network considerations and diagnostics • Supported codecs • DSCP values • Configuring DSCP values on the network • Wi-Fi best practices	
Understand the security and certificate requirements.	Understand the following: • Security requirements	For more information, see the following topics in the chapter on Security and certificate configuration:	

Task	Description	Reference	✔
	for Avaya Workplace Client • Password storage encryption methods • Security recommendations for desktop and mobile platforms • Client identity and server certificates • Guidelines to determine whether you need certificates • Procedures for obtaining Avaya product certificates • Guidelines and implications to support antivirus and malware scanning software • Supported cipher suites and limitations of blacklisting cipher suites	• Security requirements • Password storage • Desktop platform security recommendations • Mobile device security recommendations • Client identity certificates • Server certificates • Guidelines to determine whether you need certificates • Obtaining the Avaya SIP Product CA certificate • Obtaining the Avaya Aura System Manager CA certificate • Antivirus and malware scanning support • Supported cipher suites	

Task	Description	Reference	✔
		- Limitations of blacklisting cipher suites	
Set up and configure Avaya Workplace Client functionality.	Determine which Avaya Workplace Client functionality is appropriate for your enterprise. Configure the functionality according to your requirement. Review the chapter, which includes the configuration information for Avaya Workplace Client settings in an OTT deployment.	For more information, see Configuration for Over the Top deployments.	
Set up and configure Avaya Equinox® Conferencing functionality.	Determine which Avaya Equinox® Conferencing functionality is appropriate for your enterprise. Configure the functionality according to your requirement. Review the checklist, which outlines the high-level setup and configuration tasks for Avaya Equinox® Conferencing functionality.	For more information, see Checklist for configuring Avaya Equinox Conferencing functionality.	
Set up and configure remote worker functionality.	The remote worker functionality enables users that are not connected to the enterprise network to access Avaya Workplace Client. Determine which remote worker functionality is appropriate for your enterprise. Configure the	For more information, see Remote worker configuration worksheet.	

Task	Description	Reference	✔
	functionality according to your requirement. Use the worksheet to determine how to provide the remote workers with access to available functionality.		
Install the client.	If you use the command line and silent installation options on desktop platforms, then end users do not need to install Avaya Workplace Client manually. If the enterprise is using a Mobile Device Management (MDM) system with the mobile devices enrolled in it, you can push the application installation to the Android and iOS devices. MDM is a deployment of a combination of on-device applications and configurations, corporate policies and certificates, and backend infrastructure. Use MDM to simplify and enhance the IT management of end user devices.	For additional setup options on desktop platforms, see the chapter on Additional setup options for Avaya Workplace Client for Windows and Mac platforms.	

Configuration options

Avaya Workplace Client is a SIP-based solution that requires setup and preconfiguration. You must set up your network infrastructure, deploy certificates, and complete required security configuration before users can install and use Avaya Workplace Client. You must perform additional configuration so that users can access:

- Functionality in the Avaya Workplace Client UI.

- Advanced functionality that is not visible in the UI, including MDA, dual registration, Session Manager failover, and remote access.

Integration options

You can integrate Avaya Workplace Client with other components. This might change the UI functionality that is available and the type of configuration you must perform on Avaya Workplace Client. The user needs to log in to these components on Avaya Workplace Client to access the functionality. The following table lists the components with which Avaya Workplace Client can integrate:

Component	Description	Configuration information
Avaya Multimedia Messaging and Avaya Spaces	You require Avaya Multimedia Messaging or Avaya Spaces for IM on Avaya Workplace Client. Avaya Multimedia Messaging and Avaya Spaces also provide additional functionality, such as the capability to: • Attach files. • Capture photo, audio, and video on Avaya Workplace Client.	For information about deploying and administering Avaya Multimedia Messaging, see *Deploying Avaya Multimedia Messaging*.
Client Enablement Services	Client Enablement Services is supported on Avaya Workplace Client for Android and iOS. It provides additional UI functionality. **Important:** Existing customers can continue to use Client Enablement Services. New customers can use almost all Avaya Workplace Client functionality without Client Enablement Services. **Note:** Avaya Workplace Client on Avaya Vantage™ does not support Client Enablement Services.	For information about deploying and administering Client Enablement Services, see: • *Implementing Avaya one-X® Client Enablement Services* • *Administering Avaya one-X® Client Enablement Services*

Component	Description	Configuration information
Avaya Aura® Device Services	For users with multiple devices or endpoints, Avaya Aura® Device Services provides a common user experience.	For information about deploying and administering Avaya Aura® Device Services, see: - *Deploying Avaya Aura® Device Services* - *Administering Avaya Aura® Device Services*

Interface functionality configuration

The following table provides configuration information about the Avaya Workplace Client UI functionality. Choose the UI functionality that you need for your enterprise.

Functionality	Description	Configuration notes
Audio and video telephony	Avaya Workplace Client supports audio and video calls. Secure Real-Time Transport Protocol (SRTP) supports both audio and video with Avaya Aura® dependencies. **Note:** Avaya Workplace Client does not support audio or video with Polycom SRTP devices.	- Ensure that your network meets the required audio and video quality of service (QoS) requirements. - Configure the required Avaya Aura® Communication Manager and Avaya Aura® Session Manager parameters. - Obtain video licenses.
EC500	EC500 is a Communication Manager feature with which you can: - Join and answer calls from your mobile device.	Complete the required configuration in Avaya Aura® Communication Manager, including setting up feature name extensions (FNEs). You must also enable the Extend Call feature in Avaya Aura® Session Manager to use EC500 call suppression.

Functionality	Description	Configuration notes
	- Send calls to your mobile device. EC500 call suppression When EC500 call suppression is configured, users of dual-mode client applications, such as Avaya Workplace Client, receive only a single incoming call on their mobile device. The incoming call could be either VoIP or cellular. EC500 FNE auto-dialer When EC500 FNE auto-dialer is configured, you can access the following capabilities: - Make outgoing calls through Avaya Aura® Communication Manager. - Access simultaneous ringing on your deskphone and mobile device. - Join active calls. - Send all calls to your voice mail. - Extend calls. - Forward calls. - Enable or disable EC500 on the UI as needed. - Access EC500 station security codes.	The user must configure the Extend Call button for EC500 call suppression to work properly.
Conferencing and desktop sharing	Avaya Equinox® Conferencing supports conference calls and desktop sharing.	- Install and configure Avaya Equinox® Conferencing.

Functionality	Description	Configuration notes
		- Obtain the required Avaya Equinox® Conferencing licenses.
Contact management and enterprise search	You can manage local contacts, Avaya Aura® contacts, and Client Enablement Services contacts with Avaya Workplace Client. You can also perform searches for enterprise users that are not on your local contact list. **Note:** Client Enablement Services is only supported on mobile platforms. If Avaya Spaces is configured, you can search for enterprise contacts from the Avaya Spaces directory if Avaya Aura® Device Services is disabled.	- Configure LDAP for enterprise search on desktop platforms. Ensure that you are using a supported LDAP directory. **Note:** Mobile clients do not support direct LDAP search. - For remote workers, you must also configure LDAP on SBCE. - Configure Client Enablement Services for enterprise search on mobile platforms. - Configure Avaya Spaces for enterprise search.
Presence and instant messaging (IM)	With Avaya Workplace Client, you can view the presence status of other users and change your own presence status. You can additionally set your status message. You require Avaya Multimedia Messaging or Avaya Spaces Direct Messaging for IM on Avaya Workplace Client.	- Install and configure Avaya Aura® Presence Services. You must also configure Avaya Aura® Session Manager to support Avaya Aura® Presence Services. - Install and configure Avaya Multimedia Messaging. - Obtain the required licenses. To access certain Avaya

Functionality	Description	Configuration notes
		Multimedia Messaging capabilities, users require enhanced Avaya Multimedia Messaging licenses.

Advanced functionality configuration

The following table provides information about advanced functionality that is not configurable in the Avaya Workplace Client UI. Choose the advanced configuration options that you need for your enterprise.

Functionality	Description	Configuration notes
Enable dual registration.	To log in and join calls with an H.323 device and your SIP-based Avaya Workplace Client at the same time. In many enterprises, deskphones use H.323 signaling. However, Avaya does not recommend the use of H.323 and dual-registration is supported as is.	Enable dual registration by using the non-SIP user communication profile in Avaya Aura® System Manager. For more information about configuring the **Allow H.323 and SIP Endpoint Dual Registration** field, see *Administering Avaya Aura® System Manager*. Alternatively, you can configure additional fields in Avaya Aura® Communication Manager. For more information, see *Administering Avaya Aura® Communication Manager*.
Enable Multiple Device Access (MDA).	To log in, join, and answer calls with multiple SIP devices at the same time.	Configure additional fields in Avaya Aura® System Manager.
Enable Bridge Line Appearance (BLA)	To make, answer, and bridge onto calls to or from the telephone number of another user.	Configure additional fields in Avaya Aura® Communication Manager. For more information, see *Avaya Aura® Communication Manager*

Functionality	Description	Configuration notes
		Feature Description and Implementation.
Enable survivability or Avaya Aura® Session Manager failover.	To continue to use Avaya Workplace Client if the primary Session Manager fails.	• You must have a primary and secondary Session Manager server. • Ensure each Session Manager server is configured in Avaya Aura® System Manager.
Set up remote workers.	To use Avaya Workplace Client from home or from a location outside the enterprise network. Avaya Workplace Client uses SBCE for remote worker functionality.	• Install and configure SBCE. You might also need to complete additional configuration on other components for remote workers to access all Avaya Workplace Client functionality. • Provision DNS entries for Avaya Aura® Session Manager, Presence Services, and the LDAP enterprise search server. • Resolve to the internal service IP address for internal DNS clients. • Resolve to the external service SBCE IP address for external DNS clients.

Functionality	Description	Configuration notes
Set up automatic configuration.	To automatically populate the Avaya Workplace Client settings. After installing Avaya Workplace Client, users must select whether to automatically configure settings by using a web address or an email address. You must provide this information to users before installation. If automatic configuration is not enabled, users must configure their client settings manually.	Set up the following: • Settings file. The parameters you must add to the settings file depend on the functionality you have configured. • DNS server. Alternatively, you can configure Avaya Aura® Device Services as the source of the settings file. **Note:** By default, Avaya Workplace Client sends anonymous usage information to the Google Analytics service. Use the ANALYTICSENABLED configuration parameter in the settings file to change the parameter value if required.
Configure Avaya Workplace Client for Windows to work in a Citrix, XenApp, or VMWare environment.	To access and use Avaya Workplace Client for Windows in a Citrix, XenApp, or VMWare environment. This is an optional feature. This option is not supported with Avaya Workplace Client on other platforms.	Set up this option using a command line.

Functionality	Description	Configuration notes
	In a Citrix environment, Avaya Workplace Client for Windows works in the Desk Phone mode.	

Avaya Workplace Client for Android on Google Chromebook

Avaya Workplace Client for Android on Google Chromebook

With a laptop form factor, low power consumption, and a low-price target, Chromebooks were initially aimed to be multimedia devices focused on web browsing. With the introduction of Chrome OS version M53, you can now access the whole Android applications catalog from the Google Play Store on Chromebooks.

Chromebooks have started becoming productivity devices. As Avaya Workplace Client for Android was designed with mobiles in mind, the Workplace experience on Chromebook was reviewed and enhanced in the following areas:

- Window mode support was added for Chromebooks: Workplace used to be a full-window mode application only. With this enhancement, you can now use the application in a free-form window, with all the facilities a desktop user would expect, such as minimizing, maximizing, and resizing.
- Incoming call notifications experience was enhanced for Chrome OS.
- Keyboard support was enhanced.

Recommendations for using Avaya Workplace Client on Google Chromebook as a media client

If you are using Avaya Workplace Client on Google Chromebook as a media client for Avaya Workspaces for Call Center Elite, Avaya Oceana®, or other CTI control scenarios, Avaya recommends the following based on recent testing:

- If you are using multiple applications on your Chromebook with Avaya Workplace Client, low-end Chromebooks based on AMD A4/A6 or Intel Celeron CPUs can have issues providing a high-quality voice experience when multi-tasking. Hence, Avaya does not recommend these for agent use.

- Chromebooks with an Intel Core i5 CPU provide a good quality voice with no drop-outs when running multiple applications and multi-tasking. Enterprise-class Chromebooks have an Intel Core i5 or i7 CPU. Avaya does not recommend specific brands or models of devices.
- Validate the complete specific set of applications that agents use before bulk purchasing Chromebooks. You must validate to ensure that the Chromebook model provides the desired voice quality experience.

Installing Avaya Workplace Client for Android on Google Chromebook

About this task

Use this procedure to perform centralized management of Avaya Workplace Client for Android on Google Chromebook. You can add Avaya Workplace Client to your Chrome OS devices. You can then provision the automatic configuration URL for your environment. This is the URL to the Avaya Aura® Device Services configuration or a 46xx settings file.

Procedure

1. Log in to http://admin.google.com with your administrator credentials.
2. Click **Devices** > **Mobile & endpoints** > **Chrome devices** > **Apps & extensions**.
3. Click +, and click **Add from Google Play**.
4. Search for `Avaya Workplace`, and click the application.
5. Click **Force install + pin**.
   Read the Google guidance on force installing applications. Ensure that you grant the required permissions to the application to suppress permission prompts for end-users.
6. In **Managed configuration**, enter the automatic configuration URL for your environment.
   The following URL is an example:

   ```
   {
           "AUTO_CONFIG_URL": "https://aads.example.com/acs/resources/configurations"
   }
   ```

   Ensure that the JSON configuration is correct.
7. Test by logging into Google Chromebook with a managed user account.
   After a short time, Avaya Workplace Client automatically installs and gets pinned to the ChromeOS Shelf.
8. Open Avaya Workplace Client, and accept the end-user license agreement.
9. To start using Avaya Workplace Client, enter your application credentials.

Limitations with Avaya Workplace Client for Android on Google Chromebook

These are the limitations:

- Double-clicking in Avaya Workplace Client on Google Chromebook does not produce the same result as double-clicking in Avaya Workplace Client on an Android mobile device. Hence, single click in all tabs of the client on Google Chromebook instead of double-clicking.
- You cannot toggle between different audio devices while using Avaya Workplace Client on Google Chromebook. Only one audio device is available on the user interface. However, you can change the audio device selection from the Chrome OS settings.
- Video call resolution is 180 pixels on Google Chromebook. Hence, video call performance on Google Chromebook with dual-core AMD processors is poor. Avaya Workplace Client functions slowly, and the video stutters.
- You cannot make or receive VoIP calls on Google Chromebook when you are connected to an internal network on IPv4. To make or receive VoIP calls, you must connect through VPN or Avaya Session Border Controller, or an internal network on IPv6.

Planning tools and utilities

Tool or Utility	Description
Avaya PLDS	Register for Avaya Product Licensing and Delivery System (PLDS) to obtain Avaya software and licenses. You can register for Avaya PLDS at http://plds.avaya.com/.

Tool or Utility	Description
Avaya Aura® server	Deploy planning components, such as Avaya Aura® solution components, on a physical or virtualized server.

Licensing requirements

Licensing requirements

Suite user licenses include all the required licenses. You need licenses depending on the functionality and services that you want to access through Avaya Workplace Client.

- EC500 features require EC500 licenses. This is included in Core and Power Suite.
- VoIP features require Mobile SIP licenses. This is included in Core and Power Suite.
- Avaya Multimedia Messaging features require Avaya Multimedia Messaging licenses.
- All video communications, including point-to-point video and video conferencing, require Communication Manager licenses. For only video conferencing, you need Avaya Equinox® Conferencing licenses. Point-to-point video is included in Core and Power Suite. For UC and conferencing deployments, you need Avaya UC licenses.
- Callback Service feature requires Communication Manager licenses. The licenses are included in Core and Power Suite. On Communication Manager, the Callback Service feature is known as Enterprise Mobility Experience (EMX).
- Client Enablement Services features require Client Enablement Services licenses. This is included in Core and Power Suite.
- Presence features require Presence Services licenses. This is included in Core and Power Suite.
- Remote worker features require Session Border Controller licenses. If Client Enablement Services is also required, you need Session Border Controller and Client Enablement Services licenses.
- Avaya Spaces features require Avaya Spaces licenses. License types include Essential, Business, and Power.
- Avaya Workplace VDI features require Avaya Workplace VDI licenses. For each Avaya Workplace VDI client, you need a separate license.

Contact Center agent feature licensing

The Avaya Contact Center Elite Agent features in Avaya Workplace Client for Windows are available with a feature license that is not included with the Core or Power Suite license or subscription. You must load the feature license in WebLM for the total concurrent quantity of agents that are going to use the feature. Avaya Workplace Client consumes these licenses from WebLM when you enable the feature.

- For customers using subscription licensing, the agent feature is included in the Basic Voice Agent subscription bundle.
- For customers using perpetual licensing, order codes are available in Avaya One Source for agent features on Avaya Workplace Client for Windows to support new license orders. In addition, you can use existing advanced licenses for Avaya one-X® Agent or Avaya Agent for Desktop to acquire the Avaya Workplace Client for Windows agent feature license at no cost.

If you are using Avaya Workplace Client for Windows in the Desk Phone mode, Avaya Workplace Client does not acquire a WebLM license. If you want Avaya Workplace Client for Windows on the virtual desktop to control Avaya Agent for Desktop on the end-user device, you need the Avaya Agent for Desktop license.

WebLM requirements

Supported release	WebLM 6.3.4 or later. Both the WebLM standard installation, that is .bin, or the Web Virtualization Enablement (VE) vAppliance, that is .ova, are supported. **Note:** Avaya Aura® System Manager also has a built-in WebLM instance. This WebLM instance is not supported when Avaya Agent for Desktop is deployed in a production environment.
Number of Avaya Agent for Desktop instances supported by a single WebLM server (standard or virtual)	10,000

Best practices

Avaya recommends that you implement the following tasks so that Avaya Workplace Client users have the best end-user experience:

Task	Notes
Use SIP instead of H.323 for all the user devices.	Avaya Workplace Client is a SIP client. Avaya recommends the use of SIP so that users can use the advanced functionality that Avaya Workplace Client provides. If H.323 is needed, users can perform dual-registration using a SIP endpoint. However, Avaya does not recommend the use of H.323 and dual-registration is supported as is.
Enable Multiple Device Access (MDA).	Deskphones and multiple clients can log in simultaneously. For more information about MDA configuration, see Avaya Workplace Client settings in Avaya Aura Session Manager.
Use TLS for all connections.	Avaya recommends the use of TLS to provide security for all network connections. For example, TLS is a must for presence, MDA, and Desk Phone mode. **Note:** If you are using the OAuth server for automatic configuration of Avaya Workplace Client, ensure that TLS 1.3 is enabled on Avaya Aura® Session Border Controller.
Configure settings for privacy and security.	If you configure the Exclusion feature on Communication Manager, users can maintain privacy of conversations and ensure that unwanted parties cannot join the call. In the Manual Exclusion mode, the user presses the Exclusion button to activate and deactivate Exclusion. For more information, see *Using Avaya Workplace Client for Android, iOS, Mac, and Windows*

Task	Notes
	Automatic exclusion is a feature with which a user of a SIP or H.323 endpoint can prevent others with MDA of the same extension from bridging onto an existing call. For more information, see Avaya Workplace Client settings in Avaya Aura Communication Manager. You can also enable the barge-in tone for a user extension on Communication Manager to warn users if someone else joins the call.
Enable automatic discovery of the automatic configuration URL using: • DNS-based discovery of the settings file for all platforms • Avaya accounts-based method • A parameter during installation for Mac or Windows if using an automated software distribution system and silent install	For more information, see the chapters on Automatic configuration and Additional setup options for Avaya Workplace Client for Windows and Mac platforms.
Use split-horizon DNS FQDN addresses.	Purpose is to send the Workplace traffic to the SBC when remote for security purposes, but not through the SBC when inside the enterprise network for performance and scaling purposes. For more information, see Solution architecture, Remote worker and cloud access configuration, and Remote worker configuration worksheet.
Use split-tunneling configuration when a VPN is in use.	Purpose is to send the Workplace traffic to the SBC when remote, even if the user is logged into VPN for other data security purposes. It is to keep the Workplace traffic outside the VPN to improve the network quality and the networking experience.
Use private trust store and automatic configuration to distribute certificates.	Useful if using certificates that are not issued by a CA with a certificate already in the device OS. For more information, see Certificate distribution.

Task	Notes
Use Avaya Aura® Device Services to provide single credential sign-in.	Useful as it removes the need for the user to enter phone credentials. For more information, see Avaya Aura Device Services parameters
Use enterprise credentials for authentication.	Based on your environment, you can use Avaya Authorization Service or unified login or Integrated Windows Authentication (IWA). Avaya Authorization Service is an authorization mechanism that enables users to authenticate using a combination of enterprise credentials and other factors that the enterprise has chosen, including enterprise Single Sign-On (SSO) and multi-factor authentication. Unified login is a feature with which users can use the same set of credentials for accessing two or more services in Avaya Workplace Client. You can use unified login with your enterprise credentials from Active Directory or LDAP. Avaya recommends the use of unified login for all services to avoid potential issues with credentials management. **Note:** If a server tends to report false failures for password authentication, Avaya recommends that you do not configure that server with Unified Login. You can then easily differentiate between these types of failures from Unified Login failures. For more information, see Unified Login parameters. If you want to remove the authentication step for the client, use Integrated Windows Authentication (IWA).
On mobile platforms, only configure the telephony methods that you require.	Useful as it simplifies the configuration as much as possible.
Use E.164 dial plans.	Avaya recommends the use of E.164 dial plans for new deployments.

Task	Notes
	For more information about Avaya Workplace Client dial plans, see *Avaya Workplace Client Overview and Specification for Android, iOS, Mac, and Windows*.

Considerations while disabling a service when using Unified Login

- If you plan to decommission a service, you must update the Avaya Workplace Client configuration using Avaya Aura® Device Services or 46xx settings file before decommissioning the service.
- If a service remains accessible, Avaya Workplace Client attempts to access the service.
- If a service, for example, Conferencing, is partially up, the Conference service returns a 401 unauthenticated response to the Avaya Workplace Client login query. Avaya Workplace Client treats this response as an invalid or bad password and does not connect to any service associated with the Unified Login credentials. This functionality is designed intentionally to ensure that the account does not get locked out.
- If the Conferencing Login API is shut down explicitly or if a server is shut down completely, Avaya Workplace Client receives a different response code. Avaya Workplace Client does not treat this response as a login or password issue for Unified Login services.
- If the Conferencing credentials are unique, that is, not part of Unified Login, a login failure does not affect other services.

To ensure that Avaya Workplace Client uses the latest configuration, you can configure

```
SET SETTINGS_CHECK_POLICY
        1
```

.

VMWare Workspace ONE

VMWare Workspace ONE is a Mobile Device Management (MDM) tool that interacts with Android, iOS, and Windows systems to deploy and manage OS features and individual applications. You can use VMWare Workspace ONE to automatically deploy and manage Avaya Workplace Client for iOS 3.34 into the user’s devices.

For more information on VMWare Workspace ONE, see https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/index.html.

Use the VMWare Workspace ONE administration portal to support the following functionalities:

- Configure passcodes and biometric
- Perform application configuration
- Disable copy and paste
- Use VMWare Workspace ONE Per App VPN

Configuring passcode and biometric

About this task

Use this procedure to configure the usage of passcode for authentication and to enable the biometric mode. Avaya Workplace Client for iOS then displays the VMWare Workspace ONE dialog. Users can enter their VMWare Workspace ONE credentials on their devices. On successful authentication by VMWare Workspace ONE, users can access Avaya Workplace Client.

Procedure

1. Log in to the VMWare Workspace ONE administration portal.
2. Go to **Apps & Books** > **All Apps & Books Settings** > **Settings and Policies** > **Profiles** > **[your profile name]** > **Authentication**.
3. Configure the following fields:
    - **Authentication Type**: Click **Passcode**.
    - **Biometric Mode**: Click **Enabled**.
4. Save the changes.

Performing application configuration

About this task

Use this procedure to configure one or more Avaya Workplace Client for iOS supported parameters in VMWare Workspace ONE.

- If you configure all the parameters, users are automatically logged in to Avaya Workplace Client for iOS.

- If you do not configure all the parameters, Avaya Workplace Client for iOS automatically populates the appropriate fields but does not trigger the login process.

Procedure

1. Log in to the VMWare Workspace ONE administration portal.
2. Go to **Apps & Books** > **Applications** > **Native** > **Public** > **[radio option next to your app name]** > **Assign** > **[your assignment name]** > **Application Configuration**.
3. Enable **SendAppConfiguration not globalized**.
4. In the Configuration Key column, configure the following parameter names:
   - MDM_TYPE
   - AUTO_CONFIG_URL
   - ENTERPRISE_LOGIN
   - ENTERPRISE_PASSWORD
   - ENTERPRISE_USER_NAME
5. Configure the following values for the parameters:
   - MDM_TYPE: `airwatch`
   - AUTO_CONFIG_URL: URL to access Avaya Aura® Device Services automatic configuration
   - ENTERPRISE_LOGIN: Valid user name for Avaya Aura® Device Services authentication
   - ENTERPRISE_PASSWORD: Valid password for Avaya Aura® Device Services authentication
   - ENTERPRISE_USER_NAME: Valid email address to find the Avaya Aura® Device Services URL by using the DNS server
6. In the Value Type column, click “String”.
7. Save the changes.

Disabling copy and paste

About this task

Use this procedure to prevent the user from copying or pasting anything from and to Avaya Workplace Client for iOS.

After disabling copy and paste, if a user tries to copy and paste, Avaya Workplace Client for iOS displays the following error message: `Your admin has disallowed pasting from unmanaged sources`.

Note:

A user can copy and paste from one application to another if both applications are installed through the Mobile Device Management (MDM) tool.

Procedure

1. Log in to the VMWare Workspace ONE administration portal.
2. Go to **Apps & Books** > **All Apps & Books Settings** > **Settings and Policies** > **Profiles** > **[your profile name]> Restrictions**.
3. Select the **Enable Data Loss Prevention** check box.
4. Clear the **Enable Copy and Paste Out** and **Enable Copy and Paste Into** check boxes.
5. Save the changes.

Using VMWare Workspace ONE Per App VPN

About this task

VMWare Workspace ONE Per App VPN enables devices to establish a Virtual Private Network (VPN) connection when specific managed apps are launched. A VPN ensures that all data is transmitted through the secured tunnel and strictly requires authentication or a special certificate to establish connectivity.

You can select the application for which the VPN is set up.The Mobile Device Management (MDM) system pushes a per-app VPN configuration to the Avaya Workplace Client for iOS. The MDM system then installs a managed application on the device and configures the application to use the VPN.

You can configure Avaya Workplace Client for iOS to use the VPN of VMWare Workspace ONE.

Procedure

1. Log in to the VMWare Workspace ONE administration portal.
2. Go to **Devices** > **Profiles & Resources** > **Profiles**.
3. Configure the Per App VPN Profile.
4. Save the changes.
5. Go to **Apps & Books** > **Applications** > **Native** > **Public** > **[radio option next to your app name]** > **Assign** > **[your assignment name]** > **Tunnel & Other Attributes** > **Per App VPN Profile**.
6. Configure Avaya Workplace Client for iOS to use the Per App VPN Profile.
7. Save the changes.

Site preparation

This chapter includes information on the:

- Network considerations and diagnostics for Avaya Workplace Client
- Supported codecs and DSCP configuration
- Wi-Fi best practices
  Configure the Wi-Fi infrastructure and learn about changes in the device functionality based on access point changes.

Network considerations and diagnostics

Network diagnostics

Media quality on a consumer device is affected by many factors. For example, by the network in which the device is deployed and the Avaya Aura® system configuration deployed. The way in which the device is connected to the wireless network also has an impact.

The Avaya Workplace Client video encoders adjust to fit within the bandwidth envelope that the network provides. However, the available bandwidth affects the resulting video quality. With increased bandwidth, the video quality improves.

You can view the audio and video statistics for the current call session and use them to determine the network conditions affecting the session.

Network transition

You cannot transition from a non-corporate network to a corporate network and vice-versa. Example of non-corporate network include external Wi-Fi, home Wi-Fi, LTE, and WWAN. Such transition requires addition or removal of Avaya Session Border Controller from signaling path, which is not supported by current signaling.

Packet loss

Packet loss characteristics affect 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. As you approach 1% packet loss, you might see visual artifacts, such as broken images, or hear audible artifacts. As you approach 2 to 3% packet loss, you might encounter consistent visual and audible artifacts.

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 delays. 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. Network and network engineering issues can influence this statistic.

Avaya Aura® configuration

The Avaya Aura® solution enables you 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.

Note:

Ensure that Avaya Workplace Client is not connected to Session Manager through Network Address Translation (NAT). This often causes connection problems with SIP signaling. The client is connected, but does not operate correctly. To address problems with NAT, you can use a VPN client or SBCE for remote endpoint deployments.

Virtual Private Networks

Virtual private networks (VPN) provide a significant challenge to high-quality video because, as a security measure, the VPN assigns video packets the same priority as 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. This can be problematic for media packets that depend on timely receipt of all video packets.

Troubleshooting logs

When troubleshooting issues, it might become necessary to report logs to your support organization. Logging for Avaya Workplace Client includes media quality statistics that record information about network performance. These logs can assist support teams in diagnosing media issues due to network performance.

To enable these logs, users must set **Enable Diagnostics** in the Settings dialog box.

Supported codecs

For information about bandwidth requirements for different codecs, see “Codec Selection” in *Avaya IP Voice Quality Network Requirements*.

Audio codecs

Codec	Supported on Avaya Workplace Client on mobile platforms	Supported on Avaya Workplace Client on desktop platforms
Opus narrowband and wideband	Yes	Yes

Codec	Supported on Avaya Workplace Client on mobile platforms	Supported on Avaya Workplace Client on desktop platforms
G.722	Yes	Yes
G.711 A-law (PCM-A)	Yes	Yes
G.711 U-law (PCM-U)	Yes	Yes
G.726	Yes	Yes
G.729A	Yes	Yes
G.729B (G.729A with annex B silence suppression)	Yes	Yes

Video codecs

Avaya Workplace Client on desktop platforms support H.264 Advanced Video Coding (AVC) and H.264 Scalable Video Coding (SVC). Avaya Workplace Client on mobile platforms support basic H.264 and H.264 AVC.

If Avaya Equinox® Conferencing is used by OTT guest and signed users on mobile and desktop platforms, H.264 SVC is supported.

Guidance on using QoS and DSCP

Avaya Workplace Client for Windows supports two methods to set Differentiated Service Code Point (DSCP) markings on data packets created by the application for the voice traffic. Network equipment uses these markings in managed, private networks to prioritize traffic.

Method 1 – MS QWAVE APIs – This is on by default

In this method, you can set a policy using Windows Group Policy to mark packets based on the application name, protocol type, and port range. For recommendations, see DSCP values.

When using MS QWAVE to set the policy for audio traffic, you can mark the UDP traffic from the Avaya IX Workplace.exe process with the range of ports configured for your system to a DSCP value of 46.

Microsoft has a set of APIs that allow applications to set packet markings directly without the use of Group Policy administration, but these APIs require the application to be running as part of the Administrators group. This is typically not feasible and not required when you use Group Policy. Avaya does not expect or require users to run Avaya Workplace Client as an administrator.

Method 2 – Avaya QoS Service

In this method, instead of relying on the MS QWAVE and Group Policy to mark traffic, Avaya Workplace Client works in conjunction with an installed QoS Service to mark packets. One benefit of this approach is that audio and video traffic can be marked with different values to prioritize audio and video traffic independently on the network.

Using this solution, the Avaya Aura® administrator can also manage QoS DSCP markings across the Avaya solution centrally for multiple Avaya devices and applications. For more information about configuring DSCP values, see Configuring DSCP values on the network.

To use the Avaya QoS Service, you must perform the installation when installing Avaya Workplace Client using an install time parameter. For more information about enabling the DSCP driver, see Avaya Workplace Client for Windows command line and silent installation options.

Summary

Here is a summary of some of the key considerations for choosing between these options:

	MS QWAVE & Group Policy	**Avaya QoS Service**	**Comments**
Mark audio and video packets separately	No	Yes	
Central Management with Avaya Aura® System Manager	No	Yes	
Requires additional network driver installed and running	No	Yes	
Works with non-domain-managed PCs such as BYOD, personally-owned PCs	No	Yes	

	MS QWAVE & Group Policy	Avaya QoS Service	Comments
User must run Avaya Workplace Client with administrator rights	No	No	Packets are marked by a separate service from the user application process.

DSCP values

Differentiated Services Code Point (DSCP) is a field in an IP packet that you can use to assign different levels of service to network traffic.

You can set the DSCP values in the settings file. If the DSCP settings are available in the settings file, Avaya Workplace Client stores the same value in the configdata.xml file.

- For Avaya Aura® deployments, the PPM value overrides the value in the settings file. Hence, Avaya Workplace Client uses the following PPM default values: DSCPSIG:46, DSCPAUD:46, and DSCUPVID:34.
- For non-Avaya Aura® deployments, Avaya Workplace Client uses the values from the settings file.

If you do not set the DSCP values in the settings file, Avaya Workplace Client uses the following default values: DSCPSIG:24, DSCPAUD:46, and DSCUPVID:34.

By default, the Avaya QoS service, that is, DSCP driver, is not installed. If you do not install the Avaya QoS service using the silent install parameter, the Microsoft QWAVE API is used.

To set the DSCP value, follow the instructions on Microsoft QoS policy. For example, for Windows Server 2016, see https://docs.microsoft.com/en-us/windows-server/administration/server-manager/install-or-uninstall-roles-role-services-or-features.

Attributes	Audio policy	Video policy	Signaling policy
Application name	Avaya IX Workplace.exe	Avaya IX Workplace.exe	Avaya IX Workplace.exe
Protocol	UDP	UDP	TCP

Attributes	Audio policy	Video policy	Signaling policy
Port number or range	Corresponding port number or range from the SIP profile on Avaya Aura® Communication Manager.	Corresponding port number or range from the SIP profile on Avaya Aura® Communication Manager.	• 5060 for SIP • 5061 for secure SIP **Note:** Do not use TCP port number 5060 on Avaya Workplace Client for Android as the client displays a configuration error.
DSCP value (recommended defaults)	46	34	24

If the customer wants to use the Avaya Aura® settings or set audio and video separately, then you must install the DSCP driver using the silent install parameter. This method precedes the Microsoft APIs, which limits to setting audio and video with the same value.

The DSCP configuration on System Manager is done in the Device Settings Groups section.

Configuring DSCP values on the network

About this task

To set DSCP values on the network, you must identify the different streams from Avaya Workplace Client:

- Media streams: When using the Avaya QoS service, you can assign different DSCP values to audio and video streams.
  For example, audio media streams marked as Expedited Forwarding (EF), that is, DSCP 46 and video media streams marked as Class 4 Assured Forwarding (AF41), that is, DSCP 34.
- Signaling streams: You can mark signaling traffic between the client and servers.
  For example, signaling packets as Class Selector 3 (CS3), that is, DSCP 24.

The DSCP values mentioned here are recommended defaults. You can set different DSCP values as required.

Before you begin

- Install all planning components.
- Configure Avaya Aura® System Manager.

Procedure

1. Log in to Avaya Aura® System Manager.
2. Click **Elements** > **Session Manager**.
3. In the navigation pane, click **Device and Location Configuration** > **Device Settings Groups**.
4. On the Device Settings Groups page:
    a. Choose the appropriate group.
       The group might be a default group, a terminal group, or a location group.
    b. Click **Edit**.
    c. Click the right-arrow for **DIFFSERV/QOS Parameters**.
    d. Configure the PHB values.
    e. Click **Save**.
5. In the navigation pane, click **Device and Location Configuration** > **Location Settings**.
6. On the Location Settings page, for each location, choose the device settings group that you modified in the **Device Setting Group** field.
7. Click **Save**.

Wi-Fi best practices

While calculating the bandwidth that you require for your enterprise connection, consider the codec to use in each call scenario based on your deployment configuration. When you use Avaya Workplace Client as a VoIP client on a Wi-Fi network, various factors ensure best performance, security, and reliability.

Before operational deployment, test Avaya Workplace Client 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 Avaya Workplace Client can vary.

To ensure that Avaya Workplace Client calls are preserved while moving from WLAN to 4G/LTE data, use the Session Border Controller address on mobile platforms for Session Manager address. Do not use split-horizon DNS.

Configuring the Wi-Fi infrastructure

About this task

Use this procedure to learn and set up the guidelines about the parameters of the Wi-Fi network and supporting infrastructure, which you can use to optimize performance and security.

Procedure

- 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:
  1. Establish a VLAN for traffic use on your new Service Set Identifier (SSID).
  2. Configure the new VLAN with dedicated bandwidth control on Session Manager.
  3. Configure the switch or router so that all inbound traffic to the new SSID gets higher traffic priority.

  Note:

  This feature might be unavailable on some Wi-Fi switches or routers.
- Disable hidden networks.

  Hidden networks do not broadcast the SSID. Your device might not be able to easily detect the hidden network, resulting in increased connection time and reduced reliability of automatic connections.
- If you experience delays or packet loss, disable TSPEC.

  TSPEC is an 802.11 Traffic Specification configuration. Certain devices might be adversely affected when TSPEC is enabled on the wireless network.
- Set your security mode as follows:
  1. Set security to the WPA2 mode, known as AES.

     AES is the strongest form of security that Wi-Fi products offer.
  2. When you enable WPA2, choose a strong password based on your enterprise guidelines.

- If your device does not support WPA2, choose one of the following:
    - WPA/WPA2 mode, known as the WPA mixed mode. In the WPA mixed mode, new devices use the stronger WPA2 AES encryption, while older devices connect to the old WPA TKIP-level encryption.
    - WPA TKIP mode if your Wi-Fi router does not support the WPA/WPA2 mode.
- Disable 40 MHz in the 2.4 GHz settings on the Wi-Fi router to reduce interference issues.
- Disable lower speeds, such as, 1, 2, and 5.5 Mbps, and do the following:
    1. Change 6 Mbps to `Mandatory` and the beacon rate to 6 Mbps.
    2. Set multicast to `Automatic`.
    3. Set all other rates to `Supported`. This setting might be unavailable on a home Wi-Fi router.

Access point changes

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 the user is on a call.

Areas with weak signals cause voice quality issues and, at times, dropped calls. A signal strength and bandwidth that support degraded data transmission might cause VoIP calls to drop or be of poor quality.

Do a proper site survey and ensure that the concentration of APs in high traffic areas is sufficient for the expected number of calls made from devices in these areas. A Wi-Fi network that works for dedicated handsets does not imply that the Wi-Fi network is suitable for VoIP phones or other smart phones.

Many combinations of subnetworks and SSIDs require manual intervention. 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 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

Condition	1	2	3	4	5
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, applies to a new SSID that was previously not associated.	No	Yes, applies to a new SSID that was previously not associated.	No
Renew the DHCP	No	No	Yes	No	No

Note:

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

Security and certificate configuration

This chapter includes information about the following:

- Security requirements for Avaya Workplace Client
- Password storage encryption methods
- Security recommendations for desktop and mobile platforms
- Client identity and server certificates
  Read the guidelines to determine whether you need certificates.
- Procedures for obtaining Avaya product certificates
- Guidelines and implications to support antivirus and malware scanning software
- Supported cipher suites and limitations of blacklisting cipher suites

The default security settings of Avaya Workplace Client allow it to connect to many existing systems. You must configure the following security setting on desktop platforms, `SET REVOCATIONCHECKENABLED 1`.

Older server versions, or newer server versions with certificates that are maintained across server upgrades, might conflict with the following security settings:

- `SET TLSSRVRID 1`
- `SET TLS_VERSION 1`

For more information on these settings, see the chapter on Automatic configuration.

Security requirements

Avaya recommends the use of TLS v1.3 to provide security for all network connections. TLS server certificates must have:

- Minimum key length of 2048
- Minimum certificate signature algorithm of SHA-2. However, do not select SHA-2 CBC.
- Maximum validity period of 2 years

TLS server certificates must present the DNS name of the server in the Subject Alternative Name extension of the certificate. Also, TLS server certificates must contain an ExtendedKeyUsage (EKU) extension containing the id-kp-serverAuth OID.

The CA used to sign these certificates can be a public CA if the certificate contains only domain names already owned by the organization and no IP addresses.

Users of Avaya Workplace Client can securely connect to network resources when using a secure server certificate obtained from a certificate authority.

To maintain a secure environment for Avaya Workplace Client, administrators of all related components must do the following:

- 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 and audit logs regularly to ensure that the system is operating correctly.
- Review security logs and alarms regularly to monitor possible security events.

Configuring the Listen ports for endpoint connection

About this task

Avaya recommends the use of TLS for all connections with Avaya Workplace Client. If you must use TCP for SIP connections, this cannot be configured by using the SIP server address in the client settings.

Avaya Workplace Client gives priority to TLS after it is received from PPM. For the client to use TCP, you must configure the Listen port for endpoint connection for all Session Manager and PPM servers to TCP and remove TLS from it.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Select the SIP entity that you want to modify.
3. Click **Edit**.
4. In Listen Ports, do the following:
    - Clear the check box for Endpoint on TLS protocol.
    - Select the check box for Endpoint on TCP protocol.
5. Click **Commit**.

Password storage

Disabling password storage requires passwords to be retained only in the application memory. Enabling password storage allows passwords to be stored securely and loaded into memory for the duration that the password is required.

Android

Login credentials are encrypted and stored in the private internal storage of the application. To ensure protection of user data on Android, Avaya recommends that Avaya Workplace Client users implement a device passcode and enable full-disk encryption.

On first startup, the application generates a 256-bit symmetric key for AES that uses Java's SecureRandom class. This key is stored in a Java keystore file in the per-application private storage provided by the OS. Passwords are encrypted using this secret key with the

`AES/ECB/PKCS5Padding`

cipher. The results are encoded in Base64 and stored as key or value pairs with the standard Android Preferences API.

iOS

Passwords are encrypted using the iOS keychain. For details about the encryption, see Apple's security documentation - *iOS Security*.

Mac

For details about the macOS keychain that corresponds to the version of macOS used in your deployment, see Apple's documentation.

Windows

Windows Crypto API is used to store passwords by using RC4 (128-bit). RC4 is an algorithm for encrypting data streams.

Desktop platform security recommendations

For the desktop platforms, Avaya recommends that you follow the deployment guidance provided by Apple and Microsoft for the Mac OS and Windows platforms.

To secure the desktop environment where Avaya Workplace Client will be used, you must:

- Keep OS components up-to-date.
- Use full disk encryption.

- Use anti-virus, anti-phishing, and other security tools.

Mobile device security recommendations

Use Avaya Workplace Client on standard-issue hardware running original versions of vendor-approved software. To ensure the protection of user data, you must secure devices using a passcode. Enable full-disk encryption on Android. Full disk encryption is the default behavior on Android devices with OS 8 and later and iOS devices.

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

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

Jailbroken or Rooted devices

The Avaya Workplace Client applications implement techniques for detecting jailbroken or rooted devices. If Client Enablement Services is in use, you can disable the use of the application on a device that was detected as compromised. However, jailbreak or rooting technology evolves quickly, and Avaya cannot guarantee that the techniques effectively detect all compromised devices. Jailbreaking or rooting a device compromises the built-in security mechanisms, and no security guarantees can be made if the user has compromised the device.

Use of Enterprise Mobility Management Solutions

Avaya Workplace Client is supported when run as an unmodified application on mobile devices. Application wrapping is not supported and might impact correct operation.

Avaya does not distribute mobile applications outside the official vendor application stores such as the Google Play Store and Apple iTunes App Store.

To use Enterprise Mobility Management Solutions to enhance security, you can enforce policies such as:

- The requirement of a device passcode. You can specify a minimum length for the passcode.
- Full-disk encryption on Android.
- Use of a per-app VPN tunnel if the recommended approach of using Avaya Session Border Controller is not used.

- Configure the DISABLE_COPY_PASTE parameter to prevent copying and pasting from and to Avaya Workplace Client for iOS.

Server identity validation

Avaya Workplace Client includes server identity validation on all secure connections.

If you use the client to connect to a service, Avaya Workplace Client performs host name verification to ensure communication with the correct server. With HTTPS connections, you must ensure that the certificate on the server has a Common Name or Subject Alternative Name that matches the FQDN or IP address.

For the VoIP service, the client logic varies slightly. Avaya Workplace Client can communicate with multiple Session Manager servers. If the Session Manager server certificate has the appropriate information about the SIP domain, Avaya Workplace Client accepts the server identity validation.

If Avaya Workplace Client detects a host name validation failure, the logs include the security certificate or host name validation details. Host name validation failure is fatal, and the user cannot continue with the login process if both 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 the TLSSRVRID parameter to a value of 1.

The user can continue with the login process only if the default value of the TLSSRVRID parameter, which is 0, is retained.

Note:

If you set the TLSSRVRID parameter to a value of 1, Avaya Workplace Client for iOS shuts down automatically when it detects this value from the settings file. The user must manually start the application and proceed with automatic configuration.

Remote Wipe overview — Avaya Workplace Client for Android and iOS

For lost or stolen mobile devices, the Client Enablement Services administration website provides the **Lost or Stolen Device** check box. When you select this check box, the Client Enablement Services server notifies the application to:

- Remove all locally stored data. For example, downloaded voice mails if downloading is permitted by the Client Enablement Services voice mail policy.
- Clear the account information.

- Force the user to log in again to gain access to the application.

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

Port configuration

For information about the ports and protocols that Avaya Workplace Client uses, see the Avaya Workplace Client Port Matrix document at https://downloads.avaya.com/css/P8/documents/101065872.

Client identity certificates

You can use client identity certificates to provide an identity of the client to the server. Each client has its own unique identity certificate issued by the Certification Authority or Registration Authority. Avaya Workplace Client can get the certificates issued in one of the following ways:

- Through Simple Certificate Enrollment Protocol (SCEP) servers, such as Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS).
  Avaya Workplace Client for Android and iOS support the SCEP method of installing client identity certificates.
- By manual installation: Users must provide the necessary certificate file by using out-of-band mechanism.
  Avaya Workplace Client for Mac and Windows support the manual method of installing client identity certificates.
- By a URL installation: The settings file contains the PKCS12URL location from where the user can download the certificate.
  Avaya Workplace Client for Android and iOS support the URL method of installing client identity certificates.

If SCEP and PKCS12URL are available, PKCS12URL is used to install the client identity certificate.

For Windows platforms, you can automatically enroll client computer certificates to domain member computers. For more information, see Microsoft Support site at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj129705(v=ws.11).

The server receives the client certificate through TLS mutual authentication and the certificate is verified. For more information, see *Administering Avaya Aura® Session Manager*.

You can use a blank string to remove the installed certificates. For example,

```
SET PKCS12URL ""
```

.

If a user tries to log in and receives an error message stating that the certificate is not trusted, Avaya recommends that you check if the following steps have been performed:

1. The user certificate with intermediate(s) and root is added to the Client Keystore on the personal computer.
2. The user certificate must include the Key encipherment attribute under Key Usage within the identity certificate.
3. The user certificate with intermediate(s) and root is installed into the SBC with the PEM file being offered on the SIP ports.

Server certificates

You must determine whether the following servers in your infrastructure use certificates signed by a certificate authority that the operating system of the device trusts:

- Avaya Aura® Device Services
- Avaya Aura® Presence Services
- Avaya Aura® Session Manager
- Avaya Aura® Web Gateway
- Avaya Session Border Controller
- Avaya Cloud Services
- Avaya Equinox® Conferencing
- Avaya Multimedia Messaging
- Exchange Calendar, Office 365, or Exchange Online
- Web server, which you use to host the settings file for automatic configuration
- LDAP
- Client Enablement Services for Avaya Workplace Client for Android and iOS. Avaya Workplace Client on Avaya Vantage™ does not support Client Enablement Services.

If you deploy Avaya Workplace Client with Client Enablement Services and plan to use System Manager signed certificates for the client facing interface on Client Enablement Services, Avaya recommends that you upgrade Client Enablement Services to 6.2.3 or later. This is to make use of the script enhancements in Client Enablement Services 6.2.3 that make the process of managing these certificates on Client Enablement Services simpler.

Avaya Workplace Client validates the server identity certificate during the TLS connection establishment process. For every TLS connection, basic checks for trust chain validation and expiry are performed. If Avaya Workplace Client cannot establish a TLS connection because of an inability of the device to validate the certificate, Avaya Workplace Client displays an error message.

Intermediate certificates

If you installed the intermediate and root certificates in the system keychain on iOS, iOS recognizes the root certificates, but not the intermediate certificates. This causes a server trust evaluation failure when the user tries to configure Avaya Workplace Client by using the automatic configuration web address.

To resolve the intermediate certificates issue, Apple recommends that you provide intermediate certificates along with server certificates. This is so that the entire certificate chain leads to the root certificate.

For Avaya SBC, you must combine both the intermediate and root certificate files into a single certificate file. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end. For more information, see *Administering Avaya Session Border Controller*.

Third-party certificates

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

Guidelines to determine whether you need certificates

Use the following guidelines to determine whether you need to install certificates. For more information, see *Updating server certificates to improve end-user security and client user experience*.

If your servers use:

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

Split-Horizon Domain Name System (DNS) scenario

For the TLS handshake between Avaya Workplace Client and Avaya SBC, Avaya SBC shares a server certificate. This certificate has a subject alternate name with FQDN that resolves to the B1 IP address, where B1 is the external interface. For mutual authentication between Avaya Workplace Client and Avaya SBC, the subject alternate name must be blank in the certificate that Avaya Workplace Client shares. For more information, see *Administering Avaya Session Border Controller*.

Certificate distribution

Avaya recommends the use of automatic configuration to distribute the CA certificates needed for Avaya Workplace Client.

The Avaya Aura® Device Services or automatic configuration server certificate must be available in the platform trust store. Avaya Workplace Client can then connect to Avaya Aura® Device Services or the automatic configuration server to get the rest of the certificates.

The application-controlled trust store is also known as the private trust store. The OS trust store is also known as the platform trust store. Certificates distributed using the settings file are stored in the private trust store of the application, and not the trust store of the device.

Private trust store

The CA certificates can be hosted on the automatic configuration server to be distributed to Avaya Workplace Client. Certificates distributed using the settings file are stored in the private trust store of the application, and not the trust store of the device. The application-controlled trust store is also known as the private trust store.

Use the private trust store to have a better control over the usage of these certificates without affecting the security policy on the whole platform.

- The private trust store is secure and isolated.
  Certificates contained in the private trust store are unavailable in the device trust store. You can lock down the private trust store.
- If the private trust store exists, Avaya Workplace Client uses the certificates in the private trust store for all operations.
  Hence, even if the certificates are locally available in the operating system, Avaya Workplace Client does not use these local certificates.
- You can add server certificates to the private trust store only by using automatic configuration.
  You cannot add server certificates to the private trust store by using the user interface or application settings.
- The automatic configuration process downloads certificates specified in the TRUSTCERTS settings parameter.
- The certificate for the automatic configuration URL must exist on both the device and in the TRUSTCERTS parameter.

The certificate is needed to connect to the automatic configuration URL. If the private trust store does not include this certificate, connection to the automatic configuration URL is denied.

- You can use the TRUST_STORE setting to combine the private and platform trust stores.
- The private trust store is deleted during application reset and uninstallation.

Obtaining Avaya product certificates

Obtaining the Avaya SIP Product CA certificate

Procedure

1. On System Manager Web Console, in the Services area, click **inventory** > **Manage Elements**.
   The system displays the Manage Elements screen.
2. Choose the appropriate Session Manager instance from the list.
3. In the **More Actions** field, click **Manage Trusted Certificates**.
   The system displays the Manage Trusted Certificates screen.
4. Choose 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. For Avaya Workplace Client for Android and Windows, change the certificate extension from PEM to CRT.
   Only Avaya Workplace Client for iOS and Mac recognize a certificate file with the PEM extension.
8. To download the CA certificate to Avaya Workplace Client, do the following:
   a. Upload the CA certificate to the file server preferably Avaya Aura® Device Services.
   b. In the 46xxsettings.txt file, modify the TRUSTCERTS parameter value to include the CA certificate file.

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 distribute the Avaya Aura® System Manager CA certificate to the user's device using this procedure.

Procedure

1. On System Manager Web Console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Download PEM file**.
5. Save the file to a location on your system.
6. For Avaya Workplace Client for Android and Windows, change the certificate extension from PEM to CRT.

   Only Avaya Workplace Client for iOS and Mac recognize a certificate file with the PEM extension.
7. To download the CA certificate to Avaya Workplace Client, do the following:
   a. Upload the CA certificate to the file server preferably Avaya Aura® Device Services.
   b. In the 46xxsettings.txt file, modify the TRUSTCERTS parameter value to include the CA certificate file.

Antivirus and malware scanning support

Avaya products cannot certify all third-party applications, because their versions, deployment options, and other factors create many variations and complex interactions. Use the following guidelines to support antivirus and malware scanning software on Avaya Workplace Client:

- Test Avaya Workplace Client prior to deployment. You must be able to install and start Avaya Workplace Client on a minimal machine, and be able to perform the following functions:
  - Avaya Workplace Client conference call, with video, and sharing as a presenter
  - Avaya Workplace Client conference call, with video, and sharing as a viewer
  - Messaging with Avaya Multimedia Messaging and Spaces
- In applications such as McAfee Endpoint Security, features like Adaptive Threat Protection can cause problems with video calls as these features scan all traffic flowing in and out of the desktop device. You must exclude Avaya Workplace Client based on the executable path to the program.
- Whitelist the client process name to ensure that real-time access scans are not scanning diagnostic log files as they are written. In some cases, such scanning can cause high CPU usage and application performance problems.
- Ensure that there are no TCP/UDP port conflicts and other protocol conflicts.
- Ensure that adequate hardware is available to meet the requirements of both the Avaya applications and third-party applications. For Windows, you need:
  - CPU requirements for 1080p:

    - CPU core requirements: At least 4 logical cores
    - CPU frequency requirements: Base frequency of 2.4 GHz or greater OR Turbo frequency of 3.0 GHz or greater
    - CPU instruction set requirements: AVX 2.0
    - Alternate CPU: All Apple Silicon CPUs can do 1080p

    Test Avaya Workplace Client on minimum CPU hardware. Scanning software must only use 5% or less of the CPU capacity while scanning and less than 5% when not scanning.
  - CPU requirements for 720p:
    - CPU core requirements: At least 2 logical cores with frequency restrictions OR At least 4 logical cores with no frequency restrictions
    - CPU frequency requirements: Base frequency of 2.0 GHz or higher if greater than or equal to 2 logical cores
    - CPU instruction set requirements: SSE 4.2, SSE 4a, or AVX

    Test Avaya Workplace Client on minimum CPU hardware. Scanning software must only use 5% or less of the CPU capacity while scanning and less than 5% when not scanning.
  - Minimum 2 GB of RAM
  - 100 MB of dedicated video RAM
  - 1.5 GB of free hard disk space
  - Keyboard
  - Mouse or other compatible pointing device
  - Video adapter and monitor with 1024 x 768 or higher resolution
  - Headset for This Computer mode
  - HD camera up to 720p that supports 30fps video when connected to a USB 2.0 or higher port
- Ensure that you monitor the performance of the OS and applications, including the following symptoms of performance degradation:
  - Missed or excessive alarms
  - Dropped remote access sessions
  - Slow user interface response
- During the course of an Avaya support engagement, you might need to uninstall third-party software if it is contributing to or causing an issue.

- Ensure that your antivirus software is active and up-to-date. If your antivirus software is out of date, Microsoft Outlook may display warning messages.

Supported cipher suites

Supported cipher suites

Cipher suite is a set of algorithms that help secure a network connection that uses TLS.

Avaya Workplace Client supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_DH_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DH_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DH_RSA_WITH_AES_256_CBC_SHA256
- TLS_DH_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DH_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DH_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DH_DSS_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

Limitations of blacklisting cipher suites

- If you blacklist all the supported ciphers using the CIPHER_SUITE_BLACKLIST parameter, the cipher list to be published in SSL handshake remains empty. In such cases:
    - On iOS, Android, and Mac, the SSL library populates the default cipher suite list in SSL handshake depending on the TLS version. So, the SSL connection succeeds.
    - On Windows, the SSL library does not add anything to the default list. Hence, the SSL connection fails due to handshake failure.
- On Avaya Workplace Client for iOS and Mac, you cannot use the cipher list to configure the connections set up using NSURLSession. The platform publishes the default cipher list based on the TLS version. Services include OAuth, Exchange Web Services, PPM, and the connection failed over from WebSocket to HTTP for messaging.
- You cannot configure Avaya Workplace Client for Windows with cipher suites for OAuth and Exchange Web Services because .Net framework’s ServicePointManager class does not expose any API to configure cipher suites.
- You cannot configure Avaya Workplace Client in the Guest mode with blacklisted ciphers because guest users do not have access to download the blacklisted cipher suites.

Configuration for Unified Communications deployments

This chapter describes:

- The configuration of Avaya Workplace Client settings in the core Avaya Aura® components.
- Session Manager failover.
- Functionality that is available on the Avaya Workplace Client interface.
- Some advanced functionality options, including MDA and dual registration.
  Other advanced configuration options, such as remote worker and automatic configuration, are described in the following chapters.

Infrastructure configuration

Infrastructure configuration prerequisites

Before configuring the Avaya Workplace Client functionality, you must:

- Choose the UI and advanced functionality to configure for your enterprise.
- Install all planning components.
- Configure Avaya Aura® System Manager as a centralized management system for all Avaya Aura® components and servers.

Checklist for configuring Unified Communications infrastructure

The following checklist outlines the high-level setup and configuration tasks for core Avaya Aura® components in a Unified Communications deployment. Configure the core Avaya Aura® components according to your requirement.

Component	Reference	✔
Avaya Aura® Communication Manager	- Avaya Workplace Client settings in Avaya Aura Communication Manager - Call appearances configuration - Alternate Route Timer configuration	
Avaya Aura® Session Manager	- Avaya Workplace Client settings in Avaya Aura Session Manager - Session Manager survivability	
Avaya Aura® System Manager	- Configuring simultaneous registration in Avaya Aura System Manager - Enabling VoIP Monitoring in Avaya Aura System Manager	

Avaya Workplace Client settings in Avaya Aura Communication Manager

Use the Avaya Aura® System Manager administration interface to change the Avaya Aura® Communication Manager settings.

Task or feature	Configuration
Configure endpoints	At least, enable the following: - **IP SoftPhone**. - **IP Video SoftPhone**.

Task or feature	Configuration
For the Communication Manager signaling group associated with Avaya Aura® Session Manager	Set the following in IP network regions: • Transport Method to `tls`. • Enforce SIPS URI for SRTP to `y`. • Direct IP-IP Audio Connections to `y`. • Initial IP-IP Direct Media to `y`. With direct media enabled, there is no mechanism to provide a ring back to the other phone device. Avaya designed this functionality to support early media call flows. • DTMF over IP to `rtp-payload` to enable Communication Manager to send DTMF tones by using RFC 2833. Avaya Workplace Client does not support sending tones by using in-band or out-of-band DTMF.
Trunk signaling with the PRI line	In Trunk parameters, set Disconnect Supervision - Out to `y`. This setting is required for point-to-point call transfers in Avaya Workplace Client.
Secure calls	Do the following: • In System parameters - features, set Initial INVITE with SDP for secure calls? to `y`. • In System parameters - IP options, set Override ip-codec-set for SIP direct-media connections to `n`. • In System parameters - customer options, set Media Encryption Over IP? to `y`.
Media encryption	In the IP codec set, Media encryption area, set the following: • 1 to `1-srtp-aescm128-hmac80`. • 2 to `2-srtp-aescm128-hmac32`.

Task or feature	Configuration
	- 9 to `none`. - 10 to `10-srtp-aescm256-hmac80`. - 11 to `11-srtp-aescm256-hmac32`.
H.323 and SIP dual registration	Set the following: - Configure off-pbx-telephone station-mapping. - On the Stations With Off-Pbx Telephone Integration screen, add an `OPS` entry. When adding the Off-Premises Station (OPS) entry, set the **Call Limit** field to at least one more than the number of appearances assigned to the extension. For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*. - For conferencing users, set Fast Connect on Origination in Configuration set to `n`. You can do this by using the change off-pbx-telephone configuration-set n command, where “n” is the configuration set number.
Call Pickup	Do the following: - Ensure that the no-ring parameter is disabled. - To enable call pickup alerting, on the Feature-Related System Parameters screen, set the **Call Pickup Alerting** field to `y`. - To enable the enhanced call pickup alerting capability, on the Feature-Related System Parameters screen, set the **Enhanced Call Pickup Alerting** field to `y`. The system displays the **Enhanced Call Pickup Delay Timer (sec.) Display** and

Task or feature	Configuration
	Audible Notification fields only if you set the Enhanced Call Pickup Alerting field to y. To administer the alerting options for a button, set the button assignment by using the `change station n` command. - To enable audible indication of incoming calls to a member of the call pickup group, on page 2 of the Class of Restriction screen, set the **Block Enhanced Call Pickup Alerting** field to n.
Automatic Callback	Do the following: - Assign an FAC for Automatic Callback. - Enable **Automatic Callback With Called Party Queuing**. - Set the no-answer timeout interval for Automatic Callback. - Set the Queue length for Ringback Queuing. - Enable CCBS. For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*.
Call Park	If a user parks a call and does not disconnect after hearing the confirmation tone, the user stays connected to other parties on the call. To automatically disconnect the call, set the **Drop Parking User From The Call After Timeout** field on the Feature-Related System Parameters screen to y. The system then drops the parked call after the default time limit of 5 seconds if the user does not disconnect the call. You cannot change the default time limit. For more information about Call Park administration, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Task or feature	Configuration
Enable EC500	For Client Enablement Services, if EC500 is disabled, call suppression does not work. Hence, you must enable the **EC500** button.
Configure third party call control (3PCC)	For information about 3PCC administration, see *Avaya Aura® Communication Manager Feature Description and Implementation*.
Configure FNEs and FNUs	For more information, see *Administering Avaya Aura® Communication Manager*.
Assign and configure a station security code	
Configure SRTP support settings	
Configure the barge-in tone alert for a user extension	
Exclusion	Do the following: • On the Feature-Related System Parameters screen, set the value of the **Automatic Exclusion by COS** field to y. • For automatic exclusion, on the Class of Service screen, set the value of the **Automatic Exclusion** field of the COS group to y. For non-automatic exclusion, set the value to n. For more information about Exclusion administration, see *Avaya Aura® Communication Manager Feature Description and Implementation*.
Limit Number of Concurrent Calls (LNCC)	Do the following: • Configure the **limit-call** button for the user. • Assign an FAC for LNCC. • Activate the LNCC feature. • Configure the coverage path for LNCC. • View the status of the LNCC feature.

Task or feature	Configuration
Offline Call Journaling	Log in to the System Manager administration interface and enable **User Management** > **Communication Profile** > **Call History**.

Call appearances configuration

To support adhoc conferencing with Avaya Equinox® Conferencing, if you are using Communication Manager Release:

- Earlier than 8.1.1, you need to configure eight call appearances for Avaya Workplace Client.
- 8.1.1 or later, you need to configure a minimum of three call appearances for Avaya Workplace Client.

Note:

The content in this topic is applicable if you are using a release earlier than Communication Manager 8.1.1.

If you are adding Avaya Workplace Client to an existing deployment and:

- If you do not have Avaya Equinox® Conferencing, there is no need for eight call appearances.
- If you have disabled SIP Endpoint Managed Transfer (SEMT) as Avaya Aura® Contact Center or Avaya Aura® Call Center Elite are in the same deployment, then there is no need for eight call appearances. In these deployments, adhoc conferences use the more basic Communication Manager adhoc call. This eliminates the need for the extra three temporary appearances during the creation of an adhoc conference.

If you are doing a new deployment, configure everyone with eight appearances.

Avaya recommends that the configuration must be such that you put the:

- Primary appearances on the main button list in System Manager
- Additional appearances at the end of the feature button or button configurations area

This configuration ensures that the interface on phones such as the J169 and J179 phones is optimized to show the main appearances and other frequently used buttons such as Send All Calls and EC500 on the main screen.

Use case for eight call appearances

- User might have at most three or four calls, where one is active and the rest are held.
- Last line appearance is usually reserved for outgoing emergency calls.

- To create an adhoc conference call with Avaya Equinox® Conferencing by merging two calls together, you need five line appearances:
  - Two for the point-to-point calls that you are trying to merge
  - One for the conference call to conference bridge
  - Two for the transfer operation

Alternate Route Timer configuration

The Alternate Route Timer parameter on Communication Manager is configurable because:

- Different customers have different needs about how long they want to wait before trying to find a different network route.
- The configuration allows Avaya to cater to different types of networks, which can have a different response time.

You must configure the timer value such that it:

- Allows for the network delay
- Ensures that Communication Manager does not wait for too long for a response from the far-end

If the cellular network has delays, you can increase the time-out value from 6-7 seconds to suit your network. You can configure this value on page 1 of the Signaling Group page using the Alternate Route Timer (sec) parameter.

Avaya Workplace Client settings in Avaya Aura Session Manager

You can use the Avaya Aura® System Manager administration interface to change the Avaya Aura® Session Manager settings for each Avaya Workplace Client extension. You can also add or change user profiles with Avaya Aura® Session Manager.

You can use VoIP Push Notifications for:

- Android with Session Manager Release 10.1 and later
- iOS with Session Manager Release 8.1.3.3 and later

Important:

Avaya recommends the use of Session Manager for push notifications on Android and iOS devices.

Task or feature	Configuration
For each extension.	Set an Avaya SIP communication address. If you have E.164 numbers in your enterprise directory, set an Avaya E.164 communication address for each extension.
Select the originating and terminating feature server name.	Set Origination Application Sequence and Termination Application Sequence to the Communication Manager server.
Choose the appropriate template option for your enterprise.	Do the following: • For a SIP implementation, choose a J169 or J179 SIP template. • For a setup that involves SIP and H.323 dual registration, choose a J169 or J179 H.323 template. When you select a template, the system populates the corresponding set types. Avaya recommends the use of SIP so that users can use the advanced functionality that Avaya Workplace Client provides.
For simultaneous device registration and Multiple Device Access (MDA).	Do the following: • In Max. Simultaneous Devices, enter the maximum number of devices that can be logged in simultaneously. For example, if you set Max. Simultaneous Devices to 3, only 3 devices can log in at a time. • Select the **Block New Registration When Maximum Registrations Active?** check box. When you select this check box, if the user tries to log in with a device after reaching the maximum limit, the system denies access to the new device.
Configure the extend call feature.	Assign the extnd-call feature option to users.

Task or feature	Configuration
	You must configure the extend call feature for EC500 call suppression to remain active.
Support direct media and enhance SIP SRTP in Communication Manager.	Enable capability negotiation within a media rule.
Configure push notification	On the System Manager web console, click **Elements** > **Session Manager** > **Global Settings** > **Enable Mobile Push Notification**.
Configure notification provider settings	On the System Manager web console, click **Elements** > **Session Manager** > **Network Configuration** > **Push Notification** > **Notification Provider** and configure the settings.
Configure notification application settings	On the System Manager web console, click **Elements** > **Session Manager** > **Network Configuration** > **Push Notification** > **Notification Application** and configure the settings.

Session Manager survivability

The following registration options are available for Session Manager:

- Non-redundant configuration: Registration to only one Session Manager server. With this configuration, survivability or failover is unavailable.
- Simultaneous registration: Registration to multiple Session Manager servers as a redundancy mechanism.
- Simultaneous registration with branch failover: Registration to multiple Session Manager servers with potential failover to a Session Manager in a Branch environment.

Survivability or failover is possible when multiple Session Manager severs are registered in Avaya Aura® System Manager. When you have more than one Session Manager server, the first server must be registered as the primary server, and the additional servers must be registered as secondary or survivability servers.

If Avaya Workplace Client cannot connect to the primary Session Manager, Avaya Workplace Client automatically fails over to the secondary Session Manager without user intervention. This is to ensure service continuity for Avaya Workplace Client users. If failover occurs while a user is on an active call, Avaya Workplace Client preserves the call, but the user cannot resume the held call.

Configuring simultaneous registration in Avaya Aura System Manager

About this task

Use this procedure to configure the primary and secondary Session Manager servers in Avaya Aura® System Manager. This will provide failover or survivability for Avaya Workplace Client users.

Before you begin

Deploy multiple Session Manager servers.

Procedure

1. Log in to Avaya Aura® System Manager with your administrator credentials.
2. Navigate to **Users** > **User Management** > **Manage Users** > **User Communication Profile** > **Session Manager Profile**.
3. From the drop-down menu, choose the appropriate primary Session Manager.
4. From the drop-down menus, choose the secondary Session Manager, and if required, a survivability server.
   Avaya Workplace Client registers and receives the list of primary, secondary, and Branch Session Manager servers through Personal Profile Manager (PPM).

Enabling VoIP Monitoring in Avaya Aura System Manager

Procedure

1. Log in to Avaya Aura® System Manager.

2. Click **Elements** > **Session Manager**.
3. In the navigation pane, click **Device and Location Configuration** > **Device Settings Groups**.
4. Choose the appropriate group.
   The group might be a default group, a terminal group, or a location group.
5. Click **Edit**.
6. Set the VoIP Monitoring (VMON) Manager settings.
7. Commit the changes.
   Within two or three minutes, System Manager sends SIP NOTIFYs to the SIP phones based on either Terminal Group, Location Group, or to everyone if you configured the Default Group VMON settings. The SIP phones then perform a PPM
   `getAllEndpointConfiguration`
   request, and then PPM returns the new VMON settings in the
   `getAllEndpointConfigurationResponse`
   .
   Avaya Workplace Client receives the Endpoint Configuration Response over HTTP and if the VMON settings are present in the response then VMON is enabled on Avaya Workplace Client.

Configuring Alternate-CLI headers

Before you begin

Download the appropriate file from PLDS.

Procedure

1. On the home page of the System Manager web console, click **Elements** > **Session Manager** > **Global Settings**.
2. Select the **Enable Regular Expression Adaptation** check box and commit the changes.
3. On the home page of the System Manager web console, click **Elements** > **Routing** > **Adaptations** > **Regular Expression Adaptations**.
   The System Manager web console displays the Regular Expression Adaptations Details page.
4. Click **More Actions** > **Import**.
5. Select the file that you downloaded from PLDS and click **Import**.
6. On the home page of the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
7. In the Adaptations area, associate the adaptation with the Communication Manager entity link where the Alternate-CLI header insertion is done.

After these changes replicate to the Session Manager servers in the network, Alternate-CLI headers from Session Manager are acted upon by Session Manager.

Functionality configuration

Client and server requirements

Component	Requirement
Supported clients	• Avaya Workplace Client on mobile platforms • Avaya Workplace Client on desktop platforms • Avaya Workplace Client conference portal
Supported servers	• Avaya Aura® Session Manager • Avaya Aura® System Manager • Avaya Aura® Device Services • Avaya Aura® Communication Manager • Avaya Multimedia Messaging • Avaya Aura® Presence Services • Avaya Aura® Media Server • Avaya Session Border Controller • Avaya Equinox® Conferencing • Unified Portal • Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Client configuration

DNS auto discovery

DNS auto discovery is mandatory to support Avaya Workplace Client in the UC deployment.

Automatic configuration settings

The automatic configuration parameters included in the following table are necessary to support Avaya Workplace Client in the UC deployment. The table includes the recommended values. For complete information about these parameters, see the chapter on Automatic configuration.

Automatic configuration parameter	Recommended value	Notes
CONFERENCE_FQDN_SIP_DIAL_LIST	Enter a list of all internal FQDNS, the Avaya Workplace Client conference portal FQDN and Scopia Desktop Server portal FQDN, that can be reached through direct SIP dialing. For example, "scopia.slav.com,alphaportal.slav.com,aacmeeting.slav.com".	If the virtual room number range is not routable within Avaya Aura®, then do not put the portal server FQDN into this automatic configuration setting. Avaya Workplace Client uses this setting to determine whether to use SIP or HTTP to join a meeting.
UNIFIEDPORTALENABLED	1	You must enable this parameter for all users who can sign in to the Avaya Workplace Client conference portal.
CONFERENCE_PORTAL_URI	Enter the unified portal home URL. For example, "https://alphaconfportal.slav.com:8443/portal".	You need this parameter to support the Scopia Desktop Conference (SDC) replacement features.
UNIFIED_PORTAL_SSO	1	Clients can use the enterprise user name and password to sign in to the Avaya Workplace Client conference portal.
ENABLE_MEDIA_HTTP_TUNNEL	1	This parameter enables the HTTP Tunneling feature in the foreign Avaya Workplace Client conference calls.
BFCP_TRANSPORT	0	Binary Floor Control Protocol (BFCP) is a protocol which is used

Automatic configuration parameter	Recommended value	Notes
		to control the access to the media resources in a conference.
BFCP_UDP_MINIMUM_PORT	5204	—
BFCP_UDP_MAXIMUM_PORT	5224	—
MEDIAENCRYPTION	10,1,2,9	This parameter enables the best effort SRTP with AES 128. You can also enable AES 256 by using the values 10 and 11.
ENCRYPT_SRTCP	0	You must disable this parameter unless SRTCP is supported by all endpoints and servers in Avaya Aura®.
ENABLE_OPUS	1	—
OPUS_PAYLOAD_TYPE	116	—
RTP_PORT_LOW	5004	You must change this parameter value depending on the firewall port ranges.
RTP_PORT_RANGE	200	—
VIDEO_MAX_BANDWIDTH_ANY_NETWORK	1280	—
VIDEO_MAX_BANDWIDTH_CELLULAR_DATA	512	—
APPCAST_ENABLED	1	—
APPCAST_URL	Enter the Avaya Aura® Device Services Web Deployment Sparkle URL. For example, "https://ucserver.slav.com/webdeployment/sparkle/avaya-communicator".	—

Automatic configuration parameter	Recommended value	Notes
APPCAST_CHECK_INTERVAL	1	—
ACSENABLED	1	Avaya Aura® Device Services contact service is mandatory to support the terminal search feature in SDC replacement clients.
ACSSRVR	Enter the Avaya Aura® Device Services contact service FQDN.	—
ACSPORT	Enter the Avaya Aura® Device Services contact service port number.	—
ACSSECURE	1	—
SETTINGS_FILE_URL	Enter the Avaya Aura® Device Services contact service URL. For example, "https://ucserver.slav.com/autoconfiguration/settings.txt".	—
CONTACT_MATCHING_SEARCH_LOCATION	1	—
EWSENABLED	1	EWS is mandatory to support the Top of Mind feature in SDC replacement clients.
EWSSSO	1	Clients can use the enterprise user name and password to authenticate with EWS.
EWSSERVERADDRESS	Enter the EWS server address.	—
EWSDOMAIN	Enter the EWS server FQDN.	—
TRUSTCERTS	""	You must enable the private trust store depending on the security requirements.
TRUST_STORE	1	This parameter value must be set to 1. Else, Avaya Workplace Client

Automatic configuration parameter	Recommended value	Notes
		might not be able to join a foreign enterprise Avaya Workplace Client meeting as a guest user. ⚠ **Caution:** If required by your security policy, you can set the value to 0. However, you cannot join a foreign conference by using Avaya Workplace Client.
CONFERENCE_FACTORY_URI	This parameter value must match the Avaya Equinox® Management's advanced parameter setting vnex.vcms.core.conference.factory URI For example, 816543@avayamcs.com.	You must enable this parameter for all users who can sign in to the Avaya Workplace Client conference portal.

Server configuration

Server external access

The following table includes the list of servers that can be accessed externally through Avaya Session Border Controller or Third-Party Reverse Proxy:

Server	TLS traffic	Internal Avaya Aura® users	External guest users	Server certificates signed by third-party CA	Mutual authentication on the server for internal traffic	Mutual authentication on SBC or Reverse Proxy for external traffic
Session Manager	SIP and HTTPS (for PPM)	Yes	No	Optional	Optional	Optional

Server	TLS traffic	Internal Avaya Aura® users	External guest users	Server certificates signed by third-party CA	Mutual authentication on the server for internal traffic	Mutual authentication on SBC or Reverse Proxy for external traffic
Avaya Multimedia Messaging	HTTPS	Yes	No	Optional	Optional	Optional
Avaya Aura® Device Services	HTTPS	Yes	Yes	Mandatory	Disabled	Disabled
Avaya Aura® Web Gateway or Unified Portal	HTTPS	Yes	Yes	Mandatory	Disabled	Disabled
Equinox Conference Control	HTTPS	Yes	Yes	Mandatory	Disabled	Disabled
WCS	HTTPS	Yes	Yes	Mandatory	Disabled	Disabled

Split Horizon DNS

Avaya recommends the use of split horizon DNS so that the same FQDN is used for any server by both the internal and external clients. The benefits are:

- Administration of the overall system is simplified.
- Single settings file can serve both the internal and external clients.
- Hair-pinning of WCS and Equinox Conference Control traffic by the internal Avaya Workplace Client native clients through SBC is removed.

Server certificate and mutual authentication

Servers that need to support guest access require third-party, CA-signed certificates. This includes Avaya Aura® Web Gateway, Equinox Conference Control, WCS, and Avaya Aura® Device Services. Disable mutual authentication on SBC for external access to these servers.

Do not use an IP address in the CN/SAN field of the certificates.

Avaya Aura® Device Services configuration

- Use the Automatic Configuration service to support Avaya Workplace Client used by the Avaya Aura® users.
- Configure the Contact Server to link with Avaya Equinox® Management for searching the Avaya Equinox® Management terminals.
- Enable the Picture Service to support the client contact pictures.
- Enable the Web Deployment service to support the Avaya Workplace Client software updates.
  The Sparkle service is used only by the Avaya Aura® users. However, the client software download service is used by both Avaya Aura® and guest users.

Avaya Aura® Web Gateway configuration

Unified Portal setting	Recommended value	Notes
Conference Clients	"Equinox Desktop Client, Equinox Mobile Client, and Web Client"	This parameter enables the portal to open Avaya Workplace Client with a higher priority than the Web Client.
Avaya Equinox Client Aura Domain	Enter the Avaya Aura® SIP domain. For example, avayamcs.com.	

Note:

Do not change the default values of the other unified portal settings.

Avaya Equinox® Management extension mapping

When a user dials into an Avaya Workplace Client meeting through SIP, Avaya Equinox® Management attempts to map the caller ID of the user to the stored Avaya Equinox® Management users. If a match is found, Avaya Equinox® Management considers the user as an Avaya Equinox® Management internal user, not a guest user. If the matched user is the owner of a virtual room, Avaya Equinox® Management bypasses the virtual room PIN and moderator PIN, and assigns the moderator role to the user.

Checklist for configuring Avaya Workplace Client functionality for Unified Communications

The following checklist outlines the high-level setup and configuration tasks for Avaya Workplace Client functionality in a Unified Communications deployment. Configure the functionality according to your requirement.

Functionality	Reference	
Client and server configuration	- Client and server requirements - Client configuration - Server configuration	
Alphanumeric dialing	- Telephony - Alphanumeric dialing - Routing server configuration - Setting up an alphanumeric SIP handle on Avaya Aura	
EC500	Extend and send calls to your mobile device with EC500	
Avaya Equinox® Conferencing	Checklist for configuring Avaya Equinox Conferencing functionality	
Avaya Aura® Communication Manager conferencing	Adhoc conferencing by using Avaya Aura Communication Manager	
Call journaling	Call journaling	
Push Notification using Session Manager	Migrating from Avaya Aura Web Gateway to Session Manager for Push Notifications	
Multiple Device Access and dual registration	Multiple Device Access and dual registration	
Bridged Line Appearance	- Bridged Line Appearance overview - Interactions for Bridged Line Appearance - Administering Bridged Line Appearance	
Hunt Groups	- Hunt Groups overview	

Functionality	Reference	✔
	• Setting up hunt groups and assigning stations as members • Provisioning the Hunt Group Busy feature button on the station	
Team Button	• Team Button overview • Adding the team button to the monitoring station • Administering the team button functionality • Administering the team button override functionality • Administering abbreviated or delayed transition interval • Viewing the system capacity for team button	
Presence and instant messaging	• Presence and instant messaging • Configuring Avaya Aura Session Manager to support Avaya Aura Presence Services • Configuring Avaya Aura Session Border Controller to support Avaya Aura Presence Services • Do Not Disturb status • Presence interaction with Client Enablement Services • Presence scenarios with Client Enablement Services	

Functionality	Reference	✔
	• Presence Access Control List • Managing the presence access control policy	
Contacts and enterprise search	• Contacts and enterprise search • Supported LDAP directories for Avaya Workplace Client	
Google Chrome browser extension for Windows	• Google Chrome and Microsoft Edge Chromium browser extensions • Enabling the Google Chrome browser extension for Avaya Workplace Client for Windows • Uninstalling the Google Chrome browser extension from Avaya Workplace Client for Windows • Blocking websites to stop highlighting telephone numbers • Unblocking websites using the group policy	
IPv6 and ANAT configuration	• IPv6 and ANAT configuration • Configuring Avaya Aura Communication Manager to support IPv6 and ANAT	

Functionality	Reference	✔
	- Configuring Avaya Aura Session Manager to support IPv6 and ANAT - Configuring Avaya Aura Session Border Controller to support IPv6 and ANAT	
SSO with OAuth and SAML	SSO with OAuth and SAML	

Telephony

Use the standard Avaya Aura® Communication Manager and Avaya Aura® Session Manager configuration to enable audio and video calls in Avaya Workplace Client. You do not need to configure any other components, but you must obtain licenses for video.

Note:

The phone number that you dial must have a minimum of 10 digits.

If there are multiple soft clients, the user can choose the default soft client for telephone services. Alternatively, if you want the user to use Avaya Workplace Client for Windows as the default application for telephone services, you can use Group Policy to perform the necessary configuration. For more information about using Group Policy, see Microsoft help documentation.

Emergency calls

Do not use Avaya Workplace Client on Android or iOS to make emergency calls as you cannot rely on the use of the mobile device for location information. Avaya recommends that you check the product documentation that accompanies your mobile device to learn about the emergency calling features available on your device.

Note:

Avaya Workplace Client starts a call by using the cellular network if the following conditions are met:

- The value of the CELLULAR_DIRECT_ENABLED parameter is set to 1.
- The dialed number matches any number specified in the CELLULAR_DIRECT_NUMBER_LIST parameter.

For example, if you set the value of the CELLULAR_DIRECT_ENABLED parameter to 1 and if the user dials 911, which you specify in CELLULAR_DIRECT_NUMBER_LIST, Avaya Workplace Client starts the call by using the cellular network. You cannot use these configuration parameters for mobile devices without cellular radio capabilities. For example, iPad, iPod Touch.

Important:

You can use Avaya Workplace Client on Avaya Vantage™ to make emergency calls. For more information, see Emergency calls.

Alphanumeric dialing

Alphanumeric dialing is a feature that users can use to make and receive an audio or video call by using the alphanumeric Uniform Resource Identifier (URI). For example, users can use the alphanumeric URI to call an external user, such as a Skype for Business user, by using 123john@telenor.com.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Server configuration

You must set up:

- A routing server.
- An alphanumeric SIP handle on Avaya Aura®.

Routing server configuration

- Communication Manager supports alphanumeric dialing inside the same enterprise domain.

  Hence, you do not need to perform any additional configuration.
- For alphanumeric dialing outside the same enterprise domain, you must configure a routing server.

This server must recognize the internal URI address and know how to reach the target server. For example, internal URI address is of Avaya and target server is a Skype for Business server. For additional information, see *Administering Avaya Aura® Communication Manager*.

Setting up an alphanumeric SIP handle on Avaya Aura

About this task

Use this procedure to associate a user with a URI address.

Procedure

1. Log in to Avaya Aura® System Manager with your administrator credentials.
2. Go to **User Management** > **Manage Users**.
3. Select the user that you want to configure, and click **Edit**.
4. In the Communication Address area, click **New**.
5. In the **Type** field, click **Avaya SIP**.
6. In **Fully Qualified Address**, type an address and select a domain.

   For example, address is `aquadros` and domain is `ndtv.com`.
7. Click **Commit & Continue**.
8. Go to the CM Endpoint Profile area.
9. In the **SIP URI** field, click the SIP handle that you created in Step 6.
10. Click **Commit**.

Extend and send calls to your mobile device with EC500

EC500 is a Communication Manager feature with which you can:

- Join and answer calls from your mobile device.
- Send calls to your mobile device.

You can enable multiple EC500 functionality options. The following table summarizes the EC500 options and the configuration required for each option:

EC500 options	Description	Configuration notes
Standard EC500	This option enables you to join and answer calls from your mobile device using Avaya Workplace Client.	Enable EC500 in Avaya Aura® Communication Manager.
EC500 FNE auto-dialer	This option enables the following capabilities in Avaya Workplace Client: • Make outgoing calls through Avaya Aura® Communication Manager. • Access simultaneous ringing on your deskphone and mobile device. • Join active calls. • Send all calls to your voice mail. • Extend calls. • Forward calls. • Enable or disable EC500 on the UI as needed. • Access EC500 station security codes.	Configure FNEs in Avaya Aura® Communication Manager. **Note:** While configuring the Call Forwarding feature in Communication Manager, you must keep the extension field empty. The user must provide the extension from Avaya Workplace Client after logging in.
EC500 call suppression	This option enables Avaya Workplace Client users to receive a single incoming call on their mobile phone. Users receive an alert either by a VoIP call or a cellular call, but not both.	Configure Extend Call in Avaya Aura® Session Manager by assigning the extnd-call option to users.

Conferencing

Avaya Equinox® Conferencing provides audio and video conference functionality to Avaya Workplace Client.

If Avaya Workplace Client does not include the settings for Conference Factory URI and the user merges two calls, Avaya Workplace Client creates a Communication Manager adhoc conference call.

Adhoc conferencing by using Avaya Aura Communication Manager

Users can create a Communication Manager conference by using the user interface of a single active call. In the previous release, users had to make two separate calls to create a Communication Manager conference.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Automatic configuration settings

Do not configure the CONFERENCE_FACTORY_URI parameter.

Avaya Workplace Client setting

Users must ensure that the adhoc conference address is empty in the Avaya Workplace Client settings: **Settings** > **Services** > **Phone Service** > **Adhoc Conference Address**.

Call journaling

Users can use this feature for a consistent view of call logs that are generated whether a device is logged in or not.

Note:

If Multiple Device Access (MDA) is in use, unanswered outgoing calls from one device do not appear in the call logs of the other registered devices or clients in the MDA group. These unanswered outgoing calls are visible in the call logs of the other devices after you log out and log in to those devices.

Call logs display calls missed or placed from other clients when the client is not logged in. This improves user experience and consistency across all platforms.

Note:

Call history records might change over time due to call history re-synchronizing with the network. Network call logs vary from local call logs because of network manipulation of dialed digits that occurs during normal call processing.

On Avaya Workplace Client for Windows:

- Call logs display the name and number of the user who forwarded the call and the reason for forwarding the call.
- Call appearance displays the name or number of the user who forwarded the call and the reason for forwarding the call.

Avaya Workplace Client for Windows displays the reason for forwarding the call if the user who forwarded the call has enabled **Forward Calls Busy/No Answer**.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Automatic configuration settings

You must enable the ENABLE_PPM_CALL_JOURNALING parameter.

Server configuration

You must enable Call Journaling in Session Manager Profile for each user.

In the Avaya Aura® System Manager web interface, the **Enable Centralized Call History** setting is available in **Session Manager Profile** > **Call History Settings**.

Migrating from Avaya Aura Web Gateway to Session Manager for Push Notifications

About this task

As of Session Manager 8.1.3.3, you can now use Session Manager for the Apple Push Notification service. Before Session Manager 8.1.3.3, only Avaya Aura® Web Gateway was in use for the Push Notification service.

Important:

Avaya recommends the use of Session Manager for push notifications on Android and iOS devices.

Before you begin

- Upgrade to Session Manager 8.1.3.3.
- Ensure that the user or extension is logged in through Session Manager for SIP signaling.
- Ensure that the Push Notification service is using Avaya Aura® Web Gateway.

Procedure

In the settings file, change the value of the TELEPHONY_PUSH_NOTIFICATION_ENABLED parameter from 1 to 2.

When Avaya Workplace Client for iOS refreshes its configuration, Avaya Workplace Client does the following:

- Sends a deactivation request to Avaya Aura® Web Gateway.
- Sends a successful push activation through Session Manager.

Timer configuration for routing unanswered call to voice mail

Avaya Aura® Communication Manager has a configuration parameter that controls how many ring cycles the call can alert before the call is directed to a coverage path. By default, Communication Manager waits for two ring cycles. If you enable push notification, Avaya recommends increasing the number of ring cycles from two to four.

You can configure the ring cycles in **Local Coverage Subsequent Redirection/CFWD No Answer Interval** on the System Parameters Call Coverage/Call Forwarding screen.

Multiple Device Access and dual registration

Avaya Workplace Client 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.

For information about the MDA and dual registration configuration options in Session Manager, see Avaya Workplace Client settings in Avaya Aura Session Manager. For complete information on MDA and dual registration, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Maximum registration configuration

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.

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

Avaya Workplace Client supports this feature with Session Manager 6.3.3, that is, Avaya Aura® 6.2 FP2 SP1 or later. If you are using Avaya Workplace Client with an earlier version of Session Manager, you must clear the **Block New Registration When Maximum Registrations Active?** check box.

Limitations

- MDA works with endpoints connected through TLS or TCP. However, if a user logs into an extension with a TCP device, an incoming secure call does not ring the TCP device. Also, the user cannot bridge onto a secure call from that device. This same limitation applies to devices that register through TCP without MDA.
- Some MDA limitations exist for IM and Presence between Avaya Workplace Client and other applications. For more information, see Multiple Device Access White Paper.
- If the user uses Avaya Workplace Client in the dual registration mode with Avaya one-X® Communicator (H.323) and answers a call on Avaya one-X® Communicator, Avaya Workplace Client displays one missed call and one answered call in the call history.

- For more information about MDA end user limitations, see *Using Avaya Workplace Client for Android, iOS, Mac, and Windows*.

Bridged Line Appearance overview

Use the Bridged Line Appearance (BLA) feature to give single-line and multi-appearance telephones an appearance of another telephone number. With BLA, you can make, answer, and bridge onto calls to or from the telephone number of another user.

The terms primary number, primary telephone, and primary station all mean the same thing.

The primary number is the extension that you want other extensions to bridge onto. For example, you want extension A as the primary number to also have call appearances on extensions B, C, and D.

A typical use case for the BLA feature is a boss and secretary scenario. In this scenario, the primary number is of the boss and call appearances of the primary number are configured on the extension of the secretary. When someone calls the boss, either the boss or secretary can answer the call. If the call is answered first by the secretary, the boss can bridge onto the call.

If a call is made to the extension of the secretary, the boss cannot see this call or bridge onto it.

To make a call using the BLA extension, you must first select the primary extension appearance and then dial on behalf of the primary extension.

When you receive a call on the primary extension, the call rings on the primary extension and the secondary extension. In this case, the secondary extension displays that the call is for the primary extension. The user of the secondary extension can select and answer this call. After the call is answered, the secondary extension displays that the active answered call is for the primary extension. On the primary extension, Avaya Workplace Client displays a bridge appearance to bridge onto the call answered on the secondary extension.

Interactions for Bridged Line Appearance

This section provides information about how the Bridged Line Appearance (BLA) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of BLA in any feature configuration. For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Note:

Enhanced conferencing using Avaya Equinox® Conferencing is not supported with BLA. If a BLA watcher wants to be a participant in an enhanced conference, the BLA watcher must join the enhanced conference directly.

Automatic Callback

Automatic Callback calls cannot originate from a BLA. However, when Automatic Callback is activated from the primary telephone, the callback call rings on all bridged appearances of the extension and the primary telephone.

Call Forwarding All Calls, Call Forward Busy, and No Answer

Call Forwarding can be activated or canceled for the primary extension from any BLA of that extension using a feature access code. When activated, calls to the primary extension do not terminate at the BLAs, but go to the designated forwarding destination.

Call Park

When a call is parked from a BLA, it is parked on the primary extension associated with the BLA.

Call Pickup

Calls that are made to a primary telephone can only be answered by pickup group members of the primary number. This refers to calls with alerting at bridged appearances of the primary telephone.

- The **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to `n`: In this case, the primary appearance and all bridged appearances of the call are dropped after Call Pickup is used to answer the call.
- The **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to `y`: In this case, the primary and bridged call appearance lamps stay lit after Call Pickup is used to answer the call.
- The primary telephone and the BLA are not in the same pickup group: In this case, members in the same pickup group as the BLA telephone cannot answer a call that is made to the primary telephone.

  Note:

  The primary telephone and the BLA cannot be in the same pickup group. This is not a supported configuration.

When you dial the Call Pickup FAC on a BLA, the system interprets the action as an attempt to answer a call from the call pickup group of the primary telephone. When operating this way, the covering user can act as the primary user and provide the same call pickup coverage if required. Covering user is the user associated with the extension number that is configured to have call appearances of the primary number.

Call Transfer or Conference Call

When a single-line or multi-line device is administered as a BLA, and you initiate a call transfer or conference call, you can use the idle bridged call appearance or idle primary call appearance.

Send All Calls

Single-line device: When a single-line device is administered as a BLA, you cannot start Send All Calls for the extension of the device. You do not have a Send All Calls button, and the call appearance is associated with another extension, that is, the primary extension. When you dial an FAC, Send All Calls is activated for the extension associated with the call appearance.

Multi-appearance telephones: If you have BLAs, you can activate or deactivate Send All Calls for a primary telephone from the bridged appearance.

Administering Bridged Line Appearance

Procedure

- On Communication Manager:
  - To prohibit bridging onto Data Privacy calls, on the Feature-Related System Parameters screen, type y in the **Prohibit Bridging Onto Calls with Data Privacy** field.
  - To skip a coverage point, on the Coverage Path screen, type n in the **Terminate to Coverage Pts. with Bridged Appearance** field.
  - On the Station screen, create a bridged line appearance on a single-line telephone or a multiappearance telephone.
  - Enable bridged call alerting on the extension.
    The bridged appearance rings when a call arrives at the primary telephone.
    If you have enabled per-button ring control for the extension, then you must set each button to have y for the ring parameter.

  For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*.
- On System Manager, use the System Manager web console.
  For more information, see *Administering Avaya Aura® System Manager*.

Hunt Groups overview

You can use the Hunt Groups feature to set up a group of extensions that can handle multiple calls to a telephone number. Additionally, you can choose the call distribution method to route calls. For each call to the number, the system hunts for an available extension in the hunt group, and connects the call to that extension.

A hunt group is especially useful when you expect a high number of calls to a particular telephone number.

A hunt group might consist of people who are trained to handle calls on specific topics. For example, the group might be a:

- Benefits department within a company
- Service department for products that a company sells
- Travel reservations service
- Pool of attendants

Setting up hunt groups and assigning stations as members

About this task

Use this procedure to set up hunt groups on Avaya Aura® System Manager and assign the stations as members to the hunt group.

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Groups** > **Hunt Group**.
2. Select a Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. To create a new hunt group, in the Hunt Group List area, click **New**.
5. Type the hunt group number as a qualifier, and click **Add**.
6. On the New Hunt Group page, type the details in the **Group Name** and the **Group Extension** fields.
7. Select the **ACD** check box.
8. Click **Next Page** until you reach the Group Member Assignments screen.
9. Enter the group member assignments by assigning the stations to the hunt group.
10. To apply the configuration changes, click **Enter**.

Provisioning the Hunt Group Busy feature button on the station

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. Select the user for which you want to provision the Hunt Group Busy feature button.
3. Go to the **Communication Profile** tab, and click **Endpoint Editor** > **Button Assignment** > **Feature Buttons**.
4. In **Button Feature**, select **hntpos-bsy**.
5. In the **Grp** field, type the group number.
6. Click **Done**.
7. To apply the changes, click **Commit**.

Team Button overview

Avaya Workplace Client on mobile platforms and Avaya Workplace Client for Windows support the Team Button feature. With this feature, at the monitoring station, you can do the following:

- View the state of a monitored station.
- View all calls that ring on the monitored station and selectively answer any.
- Speed dial, that is, place a call, to the monitored station.
- Blind transfer any call to the monitored station.
- Configure the audible ringing and visual alert notification.

Monitoring Station

The station which is used to monitor the state of another station. This is the station that displays the Team Button.

Monitored Station

The station whose state is being monitored.

Adding the team button to the monitoring station

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.

2. Search for the station to which you want to add the team button.
3. Select the user profile of the monitoring station, and click **Edit**.
4. In the User Profile edit page, go to the CM Endpoint Profile area.
5. Click **Endpoint Editor** > **Button Assignment** > **Feature Buttons**.
6. In the **Button Feature** field, select **team**.
7. In the **Ext** field, type the extension of the monitored station.
8. In the **Ring** field, type one of the following ring types:
    - **n**: No ringing
    - **r**: Continuous ringing
    - **d**: Delayed ringing
    - **a**: Abbreviated (single) ringing
    - **i**: Intercom ringing
9. Click **Done**.
10. To apply the changes, click **Commit**.

Administering the team button functionality

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Element Cut-Through**.
2. On the Element Cut-Through page, click a Communication Manager instance.
3. In the **Command** field, type `change cor <COR of station>`.
4. Click **Send**.
5. Click **Next Page** until you reach Page 3.
6. **Optional** To enable audible ringing, set **Team Btn Silent if Active** to `n`.
7. **Optional** To enable priority ringing, set **Priority Ring** to `y`.
8. **Optional** To display the monitored station name instead of the number, set **Team Btn Display Name** to `y`.
9. **Optional** To enable pick up of a call by going off-hook, set **Pick Up by Going Off Hook** to `y`.
10. To apply the configuration changes, click **Enter**.

Administering the team button override functionality

About this task

This team button functionality is controlled by Class of Restriction (COR) settings and a setting on the monitoring station.

Note:

Avaya Workplace Client does not support blind transfer by using the team button override functionality.

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Element Cut-Through**.
2. On the Element Cut-Through page, click a Communication Manager instance.
3. In the **Command** field, type `change cor <COR of station>`.
4. Click **Send**.
5. Click **Next Page** until you reach Page 3.
6. **Optional** For the monitoring station, to override Send All Calls and Call Forwarding by using the team button, set **SAC/CF Override by Team Btn** to `y`.
7. **Optional** For the monitored station, set **SAC/CF Override Protection for Team Btn** to `n`.

   This setting affects all monitored stations that use the same COR. If you set the value in this field to `y`, the system enables override protection. Also, the monitoring station cannot override call redirection set at the monitored station.
8. To apply the configuration changes, click **Enter**.
9. In the **Command** field, type `change <monitoring station>`.
10. Click **Send**.
11. Click **Next Page** until you reach Page 3.
12. In the **SAC/CF Override** field, select one of the following:
    - **n(o)**: Cannot override rerouting.

      The station cannot override rerouting.
    - **y(es)**: Can override rerouting.

      The station can override the rerouting that the monitored station has set only if one incoming call appearance is free. If a free call appearance is unavailable, the call fails and the user of the monitoring station hears a busy tone.
    - **a(sk)**: Questions whether the user wants to override rerouting.

      When the user of the station decides whether rerouting must take place or not, Avaya Workplace Client sends a message to the station.

13. To apply the configuration changes, click **Enter**.

Administering abbreviated or delayed transition interval

About this task

Use this procedure to administer the abbreviated or delayed transition interval.

- Abbreviated ringing: Ringing continues for the number of cycles that you specify in the field and then changes to silent alerting.
- Delayed ringing: Visual alerting continues for the number of cycles that you specify in the field and then changes to ringing.

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Element Cut-Through**.
2. On the Element Cut-Through page, click a Communication Manager instance.
3. In the **Command** field, type `change system-parameters features`.
4. Click **Send**.
5. In the **Auto Abbreviated/Delayed Transition Interval (rings)** field, type the number of rings before the system performs an automatic abbreviated transition or delayed transition for a call.
   You can type a number from 1 to 16. Each ring is equal to a 5 second delay.
6. To apply the configuration changes, click **Enter**.

Viewing the system capacity for team button

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Element Cut-Through**.
2. On the Element Cut-Through page, click a Communication Manager instance.

3. In the **Command** field, type `display capacity`.
4. Click **Send**.
5. Click **Next Page** until you can view the **Team button / Monitored stations** field.
   The system displays the used, available, and system limit for team buttons.

Presence and instant messaging

All Avaya Workplace Client platforms require Avaya Aura® Presence Services to provide the Presence functionality. With the Presence feature, you can change your availability and see the availability of other users. Avaya Workplace Client on mobile platforms support direct presence and are not dependent on Client Enablement Services for presence when logged in to VoIP.

You can exchange instant messages with other users by using both Avaya Multimedia Messaging and Spaces Direct Messaging. Avaya Multimedia Messaging is used as the default over Spaces Direct Messaging. The messaging platform can be chosen on a per conversation basis.

Note:

Avaya Workplace Client does not provide the IM functionality with Avaya Aura® Presence Services.

The IM features that users can access when Avaya Workplace Client is configured to use Avaya Multimedia Messaging vary depending on whether they have enhanced Avaya Multimedia Messaging user privileges.

You can hold a Spaces Direct Messaging conversation only with members of Spaces. You cannot invite non-members to join you on Spaces using Avaya Workplace Client.

Avaya Workplace Client supports IM exchange with XMPP federated contacts. With XMPP federation, users in one enterprise domain can exchange IMs with users in external domains. Avaya Multimedia Messaging supports federation with Microsoft Lync, Openfire, and Cisco Jabber.

Configuring Avaya Aura Session Manager to support Avaya Aura Presence Services

About this task

Avaya Aura® Session Manager must be configured to support the Presence Services server that you are using. For more information, see *Administering Avaya Aura® Session Manager*.

Note:

For Presence Services 7.0 and later versions, this configuration is not required.

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 you must use is
   `.*@ps-fqdn`
   .

Configuring Avaya Aura Session Border Controller to support Avaya Aura Presence Services

About this task

If you are deploying Avaya Workplace Client with Presence for remote workers, you must configure the Avaya Aura® Session Border Controller Personal Profile Manager (PPM) profile mapping correctly to support Presence.

Procedure

In **PPM Services** > **Mapping Profiles**, configure the FQDN or IP address of the Presence server.

Do Not Disturb status

In Avaya Aura® Presence Services Feature Pack 4 and later, you can enable the mod_dnd parameter. When you set this parameter, users continue to receive IMs when their presence status is set to Do Not Disturb, but notifications are suppressed.

When the mod_dnd parameter is enabled, users can still start IM conversations and receive immediate responses.

Note:

Avaya Workplace Client on mobile platforms using only Client Enablement Services for presence do not support the Do Not Disturb (DND) status. DND users continue to receive audio and visual notifications for new messages.

Presence interaction with Client Enablement Services

When Avaya Workplace Client on mobile platforms are integrated only with Client Enablement Services, the Client Enablement Services server delivers the presence information to the Avaya Workplace Client on mobile platforms. For guidance on using presence Access Control List (ACL) requests with Client Enablement Services, see the Client Enablement Services product documentation.

Limitations

- Client Enablement Services supports only a single Presence Server.
- Avaya Workplace Client on mobile platforms using only Client Enablement Services for presence do not support the Do Not Disturb (DND) status. 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 multidomain configuration, you can only configure presence for users in one domain.
- If the user selects the **Automatic** option for presence, Avaya Workplace Client does not influence presence in any way. If the user is logged in to Avaya Workplace Client, the user might still appear offline if other devices are offline.

Presence scenarios with Client Enablement Services

The following pertain to a single Client Enablement Services client when the user’s presence status is updated automatically:

- If Client Enablement Services is deployed without Application Enablement Services (AES), then the presence status of the user is always Offline.
- If Client Enablement Services is deployed with AES, then the presence status of the user is Available unless the user is on a call. In this case, the status is Busy.

  Note:

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

Users can also update their presence status manually.

If the Client Enablement Services user has more than one client that supports presence, such as Avaya one-X® Communicator and Avaya Workplace Client, then self-presence is subject to the aggregation rules on Presence Services. Without AES, Client Enablement Services does not publish presence.

The following table summarizes Client Enablement Services configuration options and the corresponding presence status:

AES configured	User client configuration	Automatic	Result
No	Single client: Client Enablement Services	Yes	The presence status is always Offline.
No	Single client: Client Enablement Services	No: User sets presence manually.	The presence status is what the user sets manually.
No	Multiple clients: Client Enablement Services and other presence-enabled clients, such as Avaya Workplace Client	Yes	The presence status is what the other client, such as Avaya Workplace Client, publishes.
No	Multiple clients: Client Enablement Services and other presence-enabled clients, such as Avaya Workplace Client	User sets presence manually on Client Enablement Services.	Client Enablement Services pushes the manual presence update to Presence Services. Presence Services then updates the self-presence status of the user. The presence status is what the user sets manually.
Yes	Single client: Client Enablement Services	Yes	The presence status is always Available. If the

AES configured	User client configuration	Automatic	Result
			user is on a call, the presence status is Busy. **Note:** This result is true and valid until Avaya Aura® FP3, at which point if Client Enablement Services is the only client, then the presence status is always Offline. If the user is on a call, the presence status is Busy.
Yes	Single client: Client Enablement Services	No: User sets presence manually.	The presence status is what the user sets manually.
Yes	Multiple clients: Client Enablement Services and other presence-enabled clients, such as Avaya Workplace Client	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 presence status as Available and Avaya Workplace Client logs out and goes offline. Then the presence status of the user is always Available. **Note:** This result is true and valid until Avaya Aura® FP3. Else, for Avaya Aura® FP3, AES publishes the presence status as Available if an H.323 device is registered. Otherwise, AES publishes the

AES configured	User client configuration	Automatic	Result
			presence status as Offline.
Yes	Multiple clients: Client Enablement Services and other presence-enabled clients, such as Avaya Workplace Client	User sets presence manually on Client Enablement Services.	Client Enablement Services pushes the manual presence update to Presence Services. Presence Services then updates the self-presence state of the user. The presence status is what the user sets manually.

Presence Access Control List

With the Presence Access Control List feature, users can control who can see the user's presence.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Avaya Workplace Client setting

In Avaya Workplace Client settings, the user can click **Services** > **Presence Followers** and configure the presence followers.

Managing the presence access control policy

About this task

Use this procedure to define rules for accessing the presence information by one or more watchers.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. Click the **Service Profiles** tab.
3. In the **Profile** field, click the presence service profile that you want to configure.
4. In the **Service** field, click **Presence Services**.
5. In the Access Control area, for Access Control Policy:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type **Confirm**.
6. Click **Commit**.
   Avaya Workplace Client prompts the user for each request to track the user's presence. The user can allow or deny the request to track the presence.

Contacts and enterprise search

Users can use Avaya Workplace Client to search for and connect with other users in their enterprise. You can configure Avaya Aura® Device Services to manage common contacts and enterprise search. Common Avaya Aura® Device Services configuration ensures that the experience across clients is consistent.

Note:

If you search for an enterprise contact that has a German umlaut character in the name, Avaya Workplace Client does not provide the presence status for that contact.

Avaya Workplace Client can connect directly to LDAP to manage enterprise search, or it can connect indirectly through another service. For example, existing Avaya Workplace Client deployments on mobile platforms might be configured to use Avaya one-X® Client Enablement Services.

When users search for a contact, Avaya Workplace Client performs a search for that contact in the various directories according to the following priority:

- Avaya Aura® Device Services
- Client Enablement Services or LDAP
- Avaya Cloud Services
- Local

Note:

Configure the enterprise policy to enable Avaya Workplace Client to access local contacts from Microsoft Outlook. Check with your IT team if you need to update the Outlook security registry. For more information, see Microsoft Support.

Supported LDAP directories for Avaya Workplace Client

LDAPv3 support

Avaya Workplace Client can connect directly to LDAP to manage enterprise search or it can connect indirectly through another service. For example, existing Avaya Workplace Client deployments on mobile platforms might be configured to use Avaya one-X® Client Enablement Services. In this case, LDAP integration is done through Client Enablement Services.

The preferred option is to connect to LDAP using Avaya Aura® Device Services. For more information, see *Deploying Avaya Aura® Device Services* and *Administering Avaya Aura® Device Services*.

Only desktop clients have direct connectivity to LDAP and they support Avaya Aura® Device Services. Mobile clients connect with LDAP using Avaya Aura® Device Services or Client Enablement Services. On mobile platforms, users can perform an LDAP search using Microsoft ActiveSync if you provision the same.

Note:

On Avaya Workplace Client for iOS, to use a Gmail account for an LDAP search using Microsoft ActiveSync, you must provision the Gmail account as Exchange account type. If you add another Exchange account with Gmail, Avaya Workplace Client can search contacts from both the Exchange and Gmail accounts.

This section describes LDAP support for Avaya Workplace Client that connect to an LDAP directory directly.

Avaya Workplace Client supports LDAPv3, which includes standard LDAP and secure LDAP, with Microsoft Active Directory. Avaya Workplace Client on desktop platforms also support Novell eDirectory and IBM® Lotus Domino. For more information about supported directory versions for each Avaya Workplace Client, go to https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml and select the appropriate Avaya Workplace Client.

Note:

The default directory type used by Avaya Workplace Client on desktop platforms is Microsoft Active Directory. If you want to use any other directory type, you must set the DIRTYPE parameter using the settings file. For information about the automatic configuration options, see the chapter on Automatic configuration.

You can set up the LDAP server using an FQDN or an IP address.

Search attributes

During an LDAP search, Avaya Workplace Client searches the following attributes:

- cn: Common name, that is, First name plus Last name
- sn: Last name
- givenName: First name
- displayName: Display name

If Avaya Aura® Device Services is enabled, Avaya Workplace Client searches the following attributes:

- displayName
- Alias
- FirstName
- LastName
- number
- handle: email or im handle

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

After the search, Avaya Workplace Client constructs the name using the sn and givenName attributes.

If Avaya Aura® Device Services is enabled and the user performs an advanced search, Avaya Workplace Client searches the following LDAP attributes:

- givenName
- sn
- displayName
- l: Location
- department: Department name

If the user populates the **Name** field, Avaya Workplace Client automatically searches for givenName, sn, and displayName using the same algorithm that is used in unified search. You cannot search for only givenName or sn, etc.

If a user adds a contact who is already an enterprise contact as an Avaya Workplace Client 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 local contact. The enterprise contact photo takes precedence over the local contact photo.

Note:

For Avaya Aura® Device Services deployment, self-contact resolution is available. However, for PPM and LDAP deployments, self-contact resolution is unavailable.

Google Chrome and Microsoft Edge Chromium browser extensions

Use the Chrome Web Store to distribute the Google Chrome and Microsoft Edge Chromium extensions.

- If users are using Chrome browser version 76 and later or Edge Chromium, they do not need to install the extension manually because Avaya Workplace Client for Windows installs the extension automatically.
- If users are using Chrome browser version 76 and later or Edge Chromium, they do not need to uninstall the extension manually because Avaya Workplace Client for Windows uninstalls the extension automatically.
- If the NativeMessagingBlocklist configuration parameter includes the “*” value on Chrome or Edge Chromium browsers, you must add the NativeMessagingAllowlist configuration parameter with the “com.avaya.adce” value.
- Use the procedures in the following sections to install and uninstall the extension only on Chrome browser version 75 and earlier.
- Avaya Workplace Client for Windows flags the installation of the extension as a third-party installation. If users remove the Chrome or Edge Chromium extension manually from the UI, the local blocklist includes the extension, which prevents new installations by third parties.
    - Hence, when users subsequently install Avaya Workplace Client for Windows, the extension is not installed.
    - If users want to use the extension again, they must manually install the Avaya Browser Extension from the Chrome Web Store. This action removes the extension from the block list allowing installations from third parties.

Note:

- Chrome on Mac OS does not support the browser extension.

- After enabling the browser extension, you must refresh the previously opened browser tabs. This is to ensure that the browser extension functionality works as expected.

Enabling the Google Chrome browser extension for Avaya Workplace Client for Windows

About this task

Google indicates that you must use the enterprise policy to install browser extensions. Use this procedure to enable the Google Chrome browser extension for Avaya Workplace Client for Windows only if you are using Chrome browser version 75 and earlier. If you are using Chrome browser version 76 and later, Avaya Workplace Client for Windows installs the extension automatically.

For information about using the on-premise tools to set Google Chrome policies in an enterprise, see https://support.google.com/chrome/a/answer/187202?hl=en.

Before you begin

Install Avaya Workplace Client for Windows.

Procedure

1. To download the Chrome policy templates for Windows and install them, use the enterprise policy to configure the registry values:
   a. Open your Group Policy Management console.
   b. Go to User Configuration\Administrative Templates\Google\Google Chrome\Extensions.
   c. Go to the **Configure the list of force-installed apps and extensions** setting.
   d. Set the value to:
   `ildhoddlaaaneelljhohbndmjbjbfgcl;file:///C:/Program%20Files%20(x86)/Avaya/Avaya%20IX%20Workplace/fTarget/accs_crx_update_manifest.xml`
   e. Save the changes.
   f. Go to the **Configure extension, app, and user script install sources** setting.
   g. Set the value to:
   `file:///C:/Program%20Files%20(x86)/Avaya/Avaya%20IX%20Workplace/fTarget/*`
   h. Save the changes.

2. Apply group policy for the users.
3. Restart the Google Chrome browser.
4. Open Google Chrome and enter `chrome://extensions` in the address bar.
   The system displays the Avaya Workplace Client for Windows add-in for the Chrome browser, which works properly on Google Chrome.

Uninstalling the Google Chrome browser extension from Avaya Workplace Client for Windows

About this task

Use this procedure to uninstall the Google Chrome browser extension for Avaya Workplace Client for Windows only if you are using Chrome browser version 75 and earlier. If you are using Chrome browser version 76 and later, Avaya Workplace Client for Windows uninstalls the extension automatically.

Before you begin

Exit the Google Chrome browser.

Procedure

1. To delete the group policy:
   a. Open your Group Policy Management console.
   b. Go to User Configuration\Administrative Templates\Google\Google Chrome\Extensions.
   c. Go to the **Configure the list of force-installed apps and extensions** setting.
   d. Delete:
   `ildhoddlaaaneelljhohbndmjbjbfgcl;file:///C:/Program%20Files%20(x86)/Avaya/Avaya%20IX%20Workplace/fTarget/accs_crx_update_manifest.xml`
   e. Save the changes.
   f. Go to the **Configure extension, app, and user script install sources** setting.
   g. Delete:
   `file:///C:/Program%20Files%20(x86)/Avaya/Avaya%20IX%20Workplace/fTarget/*`
   h. Save the changes.

2. Apply group policy for the users.

3. Restart the Google Chrome browser.
4. Open Google Chrome and enter `chrome://extensions` in the address bar.
   The system does not display the Avaya Workplace Client for Windows add-in for the Chrome browser.

Blocking websites to stop highlighting telephone numbers

About this task

You can block a website using a group policy. The Administrator has disabled the following site(s) list in the Browser Add-in General tab displays blocked websites with a red icon. Avaya Browser Extension does not highlight telephone numbers on blocked websites.

After you add any website to the blocked websites in the registry, Avaya Browser Extension blocks all websites where the hostname equals the hostname of the blocked website.

Note:

Users can manually block websites by going to the Country selection menu in the browser and then clicking **General** > **Disable**. Users can see the websites that you have blocked in the registry.

Procedure

1. In the Windows registry, update the group policy as follows:
   - For 64–bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AVAYA\Collaboration\BlockedHost
   - For 32–bit: HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\Collaboration\BlockedHost
2. Create a new value name with the `REG_SZ` type.
3. In **Value name**, type the site address.
4. In **Value data**, type `Blocked`.
5. To apply the new configuration, close all the open browsers.

Unblocking websites using the group policy

About this task

Using the group policy, you can unblock websites. Avaya Browser Extension highlights telephone numbers on websites that are unblocked.

Procedure

1. In the Windows registry, update the group policy as follows:
   - For 64–bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AVAYA\Collaboration\BlockedHost
   - For 32–bit: HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\Collaboration\BlockedHost
2. Remove the site address (value name) that you want to unblock.
3. To apply the new configuration, close all the open browsers.

IPv6 and ANAT configuration

To enable dual stack network on Wi-Fi, the router must support IPv6 advertisement.

You must configure the following parameters so that Avaya Workplace Client can support IPv6 and Alternative Network Address Type (ANAT) in a dual stack environment:

- SIGNALING_ADDR_MODE
- MEDIA_ADDR_MODE
- SIP_CONTROLLER_LIST

ANAT mechanism helps to achieve media level interworking between IPv4 and IPv6.

Parameter name	Required for non-ANAT deployment	Required for ANAT deployment	Allowed values
SIGNALING_ADDR_MODE	Yes	Yes	4 or 6
MEDIA_ADDR_MODE	No	Yes	4 or 6 - Disables ANAT capability 46 or 64 - Enables ANAT capability
SIP_CONTROLLER_LIST	Yes	Yes	Examples:

Parameter name	Required for non-ANAT deployment	Required for ANAT deployment	Allowed values
			• "proxy1:5555;transport=tls,proxy2:5556;transport=tls" • "135.20.247.77:5555;transport=tls,135.20.247.87:5556;transport=tls" • "[2007:7::5054:ff:fe35:c6e]:5060;transport=tcp, [2007:7::5054:ff:fe80:d4b0]:5060;transport=tcp"

Note:

To enable dual stack network deployments on clients, you must configure SIP_CONTROLLER_LIST with FQDN, which must resolve to both IPv4 and IPv6 address.

Configure the following values on Avaya Workplace Client:

Network	SIGNALING_ADDR_MODE	MEDIA_ADDR_MODE
Single stack client	4	4
	6	6
Dual stack client	4	4
	6	6
	4	46
	6	64

Note:

The MEDIA_ADDR_MODE value in the settings file must match the configuration of media address mode on System Manager. This setting is available in Device Group settings.

Configuring Avaya Aura Communication Manager to support IPv6 and ANAT

About this task

For complete information about how to perform these steps, see Avaya Aura® Communication Manager documentation.

Procedure

- If you are using vCenter to deploy Communication Manager OVA, then configure **IPv6 Address**, **Prefix**, and **Gateway** details during deployment of ovf.
  After Communication Manager is up, use ifconfig to verify whether eth0 has IPv6 address.
- If you are using the vSphere client/ESXi web page to deploy Communication Manager, then you must configure the IPv6 address on Communication Manager from the Communication Manager SMI page.
  1. Configure Communication Manager IPv4 address on the first boot of Communication Manager after deployment.
  2. Log in to the Communication Manager SMI page using IPv4 address.
  3. Navigate to **Administration** > **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
  4. In the **IPv6 is currently** field, click **Enabled**.
     This enables the text boxes where you can configure the IPv6 address details.
  5. Configure **IPv6 Address**, **Prefix**, and **Gateway** for eth0 and eth1(simplex)/eth2(duplex) if OOB is enabled, and click **Change**.
     If required, restart Communication Manager.
  6. Reboot Communication Manager from the OS level.
  7. After Communication Manager is up, use ifconfig to verify whether eth0 has IPv6 address.

- Go to the Communication Manager SAT interface and do the following:
  1. Run the add ip-int procr command to deploy a new instance of Communication Manager or run the change ip-int procr command to enable IPv6 on existing Communication Manager.
  2. Go to page #2 and configure **Enable Interface?** to **Y**.
  3. Submit the form.

- Enable ANAT on system-parameters ip-options and ip-network-region forms.
- Configure IPv4 and IPv6 in the ip-codec-set form.
- Configure IPv4 and IPv6 IPs to media resource for Media Gateway and Avaya Media Server.
- Ping the IPv6 address of Communication Manager by using the **ping6** command from another IPv6 enabled system to verify that Communication Manager is accessible on the network.
- Add the IPv6 address of Communication Manager in SIP entity and select the IP tolerance flag.

Configuring Avaya Aura Session Manager to support IPv6 and ANAT

About this task

For complete information about how to perform these steps, see *Administering Avaya Aura® Session Manager*.

Procedure

1. On the System Manager web console, in **Elements**, click **Routing** > **SIP Entities**.
2. Click the Session Manager SIP entity for which you need to configure the IPv6 address.
3. Configure the following:
   a. **IP Address Family** to **Both** if configuring dual stack, or select **IPv6** for v6 only entity.
   b. Configure a valid IPv6 address.
      This IPv6 address is the asset IP of Session Manager.
   c. Click **Commit**.
4. Ping the IPv6 address of Session Manager by using the ping6 command from another IPv6 enabled system to verify that Session Manager is accessible on the network.
5. Configure the SIP entity link between Communication Manager and Session Manager, select the IP address family as IPv6.
6. To make calls in a dual stack network, enable ANAT on system-parameters ip-options and ip-network-region forms and configure IPv4 and IPv6 in the ip-codec-set form.
7. To get media channels on the IPv6 network, configure IPv6 IP for Media Gateway and Avaya Media Server.
   a. Create Avaya Media Server SIP sig group with IPv6 IP.

b. Configure IPv4 and IPv6 IP for Media Gateway Controller (MGC) on Media Gateway.

Configuring Avaya Aura Session Border Controller to support IPv6 and ANAT

About this task

For complete information about how to perform these steps, see *Administering Avaya Session Border Controller*.

Note:

Media unanchoring is not supported with IPv6. Media unanchoring is used to enhance bandwidth usage for endpoints within the same subnetwork and to allow direct media to flow between these endpoints.

Procedure

- Provision the IPv6 address in the signaling address interface.
- Ensure that the media interface has primary and secondary interface publishing both IPv4 and IPv6 addresses.
- Enable the **Tolerant** field in the server flow.
- To enable ANAT for media rules, on the Media Rules screen, in the Advanced tab, select the **ANAT Enabled** check box.
- Configure the following in the Endpoint flow screen:
    - On the Add Subscriber Flow Profile screen, in the **Secondary Media Interface** field, click the secondary media interface option to be used for this Server End Point Flow.
    - On the Add Server Flow screen, specify **Media Interface** and **Secondary Media Interface**.
      Media Interface is a drop-down menu from which you select the media interface to be used for this Server End Point Flow. Select the internal or external media interface depending upon the direction of the flow of traffic.
      Secondary Media Interface is a drop-down menu from which you select the secondary media interface to be used for this Server End Point Flow.

SSO with OAuth and SAML

Avaya Workplace Client supports SSO with Open Authorization (OAuth) and Security Assertion Mark-up Language (SAML).

Note:

Avaya Workplace Client on Avaya Vantage™ does not support SSO with OAuth and SAML.

Use this feature to integrate Avaya Workplace Client SSO with a supported enterprise Identity Provider (IDP) solution for authentication, including multi-factor authentication. Services included with the solution are Avaya Aura® Device Services Release 8.0 and later and the Avaya Multimedia Messaging service on Avaya Aura® Presence Services Release 8.1 and later.

Note:

If you change the IDP and perform user deletion in Keycloak, you must instruct users to reset the Avaya Workplace Client application on all platforms. For example, if a user uses the Windows and Android clients but resets only the Windows client, the user continues to receive the Authorization Unavailable error.

A user can log in using OAuth and SAML and get an SSO experience for:

- Voice service: Avaya Aura® Device Services provides the SIPSHA1 token
- Services provided by Avaya Aura® Device Services, including automatic configuration, contacts, and enterprise search
- Presence using SIP
- Avaya Multimedia Messaging service on Avaya Aura® Presence Services
- Avaya Aura® Web Gateway for Apple Push Notifications
- Avaya Equinox® Conferencing
- Exchange Web Services

The SCEP certificate installation service does not use the OAuth and SAML login flows.

The following services continue to use the existing authentication methods with individual sign-on or unified login with a shared Avaya Workplace Client credential:

- Client Enablement Services
- Standalone Avaya Multimedia Messaging

Avaya Spaces login continues to use the Avaya Cloud Accounts login. Further integration is planned for a future release.

To configure Avaya Workplace Client to use OAuth for the Avaya Aura® Device Services configuration service, you must append the configuration URL with the preferredAuth property. This property directs the Avaya Aura® Device Services configuration service not to provide the user name and password authentication. By default, Avaya Workplace Client provides the user name and password authentication for backward compatibility, unless there is a single authorization mechanism returned to Avaya Workplace Client.

The preferredAuth property directs Avaya Aura® Device Services to return a single authorization mechanism. Also, `bearer` indicates that OAuth is supported.

After Avaya Workplace Client downloads the configuration, the provider SSO parameters direct Avaya Workplace Client on which authorization credential is required for the provider.

You can configure the following parameters for SSO with OAuth:

- AUTOCONFIG_USESSO: 3. Indicates that the automatic configuration credentials are the same as the Avaya Authorization Service credentials.
- ESMSSO: 3. Indicates that Avaya Multimedia Messaging uses Avaya Authorization Service.
- ACSSSO: 3. Indicates that Avaya Aura® Device Services uses Avaya Authorization Service.
- EWSSSO: 4. Indicates that EWS uses Microsoft Modern Authentication.
- UNIFIED_PORTAL_SSO: 3. Indicates that Unified Portal uses Avaya Authorization Service.
- AVAYA_AUTHORIZATION_REALM: This parameter identifies the OAuth realm for UC Services integrating with Avaya Authorization Service.

For more information on these parameters, see the chapter on Automatic configuration.

For example, if the Avaya Aura® Device Services server is provisioned to support Avaya Authorization Service (KeyCloak) and Avaya Breeze Authorization Service, you must provision the AVAYA_AUTHORIZATION_REALM property for Avaya Workplace Client. Note that Avaya Workplace Client is configured to use Avaya Authorization Service.

The realm that you provision in the AVAYA_AUTHORIZATION_REALM property must match with that provisioned on the resource server. Examples of resource servers include Avaya Aura® Device Services, Avaya Multimedia Messaging service on Avaya Aura® Presence Services, and Avaya Aura® Web Gateway. Avaya Workplace Client supports a single realm for all the UC Application Resource servers. The default realm on Avaya Aura® Device Services is SolutionRealm. Failure to provision the AVAYA_AUTHORIZATION_REALM property might result in inconsistent loss of service for Avaya Workplace Client.

For more information about OAuth with Avaya Aura® Device Services, see the “OAuth2 management with the Keycloak administration portal” chapter in the *Administering Avaya Aura® Device Services* document.

Note:

If you are using the OAuth server for automatic configuration of Avaya Workplace Client, ensure that TLS 1.3 is enabled on Avaya Aura® Session Border Controller.

Configuration for Over the Top deployments

This chapter describes the configuration of Avaya Workplace Client settings in an Over the Top (OTT) deployment.

If you do not have Avaya Aura® in your configuration, OTT deployment is mandatory to use Avaya Workplace Client.

Complete client and server configuration before configuring the appropriate functionality.

Client and server configuration

Client and server requirements

Component	Requirement
Supported clients	• Avaya Workplace Client on mobile platforms • Avaya Workplace Client on desktop platforms • Avaya Workplace Client conference portal
Supported servers	• Avaya Session Border Controller • Avaya Equinox® Conferencing • Unified Portal • Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Client configuration

DNS auto discovery

DNS auto discovery is mandatory to support Avaya Workplace Client in the OTT deployment.

Automatic configuration settings

The automatic configuration parameters included in the following table are provided by the Portal auto configure service to support Avaya Workplace Client in the OTT deployment. The table includes the recommended values. For complete information about these parameters, see the chapter on Automatic configuration.

Automatic configuration parameter	Recommended value	Notes
UNIFIED_PORTAL_SSO	1	Clients can use the enterprise user name and password to sign in to the Avaya Workplace Client conference portal.
SUPPORTWINDOWSAUTHENTICATION	0	The Portal only supports Kerberos, not NTLM. Therefore, ensure that you do not enable this parameter if NTLM is used.
BFCP_UDP_MINIMUM_PORT	5204	—
BFCP_UDP_MAXIMUM_PORT	5224	—
RTP_PORT_LOW	5004	Change this parameter value depending on the firewall port ranges.
RTP_PORT_RANGE	200	—
APPCAST_CHECK_INTERVAL	1	—
EWSENABLED	1	EWS is mandatory to support the Top of Mind feature in SDC replacement clients.
EWSSSO	1	Clients can use the enterprise user name and password to authenticate with EWS.
EWSSERVERADDRESS	Enter the EWS server address.	—

Automatic configuration parameter	Recommended value	Notes
EWSDOMAIN	Enter the EWS server FQDN.	—

Server configuration

Server external access

The following table includes the list of servers that can be accessed externally through Avaya Session Border Controller or Third-Party Reverse Proxy:

Server	TLS traffic	Internal Avaya Aura® users	External guest users	Server certificates signed by third-party CA	Mutual authentication on the server for internal traffic	Mutual authentication on SBC or Reverse Proxy for external traffic
Avaya Aura® Web Gateway or Unified Portal	HTTPS	Yes	Yes	Mandatory	Disabled	Disabled
Equinox Conference Control	HTTPS	Yes	Yes	Mandatory	Disabled	Disabled
WCS	HTTPS	Yes	Yes	Mandatory	Disabled	Disabled

Split Horizon DNS

Avaya recommends the use of split horizon DNS so that the same FQDN is used for any server by both the internal and external clients. The benefits are:

- Administration of the overall system is simplified.
- Single settings file can serve both the internal and external clients.
- Hair-pinning of WCS and Equinox Conference Control traffic by the internal Avaya Workplace Client native clients through SBC is removed.

Server certificate and mutual authentication

Servers that need to support guest access require third-party, CA-signed certificates. This includes Avaya Aura® Web Gateway, Equinox Conference Control, and WCS. Disable mutual authentication on SBC for external access to these servers.

Do not use IP address in the CN/SAN field of the certificates.

User Portal and Web Gateway settings on Avaya Equinox® Management

Avaya recommends that you retain the default value of Client Ranking as Equinox Desktop Client, Equinox Mobile Client, and Web Client. This enables the portal to open Avaya Workplace Client with a higher priority than the Web Client.

Contacts and enterprise search functionality configuration

Users can use Avaya Workplace Client to search for and connect with other users in their enterprise. Avaya Workplace Client can connect directly to LDAP to manage enterprise search.

If Avaya Spaces is configured, users can search for enterprise contacts from the Avaya Spaces directory as Avaya Aura® Device Services is disabled in OTT deployments.

Supported LDAP directories for Avaya Workplace Client

LDAPv3 support

Only desktop clients have direct connectivity to LDAP. On mobile platforms, users can perform an LDAP search by using Microsoft ActiveSync if it is provisioned.

Note:

On Avaya Workplace Client for iOS, to use a Gmail account for an LDAP search using Microsoft ActiveSync, you must provision the Gmail account as Exchange account type. If you add another Exchange account with Gmail, Avaya Workplace Client can search contacts from both the Exchange and Gmail accounts.

This section describes LDAP support for Avaya Workplace Client that connect to an LDAP directory directly.

Avaya Workplace Client supports LDAPv3, which includes standard LDAP and secure LDAP, with Microsoft Active Directory. Avaya Workplace Client on desktop platforms also support Novell eDirectory and IBM® Lotus

Domino. For more information about supported directory versions for each Avaya Workplace Client, go to https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml and select the appropriate Avaya Workplace Client.

Note:

The default directory type used by Avaya Workplace Client on desktop platforms is Microsoft Active Directory. If you want to use any other directory type, you must set the DIRTYPE parameter using the settings file. For information about the automatic configuration options, see the chapter on Automatic configuration.

You can set up the LDAP server by using an FQDN or an IP address.

Search attributes

During an LDAP search, Avaya Workplace Client searches the following attributes:

- cn: Common name, that is, First name plus Last name
- sn: Last name
- givenName: First name
- displayName: Display name

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

After the search, Avaya Workplace Client constructs the name by using the sn and givenName attributes.

If a user adds a contact who is already an enterprise contact as an Avaya Workplace Client 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 local contact. The enterprise contact photo takes precedence over the local contact photo.

Avaya Equinox Conferencing functionality configuration

Use the procedures in this chapter to configure the Avaya Equinox® Conferencing functionality. All functionality is applicable to both UC and OTT deployments, unless explicitly specified.

Checklist for configuring Avaya Equinox Conferencing functionality

The following checklist outlines the high-level setup and configuration tasks for Avaya Equinox® Conferencing functionality. Configure the functionality according to your requirement.

Functionality	Reference	✔
Custom branding logo	• Custom branding logo • Configuring the Avaya Equinox Management server for custom branding logo	
Adhoc conferencing	• Adhoc conferencing by using Avaya Workplace Client • Configuring the Avaya Equinox Management server for adhoc conferencing • Configuring the Avaya Equinox Management server for limiting the sharing capability	
Conference access controls	Conference access controls using Avaya Workplace Client	
Slider	• Slider in Avaya Equinox Conferencing	

Functionality	Reference	✔
	- Configuring the Avaya Equinox Management server for the Slider functionality	
Chat	Configuring the Avaya Equinox Management server for disabling the chat capability	
Personal layout	Configuring the Avaya Equinox Management server for disabling the personal layout capability	
Conference PIN policy	Configuring the Avaya Equinox Management server for the conference PIN policy	
Enable or deny participants to unmute self in a conference	Configuring the Avaya Equinox Management server to enable or deny participants to unmute self in a conference	
Multi-stream switching	- Multi-stream switching with Avaya Equinox Conferencing - Configuring the Avaya Equinox Management server for Multi-stream switching	
Dial-in information	Avaya Equinox Conferencing dial-in information	
Dial-out information	- Avaya Equinox Conferencing dial-out information - Configuring the Avaya Equinox Management server for the Avaya Equinox Conferencing dial-out information	

Functionality	Reference	✔
Avaya Mobile Link	• Avaya Mobile Link • Configuring the XT endpoint for Avaya Mobile Link	
HTTP tunneling	• HTTP tunneling • Configuring initial settings on Avaya SBC • Creating a new policy group with video enabled • Creating a load monitoring profile on Avaya SBC • Managing server flow configuration on Avaya SBC • Configuring Avaya Session Border Controller in Avaya Aura Web Gateway • Avaya SBC connectivity status indicators • Configuring Avaya Session Border Controller in Avaya Equinox Management • External access configuration • Configuring Avaya Aura Web Gateway for external users access • Configuring TLS for Avaya SBC by using System Manager • Configuring reverse proxy on Avaya SBC	

Functionality	Reference	✔
HTTP proxy configuration	HTTP proxy configuration	

Custom branding logo

Custom branding logo

When joining the Avaya Workplace Client meeting, Avaya Workplace Client can display the custom branding logo in the splash screen only when the logo is configured in Avaya Equinox® Management.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Equinox® Conferencing
- Unified Portal
- Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Configuring the Avaya Equinox Management server for custom branding logo

Procedure

In **Settings** > **Advanced** > **Branding**, upload the custom logo image as part of the ACBranding.zip file.

Adhoc conferencing by using Avaya Workplace Client

Adhoc conferencing by using Avaya Workplace Client

Users can create an Avaya Workplace Client adhoc conference by using Avaya Equinox® Conferencing in the following ways:

- Merge two point-to-point (P2P) calls.
  A P2P call refers to a communications connection between two communication endpoints.
- Add a new participant to an existing P2P call.
- Create a conversation by dialing the numbers of multiple participants at the same time.
- Start sharing while on a P2P call on desktop platforms.
- Escalate a multi-party chat to an audio or video conference call.

Note:

You cannot use Avaya Workplace Client to make adhoc conference calls in an OTT deployment.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Equinox® Conferencing
- Unified Portal

- Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Avaya Workplace Client setting

The adhoc conference address in Avaya Workplace Client at **Services** > **Phone Service** > **Adhoc Conference Address** must match the Avaya Equinox® Management server's **Conference Factory URI for SIP Adhoc Conferencing** value. For example, 816543@avayamcs.com.

Automatic configuration settings

You must include the adhoc conference URL in the CONFERENCE_FACTORY_URI parameter.

Configuring the Avaya Equinox Management server for adhoc conferencing

Procedure

- In **Settings** > **Meetings** > **Policies** > **Conference Factory URI for SIP Adhoc Conferencing**, set a value for the factoryURI property.
  For example, `816543@avayamcs.com`.
- In Advanced Parameters, set a value for the vnex.vcms.core.conference.defaultDomain property.
  For example, `avayamcs.com`.
- In Advanced Parameters, set the value for the vnex.vcms.core.conference.enableDialoutAsSIP property as `true`.
- **Optional** If multiple Outbound SIP servers are defined in the Avaya Equinox® Management server, you can specify one server by going to **Settings** > **Meetings** > **Policies** > **Default SIP Domain**.
  The default value is the domain of the first SIP server configured in Avaya Equinox® Management. You can change the value to whichever SIP server you want to use for outbound calls.

Configuring the Avaya Equinox Management server for limiting the sharing capability

About this task

Use this procedure to configure the sharing capability for Avaya Equinox® Conferencing users.

Note:

This feature is supported only on OTT deployments.

Procedure

1. Go to **Settings** > **Users** > **Policies** > **User Policies**.
2. In the Enable sharing for area, select one of the following:
    - **Everyone**: All users can share content.
    - **Moderator and registered users**: Only the moderator and registered users can share content.
    - **Moderator only**: Only the moderator can share content.
3. Save the changes.

Conference access controls using Avaya Workplace Client

To access a conference, users can enter the meeting PIN and use the Knock on Door feature through the UCCP connection.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Equinox® Conferencing
- Unified Portal
- Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Slider in Avaya Equinox Conferencing

Slider in Avaya Equinox Conferencing

Use this feature to view the presentation content that was presented previously during the meeting. The Slider feature provides navigation keys at the top of the screen, above the presentation content.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms
- Avaya Workplace Client conference portal

Supported servers

- Avaya Equinox® Conferencing
- UCCS

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Configuring the Avaya Equinox Management server for the Slider functionality

Procedure

In **Settings** > **Meetings** > **Meeting Types**, configure the **Enable Slider** check box.

Configuring the Avaya Equinox Management server for disabling the chat capability

About this task

If you use this procedure to disable the chat capability, Avaya Workplace Client users cannot view the chat option when they join a conference as a moderator or participant.

Procedure

1. Go to **Settings** > **Meetings** > **Policies**.
2. To disable the chat capability, clear the **Conference Chat** check box.

3. Save the changes.

Configuring the Avaya Equinox Management server for disabling the personal layout capability

About this task

If you use this procedure to disable the personal layout capability, Avaya Workplace Client users who join a conference as participants cannot view the option to customize the video layout. However, moderators can view the option to customize the video layout.

Procedure

1. Go to **Settings** > **Meetings** > **Policies**.
2. To disable the personal layout capability, clear the **Personal Layout** check box.
3. Save the changes.

Configuring the Avaya Equinox Management server for the conference PIN policy

About this task

Use this procedure to configure the virtual room with a one-time PIN. You can specify the minimum number of digits the moderator or virtual room owner must enter as a PIN. Avaya Workplace Client displays an error message if the moderator or virtual room owner enters fewer digits than the configured number.

Note:

Users can also configure the virtual room with a one-time PIN using the meeting portal. Users can enter a maximum of 16 digits as the PIN.

Procedure

1. Go to **Users** > **Users from Active Directory** > **All**.
2. Click the link in the **Name** column for the user you require.
3. Enter the user ID and last name in the relevant fields.
4. Click the **Virtual Room** tab.
5. To protect meetings using this virtual room, select the **Protect meeting with a PIN** check box.
6. Click **Use one-time PIN for each meeting**.
7. Save the changes.
8. Go to **Settings** > **Meetings** > **Policies**.
9. In **Meeting PIN minimum length**, enter the minimum number of digits required for the meeting PIN.
10. In **Moderator PIN minimum length**, enter the minimum number of digits required for the moderator PIN.
11. Save the changes.

Configuring the Avaya Equinox Management server to enable or deny participants to unmute self in a conference

About this task

You can choose whether participants in a conference can only listen to the moderator or unmute and speak.

Procedure

1. Go to **Settings** > **Meetings** > **Policies**.
2. To enable participants to unmute and speak in the conference, select the **Participants Can Unmute** check box.

3. Save the changes.

Multi-stream switching with Avaya Equinox Conferencing

Multi-stream switching with Avaya Equinox Conferencing

Avaya Workplace Client on desktop platforms support Multi-stream switching (MSS) when the user is connected to an Avaya Equinox® Conferencing-based meeting if Avaya Workplace Client is configured for switching. Avaya Workplace Client can render up to four streams of video based on screen real-estate, connection quality, and decoding capability of the underlying device.

Supported clients

- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Equinox® Conferencing
- Unified Portal
- Avaya Aura® Web Gateway
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Automatic configuration settings

ENABLE_MSS_VIDEO

By default, this parameter is enabled. For Unified Communications deployments, you can disable this feature.

Note:

In Unified Communications deployments, if you enable BFCP in Avaya Workplace Client to work with third-party video systems, you must disable MSS in Avaya Workplace Client. This is due to an Avaya Aura® limitation.

VIDEO_MAX_BANDWIDTH_ANY_NETWORK

In Unified Communications deployments, you must set the Avaya Workplace Client video bandwidth by using this parameter. This value must not exceed the video bandwidth in both the Session Manager location bandwidth and the Communication Manager network region bandwidth.

For example, you set the following:

- Communication Manager network region bandwidth to `y`
- Session Manager location bandwidth to `z`
- VIDEO_MAX_BANDWIDTH_ANY_NETWORK to `x`

In this case, you need to ensure that
`x=<y-64`
and
`x=<z-64`
, where 64 is the audio bandwidth. To support the MSS functionality, Avaya recommends that you set y=z.

Relationship between VIDEO_MAX_BANDWIDTH_ANY_NETWORK and maximum number of received video streams supported

VIDEO_MAX_BANDWIDTH_ANY_NETWORK	Maximum number of received video streams supported
>=512	4
>=384	3
>=256	2
>=128	1

Recommended VIDEO_MAX_BANDWIDTH_ANY_NETWORK value

To support the four receiving video streams with 360p each, Avaya recommends the following bandwidth values:

Component	Setting	Value
Avaya Workplace Client	VIDEO_MAX_BANDWIDTH_ANY_NETWORK	1280
Communication Manager	Network region bandwidth per call	1344
Session Manager	Location bandwidth per call	1344

Unified Portal configuration

Users can set their virtual room meeting type to MSS from the Avaya Equinox® Conferencing user portal if you have defined the MSS meeting type.

Configuring the Avaya Equinox Management server for Multi-stream switching

Procedure

1. To configure the MSS meeting type, go to **Settings** > **Meetings** > **Meeting Types**.
2. To assign a virtual meeting room type to MSS, go to **Users** > **Users from Active Directory** > **All** > **Virtual Room**.

Avaya Equinox Conferencing dial-in information

Users can get the conference dial-in information during a meeting, for example, in the presentation-only mode.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms
- Avaya Workplace Client conference portal

Supported servers

- Avaya Session Border Controller
- Avaya Equinox® Conferencing
- Unified Portal
- Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Avaya Equinox® Management server configuration

Configure the Meeting Invitations in simple HTML without buttons and tables so that the Avaya Equinox® Management server can convert HTML into text version correctly for Avaya Workplace Client dial-in display.

On Avaya Equinox® Management server, configure the **Location** field by going to **Settings** > **Meetings** > **Invitations**. You can use one of the following options:

- If you did not configure the PSTN dial-in variables and do not want to include any preferred PSTN dial-in number in the **Location** field, set location in different languages to https://PortalFQDN/portal/tenants/default/?ID=[E164].
- If you configure the PSTN dial-in variables and want to include any preferred PSTN dial-in number in the **Location** field, set location in different languages to https://PortalFQDN/portal/tenants/default/?ID=[E164] || [DIAL-IN-LABEL]: [DIAL-IN-STRING].

You must configure the invitation template in HTML and TXT format.

Example of an invitation template in HTML format

Note:

Use hyperlink for URL and phone numbers.

You have been invited to an Avaya Workplace Meeting: [**VIRTUAL_ROOM_NAME**]

Conference information

Meeting ID: [MEETING_ID][PIN_START]

Meeting PIN: [PIN][PIN_END]

Join by Video Conference System

Dial the Meeting ID[PIN_START] followed by the Meeting PIN[PIN_END]

Join by Phone

Use one of the numbers below and if prompted enter the Meeting ID[PIN_START] and PIN[PIN_END]

New York: +1-212-555-5000

London: +44-020-7946-0500

Example of an invitation template in TXT format

```
Join the Meeting

[DESKTOP_MOBILE_ACCESS_LINK]

 Meeting ID: [MEETING_ID][PIN_START]
 Meeting PIN: [PIN][PIN_END]

Join by Phone

Use one of the numbers below and if prompted enter the Meeting ID[PIN_START]
and PIN[PIN_END]

 New York: +1-212-555-5000
 London: +44-020-7946-0500
```

Avaya Equinox Conferencing dial-out information

Avaya Equinox Conferencing dial-out information

Users can dial out of a conference in the following use cases:

- Join a meeting in presentation-only mode by using a call back number.
- Add a participant during the meeting by using a call back number. Only a moderator can do this.

The call back number can be an E.164 number, a terminal number, or a room system IP address.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms
- Avaya Workplace Client conference portal

Supported servers

- Avaya Equinox® Conferencing
- Unified Portal
- Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Configuring the Avaya Equinox Management server for the Avaya Equinox Conferencing dial-out information

Procedure

- Configure the vnex.vcms.core.conference.defaultDomain parameter.
  - UC deployment: If the dial out calls need to be routed through Avaya Aura®, you can set the parameter to the Avaya Aura® SIP domain.
  - OTT deployment: If you are using the SIP server to dial out, you can set the parameter to the SIP server domain.
- Configure the vnex.vcms.core.conference.enableDialoutAsSIP parameter.
  - UC deployment: If the dial out calls need to be routed through Avaya Aura®, you can set the parameter to True.
  - OTT deployment: If you are using the SIP server to dial out, you can set the parameter to True.
  - OTT deployment: If you are using the H.323 gateway to dial out, you can set the parameter to False.
- Configure the com.vcms.conference.dialout.enabled parameter.
  - UC deployment: If you set this parameter to false, the conferencing server disallows any dial out.
  - OTT deployment: If you set this parameter to false, the conferencing server disallows any dial out.

To dial out, Avaya Equinox® Management must include minimum one configured outbound SIP server. The domain of the first outbound SIP server is the default domain.

- If not configured, you can configure a policy for outbound SIP messaging in **Settings** > **Meetings** > **Policies** and select one of the SIP servers.

The default is the first SIP server.

Avaya Mobile Link

Avaya Mobile Link

Users connected on a video conference can use Avaya Mobile Link to transfer the video conference onto an XT Series endpoint. Users can transfer the video conference without connecting the mobile or desktop device to the endpoint with a cable. The XT Series endpoint is used for audio, video, and presentation of the meeting. Avaya Equinox® Conferencing continues to run on the device in the Companion mode to support moderation and chat. Companion mode includes everything except the audio and video capture and rendering features.

With Avaya Mobile Link, users can enjoy the XT Series endpoint’s crystal-clear audio, HD camera, and large display during a video conference.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms
- XT system

Supported servers

- Avaya Session Border Controller
- Avaya Equinox® Conferencing
- Unified Portal
- Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Avaya Equinox® Management server configuration

If you are connected to the Avaya Workplace Client 9.0.2 meetings, Avaya Workplace Client can only initiate Mobile Link with XT endpoints that are managed by the same Avaya Equinox® Management server. The XT endpoints can register as SIP or H.323. The following XT endpoints cannot connect with Mobile Link:

- Non-managed or non-registered XT endpoints
- Remote XT endpoints: A guest to the meeting from a remote organization cannot pair with the local XT because that XT is remote to the Avaya Equinox® Management server.

All supported XT endpoints must be in the same network as the Avaya Equinox® Management server without going through any proxy. If Avaya SBC instances are deployed with Avaya Equinox® Conferencing, ensure that the following Avaya Equinox® Management advanced settings are set as:

- com.radvision.airpair.forceuseproxyIP=true
- com.radvision.airpair.proxyIP=x.x.x.x
  where x.x.x.x is the Avaya Equinox® Management server's IP address.

Configuring the XT endpoint for Avaya Mobile Link

About this task

Use this procedure to configure the SIP or H.323 registered XT endpoint for Avaya Mobile Link.

Procedure

1. Open the Avaya Equinox® Management administrator portal.
2. Click the **Endpoints** tab.
3. Choose the endpoint that you want to configure.
4. Click the **Advanced Configuration** tab.
5. In the Remote Access area, in the **Mode** field, click one of the following:
   - **Enable - No PIN**: Users can automatically access the endpoint remotely without a PIN.
   - **Enable - Ask PIN (Manual Pairing)**: Users must enter a PIN only while accessing the endpoint manually.
   - **Enable - Ask PIN (Always)**: Users must enter a PIN while accessing the endpoint remotely.
6. Click **Apply**.

HTTP tunneling

Use the HTTP tunneling feature to set up a media connection over TLS for users calling from external networks through Avaya SBC. A firewall exists in between that blocks UDP(RTP) ports.

If a guest user tries to join a remote conference in the UC deployment, HTTP-UA is used and HTTP tunneling is supported through Avaya SBC. If the Avaya Workplace Client conference is in the OTT deployment, then signed-in or guest users join the meeting through Avaya SBC, which uses HTTP-UA and supports HTTP tunneling.

Note:

- Media interworking is not supported for HTTP tunneled calls.

- BFCP is not supported in HTTP tunneling. However, BFCP is supported in the HTTP-UA non-tunneled case.

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Session Border Controller
- Avaya Equinox® Conferencing
- Unified Portal
- Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Automatic configuration settings

You must enable the HTTP tunneling feature by using the ENABLE_MEDIA_HTTP_TUNNEL parameter. If the UDP ports are blocked by external firewalls and a user joins the meeting through Avaya SBC where HTTP media tunneling is enabled, the media in the conference call uses TLS.

Configuring initial settings on Avaya SBC

About this task

Use this procedure to perform the initial configuration on Avaya SBC. On Avaya Aura® Web Gateway, you must also enable remote access and perform reverse proxy configuration as described in the sections under External access configuration.

Before you begin

Get Avaya SBC Release 7.2. Apply the Release 7.2 patch for Media Tunneling for the solution to work correctly.

Procedure

1. Log in to the Avaya Session Border Controller web administration portal: `https://<Management_Interface>/sbc/`.
2. Go to **Device Specific Settings** > **Network Management** > **Network** and ensure that the following interfaces are set to minimum:
   - M1: Management interface, which is configured as part of the installation process
   - A1: Internal interface
   - B1: External interface with at least two associated IP addresses
3. Configure certificates for the following nodes:
   a. Avaya Equinox® Management: Use the Avaya Equinox® Management FQDN signed with the same CA as Avaya Equinox® Management.
   b. Avaya Aura® Web Gateway: Use the global FQDN signed with the same CA as Avaya Aura® Web Gateway.
4. Enable the Media Tunneling feature for tunneling support:
   a. Go to **Device Specific Settings** > **Advanced Options** > **Feature Control**.
   b. Select **Media Tunneling**.
   c. Click **Save**.
5. Create the signaling interface:
   a. Go to **Device Specific Settings** > **Signaling Interface** and then click **Add**.
   b. Specify a name for the signaling interface.
   c. Set the IP address to the internal interface (A1).
   d. Set the TCP port to 5060.
   e. Leave the UDP port blank.
   f. Set the TLS port to 5061.
   g. For the TLS profile, select any server profile that you added before.
6. Create the TLS server profile for the external media interface if the Media Tunneling feature is required:
   a. Go to **TLS Management** > **Server Profiles**.
   b. Specify a profile name.
   c. In **Certificate**, select any existing certificate.
   d. Set **Peer Verification** to **Optional**.
   e. Do not select anything for **Peer Certificate Authorities** or **Peer Certificate Revocation Lists**.
   f. Set **Verification Depth** to **1**.
   g. Retain the default values in the other settings.
   h. Click **Next** and then click **Finish**.

7. Configure the external media interface:
   a. Go to **Device Specific Settings** > **Media Interface** and then click **Add**.
   b. Specify a name for the media interface.
   c. Specify the B1 IP address that does not match with the IP address used to redirect requests to Avaya Aura® Web Gateway in the reverse proxy settings.
   This IP address cannot be used for any other interface that uses port 443. It will be used for HTTP tunneling.
   d. Specify the TLS server profile for the media interface if the Media Tunneling feature is required.
   For self-signed certificates on the client, you must use the TLS server profile created for the external media interface.
   e. **Optional** In Avaya SBC 7.2.1 and later, in the **Buffer Size** field, select the buffer size from the list that includes values from 400 to 1000 in KB.
   Avaya SBC stores the specified size of video frames on its network buffer. For example, if you set the value as 400 KB, then Avaya SBC stores approximately 6 seconds of video in a congested network. Avaya SBC drops all video frames beyond this buffer size.

   Note:

   The **Buffer Size** field is visible only if you enable the Media Tunneling feature.
   f. Retain the default values in the other settings.

8. Configure the internal media interface:
   a. Go to **Device Specific Settings** > **Media Interface** and then click **Add**.
   b. Specify a name for the media interface.
   c. Specify the A1 IP address.
   d. Retain the default values in the other settings.

Next Steps

If you require video, or a BFCP or FEC connection for calls, create a policy group with video enabled. Else, configure load monitoring.

Creating a new policy group with video enabled

Procedure

1. To enable video:

   a. On the Avaya Session Border Controller web administration portal, go to the **Domain Policies** > **Application Rules** page.
   b. Clone the existing application rule or add a new rule.
   c. Enable In/Out Audio/Video application types, and specify maximum concurrent sessions and maximum sessions for each endpoint.

2. To configure media encryption and enable BFCP or FEC:
   a. Go to **Domain Policies** > **Media Rules**.
   b. Clone the existing media rule or add a new media rule.
   c. On the Encryption tab, in **Miscellaneous**, set the **Capability Negotiation** flag.
   d. Switch to the **Advanced** tab and set the **BFCP Enabled** and **FECC Enabled** flags.

3. Go to **Domain Policies** > **End Point Policy Group**.
   a. Clone the existing policy group or add a new policy group.
   b. Specify the created application rule and media rule for the policy group.

Creating a load monitoring profile on Avaya SBC

About this task

Use this procedure to configure load monitoring on Avaya SBC.

Before you begin

Configure the initial settings.

Procedure

1. On the Avaya Session Border Controller web administration portal, go to **Device Specific Settings** > **Advanced Options** > **Load Monitoring**.
2. Click **Add** and do the following:
   a. Set **Load Balancer Type** to **INTERNAL**.
   b. Set **Load Balancer IP** to the IP of the Avaya Aura® Web Gateway server.
      In case of cluster configuration, add load monitoring profile for each cluster node.

c. Set **Load Balancer Port** to 80 for TCP or 443 for TLS.
d. **Optional** If you are using TLS, in **TLS Profile**, select an Avaya Aura® Web Gateway profile.
e. In **Listen IP**, enter the internal interface (A1) address.
f. Click **Finish**.

Next Steps

Configure server flows on Avaya SBC.

Managing server flow configuration on Avaya SBC

About this task

Use this procedure to manage the server flow for the Avaya Aura® Web Gateway and Avaya Equinox® Management servers.

Procedure

1. On the Avaya Session Border Controller web administration portal, go to **Global Profiles** > **Server Configuration**.
2. Click **Add** and do the following:
   a. Set **Server Type** to **Trunk Server**.
   b. **Optional** In **TLS Client Profile**, select the previously created Avaya Aura® Web Gateway client profile if the TLS port is specified.
   c. Add the Avaya Aura® Web Gateway FQDN with the port and protocol specified: TCP or TLS.
      All cluster nodes must be added.
   d. Retain the default values in the other settings.

3. To complete the Avaya Equinox® Management server configuration, do the following:
   a. Set **Server Type** to **Trunk Server**.
   b. **Optional** In **TLS Client Profile**, select the previously created Avaya Equinox® Management client profile if the TLS port is specified.
   c. Add the Avaya Equinox® Management FQDN with the port and protocol specified: TCP or TLS.
   d. Retain the default values in the other settings.

4. Go to **Device Specific Settings** > **End Point Flows** > **Server Flows**.
5. To add a flow for the Avaya Aura® Web Gateway server, do the following:
    a. In **Server Configuration**, select the configuration for the Avaya Aura® Web Gateway server.
    b. Set **Received Interface** to the internal interface (A1).
    c. Set **Signaling Interface** to the internal interface (A1).
    d. Set **Media Interface** to the external interface (B1).
    e. Select the appropriate **End Point Policy Group**.
    f. Retain the default values in the other settings.

6. To add a flow for the Avaya Equinox® Management server, do the following:
    a. In **Server Configuration**, select the Avaya Equinox® Management configuration.
    b. Set **Received Interface** to the internal interface (A1).
    c. Set **Signaling Interface** to the internal interface (A1).
    d. Set **Media Interface** to the internal interface (A1).
    e. Select the appropriate **End Point Policy Group**.
    f. Retain the default values in the other settings.
    g. Click **Finish**.

Configuring Avaya Session Border Controller in Avaya Aura Web Gateway

About this task

Use this procedure only in UC deployments of Avaya Workplace Client.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, go to **External Access** > **Session Border Controller**.
2. Click **Add** to add a new Avaya SBC.
3. Complete the following settings:
    a. In **SIP Address**, type the address of the internal interface specified for signaling on Avaya SBC (A1).
    b. In **SIP Port**, type `5060` if you are using TCP or `5061` if you are using TLS.
    c. In **SIP Protocol**, select **TCP** or **TLS**.
    d. In **HTTP Address**, type the internal address specified for the load monitoring entry (A1).

   e. In **HTTP Port**, type `80` if you are using the HTTP protocol or `443` if you are using the HTTPS protocol.
   f. In **HTTP Protocol**, select **http** or **https**.
   g. In **Location**, specify the location of the Avaya SBC server.
      If SBCs are placed in different location, you must check the location priority configuration on the Location page.
      You need to specify the location for only one node, which is then propagated to all other nodes in the cluster.

4. Click **Save**.

Avaya SBC connectivity status indicators

After you add an Avaya SBC on the Avaya Aura® Web Gateway web administration portal, the connectivity status for that Avaya SBC is also displayed. The following table describes the status indicators:

Status indicator	Description
✅	The server is available and can be used for calls. When you hover over this indicator, additional details, such as audio and video session and Avaya SBC bandwidth, are displayed.
⚠	The server is overloaded and calls cannot be made.
❌	Load monitoring cannot be retrieved for the server.
●	The server status has not been fetched.

Configuring Avaya Session Border Controller in Avaya Equinox Management

About this task

Use this procedure only in OTT deployments of Avaya Workplace Client.

Procedure

1. Access the Avaya Equinox® Management administrator portal.
2. Go to **Devices** > **Devices by Type** > **ASBCE** .
3. Click **Add**.
4. Type the details in the following fields:
   - **Name**
   - **IP Address**
   - **Location**
5. Click **OK**.
6. In the **Name** column, click the link of the ASBCE for which you want to configure the following additional settings:
   - **local SIP IP**: The address of the internal interface specified for Signaling Interface on Avaya SBC (A1).
   - **SIP protocol**: The SIP server protocol, either TCP or TLS.
   - **SIP port**: The port number of the SIP server, either 5060 or 5061.
   - **local HTTP IP**: The internal address specified for the Load Monitoring entry (A1).
   - **HTTP protocol**: The HTTP server protocol, either HTTP or HTTPS.
   - **HTTP port**: The port number of the HTTP server, either 80 or 443.
7. Click **OK**.

External access configuration

This section describes the configuration required to access Avaya Aura® Web Gateway from outside the enterprise network through Avaya Session Border Controller (Avaya SBC), which is located at the edge of the enterprise network.

Important:

Ensure that the front-end port for remote access has been enabled and set as required.

Configuring Avaya Aura Web Gateway for external users access

Procedure

1. Run the following command to open the Configuration utility:

   ```
   app configure
   ```

2. Go to Front-end host, System Manager and Certificate Configuration and set **Override port for remote access** as `y`.
3. Configure **Front-end port for remote access** as a new unassigned port.
   For example, 8444.
4. On the Avaya Aura® Web Gateway administration portal, add the Avaya SBC STUN/TURN Media Relay IP/FQDN and port on the **Server Connections** > **STUN Servers** page.
   External B1 interface or Firewall NAT'd address. For example, address:192.168.109.31 port:3478 by default on Avaya SBC.

Configuring TLS for Avaya SBC by using System Manager

Procedure

1. Log in to the System Manager web console and click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority** > **CA Functions** > **CA Structure & CRLs**.
3. Click **Download PEM file** and get the CRL.
4. Check whether Certificate Profile (SSLServerCertificateProfile) has the following features set:
   - Key Usage: Digital Signature and Key encipherment
   - Extended Key Usage: Server Authentication and Client Authentication
5. Click **RA Functions** > **Add End Entity**.
6. Type the user name and password, and enter relevant information in the following fields:
   - CN: FQDN of the server that must provide TLS support
   - DNS name
   - Certificate Profile: Appropriate key features (SSLServerCertificateProfile)
   - Token: P12 file
7. Click **Add**.
8. In the left navigation pane, click **Public Web**.
9. On the public EJBCA page, do the following:
   a. Click **Enroll** > **Create Keystore**.

   b. On the Keystore Enrollment page, type the user name and password entered while adding the end entity.

10. **Optional** Click **Certificate Chain** and save the .crt file.
11. Set the key length to 4096 bits and click **Enroll**.
12. Save the keystore (.p12) file.
13. Copy the keystore (.p12), trusted chain (.crt), and CRL files to the /home/ipcs/ directory on Avaya SBC.
14. **Optional** Run the following as required:
    - To extract the certificate from the keystore file: openssl pkcs12 -in filename.p12 -out filename.crt -nokeys -clcerts
    - To extract the key from the keystore file: openssl pkcs12 -in filename.p12 -out filename.key -clcerts
    - To convert .crt into the PEM format: openssl x509 -inform der -in filename.cer -out filename.pem
    - To convert .crl into the PEM format: openssl crl -inform der -in filename.crl -out filename.pem
15. Log in to the Avaya SBC EMS web interface with administrator credentials.
16. In the left navigation pane, click **TLS Management** > **Certificates**, and do the following:
    a. Click **Install**.
    b. In the **Type** field, select **Certificate**.
    c. In the **Name** field, type the name of the certificate file.
    d. Select the System Manager PEM file and click **Upload**.

17. **Optional** Do the following:
    a. Click **Install**.
    b. In the **Type** field, select **Certificate Revocation List**.
    c. In the **Name** field, type the name of the certificate file.
    d. Select the System Manager CRL PEM file and click **Upload**.

18. Do the following:
    a. Click **Install**.
    b. In the **Type** field, select **Certificate**.
    c. In the **Name** field, type the name of the certificate file.
    d. Select the .crt file as certificate.
    e. Select the Avaya SBC PEM file as Trusted Chain.
    f. Select the .key file as .key (Upload Key File).
    g. Click **Upload**.

19. Repeat for all required certificates.
20. Go to directory /usr/local/ipcs/cert/key, and type `enc_key filenamepassphrase`.

21. Restart the Avaya SBC server.
22. Create a client profile by using the added certificates:
    a. In the left navigation pane, click **TLS Management** > **Client Profiles**.
    b. Click **Add**.
    c. Specify the profile name.
       For example, AAWG Client TLS.
    d. Select the uploaded certificate from Certificate List.
    e. In **Peer Certificate Authorities**, select the CA certificate.
    f. **Optional** In **Peer Certificate Revocation Lists**, select **CRL**.
    g. Set **Verification Depth** to `1`.
    h. Retain the default values in the other settings.
    i. Click **Next** and then **Finish**.

23. Create a server profile by using the added certificates:
    a. In the left navigation pane, click **TLS Management** > **Server Profiles**.
    b. Click **Add**.
    c. Specify the profile name.
       For example, AAWG Server TLS.
    d. Select the uploaded certificate from Certificate List.
    e. Set **Peer Verification** to **None**.
    f. Retain the default values in the other settings.
    g. Click **Next** and then **Finish**.

Configuring reverse proxy on Avaya SBC

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. In the **Reverse Proxy** tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
    a. In the **Service Name** field, type the reverse proxy profile name.
    b. Select the **Enabled** check box.
    c. In the **Listen IP** field, click the external Avaya SBC IP address.
    d. In the **Listen Port** field, type 443.
    e. In the **Listen Protocol** field, click HTTPS and select the Avaya Aura® Web Gateway Server TLS profile.

f. In the **Server Protocol** field, click HTTPS and select the Avaya Aura® Web Gateway Client TLS profile.
g. In the **Connect IP** field, click the internal IP address.
h. In the **Server Addresses** field, type the Avaya Aura® Web Gateway FQDN with the remote port number, 8444.

   Note:

   Avaya Aura® Web Gateway FQDN for external user must refer to Avaya SBC in the DNS.
i. Click **Finish**.

HTTP proxy configuration

Supported clients

- Avaya Workplace Client on mobile platforms
- Avaya Workplace Client on desktop platforms

Supported servers

Avaya Equinox® Conferencing

Supported proxy authentication types

- HTTP basic authentication
- HTTP digest authentication

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Automatic configuration settings

You can configure the HTTP_PROXY_CSDK_ENABLE parameter to configure the HTTP proxy settings. This parameter indicates whether Avaya Workplace Client uses the HTTP proxy configured in the OS.

Note:

Avaya has rebranded the domains used by Avaya Spaces from
`zang.io`
to
`avayacloud.com`
. If you are using Avaya Spaces and have configured the HTTP_PROXY_CSDK_ENABLE parameter with value 1 or 2, you need to configure the VPN gateway for
`avayacloud.com`
similar to
`zang.io`

.

If you enable the HTTP proxy, the HTTP Proxy Fallback feature is automatically enabled. Avaya Workplace Client retries the HTTP connection without proxy when receiving certain proxy-related errors. Errors might be related to:

- Proxy configuration
- Configured proxy being unreachable
- Proxy authentication type not supported
- Destination server being unreachable when going through proxy

Device OS proxy configurations

Not all HTTP connections in Avaya Workplace Client go through the HTTP proxy. The following table displays the HTTP connections that you must configure to bypass the HTTP proxy.

Important:

Customers must put all enterprise internal servers' IP address or host name into the device's HTTP proxy exception list settings. Else, Avaya Workplace Client might fail to make HTTP connections through the proxy to the internal servers.

HTTP service connections	Destination servers inside enterprise networks	Destination servers in the public internet	The HTTP proxy exception list configured to include the internal enterprise server's IP address or host name
PPM	Avaya Aura® Session Manager	Not Applicable	Not Applicable Avaya Workplace Client bypasses the HTTP proxy for this connection.
Avaya Aura® Device Services contact service	Avaya Aura® Device Services contact service	Not Applicable	Yes
IP Office presence and directory	IP Office premise	IP Office Cloud	Yes
File download	Avaya Aura® Device Services web deployment service Until server IP Office premise	IP Office Cloud Avaya Equinox® Meetings Online	Yes

HTTP service connections	Destination servers inside enterprise networks	Destination servers in the public internet	The HTTP proxy exception list configured to include the internal enterprise server’s IP address or host name
Sparkle	Avaya Aura® Device Services web deployment service	Avaya Equinox® Meetings Online	Yes
Avaya Multimedia Messaging	Avaya Multimedia Messaging	Not Applicable	
Avaya Aura® Web Gateway	Premise Avaya Equinox® Conferencing	Avaya Equinox® Meetings Online	Yes
Unified Portal	Premise Avaya Equinox® Conferencing	Avaya Equinox® Meetings Online	Yes
Install Manager	Premise Avaya Equinox® Conferencing	Avaya Equinox® Meetings Online	Yes
WCS	Premise Avaya Equinox® Conferencing	Avaya Equinox® Meetings Online	Yes
UCCS	Premise Avaya Equinox® Conferencing	Avaya Equinox® Meetings Online	Yes
Avaya Spaces	Not Applicable	Avaya Spaces	Not Applicable Avaya Spaces servers are always in the public internet.
Google Analytics	Not Applicable	Google	Not Applicable Avaya Workplace Client bypasses the HTTP proxy for this connection.
EWS	Premise Exchange	Office 365	Yes

Avaya Aura Device Services configuration

This chapter includes Avaya Aura® Device Services configuration information for Avaya Workplace Client. For complete information about the implementation of this configuration, see *Deploying Avaya Aura® Device Services* and *Administering Avaya Aura® Device Services*.

- Use the Automatic Configuration service to support Avaya Workplace Client used by the Avaya Aura® users.
- Configure the Contact server to link with Avaya Equinox® Management for searching the Avaya Equinox® Management terminals.
- Enable the Picture service to support the client contact pictures.
- Enable the Web Deployment service to support the Avaya Workplace Client software updates.
  The Sparkle service is used only by the Avaya Aura® users. However, the client software download service is used by both Avaya Aura® and guest users.

Avaya Aura Device Services overview

Avaya Aura® Device Services is co-resident with Session Manager, but it is delivered as a separate OVA. Avaya Aura® Device Services provides the following services to Avaya Workplace Client:

- Contact: This service provides users the ability to:
    - Add, update, and delete a contact.
    - Perform an enterprise search for contacts.
      Avaya Aura® Device Services supports directory searches of up to 300 contacts. The search results displays 50 contacts.
    - Set and retrieve information, such as, preferred names or pictures.
    - Search and retrieve information about Avaya Scopia® users and terminals. This feature is applicable only when the address of Avaya Equinox® Management is configured on Avaya Aura® Device Services.
    - Perform an advanced search.
      Users can search the contacts by name, location, and department.
    - Group their Workplace Contacts to better organize them.
      Users can then initiate calls and instant messages to the groups. For example, users might have separate groups for their project team, subordinate team members, and response teams. Contact groups are available across multiple devices.

  To use the Contact service, a user must be provisioned on the LDAP server. Avaya Aura® Device Services contact service is mandatory to support the terminal search feature in SDC replacement clients.
- Notification: This service provides a common infrastructure that a client or endpoint can subscribe to and receive events from a number of service resources by using a single connection.

- Dynamic Configuration: This service provides discovery of configuration settings to UC clients. You can customize these settings on a global, group, individual, or platform basis. The Dynamic Configuration service uses the automatic configuration feature of Avaya Workplace Client to facilitate the configuration details to the UC clients. This helps the user to avoid manual configuration of their client. To log in to the client, users must provide their email address or Windows user ID, and their enterprise credentials.
- Web Deployment: This service publishes and deploys UC client updates to end user devices. The Web Deployment service is supported on Avaya Workplace Client on desktop platforms.

Dynamic Configuration service

With the Dynamic Configuration service, the system can dynamically retrieve and deploy the device configuration settings to Avaya Workplace Client.

Dynamic Configuration provides a centralized place to administer user, group, platform, global, and exception settings. You can configure the Device Configuration settings on Avaya Workplace Client by using one of the following methods:

- DNS-based auto discovery.
- Web address: On Avaya Workplace Client, type the automatic configuration or device configuration URL.

  For example: `https://<IP address>:443/acs/resources/configurations`

Avaya Aura® Device Services auto discovers the following settings from Avaya Equinox® Management during the Avaya Workplace Client deployment:

- CONFERENCE_FACTORY_URI
- CONFERENCE_PORTAL_URI
- UNIFIEDPORTALENABLED

You can override the values for these settings from the Avaya Aura® Device Services web administration portal with any fixed user, group, or platform value. For more information about using the Avaya Aura® Device Services web administration portal, see *Administering Avaya Aura® Device Services*.

Web Deployment service

Using the Web Deployment service, you can provide appcast for clients. Currently, you can create appcast only for Avaya Workplace Client on desktop platforms. On the Web Deployment page, you can add, edit, or delete an appcast item from the appcast table that is at the bottom of the page.

Note:

Web deployments of Avaya Workplace Client require administrative privileges. Hence, to upgrade Avaya Workplace Client, users need the same privileges.

The Web Deployment service supports the upload and download of the client installer that has software update files. The system creates the upload folder automatically at the time of deployment or upgrade. You can also store any files that are necessary for the customer to download. The customer can download the necessary files from https://<aads_server_address>:8445/acs/resources/webdeployment/downloads/<file_name_with_extension>. The upload service operates from the directory /opt/Avaya/DeviceServices/ClientInstallers/.

Example of the:

- Upload URL: `<https://IP address>:8445/admin/upload`
- Download URL: `<https://IP address>:8445/acs/resources/downloads`↗.

Settings for receiving the updates from a client installer

The Dynamic Configuration service has the following settings for the Web Deployment service:

- APPCAST_ENABLED
- APPCAST_CHECK_INTERVAL
- APPCAST_URL

If the value of the APPCAST_ENABLED settings is set to true, Avaya Workplace Client for Windows or Mac receives the APPCAST_URL setting from the Dynamic Configuration service response for the Web Deployment service.

The APPCAST_URL must be set to https://<IP address of the AADS Server>:<443>/acs/resources/webdeployment

Configuring software update deployment

About this task

Use this procedure to upload and download the client installer for web deployment.

For Avaya Workplace Client for Windows, you can upload .exe or .msi installation files. For Avaya Workplace Client for Mac, you can upload .dmg installation files, which are packaged in a .zip archive.

Before you begin

Download Avaya Workplace Client for Mac or Avaya Workplace Client for Windows installation files from the Avaya Support website.

Procedure

1. **Optional** If you are uploading Avaya Workplace Client for Mac, pack the Avaya Workplace-<version>.dmg and Avaya Workplace Sparkle Update-<version>.dmg files into a .zip archive with no intermediate directories.
   If the .zip archive contains intermediate directories, re-pack the archive so that it only contains the .dmg files in the root directory
2. Log on to the Avaya Aura® Device Services web administration portal.
3. In the navigation pane, click **Web Deployment** > **Deployment**.
   The system displays the Software Update Deployment page.
4. In the **Title** field, type the name of the updates or appcast for the client installer.
5. In the **Description** field, type a description of the client installer updates.
6. In the **Version** field, type the version detail of the Avaya Workplace Client release.
7. In the **OS** field, click one of the platforms of the Avaya Workplace Client release:
   - windows
   - macOS
8. Do one of the following:
   - If you are uploading an Avaya Workplace Client for Mac installer, which requires a specific macOS version, in the **Min OS** version field, provide the minimum macOS version that is supported by the client.
   - If you are uploading an Avaya Workplace Client for Mac installer, which does not require a specific macOS version, leave the **Min OS** version field blank.
   - If you are uploading an Avaya Workplace Client for Windows installer, leave the **Min OS** version field blank.
9. In the **File** field, click **Choose File** and select one of the following files to upload:
   - For Avaya Workplace Client for Windows, select the .exe or .msi installation file.
   - For Avaya Workplace Client for Mac, select the .zip archive containing the .dmg installation files

   The maximum upload size for the client installer is 500 MB. The upload service accepts alphanumeric characters, white spaces, dots, minus, and square brackets.
   After you upload the file, the system auto populates the **Size (in bytes)** and **MD5 Hash** fields.
10. In the **Upload URL(s)** field, click one of the following, and then click **Upload**:
    - **Default**: To upload the client installer to the Avaya Aura® Device Services server. This is the default option. You cannot edit the value of the default URL.
    - **Custom**: To provide a URL of a different server for uploading the client installer.

    The system displays a pop-up to specify the user credentials to upload the client installer and a confirmation dialog box to indicate the upload status.

11. In the **Download URL(s)** field, click one of the following:
    - **Default**: To download the client installer from the Avaya Aura® Device Services server to the clients. This is the default option. You cannot edit the value of the default URL.
    - **Custom**: To provide a URL of a different server for downloading the client installer.

    To download the client installer, you must enter the credentials for client authentication.
12. Click **Save**.

    The system populates the data in the table at the bottom of the page with the details of **Title**, **Description**, **Version**, **Publish Date**, **OS**, **Downloads**, **Updates**, and **Download URL**.
13. **Optional** To edit or delete a specified setting, double-click an entry.

Avaya Aura Device Services remote access configuration

You can configure Avaya Aura® Device Services to be accessible to remote workers who use Avaya Workplace Client from outside the enterprise network. The following configuration methods are available:

- Virtual Private Network (VPN)
- Avaya Session Border Controller
- Application Delivery Controllers, formerly named Reverse Proxies

The following section contains an example for configuring the remote access feature by using Avaya Session Border Controller.

Configuring remote access

About this task

You can use Avaya SBC for relaying HTTP and HTTPS traffic between Avaya Aura® Device Services and related application clients, such as Avaya Workplace Client. For more information about relay services configuration in Avaya SBC, see *Administering Avaya Session Border Controller*.

Before you begin

- Configure one of the following to use the remote worker functionality:

  - Implement Split-Horizon DNS: Avaya recommends the use of this configuration to optimize traffic. Clients can then connect to Session Manager directly on the internal network and only use Avaya SBC when on an external network.
  - Use Public cloud model: All FQDNs or URLs must point to the reverse proxy or Avaya SBC. This configuration is used for cloud deployments and also for on premise deployments. By using this configuration, calls are preserved during any network transition from Wi-Fi to cellular data when the client IP address changes during an active call.
  - Implement for internal access only and all remote devices must use VPN: This configuration is used when a security policy is in place so that all traffic must be either internal or using VPN. The VPN solution that is deployed must have sufficient bandwidth and latency to support the expected volume of VoIP calls.
- Set the **Override port for reverse proxy** setting from the **Front-end host, System Manager and Certificate Configuration** menu to `y` (yes) if a reverse proxy or relay is configured to listen on a port other than the default port 443. You must also set a value for the **Front-end port for reverse proxy** parameter.
- Configure an external IP address for Avaya SBC to ensure HTTPS traffic relay for Avaya Aura® Device Services.

Procedure

1. In Avaya SBC, go to **Device Specific Settings** > **Relay Services**.
2. In the **Remote Configuration** field, configure the parameters with the following values:
   - **Remote Domain**: The Avaya Aura® Device Services server domain.
   - **Remote IP**: The IP address of the Avaya Aura® Device Services server.
   - **Remote Port**: The **Front-end port for reverse proxy** parameter configured during the Avaya Aura® Device Services server installation. The default value is 443.
   - **Remote Transport**: TCP.
3. In the **Device Configuration** field, configure the parameters with the following values:
   - **Published Domain**: The Avaya Aura® Device Services server domain.
   - **Listen IP**: The External Avaya SBC IP address created for the Avaya Aura® Device Services relay.
   - **Listen Port**: 443.
   - **Connect IP**: The internal Avaya SBC IP address.
   - **Listen Transport**: TCP.

Reloading the Avaya Aura Device Services or 46xx settings configuration

About this task

Use this procedure to direct Avaya Workplace Client to refresh its Avaya Aura® Device Services or 46xx settings configuration.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **System Status** > **User Registrations**.
2. Click the rows to select the SIP AST devices.
3. Click **Reload** > **Reload Config** to reload only the configuration information of the selected SIP AST subscribed devices.
4. On the Confirm Reload page, click **Confirm**.
   The System Manager web console displays a status page with the current state of scheduled and running endpoint actions.

Remote worker and cloud access configuration

The remote worker functionality enables users that are not connected directly to the enterprise network to use Avaya Workplace Client. You can also enable users to remotely access servers configured with Avaya Workplace Client, such as Presence Services, Avaya Aura® Device Services, or Avaya Multimedia Messaging.

In the Cloud Access model, all users might not be directly connected to the network that is hosting the services and will access those services through a Session Border Controller in the same manner as remote workers.

To use the remote worker functionality, you must configure one of the following:

- Implement Split-Horizon DNS. Avaya recommends the use of this configuration. This configuration optimizes traffic so that clients connect to Session Manager directly on the internal network and only use Avaya Session Border Controller (SBCE) when external.
- Use Cloud Access model. All FQDNs or URLs must point to the reverse proxy or SBCE. This configuration is used for cloud deployments and also for on-premise deployments. By using this configuration, calls are preserved during any network transition from Wi-Fi to cellular data when the client IP address can change during an active call.
- Implement for internal access only and all remote devices must use VPN. This configuration is used when a security policy is in place so that all traffic must be either internal or through VPN. The VPN solution that is deployed must have sufficient bandwidth and latency to support the expected volume of VoIP calls.

SBCE provides the following functionality to Avaya Workplace Client. Depending on your requirements, you might use one or more functionality.

- SIP-TLS to Avaya Aura® Session Manager and Avaya Aura® Presence Services for Presence functionality
- HTTPS relay to Avaya Multimedia Messaging for instant messaging functionality
- HTTPS to Avaya Equinox® Conferencing web collaboration for conferencing functionality
- PPM over HTTPS to Avaya Aura® Session Manager
- Automatic configuration using Avaya Aura® Device Services or any other web server
- LDAPS to LDAP server for desktop clients if Avaya Aura® Device Services is not in use

If SBCE includes a configuration to deny registrations from particular Avaya Workplace Client user-agents, you must configure the denied Avaya Workplace Client user-agents to directly connect to the Session Manager internal IP addresses and not through the public FQDN with Split-Horizon DNS.

Remote worker configuration worksheet

Use the following worksheet to determine how to provide remote workers access to available functionality:

Functionality available	Configuration requirement	Document references
Basic VoIP service	Set up an SBCE device.	*Administering Avaya Session Border Controller*
LDAP functionality	Ensure that all required ports are configured in SBCE.	“Port assignments” in *Avaya Session Border Controller Overview and Specification*
Instant Messaging functionality	Relay HTTP and HTTPS traffic between Avaya Workplace Client and the Avaya Multimedia Messaging server.	• For more information about relay services configuration on SBCE, see *Administering Avaya Session Border Controller* • For general configuration information about remote worker functionality in Avaya Multimedia Messaging, see *Deploying Avaya Multimedia Messaging*
Presence functionality	Create a Presence server profile in SBCE.	*Administering Avaya Session Border Controller*
Conferencing functionality	Set up Avaya Equinox® Conferencing.	See the chapters on Configuration for Unified Communications deployments and Configuration for Over the Top deployments.

SBCE deployment scenarios for failover

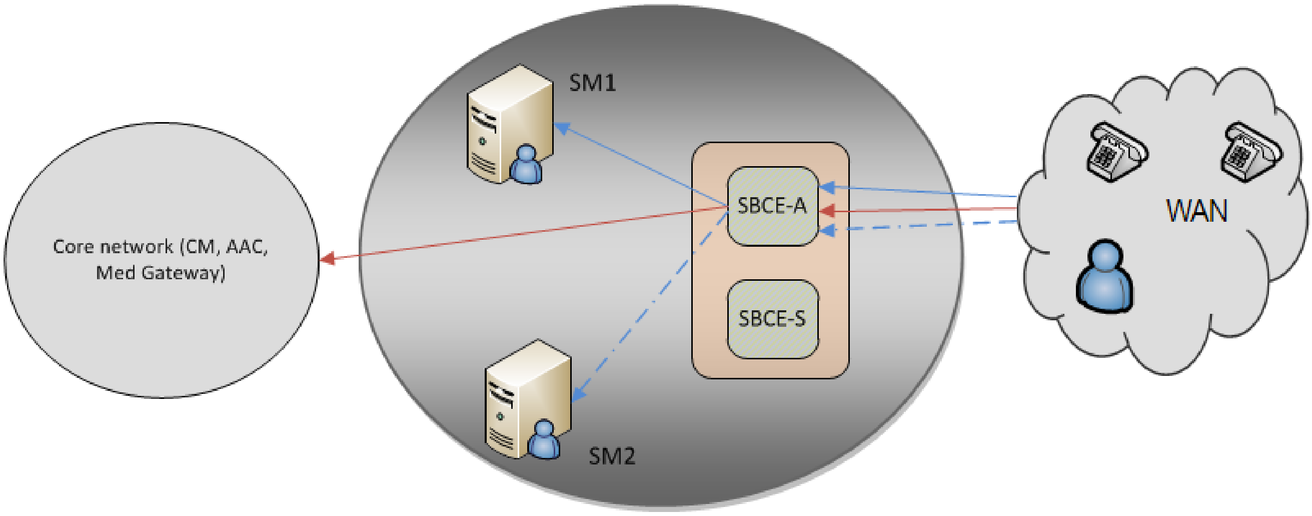
SBCE high availability

Enterprises might deploy Avaya Session Border Controller (SBCE) in high availability (HA) mode to ensure media preservation in the event of failover of the Session Border Controller server. The SBCE HA pairs are deployed within the enterprise in a parallel mode configuration. The active SBCE (SBCE-A) is the primary SBC server through which all signaling packets are routed. The interface ports on the standby SBCE (SBCE-S) do not process any traffic. When a failure is detected on SBCE-A by the Avaya Element Management System (EMS), the SBCE-A network interface ports are automatically disabled and the network interface ports of SBCE-S 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 servers with SBCE in high availability mode

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

Figure : 1. Deployment model: Single SBCE in high availability mode



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

- Signaling traffic from the endpoints:
  - When the server connectivity is lost owing to a link failure on SBCE-A, the endpoint fails over to SBCE-S.
  - 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 the trigger detecting the unreachable Session Manager, when it is not routed through SBCE.
- Media traffic:
  - In case of a link failure on SBCE-A, the endpoint fails over to SBCE-S, and all media sessions of active calls are preserved over SBCE-S.
  - In case of a network failure between the endpoints and SBCE-A, all media sessions of active calls are lost.

- Signaling traffic from the endpoints:
  - When SBCE-A is not functional, the endpoint fails over to SBCE-S.
  - 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 verification process is initiated in all future failover events.

    - The trigger initiated at the endpoint to detect the unreachable SBCE is the same as the trigger detecting the unreachable Session Manager, when it is not routed through SBCE.
- Media traffic:
    - Media sessions of active calls are preserved over SBCE-S.
    - All SIP dialogs are preserved and any subsequent SIP traffic is routed through SBCE-S. However, any transactions in progress fails.

- In the case of a socket error between SBCE-A and the primary Session Manager, all socket connections from the endpoints to SBCE-A are ended.
- In case of SIP failure detection, the OPTIONS message towards the primary Session Manager fails, and SBCE-A determines that the primary Session Manager is not functional.
- A loss of connectivity causes the endpoints to start a check and failover to the backup Session Manager if available and reachable.

Sending DTMF tones with Avaya Workplace Client

About this task

Use this procedure to configure SBCE if you have remote users using Avaya Workplace Client.

Avaya Workplace Client does not support in-band or out-of-band DTMF tones. If you want to send DTMF tones with RFC 2833, you must configure SBCE to use RTP-Payload.

If you use the default SBCE configuration, the system passes DTMF unchanged from Avaya Workplace Client.

Before you begin

Install and configure SBCE.

Procedure

1. In SBCE, go to **Domain Policies** > **Session Polices** > **Codec Prioritization**.
2. Select the **Codec Prioritization** and **Allow Preferred Codecs Only** check boxes.
3. Add **Dynamic (120)** to the preferred codec list.
   Dynamic (120) for RFC 2833 is a DTMF payload type.

Automatic configuration

The automatic configuration process automatically configures Avaya Workplace Client settings when users open the client for the first time after installation. If you do not enable automatic configuration, users must configure Avaya Workplace Client settings manually after installing the client. To avoid errors when configuring settings, Avaya recommends that you enable automatic configuration.

Users can configure the Avaya Workplace Client settings automatically by using their email address or the automatic configuration web address.

If the user types the email address and the DNS check:

- Is successful, the settings file is downloaded. If you have provisioned more than one environment, the user must choose an environment before the settings file is downloaded.
- Fails, the email address is automatically searched in the following accounts and in the following priority:
  1. Avaya Spaces
  2. Avaya Equinox® Meetings Online

By using Avaya Spaces or Avaya Equinox® Meetings Online, if the settings file is:

- Found in the URL, the settings file is downloaded.
- Not found in the URL, the user must enter a web address or manually configure the application.

  If the settings file is found in the web address, the settings file is downloaded.

In both instances, if you have provisioned more than one environment, the user must choose an environment before the settings file is downloaded.

If the settings file that is downloaded does not include the user's credentials for the various services, the user must manually enter their credentials to log in to each service.

The user might be able to view further screens related to Avaya Cloud accounts depending on whether:

- The Avaya Cloud account exists for Spaces and Messaging.
- You have enabled the Avaya Cloud account setting for the user's account.

The user can additionally configure the account to use the Avaya Equinox® Meetings Online service.

For information about automatic configuration by using Avaya Aura® Device Services, see *Administering Avaya Aura® Device Services*.

Note:

While uploading a specific build version, you must mention the full version name of Avaya Workplace Client in Web Deployment of Avaya Aura® Device Services.

MDM for automatic configuration

You can use any Mobile Device Management (MDM) tool to automatically deploy Avaya Workplace Client for Android or iOS into the user devices. You can then use the MDM tool to configure the application Key-Value pairs to configure the client automatically.

Avaya Workplace Client supports reading of pushed application configuration. When configuring the MDM tool, you can use the 46xxsettings file parameter name as the configuration key to push the Avaya Workplace Client settings. If you publish a value for the SETTINGS_FILE_URL key, Avaya Workplace Client uses the URL provided to trigger an auto-configuration data retrieval. As with any other auto-configuration mechanism, Avaya Workplace Client displays a prompt to enter user credentials.

The following is an example of a Key-Value pair:

- Configuration Key: SETTINGS_FILE_URL
- Value Type: String
- Configuration Value: https://example.com/autoconfiguration/settings.txt

You can also use the AUTO_CONFIG_URL parameter to specify the URL to access Avaya Aura® Device Services automatic configuration.

Log out through Universal Link Callback

When deploying Avaya Workplace Client using Imprivata IDP, enterprises might install Imprivata Mobile Device Access (MDA) on the mobile device. Imprivata Mobile Device Management (MDM) system uses MDA and sends a Universal Link Callback (ULC) link to the mobile clients. A ULC requests the application to log out from all devices, reset all settings, and remove configuration data. The Maps application opens after successfully logging out. The Maps application confirms that you successfully logged out of all mobile devices.

Note:

- In some cases, the Maps application might not open after successfully logigng out. You can try to login and confirm.
- MDM must be installed on the mobile device to send a ULC request to mobile clients.

Automatic configuration setup options

Users can automatically configure Avaya Workplace Client by using a settings file that you store on a central server or a settings service that you provide. You can provide the settings file URL to your users or set up DNS records for your domain. The settings file URL or DNS records that you create must be secure.

- If you use DNS, users must enter an email address in Avaya Workplace Client to activate automatic configuration.
- If you use a settings file URL, you must send the URL to your users. Users must enter the URL in Avaya Workplace Client to activate automatic configuration.

Note:

Mac OS requires the use of a web proxy for DNS-based Service Discovery.

Additionally, for Mac and Windows, you can trigger automatic configuration by configuring the address of the settings file during installation. For Windows, you can also modify the registry entry values under the appropriate Windows Group Policy Object (GPO) to discover the settings file URL.

If there are multiple soft clients, the user can choose the default soft client for telephone services. Alternatively, if you want the user to use Avaya Workplace Client for Windows as the default application for telephone services, you can use Group Policy to perform the necessary configuration. For more information about using Group Policy, see Microsoft help documentation.

⚠ **Caution:**

Do not modify the configdata.xml file at %APPDATA%/Avaya/Avaya IX Workplace. Configuration data is managed by Avaya Workplace Client using Avaya Aura® Device Services or the 46xx settings file server. Hence, you must not edit the configdata.xml file manually.

Settings file

To enable automatic configuration, you must create a settings file.

When you create a settings file, remember the following points:

- You can create the settings file in any of the following file formats:
  - 46xxsettings.txt
  - aura7cm01
  - aura7cm01.txt
- You can store all settings on the same file for endpoints such as 46xx and Avaya Workplace Client.
- You must include only numbers in the FNE values and ensure that the values are in the E.164 international format. For example,

  ```
  +<country code><national number>
  ```
  .

Avaya Workplace Client does not apply any dialing rule translation to these numbers. Use the E.164 international format to ensure that the number can be dialed from any location or network used by the device.

- You can use a blank string to clear the existing value for a setting.
  For example,
  `SET SIPUSERNAME`
  `""`
  . You can use a blank string only for non-User preference parameters and PREF_MUTE_MIC_WHEN_JOINING_MEETING and PREF_BLOCK_CAMERA_WHEN_JOINING_MEETING parameters.
- To use the default values for a parameter, you can exclude the parameter from the settings file. If you changed the default value for a parameter and now want to use the default value:
  - On desktop clients, you can exclude the parameter from the settings file.
  - On mobile clients, you must explicitly set the parameter in the settings file.
- You must not include the parameters for user name and password in the settings file if you want users to enter their credentials to access the various services in Avaya Workplace Client.
- You must configure only a single dial plan in each settings file. Users in different locations have different dial plans. Hence, create a separate settings file with a unique dial plan for each location. Ensure that the medium that you use to deliver the link to each user, for example, email, contains a link to the appropriate settings file for the region.
- You must not add line breaks in the setting code for each parameter. Avaya Workplace Client cannot parse settings file parameters with line breaks.
- You can lock down the Avaya Workplace Client settings, specifically the login parameters, as part of the configuration by using the LOCKED_PREFERENCES parameter.

Settings file parameters

The tables in the following sections describe the parameters supported on each Avaya Workplace Client.

In your settings file, you can use one of the following formatting options for a parameter and its associated values:

- `SET PARAMETER_NAME A,B,C`
- `SET PARAMETER_NAME "A,B,C"`

In these examples, A, B, and C are values that must be set for a parameter.

⚠ **Tip:**

When you are updating the settings file, you can use a blank string to clear the existing value of a parameter. For example, `SET PARAMETER_NAME ""`

.

If the same parameter is present multiple times in the settings file, Avaya Workplace Client uses the last instance of the parameter value.

Avaya Workplace Client for Windows supports different parameter values in individual groups in the settings file. For example, you can set different reason codes in the individual agent groups for the following parameters:

- LOGOUT_REASON_CODES
- AGENT_WORK_CODE
- AUX_REASON_CODES

Additionally, on Communication Manager, you must configure the IP Phone Group ID parameter with a Group ID for the appropriate station. Avaya Workplace Client for Windows then displays the reason codes based on your Group ID. You can set the Group ID value from 1 to 999.

If you change the Group ID, you must wait for Avaya Workplace Client for Windows to restart before you can view the reason codes associated with the updated Group ID. If you manually restart Avaya Workplace Client for Windows before receiving the new Group ID value from the server, Avaya Workplace Client continues to display the reasons codes associated with the previous Group ID.

Disabling unwanted features

If you disable a particular parameter that has a corresponding UI element, Avaya Workplace Client removes the unused feature from the UI. For example:

- To remove IM,
  `SET ESMENABLED 0`
  .
- To disable Avaya Spaces Direct Messaging,
  `SET ENABLE_SPACES_MESSAGING 0`
  .
- To remove the calendar on Avaya Workplace Client for Mac and Windows,
  `SET CALENDAR_INTEGRATION_ENABLED 0`
  .
- To display a simplified dialpad view on the Home screen,

`SET HOMESCREENLAYOUT 2`.

- To remove the Workplace Meetings panel from the Top of Mind screen, `SET SHOW_EQUINOX_MEETING_PANEL_IN_TOM 0`.
- To remove the **New Conversation +** option at the bottom of the main window on Avaya Workplace Client for Mac and Windows, do not configure a value for both the ESMSRVR and CONFERENCE_FACTORY_URI parameters.
- To disable Avaya Spaces integration, `SET ENABLE_AVAYA_CLOUD_ACCOUNTS 0`.
- To disable video, `SET ENABLE_VIDEO 0`.
- To disable the Top Of Mind feature, `SET ENABLE_TOP_OF_MIND 0`. Avaya Workplace Client does not retrieve any calendar information. Also, the Top Of Mind and Calendar buttons are unavailable.
- To disable the Avaya Workplace Client tutorial, `SET ENABLE_TUTORIAL 0`.
- To disable the local or Outlook contact integration, `SET ENABLE_LOCAL_CONTACT 0`.
- To disable the Outlook add-in functionality, `SET ENABLE_OUTLOOK_ADDON 0`.

You can lock a number of settings. For example,

```
SET
        LOCKED_PREFERENCES
        "SIP_CONTROLLER_LIST,SIPPROXYSRVR,SIPPORT,SIPSECURE,SIPENABLED,SIPDOMAIN
,SIPUSERNAME,SIPHA1,ACSPORT,ACSSECURE,ACSENABLED,ACSSSO,ACSSRVR,ESMSSO,ESMREFRES
H,ESMPORT,UNIFIEDPORTALENABLED,AADS_URL,ESMSECURE,ESMSRVR,SIPSSO,ESMENABLED,ENAB
LE_CALL_NOTIFICATIONS,UNIFIED_PORTAL_SSO,AVAYA_CLOUD_ACCOUNTS,ADDRESS_VALIDATION
,TRUST_STORE"
```

.

You can hide a number of settings. For example,

```
SET
        OBSCURE_PREFERENCES
        "SIP_CONTROLLER_LIST,SIPPROXYSRVR,SIPPORT,SIPSECURE,SIPENABLED,SIPDOMAIN
,SIPUSERNAME,SIPHA1,ACSPORT,ACSSECURE,ACSENABLED,ACSSSO,ACSSRVR,ESMSSO,ESMREFRES
H,ESMPORT,UNIFIEDPORTALENABLED,AADS_URL,ESMSECURE,ESMSRVR,SIPSSO,ESMENABLED,ENAB
LE_CALL_NOTIFICATIONS,UNIFIED_PORTAL_SSO,AVAYA_CLOUD_ACCOUNTS,ADDRESS_VALIDATION
,TRUST_STORE"
```

.

For more information on enabling or disabling a feature, refer to the parameters in the following sections.

Guidelines while configuring Avaya Workplace Client parameters for media-only deployment scenarios

In media-only deployment scenarios, the agent uses Avaya Workplace Client as a media endpoint. In MEGA deployments, Remote Agent Phone (RAP) calls, which are long duration service calls, are initiated through the MEGA server upon agent login. Hence, the agent cannot perform the following actions from Avaya Workplace Client:

- Cannot end the agent calls from the application or headset call controls. However, agents have full control over the UC calls.
- Cannot escalate the call to video or deescalate the call from video.
- Cannot transfer a call or initiate a conference call.

In media-only deployment scenarios, Avaya Workplace Client does not play any greeting when Avaya Workspaces for Call Center Elite receives a MEGA initiated RAP call. The RAP call is automatically answered. If there is an active RAP call and you receive a VDN call, Avaya Workplace Client plays the greeting which matches the VDN based on the greetings rules. The VDN call is automatically answered.

You can configure the following parameters on Avaya Workplace Client:

- `SET ENABLE_CALL_NOTIFICATIONS 0`
  : Users do not receive visual notifications on Avaya Workplace Client for incoming calls.
- `SET HOMESCREENLAYOUT 2`
  : Users can view a large dialpad layout on the Home screen of Avaya Workplace Client.
- `SET ENABLE_AUDIBLE_CALL_NOTIFICATIONS 0`
  : Users do not receive audible notifications on Avaya Workplace Client for incoming calls.
- `SET DESKTOP_HTTP_APPLICATION_INTEGRATION 0`
  ,

```
SET
            ENABLE_PLT_OOB_HEADSET_CALL_CONTROL 0
```

, and

```
SET
            AUDIO_DEVICE_CALL_CONTROL_ENABLED 0
```

: Users cannot end calls using headset controls.

For more information on enabling or disabling a feature, refer to the parameters in the following sections.

Checklist of settings file parameters

The following checklist outlines the settings file parameters for Avaya Workplace Client. Configure the parameters according to your requirement.

Parameters	Reference	✔
System	System parameters	
SIP	SIP parameters	
Unified Login	Unified Login parameters	
Automatic configuration	Automatic configuration parameters	
Conferencing	Conferencing parameters	
Automatic software updates	Automatic software updates parameters	
Avaya Multimedia Messaging	Avaya Multimedia Messaging parameters	
Avaya Aura® Device Services	Avaya Aura Device Services parameters	
Client Enablement Services	Client Enablement Services parameters	
Desktop integration	Desktop integration parameters	

Parameters	Reference	✔
EC500	EC500 parameters	
Dialing rules	Dialing rule parameters	
Presence	Presence parameters	
Calendar integration	Calendar Integration parameters	
LDAP	LDAP parameters	
Media	Media parameters	
Video	Video parameters	
Voice mail	Voice mail parameters	
Avaya Cloud	Avaya Cloud parameters	
Administration	Administration parameters	
Security settings	Security settings parameters	
User policy	User policy settings parameters	
User preferences	User preferences parameters	
SMS and Fax	SMS and Fax parameters	
Contact	Contact parameters	
Export conversation	Export Conversation parameter	
MLPP	MLPP parameters	

System parameters

Type	Default value	Supported platforms	Description
MODEL			
String	<platform>.<majorversion>.<minorversion>	• Android • iOS • Mac • Windows	A string of maximum 10 characters that identifies the endpoint platform and version. This value is built into the application as an identifier for the endpoint or release to allow the value to be used in conditional statements. The platform names are abbreviated. For example, for release 3.35: • aca.3.35 is the value for Avaya Workplace Client for Android. • aci.3.35 is the value for Avaya Workplace Client for iOS. • acm.3.35 is the value for Avaya Workplace Client for Mac. • acw.3.35 is the value for Avaya Workplace Client for Windows. Client Navigation: Not Applicable.

Type	Default value	Supported platforms	Description
MODEL4			
String	<platform>	• Android • iOS • Mac • Windows	A string of maximum 4 characters that identifies the endpoint platform. This value is built into the application as an identifier for the endpoint or release to allow the value to be used in conditional statements. For example: • aca is the value for Avaya Workplace Client for Android. • aci is the value for Avaya Workplace Client for iOS. • acm is the value for Avaya Workplace Client for Mac. • acw is the value for Avaya Workplace Client for Windows.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.

SIP parameters

Type	Default value	Supported platforms	Description
SIPENABLED			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether the SIP service is enabled. The options are: • 0: Indicates disabled. • 1: Indicates enabled. Client Navigation: **Settings** > **Services** > **Phone Service** > **Phone Service**.
SIP_CONTROLLER_LIST			
Numeric	Null	• Android • iOS • Mac • Windows	This parameter consolidates SIP controller parameters for an IP address, port, and transport protocol into a single configuration parameter. The parameter setting must be a list of SIP

Type	Default value	Supported platforms	Description
			controller designators, separated by commas without any intervening spaces. Each controller designator must have the following format: `host[:port][;transport=xxx]`. For example, `proxy1:5061;transport=tls,proxy2:5061;transport=tls`. **Note:** • The host value can be an FQDN or an IP address. • If you use this parameter with LOCKED_PREFERENCES and OBSCURE_PREFEFERENCES parameters, all three associated UI fields are locked. The SIP fields are **Server Address**, **Server Port**, and **Use TLS**. Client Navigation: • **Settings** > **Services** > **Phone**

Type	Default value	Supported platforms	Description
			Service > **Server Address**. • **Settings** > **Services** > **Phone Service** > **Server Port**. • **Settings** > **Services** > **Phone Service** > **Use TLS**.
SIPDOMAIN			
String	Null	• Android • iOS • Mac • Windows	The SIP domain name. Client Navigation: **Settings** > **Services** > **Phone Service** > **Domain**.
SIMULTANEOUS_REGISTRATIONS			
Numeric	Null	• Android • iOS • Mac • Windows	This parameter indicates the maximum number of servers a user can simultaneously register to. If you do not configure this parameter, Avaya Workplace Client sets the value to 0. **Note:** Session Manager accepts a value in the range of 1 to 5. If you set the parameter value to 1,

Type	Default value	Supported platforms	Description
			Session Manager return two Session Manager's, that is, Core Session Manager and Branch Session Manager if Branch Session Manager is configured. Client Navigation: Not Applicable.
SIPSSO			
Numeric	0	• Android • iOS • Mac • Windows	This parameter determines whether to use a unified login for the SIP service. If you use Avaya Aura® Device Services, you must set this parameter to 0. This is because Avaya Aura® Device Services provides SIPUSERNAME and SIPHA1 parameter values to Avaya Workplace Client, which uses them to log in to Session Manager. The user does not need to enter any SIP extension and password. The options are: • 0: Indicates disabled. Default value is needed for Avaya Aura® and IP Office deployments. • 1: Indicates enabled.

Type	Default value	Supported platforms	Description
			- 2: Indicates support for SSO with Avaya Spaces for IP Office deployment. Client Navigation: Not Applicable.
SIPUSERNAME			
String	Null	- Android - iOS - Mac - Windows	The SIP account name. Client Navigation: **Settings** > **Accounts** > **Phone Service** > **Extension**.
SIPPASSWORD			
String	Null	- Android - iOS - Mac - Windows	The SIP account password. Client Navigation: **Settings** > **Accounts** > **Phone Service** > **Password**.
ENABLE_MDA_JOIN			
Numeric	0	- Android - iOS	This parameter is used to enable MDA Join if you use a version of Communication Manager later than 6.3. The options are:

Type	Default value	Supported platforms	Description
			- 0: Indicates disabled. - 1: Indicates enabled. On Communication Manager 6.3 and earlier, Communication Manager gets reset if a user attempts to bridge into an active call from their MDA extension. Therefore, the remote line appearance **Join** button is disabled by default. Client Navigation: Not Applicable.
ENFORCE_SIPS_URI			
Numeric	1	- Android - iOS - Mac - Windows	This parameter is used to enable SIPS in URI. The options are: - 0: Indicates disabled. - 1: Indicates enabled. Client Navigation: Not Applicable.
ENABLE_PUBLISH_MAC_ADDRESS			
Numeric	0	- Android (Only on Vantage devices) - Mac - Windows	This parameter is used to publish the Ethernet MAC address of the device for Avaya Sentry for E911. The options are:

Type	Default value	Supported platforms	Description
			- 0: Indicates that the SIP instance ID does not include the Ethernet MAC address information. - 1: Indicates that the SIP instance ID includes the Ethernet MAC address of the device in all SIP messages, including the SIP INVITE messages for emergency calls in logged-out mode. Client Navigation: Not Applicable.
ENABLE_PPM			
Numeric	1	- Android - iOS - Mac - Windows	This parameter is used to enable PPM. The options are: - 0: Indicates disabled. - 1: Indicates enabled.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
ENABLE_PPM_CALL_JOURNALING			
Numeric	• For Android, Mac, and Windows: 1 • For iOS: 2	• Android • iOS • Mac • Windows	This parameter indicates whether Session Manager stores the history of the 100 most recent calls for each user. This is irrespective of whether the endpoint registers to Session Manager. The options are: • 0: Indicates disabled. • 1: Indicates enabled. • 2: Indicates enabled. If you set this value, call journaling for iOS is enabled if you do not log in to Client Enablement Services and PPM call logs are available and enabled. If the user logs in to Avaya Workplace Client on an endpoint, the endpoint downloads the latest 100 call history records from Session Manager. Subsequently, the endpoint maintains its

Type	Default value	Supported platforms	Description
			local call history, while Session Manager maintains its call history independently. With this feature, active synchronization of call history between Session Manager and the endpoints is minimal after the initial login or download. However, when a user attempts to delete call history from an endpoint, the endpoint sends a PPM request to delete the corresponding call history from the central repository of Session Manager. Call history download is initiated by the client when the client: • Recovers from a network outage or outage due to a network change. • Registers with Session Manager. Client Navigation: Not Applicable.
SHOW_TEAM_BUTTON_VISUAL_ALERT			
Numeric	1	• Android • iOS • Windows	This parameter controls the Team Button visual alert notification at the monitoring station.

Type	Default value	Supported platforms	Description
			The options are: • 0: Indicates that a visual alert notification is not displayed at the monitoring station. • 1: Indicates that a visual alert notification is displayed at the monitoring station. If you configure the parameter value as `0`, Avaya Workplace Client disables the Team Button toggle switch at the monitoring station. Client Navigation: Not Applicable.
SHOW_TEAM_BUTTON_CALLER_ID			
Numeric	1	• Android • iOS • Windows	This parameter controls the display of the caller ID on the Team Button call pick up alert at the monitoring station. The options are: • 0: Indicates that the caller ID is not displayed on the Team Button call pick up alert at the

Type	Default value	Supported platforms	Description
			monitoring station. - 1: Indicates that the caller ID is displayed on the Team Button call pick up alert at the monitoring station. Client Navigation: Not Applicable.
SIGNALING_ADDR_MODE			
Numeric	4	- Android - iOS - Mac - Windows	This parameter is used by SIP signaling on dual-mode SIP endpoints to select the preferred SIP controller IP addresses from SIP_CONTROLLER_LIST. Dual-mode SIP endpoints are configured with IPv4 and IPv6 addresses. The options are: - 4: The phone preferably registers to SIP controllers using the IPv4 address. - 6: The phone preferably registers to SIP controllers

Type	Default value	Supported platforms	Description
			- using the IPv6 address. Client Navigation: Not Applicable.
FAILED_SESSION_REMOVAL_TIMER			
Numeric	15	- Android - iOS - Mac - Windows	This parameter indicates the number of seconds for which the session line appearance is displayed after the user dials an invalid extension and does not press the End Call softkey. Valid values are 5 through 99. Client Navigation: Not Applicable.
CALL_DECLINE_POLICY			
Numeric	0	- Android - iOS - Mac - Windows	This parameter indicates the policy for declining an incoming call. The options are: - 0: Indicates that the call decline policy is disabled. If you set this value and the user presses ☎ for an incoming call, Avaya

Type	Default value	Supported platforms	Description
			Workplace Client suppresses the ringing. However, the user can answer the suppressed calls. • 1: Indicates that the user does not want to answer the call. If you set this value and the user presses ☎, Avaya Workplace Client declines the call and generates the 486 Busy response. Call history displays an entry for the calls that the user declines. **Note:** • If you set the value as 1 and the user presses ☎ for an incoming BLA or Call Pickup call, Avaya Workplace

Type	Default value	Supported platforms	Description
			Client suppresses the ringing. However, the user can answer the suppressed calls. • If the user calls a peer who has configured voice mail and the peer declines the call with a 486 Busy response, Avaya Workplace Client directs the user to voice mail. • If the user calls a peer who has not configured voice mail and the peer declines the call with a 486 Busy response, Avaya Workplace Client displays the Active Call Appearance and the user hears a busy tone. • Do not configure this

Type	Default value	Supported platforms	Description
			parameter for Contact Center users. Client Navigation: Not Applicable.
ENABLE_PPM_PERSISTENT_DATA			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Workplace Client requeries the PPM data from the server. Avaya Workplace Client requeries the PPM data for events such as application start-up, network reconnection, recovery from sleep or background, and server failover. The options are: • 0: Indicates that Avaya Workplace Client requeries the PPM data from the server. 1: Indicates that Avaya Workplace Client does not requery the PPM data from the server. If you enable this parameter in non-MEGA

Type	Default value	Supported platforms	Description
			deployments when Avaya Workplace Client is offline or not connected to a network, Avaya Workplace Client must be restarted to requery the PPM data from the server. Client Navigation: Not Applicable.
NO_SUBSCRIBE_ON_SIP_CONNECTION_RECOVERY			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Workplace Client re-registers and re-subscribes on reconnection to the SIP server. This parameter is applicable only for MEGA deployments. • If the server outage is longer than the parameter value or Avaya Workplace Client is connected to a different SIP server, Avaya Workplace

Type	Default value	Supported platforms	Description
			Client re-registers and re-subscribes on reconnection to the SIP server. • If the server outage is shorter than the parameter value or Avaya Workplace Client is reconnected to the same SIP server, Avaya Workplace Client only re-registers on reconnection to the SIP server. • If the network outage is longer than the parameter value, to re-register and re-subscribe, Avaya Workplace Client clears the previous registration and subscription. • If the network outage is shorter than the parameter value, Avaya

Type	Default value	Supported platforms	Description
			Workplace Client does not re-subscribe, assuming that all subscriptions from the previous registration are valid. The options are: • 0: Indicates that the feature is disabled. 1 to 32: Indicates the number of seconds of the outage for which Avaya Workplace Client does not re-subscribe. Client Navigation: Not Applicable.
ENABLE_PPM_CONTACTS			
Numeric	1	Windows	This parameter indicates whether Avaya Workplace Client loads the PPM contacts. The options are: • 0: Indicates that Avaya Workplace Client does not

Type	Default value	Supported platforms	Description
			load the PPM contacts. 1: Indicates that Avaya Workplace Client loads the PPM contacts. If you set: • ENABLE_PPM to 0, Avaya Workplace Client ignores the value you set for ENABLE_PPM_CONTACTS. • ENABLE_PPM_CONTACTS and ACSENABLED to 0, Avaya Workplace Client does not display the Favorites tab. • ENABLE_PPM_CONTACTS or ACSENABLED to 1, Avaya Workplace Client displays the Favorites tab. • ENABLE_PPM_CONTACTS,

Type	Default value	Supported platforms	Description
			ACSENABLED, and ENABLE_LOCAL_CONTACT to 0, Avaya Workplace Client does not display the Favorites and Contacts tabs. - ENABLE_PPM_CONTACTS and ACSENABLED to 0, and ENABLE_LOCAL_CONTACT to 1, Avaya Workplace Client does not display the Favorites tab but displays the Contacts tab. To view the enterprise search results, you must set one or more of the following parameter values to 1: - ACSENABLED - ENABLE_PPM_CONTACTS - DIRENABLED - ENABLE_AVAY

Type	Default value	Supported platforms	Description
			A_CLOUD_AC COUNTS Client Navigation: Not Applicable.
PPM_CONFIG_REQUEST_TIMEOUT			
Numeric	10	• Android • iOS	This parameter indicates the time duration in seconds for which Avaya Workplace Client waits for a server response on PPM configuration request. The value range for this parameter is 1 to 10 seconds. Client Navigation: Not Applicable.
ENABLE_CALLBACK_SERVICE			
Numeric	0	• Android • iOS	This parameter indicates whether Callback Service is available through Communication Manager and enabled. The options are: • 0: Indicates that Callback Service is disabled. • 1: Indicates that Callback Service is enabled.

Type	Default value	Supported platforms	Description
			Note: Client Navigation: **Settings** > **Services** > **Callback Service** > **Callback Service**.

Unified Login parameters

Type	Default value	Supported platforms	Description
SSOENABLED			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates whether Unified Login is enabled. The options are: • 0: Indicates disabled. Avaya Workplace Client does not display Unified Login as an authentication mechanism for any service. • 1: Indicates enabled. Avaya Workplace Client displays Unified Login as an authentication

Type	Default value	Supported platforms	Description
			mechanism for each service. Client Navigation: Not Applicable
SSOUSERID			
String	Null	• Android • iOS • Mac • Windows	The unified login user ID. This parameter is optional. Client Navigation: **Settings** > **Accounts** > **Workplace** > **Username**
SSOPASSWORD			
String	Null	• Android • iOS • Mac • Windows	The unified login password. This parameter is optional. Client Navigation: **Settings** > **Accounts** > **Workplace** > **Password**

Use of Unified Login

Unified Login is an Avaya term to describe the design approach used by Avaya Workplace Client end points to present a simplified user interface for management of credentials. These credentials are needed for the back-end services used by the client applications.

Service	Default mapping	Override parameter
SIP	Avaya Aura® credentials	SIPSSO
Avaya Multimedia Messaging	Enterprise credentials	ESMSSO
Avaya Aura® Device Services	Enterprise credentials	ACSSSO
Client Enablement Services	Enterprise credentials	CESSSO
Exchange Web Services	Enterprise credentials	EWSSSO
LDAP	Enterprise credentials	DIRSSO

Using the SSO option, administrators and users can override the use of the common credentials on a per service basis. For example, in Avaya, a user might use "petertan" as the user name for CES and AMM. However, the user must use "global\petertan" for LDAP. In this case, the user can use the Unified Login feature for all services except LDAP. For LDAP, the user must set SSO to off so that the user can manually enter the credentials in the format required to use this service.

Automatic configuration parameters

Type	Default value	Supported platforms	Description
AUTOCONFIG_USESSO			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates whether the application uses the unified login or Avaya Authorization Service credentials during the retrieval of the 46xxsettings file. Otherwise, the automatic

Type	Default value	Supported platforms	Description
			configuration credentials are unique. The options are: • 0: Indicates that the automatic configuration credentials are unique. • 1: Indicates that the automatic configuration credentials are the same as the unified login credentials. • 3: Indicates that the automatic configuration credentials are same as the Avaya Authorization Service credentials. Client Navigation: Not Applicable.
SETTINGS_CHECK_INTERVAL			
Numeric	1	• Android • iOS • Mac • Windows	The interval used to define how often endpoints will check for settings file changes. The value range for this parameter is 0 to 30 days.

Type	Default value	Supported platforms	Description
			Avaya recommends that you set this value to more than zero for your deployment. • A value of 0 indicates that configuration updates are not performed. • A value of 1 indicates daily. • A value of 7 indicates weekly. Client Navigation: Not Applicable.
SETTINGS_FILE_URL			
String	Null	• Android • iOS • Mac • Windows	The URL to move settings files from one server to another. This URL is used during the next check interval if defined. For example, `SET SETTINGS_FILE_URL "https://acquirerofexample.com/mysettingsfile.txt"`. Client Navigation: Not Applicable.
SETTINGS_CHECK_POLICY			

Type	Default value	Supported platforms	Description
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Workplace Client fetches the automatic configuration settings after each restart and sign in. The options are: • 0: Indicates that Avaya Workplace Client does not fetch the automatic configuration settings after each restart and sign in. • 1: Indicates that Avaya Workplace Client fetches the automatic configuration settings after: • The user restarts the mobile clients. • The user exits and restarts, or signs out and signs in to the

Type	Default value	Supported platforms	Description
			desktop clients. Client Navigation: Not Applicable.

Automatic configuration updates

If Avaya Workplace Client receives configuration updates from Avaya Aura® Device Services or the 46xx settings file, Avaya Workplace Client restarts automatically. Avaya Workplace Client applies the configuration updates if the following conditions are met:

- The user is logged in.
- The dashboard window is not minimized.
- There are no active calls.
- The Instant Messaging window is not in the foreground.

Conferencing parameters

Type	Default value	Supported platforms	Description
CONFERENCE_FACTORY_URI			
String	Null	• Android • iOS • Mac • Windows	The URL that defines the adhoc conference resource to be used by the endpoint. This is an optional parameter. Hence, the value can be empty. • Avaya Equinox®

Type	Default value	Supported platforms	Description
			Conferencing: This is the advanced parameter vnex.vcms.core.conference.factoryURI provisioned in Avaya Equinox® Management. • Avaya Aura® Conferencing: This parameter is the adhoc URI entered in the provisioning client. **Note:** If you do not configure a value for both the ESMSRVR and CONFERENCE_FACTORY_URI parameters and the user does not configure the corresponding values in Avaya Workplace Client settings, desktop clients do not display the **New Conversation +** option at the bottom of the main window. If this parameter is not provisioned, Communication Manager adhoc conferencing is used. For example, `SET CONFERENCE_FACTORY_URI`

Type	Default value	Supported platforms	Description
			`+15552220881@yourenterprise.com` . **Note:** If you use Avaya Workplace VDI in the Desk Phone mode on the Windows platform, this parameter value must be empty or you must not specify this parameter in the settings file as Avaya Workplace VDI does not support advanced adhoc conferencing. Client Navigation: **Settings** > **Services** > **Phone Service** > **Adhoc Conference Address**
CONFERENCE_ACCESS_NUMBER			
String	Null	• Android • iOS • Mac • Windows	The primary conference access number. This parameter populates the meeting invitation dial-in number for participants. • Avaya Equinox® Conferencing: This parameter is the Auto-Attendant number found on the Avaya Equinox® Management settings pane. This parameter is required only

Type	Default value	Supported platforms	Description
			for Avaya Equinox® Conferencing 9.0.1 and earlier versions. • Avaya Aura® Conferencing: This parameter is the Service URI in the provisioning client. The conference access numbers are found in My Meeting Resources on the Avaya Aura® Conferencing portal. For example, `SET CONFERENCE_ACCESS_NUMBER +15552221000` . Client Navigation: On desktop clients **Settings** > **Services** > **My Meeting Room** > **Conference Access Number**
ADDITIONAL_CONFERENCE_ACCESS_NUMBER_LIST			
String	Null	• Mac • Windows	The additional PSTN conference access numbers. This parameter

Type	Default value	Supported platforms	Description
			provides alternate dial-in numbers in the meeting invite. Available on Avaya Equinox® Conferencing and Avaya Aura® Conferencing. For example, `SET ADDITIONAL_CONFERENCE_ACCESS_NUMBER_LIST` `Label1:Number1,Label2:Number2,...,LabelN:NumberN` . Client Navigation: Not Applicable
UNIFIEDPORTALENABLED			
Numeric	0	• Android • iOS • Mac • Windows	This parameter determines whether the Avaya Equinox® Conferencing meeting account is enabled for a user. This parameter is mandatory for MeetMe conferences. The options are: • 0: Indicates that the Avaya Equinox® Conferencing meeting account is disabled. • 1: Indicates that the Avaya

Type	Default value	Supported platforms	Description
			Equinox® Conferencing meeting account is enabled. Client Navigation: **Settings** > **Services** > **My Meeting Room** > **My Meeting Room**
CONFERENCE_PORTAL_URI			
String	Null	• Android • iOS • Mac • Windows	The Conference Portal address for the user. This parameter is used to: • Populate the meeting invitation location field with the URL for participants to join the meeting. • Connect to the portal to retrieve the meeting invitation template. Available on Avaya Equinox® Conferencing and Avaya Aura® Conferencing. This parameter is mandatory for MeetMe conferences. For example, `SET CONFERENCE_PORTAL_URI`

Type	Default value	Supported platforms	Description
			`https://meetings.avaya.com/portal/tenants/9022/?ID=90319870153431` . In this release, you can use a short URL without the tenant information to join a meeting. For example, `https://meetings.avaya.com/portal/?ID=90319870153431`. Client Navigation: **Settings** > **Services** > **My Meeting Room** > **Meeting Address**
UNIFIED_PORTAL_SSO			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates the authentication mechanism that Unified Portal uses. The options are: • 0: Indicates that you need to enter the credentials manually. • 1: Indicates that Unified Portal uses unified login. • 3: Indicates that Unified Portal uses Avaya

Type	Default value	Supported platforms	Description
			Authorization Service. Client Navigation: **Settings** > **Services** > **Sign In Service** > **My Meeting Room**
UNIFIED_PORTAL_USERNAME			
String	Null	• Android • iOS • Mac • Windows	The Unified Portal user name. Client Navigation: **Settings** > **Accounts** > **My Meeting Room** > **Username**
UNIFIED_PORTAL_PASSWORD			
String	Null	• Android • iOS • Mac • Windows	The Unified Portal password. Client Navigation: **Settings** > **Accounts** > **My Meeting Room** > **Password**
CONFERENCE_MODERATOR_CODE			
Numeric	Null	• Android • iOS • Mac • Windows	The conference moderator code. Use this parameter to start your meetings. Users can click to join their bridge by using a UC client.

Type	Default value	Supported platforms	Description
			Only available in Avaya Aura® Conferencing. You can find the moderator code in My Meeting Resources on the Avaya Aura® Conferencing portal. For example, `SET CONFERENCE_MODERATOR_CODE 683044`. Client Navigation: **Settings** > **Services** > **My Meeting Room** > **Moderator Code**
CONFERENCE_PARTICIPANT_CODE			
Numeric	Null	• Android • iOS • Mac • Windows	The conference participant code. This parameter populates the meeting template with the code for participants to join meetings. Users can share their participant code with other users in Calendar invites by using the Share My Bridge feature. Only available in Avaya Aura® Conferencing. You can find the participant code in My Meeting Resources on the Avaya Aura® Conferencing portal. For example, `SET CONFERENCE_PARTICIPANT_CODE 03974587`

Type	Default value	Supported platforms	Description
			. Client Navigation: **Settings** > **Services** > **My Meeting Room** > **Participant Code**
CONFERENCE_PARTICIPANT_URL			
String	Null	• Mac • Windows	The conference participant URL. This parameter populates the meeting template and the location field with the URL to join the meeting. This parameter applies to Avaya Aura® Conferencing. Client Navigation: On desktop clients: **Settings** > **Services** > **My Meeting Room** > **Participant URL**
CONFERENCE_VIRTUAL_ROOM			
String	Null	• Android • iOS • Mac • Windows	The Scopia Virtual Room ID of the virtual room owner. When Avaya Aura® Device Services is integrated with Avaya Equinox® Management, the Virtual Room of the user is provided as configuration data. Only available in Avaya Equinox® Conferencing.

Type	Default value	Supported platforms	Description
			You can find the Virtual Room number in the user settings on the Avaya Workplace Client conference portal. This property is provided in Avaya Workplace Client to facilitate the user to provide the value into the Avaya Workplace Client add-in for Microsoft Outlook. For example, `SET CONFERENCE_VIRTUAL_ROOM` `+171115552224545`. Client Navigation: Not Applicable
CONFERENCE_FQDN_SIP_DIAL_LIST			
String	Null	• Android • iOS • Mac • Windows	A list of Scopia conference bridges that can support SIP Enhanced Conference Experience. Top of Mind requires this automatic configuration setting to have all the Scopia or Avaya Workplace Client portal domains that you use, so that Top of Mind click to call can work. For example, `SET CONFERENCE_FQDN_SIP_DIAL_LIST` `Scopia.slav.com,Al`

Type	Default value	Supported platforms	Description
			`phascopia.slav.com,lab.slav.com,scopia.partner.com` . Client Navigation: Not Applicable
UCCPENABLED			
Numeric	1	- Android - iOS - Mac - Windows	The parameter controls the UCCP Conferencing protocol in the client. Only available in Avaya Equinox® Conferencing. This parameter is mandatory for MeetMe conferences. The options are: - 0: Indicates that the UCCP Conferencing protocol is disabled in the client. SIP CCMP is used for conferencing. - 1: Indicates that the UCCP Conferencing protocol is enabled in the client. You must enable this parameter only: - When the Equinox

Type	Default value	Supported platforms	Description
			- Conference Control element is accessible for Avaya Workplace Client. - In enterprise networks that support WebSockets. For example, `SET UCCPENABLED 1` . Client Navigation: Not Applicable
SHOW_EQUINOX_MEETING_PANEL_IN_TOM			
Numeric	1	- Android - iOS - Mac - Windows	The parameter determines whether Avaya Workplace Client displays the Workplace Meetings panel on the Top of Mind screen. This parameter applies if you are using only Avaya Equinox® Conferencing. You must disable this parameter if you are using only Avaya Aura® Conferencing. The options are: - 0: Indicates that Avaya Workplace Client does not display the Workplace

Type	Default value	Supported platforms	Description
			Meetings panel on the Top of Mind screen. - 1: Indicates that Avaya Workplace Client displays the Workplace Meetings panel on the Top of Mind screen. Client Navigation: Select the **Top of Mind** filter, and in the Workplace Meetings area, select **Hide**.
RECEIVE_ONLY_SHARING_ENABLED			
Numeric	0	- Mac - Windows	This parameter indicates whether the collaboration is receive-only. The options are: - 0: Indicates that the collaboration is both send and receive. - 1: Indicates that the collaboration is receive only. Client Navigation: Not Applicable
PREF_MUTE_MIC_WHEN_JOINING_MEETING			

Type	Default value	Supported platforms	Description
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates the microphone setting when the user joins a meeting. The options are: • 0: Indicates disabled. The microphone is unmuted when the user joins a meeting. • 1: Indicates enabled. The microphone is muted when the user joins a meeting. Client Navigation: **Settings** > **User Preferences** > **Audio / Video** > **Mute my Microphone when Joining Meeting**
PREF_BLOCK_CAMERA_WHEN_JOINING_MEETING			
Numeric	• 0: Desktop clients • 1: Mobile clients	• Android • iOS • Mac • Windows	This parameter indicates the camera setting when the user joins a meeting. The options are: • 0: Indicates disabled. The camera is unblocked when the user joins a meeting.

Type	Default value	Supported platforms	Description
			0 is the default value for desktop clients. - 1: Indicates enabled. The camera is blocked when the user joins a meeting. 1 is the default value for mobile clients. Client Navigation: **Settings** > **User Preferences** > **Audio / Video** > **Block my Camera when Joining Meeting**
HTTPUAENABLED			
Numeric	1	Windows	This parameter indicates whether CSDK HTTP UA is enabled to connect to the Avaya Web Gateway. The options are: - 0: Indicates that CSDK HTTP UA cannot connect to the Avaya Web Gateway. - 1: Indicates that CSDK HTTP UA can connect to the Avaya Web Gateway.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable
COLLAB_WHITEBOARDING_ENABLED			
Numeric	1	Windows	This parameter indicates whether users can share their whiteboards during an Avaya Equinox® Conferencing conference call. This parameter applies to all types of Avaya Equinox® Conferencing conference calls. For example, Meet-Me conference, Adhoc conference, Presentation-only meetings, and Data-only screen sharing from an instant messaging conversation. The options are: • 0: Indicates that users cannot share their whiteboards during a conference call. • 1: Indicates that users can share their whiteboards during a conference call. Client Navigation: Not Applicable

Type	Default value	Supported platforms	Description
COLLAB_SCREENSHARE_ENABLED			
Numeric	1	Windows	This parameter indicates whether users can share their full screen or part of the screen during an Avaya Equinox® Conferencing conference call. This parameter applies to all types of Avaya Equinox® Conferencing conference calls. For example, Meet-Me conference, Adhoc conference, Presentation-only meetings, and Data-only screen sharing from an instant messaging conversation. The options are: • 0: Indicates that users cannot share their screens during a conference call. • 1: Indicates that users can share their screens during a conference call. Client Navigation: Not Applicable
COLLAB_SHAREAPPLICATION_ENABLED			

Type	Default value	Supported platforms	Description
Numeric	1	Windows	This parameter indicates whether users can share their application during an Avaya Equinox® Conferencing conference call. This parameter applies to all types of Avaya Equinox® Conferencing conference calls. For example, Meet-Me conference, Adhoc conference, Presentation-only meetings, and Data-only screen sharing from an instant messaging conversation. The options are: • 0: Indicates that users cannot share their application during a conference call. Also, Avaya Workplace Client ignores the COLLAB_SHAREAPPLICATION_FILTER value. • 1: Indicates that users can share their application during a conference call. Client Navigation: Not Applicable

Type	Default value	Supported platforms	Description
COLLAB_SHAREAPPLICATION_FILTER			
String	Null	Windows	This parameter indicates the list of applications that users can share during an Avaya Equinox® Conferencing conference call. This parameter applies to all types of Avaya Equinox® Conferencing conference calls. For example, Meet-Me conference, Adhoc conference, Presentation-only meetings, and Data-only screen sharing from an instant messaging conversation. The default value is empty, which indicates that users can share all open applications on their desktops. For example, `SET` `COLLAB_SHAREAPPLICATION_FILTER ""` . To restrict sharing access to an application, you can specify the executable name of the application. For example: • To provide access to only the PowerPoint application, `SET COLLAB_SHAREAPPLICATION_FILTE`

Type	Default value	Supported platforms	Description

			`R`
			`"POWERPNT"`
			.
			• To provide access to the PowerPoint and Microsoft Teams applications, `SET COLLAB_SHAREAPPLICATION_FILTER`
			`"POWERPNT, Teams"`
			.
			The executable name is case insensitive. For example, for the PowerPoint application, POWERPNT, Powerpnt, and powerPnt are all valid.
			Client Navigation: Not Applicable

Automatic software updates parameters

Type	Default value	Supported platforms	Description
APPCAST_ENABLED			
Numeric	0	• Mac • Windows	This parameter indicates whether the service is enabled. The options are: • 0: Indicates disabled. • 1: Indicates enabled. Client Navigation: Not Applicable
APPCAST_URL			
String	Null	• Mac • Windows	The URL that defines the appcast feed used by the endpoints. Client Navigation: Not Applicable
APPCAST_CHECK_INTERVAL			
Numeric	1	• Mac • Windows	The interval at which endpoints check for software updates. The value range for this parameter is 0 to 30 days. The value 0 indicates that automatic checking is disabled.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable

Avaya Multimedia Messaging parameters

Use the following automatic configuration parameters if you configured Avaya Workplace Client to interwork with Avaya Multimedia Messaging:

Type	Default value	Supported platforms	Description
ESMENABLED			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Multimedia Messaging is enabled. The options are: • 0: Indicates that Avaya Multimedia Messaging is disabled. • 1: Indicates that Avaya Multimedia Messaging is enabled. **Note:** If you disable the ESMENABLED parameter and leave the CONFERENCE_FACTORY_URI parameter empty and the user does not enable and configure the corresponding values in Avaya Workplace

Type	Default value	Supported platforms	Description
			Client settings, desktop clients do not display the **New Conversation +** option at the bottom of the main window. Client Navigation: **Settings** > **Services** > **Multimedia Messaging** > **Multimedia Messaging**
ESMSSO			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates the authentication mechanism that the Avaya Multimedia Messaging service uses. The options are: • 0: Indicates that you need to manually enter the credentials. • 1: Indicates that Avaya Multimedia Messaging uses unified login. • 3: Indicates that Avaya Multimedia Messaging uses Avaya Authorization Service. Client Navigation: **Settings** > **Services** > **Sign In Service** > **Multimedia Messaging**

Type	Default value	Supported platforms	Description
ESMUSERNAME			
String	Null	• Android • iOS • Mac • Windows	The Avaya Multimedia Messaging account user name. Client Navigation: **Settings** > **Accounts** > **Multimedia Messaging** > **Username**
ESMPASSWORD			
String	Null	• Android • iOS • Mac • Windows	The Avaya Multimedia Messaging account password. Client Navigation: **Settings** > **Accounts** > **Multimedia Messaging** > **Password**
ESMSRVR			
String	Null	• Android • iOS • Mac • Windows	The IP address or fully qualified domain name of the Avaya Multimedia Messaging server. **Note:** If you do not configure a value for both the ESMSRVR and CONFERENCE_FACTORY_URI parameters and the user does not configure the corresponding values in Avaya Workplace Client settings, desktop clients do not display the **New Conversation +** option at the bottom of the main window. Client Navigation: **Settings** > **Services** > **Multimedia**

Type	Default value	Supported platforms	Description
			Messaging > **Server Address**
ESMPORT			
Numeric	8443	• Android • iOS • Mac • Windows	The port of the Avaya Multimedia Messaging server. Client Navigation: **Settings** > **Services** > **Multimedia Messaging** > **Server Port**
ESMSECURE			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates whether TLS is being used. The options are: • 0: Indicates that TLS is not used. • 1: Indicates that TLS is used. Client Navigation: Not Applicable
ESMREFRESH			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates the Avaya Multimedia Messaging refresh interval in minutes. Valid values are 0, 10, 30, and 60. The default value indicates continuous mode. **Note:**

Type	Default value	Supported platforms	Description
			The manual mode option is no longer supported. Client Navigation: **Settings** > **Services** > **Multimedia Messaging** > **Polling Interval**
ESMHIDEONDISCONNECT			
Numeric	0	• Android • iOS	This parameter is used to hide Avaya Multimedia Messaging conversations and message details in the Messages screen and Messaging area of the Top Of Mind screen when not connected to Avaya Multimedia Messaging. The options are: • 0: Indicates disabled. Avaya Multimedia Messaging conversations and message details are visible when not connected to Avaya Multimedia Messaging. • 1: Indicates enabled. Avaya Multimedia Messaging conversations and message details are hidden when not connected

Type	Default value	Supported platforms	Description
			to Avaya Multimedia Messaging. Client Navigation: Not Applicable
ESMSENDREADRECEIPTS			
Numeric	1	- Android - iOS - Mac - Windows	This parameter is used to enable or disable the use of read receipts for all users. The options are: - 0: Indicates that read receipts are disabled. - 1: Indicates that read receipts are enabled. If you set a value for this parameter, the: - User preference is overwritten. - **Send read receipts** option is hidden. Client Navigation: **Settings** > **User Preferences** > **Messaging** > **Send read receipts**

Avaya Aura Device Services parameters

Use the following automatic configuration parameters if you configured Avaya Workplace Client to interwork with Avaya Aura® Device Services:

Type	Default value	Supported platforms	Description
ACSENABLED			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Aura® Device Services is enabled. The options are: • 0: Indicates that Avaya Aura® Device Services is disabled. • 1: Indicates that Avaya Aura® Device Services is enabled. Client Navigation: **Settings** > **Services** > **Device Services** > **Device Services**
ACSSRVR			
String	Null	• Android • iOS • Mac • Windows	The Avaya Aura® Device Services IP address or FQDN. Client Navigation: **Settings** > **Services** > **Device Services** > **Server Address**
ACSPORT			
Numeric	443	• Android • iOS • Mac • Windows	The Avaya Aura® Device Services port. Client Navigation: **Settings** > **Services** > **Device Services** > **Server Port**
ACSSECURE			

Type	Default value	Supported platforms	Description
Numeric	1	- Android - iOS - Mac - Windows	This parameter indicates whether TLS is being used. The options are: - 0: Indicates that TLS is not used. - 1: Indicates that TLS is used. Client Navigation: Not Applicable
ACSSSO			
Numeric	1	- Android - iOS - Mac - Windows	This parameter indicates that the authentication mechanism that Avaya Aura® Device Services uses. The options are: - 0: Indicates that you need to manually enter the credentials. - 1: Indicates that Avaya Aura® Device Services uses unified login. - 3: Indicates that Avaya Aura® Device Services uses Avaya Authorization Service. Client Navigation: **Settings** > **Services** >

Type	Default value	Supported platforms	Description
			Sign In Service > **Device Services**
ACSUSERNAME			
String	Null	• Android • iOS • Mac • Windows	The Avaya Aura® Device Services user name. Client Navigation: **Settings** > **Accounts** > **Device Services** > **Username**
ACSPASSWORD			
String	Null	• Android • iOS • Mac • Windows	The Avaya Aura® Device Services password. Client Navigation: **Settings** > **Accounts** > **Device Services** > **Password**
CONTACT_MATCHING_SEARCH_LOCATION			
Numeric	1	• Android • iOS • Mac • Windows	This parameter determines whether Avaya Workplace Client performs contact resolution using the local contact cache or by searching Avaya Aura® Device Services or both. The options are: • 1: All. • 2: Local. • 3: Avaya Aura® Device Services. Client Navigation: Not Applicable
AVAYA_AUTHORIZATION_REALM			

Type	Default value	Supported platforms	Description
String	Null	• Android • iOS • Mac • Windows	This parameter identifies the OAuth realm for UC Services integrating with Avaya Authorization Service (Keycloak). If the realm cannot be discovered dynamically, but you want to update the configuration with the ACSSSO parameter from 1 to 3, then you must do the following: • `SET ACSSSO 3`. • `SET AVAYA_AUTHORIZATION_REALM {SolutionRealm}`. • Refresh the settings file. Client Navigation: Not Applicable

Client Enablement Services parameters

Use the following parameters if Avaya Workplace Client for Android and iOS are configured to interwork with Client Enablement Services. Client Enablement Services is not supported on Avaya Workplace Client for Mac and Windows.

Note:

Avaya Workplace Client on Avaya Vantage™ does not support Client Enablement Services.

Type	Default value	Supported platforms	Description
CESENABLED			
Numeric	0	• Android • iOS	This parameter indicates whether Client Enablement Services is enabled. The options are: • 0: Indicates disabled. • 1: Indicates enabled. Client Navigation: **Settings** > **Services** > **Client Enablement (CES)**: • On Avaya Workplace Client for Android: **CES** • On Avaya Workplace Client for iOS: **Client Enablement Services**
CESSSO			
Numeric	1	• Android • iOS	This parameter indicates the authentication mechanism that Client Enablement Services uses. The options are: • 0: Indicates that you need to manually enter the credentials.

Type	Default value	Supported platforms	Description
			- 1: Indicates that Client Enablement Services uses unified login. Client Navigation: **Settings** > **Services** > **Sign In Service** > **Client Enablement (CES)**
CESUSERNAME			
String	Null	- Android - iOS	The Client Enablement Services account name. Client Navigation: **Settings** > **Accounts** > **Client Enablement Services** > **Username**
CESPASSWORD			
String	Null	- Android - iOS	The Client Enablement Services account password. Client Navigation: **Settings** > **Accounts** > **Client Enablement Services** > **Password**
CESSRVR			
String	Null	- Android - iOS	The IP address or fully qualified domain name of the Client Enablement Services server. Client Navigation: **Settings** > **Services** > **Client Enablement (CES)** > **Server Address**
CESPORT			

Type	Default value	Supported platforms	Description
Numeric	7777	- Android - iOS	The Client Enablement Services server port. Client Navigation: **Settings** > **Services** > **Client Enablement (CES)** > **Server Port**
CESSECURE			
Numeric	1	- Android - iOS	This parameter indicates whether TLS is being used. The options are: - 0: Indicates that TLS is not used. - 1: Indicates that TLS is used. **Note:** Avaya Workplace Client only supports TLS connections to Client Enablement Services. The user cannot change this value from the Settings menu in the application. Client Navigation: Not Applicable
CESVMPIN			
Numeric	Null	- Android - iOS	The voice mail PIN required for visual voice mail.

Type	Default value	Supported platforms	Description
			Client Navigation: **Settings** > **Services** > **Voicemail** > **PIN**

Desktop integration parameters

Type	Default value	Supported platforms	Description
DESKTOP_HTTP_APPLICATION_INTEGRATION			
Numeric	1	• Mac • Windows	This parameter controls the desktop HTTP application integration. The options are: • 0: Indicates that the desktop HTTP application integration is disabled. • 1: Indicates that the desktop HTTP application integration is enabled. The external application API controls the headset API integration with Poly Hub and Jabra Direct. The external application API does not control the native support for Poly and Jabra headsets.

Type	Default value	Supported platforms	Description
			Native support indicates Out-of-the-box support. Client Navigation: Not Applicable.
ENABLE_OUTLOOK_ADDON			
Numeric	1	• Mac • Windows	This parameter controls the Outlook add-in functionality. The options are: • 0: Indicates that the Outlook add-in functionality is disabled. • 1: Indicates that the Outlook add-in functionality is enabled. 1 is the default value in the UC and OTT signed-in user modes. Client Navigation: **Settings** > **Desktop Integration** > **Outlook Add-in** > **Enable Outlook Add-In**.
OUTLOOK_CALL_CONTACT			
Numeric	1	• Mac • Windows	This parameter controls the Outlook add-in Call

Type	Default value	Supported platforms	Description
			Contact functionality by deployment or user preference. The options are: • 0: Indicates that the Outlook add-in Call Contact functionality is disabled. • 1: Indicates that the Outlook add-in Call Contact functionality is enabled. Client Navigation: **Settings** > **Desktop Integration** > **Outlook Add-in** > **Allow calls from Outlook contacts**.
ENABLE_LOCAL_CONTACT			
Numeric	1	Windows	This parameter controls the local contact integration. The options are: • 0: Indicates that the local contact integration is disabled. • 1: Indicates that the local contact

Type	Default value	Supported platforms	Description
			integration is enabled. Client Navigation: **Settings** > **User Preferences** > **Contacts** > **Show Local Contacts**.
OUTLOOK_ADDON_HOST_URI			
		- Mac - Windows	This parameter indicates the HTTP location of the JavaScript Outlook add-in. Client Navigation: Not Applicable.
ENABLE_PLT_OOB_HEADSET_CALL_CONTROL			
Numeric	1	- Mac - Windows	This parameter controls the native headset integration for Poly headsets. The options are: - 0: Indicates that the native headset integration is disabled for Poly headsets. - 1: Indicates that the native headset integration is enabled for Poly headsets.

Type	Default value	Supported platforms	Description
			Customers might use multiple softclients. You can disable this parameter to minimize application integration issues with other desktop applications. Client Navigation: Not Applicable.
ENABLE_JABRA_OOB_HEADSET_CALL_CONTROL			
Numeric	1	• Mac • Windows	This parameter controls the native headset integration for Jabra headsets. The options are: • 0: Indicates that the native headset integration is disabled for Jabra headsets. • 1: Indicates that the native headset integration is enabled for Jabra headsets. Customers might use multiple softclients. You can disable this parameter to minimize application integration issues with other desktop applications. Client Navigation: Not Applicable.

Type	Default value	Supported platforms	Description
ENABLE_TOP_OF_MIND			
Numeric	1	Windows	This parameter controls the Top Of Mind feature. The options are: • 0: Indicates that the Top Of Mind feature is disabled. Avaya Workplace Client does not retrieve any calendar information. Also, the Top Of Mind and Calendar buttons are unavailable. • 1: Indicates that the Top Of Mind feature is enabled. Client Navigation: Not Applicable.
ENABLE_MEETING_SCHEDULER			
Numeric	1	Windows	This parameter controls whether to display Avaya Meeting Scheduler in the Outlook Ribbon area. The options are: • 0: Indicates that the Avaya

Type	Default value	Supported platforms	Description
			Meeting Scheduler is not displayed in the Outlook Ribbon area. - 1: Indicates that the Avaya Meeting Scheduler is displayed in the Outlook Ribbon area. **Note:** Only the desktop version is supported, and the Outlook Web plugin and MAC are not supported. Client Navigation: Not Applicable.

EC500 parameters

Type	Default value	Supported platforms	Description
EC500ENABLED			
Numeric	0	- Android - iOS	This parameter indicates whether EC500 is enabled. The options are: - 0: Indicates disabled.

Type	Default value	Supported platforms	Description
			• 1: Indicates enabled. Client Navigation: **Settings** > **Services** > **EC500 Calling** > **EC500 Calling**
EC500VOICEMAILNUMBER			
Numeric	Null	• Android • iOS	The voice mail system access number. Endpoints can retrieve this value from multiple sources. A summary of this logic is: • With SIP, the number comes from the PPM protocol, which pulls the configuration from Avaya Aura®. • With Client Enablement Services, the number comes from the Client Enablement Services server. • In other situations, the number comes from this parameter. Client Navigation: **Settings** > **Services** >

Type	Default value	Supported platforms	Description
			Voicemail > **System Number**
FNUIDLEAPPEARANCESELECT			
Numeric	Null	• Android • iOS	The number to dial for the Idle Appearance Select feature. This number is used to identify an idle line on your extension when you make a call. Client Navigation: **Settings** > **Services** > **EC500 Calling** > **Idle Appearance Select**
FNUSIMRINGENABLE or FNUOFFPBXCALLENABLE			
Numeric	Null	• Android • iOS	The number to dial for enabling Off-PBX calls. This number is used to enable your mobile phone to ring when you receive a call on your deskphone. Client Navigation: **Settings** > **Services** > **EC500 Calling** > **Off PBX Call Enable**
FNUSIMRINGDISABLE or FNUOFFPBXCALLDISABLE			
Numeric	Null	• Android • iOS	The number to dial for disabling Off-PBX calls. This number is used to disable your mobile

Type	Default value	Supported platforms	Description
			phone from ringing when you receive a call on your deskphone. Client Navigation: **Settings** > **Services** > **EC500 Calling** > **Off PBX Call Disable**
FNUCFWDENABLE or FNUCFWDALL			
Numeric	Null	• Android • iOS	The number to dial for enabling call forwarding for all calls. Client Navigation: **Settings** > **Services** > **EC500 Calling** > **Call Forward All Enable**
FNUCFWDDISABLE or FNUCFWDCANCEL			
Numeric	Null	• Android • iOS	The number to dial for canceling call forwarding. Client Navigation: **Settings** > **Services** > **EC500 Calling** > **Call Forward All Disable**
FNUACTIVEAPPEARANCESELECT			
Numeric	Null	• Android • iOS	The number to dial for the Active Appearance Select feature. This number is used to join an active call on your deskphone using your mobile phone.

Type	Default value	Supported platforms	Description
			Client Navigation: **Settings** > **Services** > **EC500 Calling** > **Active Appearance Select**
FNUSACENABLE			
Numeric	Null	• Android • iOS	The number to dial for enabling the Send All Calls feature. This number is used to send all calls to a predefined number set on the server. Client Navigation: **Settings** > **Services** > **EC500 Calling** > **Send All Calls Enable**
FNUSACCANCEL			
Numeric	Null	• Android • iOS	The number to dial for disabling the Send All Calls feature. This number is used to disable the sending of all calls to a predefined number set on the server. Client Navigation: **Settings** > **Services** > **EC500 Calling** > **Send All Calls Disable**
FNE_SETUP_DELAY			
Numeric	3	• Android • iOS	This parameter indicates the delay in seconds between the EC500 call

Type	Default value	Supported platforms	Description
			being placed and the transmission of the digits for EC500. The default value is in seconds. The purpose of this setting is to address call setup delays with specific regions and trunk providers. Client Navigation: **Settings** > **Advanced** > **FNE Setup Delay**
STATION_SECURITY_ENABLED			
Numeric	0	• Android • iOS	This parameter indicates whether EC500 station security is enabled. The station security code reduces the risk of toll fraud. The options are: • 0: Indicates that EC500 station security is disabled. • 1: Indicates that EC500 station security is enabled. Client Navigation: **Settings** > **Services** >

Type	Default value	Supported platforms	Description
			EC500 Calling > **Station Security**

Dialing rule parameters

Note:

If the number after applying dialing rules includes an emergency number as a prefix, then Avaya Workplace Client dials the initial number and does not apply the dialing rules.

Type	Default value	Supported platforms	Description
ENHDIALSTAT			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether dialing rules are enabled. The options are: • 0: Indicates disabled. • 1: Indicates enabled. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Dialing Rules**
PHNOL			
Numeric	Null	• Android • iOS • Mac • Windows	The number to dial to access an external line. Client Navigation: **Settings** > **Advanced** >

Type	Default value	Supported platforms	Description
			Dialing Rules > **Number to dial to access an outside line**
PHNCC			
Numeric	Null	• Android • iOS • Mac • Windows	The country code. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Your country code**
SP_AC or DIALPLANAREACODE			
Numeric	Null	• Android • iOS • Mac • Windows	The area or city code. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Your area/city code**
PHNPBXMAINPREFIX or DIALPLANPBXPREFIX			
Numeric	Null	• Android • iOS • Mac • Windows	The PBX main prefix. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **PBX main prefix**
PHNLD			
Numeric	Null	• Android • iOS • Mac • Windows	The number to dial for long distance calls. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Number**

Type	Default value	Supported platforms	Description
			to dial for long distance calls
PHNIC			
Numeric	Null	• Android • iOS • Mac • Windows	The number to dial for international calls. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Number to dial for international calls**
PHNDPLENGTH			
Numeric	Null	• Android • iOS • Mac • Windows	The internal extension length. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Length of internal extensions**
DIALPLANEXTENSIONLENGTHLIST			
String	Null	• Android • iOS • Mac • Windows	A list of PHNDPLENGTH values separated by commas. This parameter takes precedence over PHNDPLENGTH. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Length of internal extensions**

Type	Default value	Supported platforms	Description
PHNLDLENGTH			
Numeric	Null	• Android • iOS • Mac • Windows	The length of national phone numbers. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Length of national phone numbers**
DIALPLANNATIONALPHONENUMLENGTHLIST			
String	Null	• Android • iOS • Mac • Windows	A list of PHNLDLENGTH values separated by commas. This parameter takes precedence over PHNLDLENGTH. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Length of national phone numbers**
PHNREMOVEAREACODE or DIALPLANLOCALCALLPREFIX			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether the area code must be removed for local calls. The options are: • 0: Indicates disabled. Area code is not removed for local calls.

Type	Default value	Supported platforms	Description
			- 1: Indicates enabled. Area code is removed for local calls. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Remove area/city code for local calls**
AUTOAPPLY_ARS_TO_SHORTNUMBERS			
Numeric	1	- Android - iOS - Mac - Windows	This parameter disables the dialing rule logic that automatically appends the ARS code to numbers that are shorter than the shortest extension length. The options are: - 0: Indicates disabled. - 1: Indicates enabled. Client Navigation: Not applicable
APPLY_DIALINGRULES_TO_PLUS_NUMBERS			
Numeric	0	- Android - iOS - Mac - Windows	This parameter is used to replace the plus sign (+) with dial plan digits. When possible, configure the plus (+) dialing option in Session Manager

Type	Default value	Supported platforms	Description
			instead of enabling this parameter. The options are: • 0: Indicates false. • 1: Indicates true. Client Navigation: **Settings** > **Advanced** > **Dialing Rules** > **Apply dialing rules to '+' numbers**
ELD_SYSNUM			
Numeric	1	• Mac • Windows	This parameter indicates whether to apply the enhanced dialing rules logic to Autodial and Busy indicators. The options are: • 0: Indicates disabled. Avaya Workplace Client does not apply the enhanced dialing rules logic to Autodials and Busy indicators. • 1: Indicates enabled. Avaya Workplace Client applies the enhanced dialing rules

Type	Default value	Supported platforms	Description
			logic to Autodials and Busy indicators. **Note:** Avaya Workplace Client applies the enhanced dialing rules logic only if dialing rules are enabled, that is, the ENHDIALSTAT parameter value is 1 and the ELD_SYSNUM parameter value is 1.

Presence parameters

Type	Default value	Supported platforms	Description
DND_SAC_LINK			
Numeric	0	• Android • iOS • Mac • Windows	This parameter activates the Send All Calls feature when the user sets the presence status to Do Not Disturb. The options are: • 0: Indicates that the Send All Calls feature is not activated. • 1: Indicates that the Send All Calls feature is activated. Client Navigation: **Settings** > **User**

Type	Default value	Supported platforms	Description
			Preferences > **General** > **Activate SAC When DND Is Set**.
WINDOWS_IMPROVIDER			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client is the IM provider for Windows clients. The options are: • 0: Indicates that Avaya Workplace Client is not the IM provider for Windows clients. • 1: Indicates that Avaya Workplace Client is the IM provider for Windows clients. The IM provider enables Microsoft Outlook, SharePoint, and other applications to: • Use Avaya Workplace Client for any initiated IM or a call from a contact card. • Display presence of Avaya

Type	Default value	Supported platforms	Description
			Workplace Client contacts. Client Navigation: **Settings** > **Desktop Integration** > **IM Provider** > **Set as default IM Provider**.
WINDOWS_IMPROVIDER_RESOLVE_CONTACT_EXTERNAL			
Numeric	0	Windows	This parameter controls the Enhanced IM Provider feature. The options are: • 0: Indicates that the Enhanced IM Provider feature is disabled. If disabled, presence in Microsoft Outlook, SharePoint, and other applications is only shown for Avaya Workplace Client contacts. • 1: Indicates that the Enhanced IM Provider feature is enabled. Users can see presence of all users, including non-local and

Type	Default value	Supported platforms	Description
			non-merged users. If enabled, this parameter enables presence in Microsoft Outlook, SharePoint, and other applications if presence can be resolved for that user. Client Navigation: Not Applicable.
OBSCURE_PRESENCE_STATES			
String	Null	• Mac • Windows	This parameter is used to hide one or more presence states from the presence chooser in Avaya Workplace Client. For example, `SET OBSCURE_PRESENCE_STATES "automatic,available,busy,away,donotdisturb,outoffice,offline"` If you hide all presence states, Avaya Workplace Client disables the presence chooser and the default presence state is Automatic. Client Navigation: Not Applicable.

Type	Default value	Supported platforms	Description
AUTO_AWAY_TIME			
Numeric	10	• Android • iOS • Mac • Windows	This parameter indicates the idle time in minutes after which the presence status of the user automatically changes to **Away**. The value is normalized to 0, 5, 10, 15, 30, 60, 90, or 120. The value 0 disables the feature. **Note:** The value 5 is supported only on desktop clients. Client Navigation: **Settings** > **User Preferences** > **General** > **Auto Set to Away**.
ENABLE_PRESENCE			
Numeric	1	• Android • iOS • Windows	This parameter indicates whether Avaya Workplace Client publishes the Unified Communications (UC) or agent presence. The options are: • 0: Indicates that presence is disabled. 1: Indicates that Avaya Workplace Client publishes the UC presence. 2: Indicates that Avaya Workplace

Type	Default value	Supported platforms	Description
			Client publishes the: - UC presence when the agent is not logged in - Agent presence when the agent is logged in Client Navigation: Not Applicable.

Calendar Integration parameters

Use the following parameters if Avaya Workplace Client is configured for calendar integration including Outlook, Exchange, and Google:

Type	Default value	Supported platforms	Description
EWSENABLED			
Numeric	0	- Android - iOS - Mac - Windows	This parameter indicates whether exchange calendar integration is enabled. The options are: - 0: Indicates that the exchange

Type	Default value	Supported platforms	Description
			calendar integration is disabled. - 1: Indicates that the exchange calendar integration is enabled. Client Navigation: **Settings** > **Services** > **Exchange Calendar** > **Exchange Calendar**
EWSSSO			
Numeric	1	- Android - iOS - Mac - Windows	This parameter indicates the authentication mechanism that EWS uses. The options are: - 0: Indicates that you need to manually enter the credentials. - 1: Indicates that EWS uses unified login. - 4: Indicates that EWS uses Microsoft Modern Authentication. Client Navigation: **Settings** > **Services** > **Sign In Service** > **Exchange Calendar**
EWSSERVERADDRESS			

Type	Default value	Supported platforms	Description
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the server address that can be used to connect to EWS directly. For example, usmail.slav.com. If you configure this parameter, Avaya Workplace Client tries to establish a connection to EWS directly using the server address and avoids the Auto Discover process. Client Navigation: **Settings** > **Services** > **Exchange Calendar** > **Server Address**
EWSDOMAIN			
String	Null	• Android • iOS • Mac • Windows	The Exchange server domain. For example, avaya.com. The Auto Discover process uses EWSDOMAIN to find an EWS endpoint. Client Navigation: **Settings** > **Services** > **Exchange Calendar** > **Domain**
EWSUSERNAME			
String	Null	• Android • iOS • Mac • Windows	The Exchange account user name. This parameter must have the user name portion of a user's Exchange email address. For example, for an Exchange email address username@avaya.com,

Type	Default value	Supported platforms	Description
			EWSUSERNAME = username. - If EWS uses unified login, this parameter is ignored and SSOUSERID is used. - If EWS does not use unified login, this parameter is used. - If EWS does not use unified login and this parameter is not specified in the settings file, the user can view the EWS user name setting in the Automatic configuration wizard. Client Navigation: **Settings** > **Accounts** > **Exchange Calendar** > **Username**
EWSPASSWORD			
String	Null	- Android - iOS - Mac - Windows	The EWS account password. - If EWS uses unified login, this parameter is ignored and

Type	Default value	Supported platforms	Description
			SSOPASSWORD is used. - If EWS does not use unified login, this parameter is used. - If EWS does not use unified login and this parameter is not specified in the settings file, the user can view the EWS password setting in the Automatic configuration wizard. Client Navigation: **Settings** > **Accounts** > **Exchange Calendar** > **Password**
EWSREADTIMEOUT			
Numeric	300	Android	This parameter indicates the read timeout value. The value range for this parameter is 10 to 300 seconds. In a low-bandwidth network, Avaya Workplace Client needs sufficient time to download the required information, such as calendars and appointments with media attachments from EWS. Hence, in a low-

Type	Default value	Supported platforms	Description
			bandwidth network, specify the timeout value close to 300 seconds. However, there is a limitation with the Android client. When Avaya Workplace Client for Android waits for information from EWS, other services such as Avaya Aura® Device Services, Avaya Multimedia Messaging cannot authorize. Hence, in this case, specify the timeout value close to 10 seconds. Client Navigation: Not Applicable
CALENDAR_INTEGRATION_ENABLED			
Numeric	1	• Mac • Windows	This parameter indicates whether you want to enable all calendar integration including Outlook, Exchange, and Google with Avaya Workplace Client. The options are: • 0: Indicates that you want to disable calendar integration with Avaya Workplace Client. • 1: Indicates that you want to enable calendar integration with Avaya

Type	Default value	Supported platforms	Description
			Workplace Client. Client Navigation: Not Applicable
GOOGLE_CALENDAR_INTEGRATION_ENABLED			
Numeric	0	Windows	This parameter indicates whether you want to integrate Google calendar with Avaya Workplace Client. The options are: • 0: Indicates that you want to disable Google calendar integration with Avaya Workplace Client. • 1: Indicates that you want to enable Google calendar integration with Avaya Workplace Client. **Note:** You must enable the Google or Microsoft Exchange calendar, but not both simultaneously. If you enable both calendars using the EWSENABLED parameter and this parameter, Avaya Workplace Client displays

Type	Default value	Supported platforms	Description
			only the Microsoft Exchange calendar. Client Navigation: Not Applicable

Office 365 authorization

The Office 365 administrator must authorize calendar access if end-users do not have the necessary permission.

The Office 365 administrator can use the following URL to authorize calendar access for the Avaya Workplace Client calendar solution: https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=76626a48-7c17-4508-b5b7-0e0a6cf760d2&response_type=code&redirect_uri=com.avaya.equinox.exchange://callback&scope=https://graph.microsoft.com/.default&prompt=consent

LDAP parameters

Type	Default value	Supported platforms	Description
DIRENABLED			
Numeric	0	• Mac • Windows	This parameter indicates whether LDAP is enabled. The options are: • 0: Indicates disabled. • 1: Indicates enabled. Client Navigation: **Settings** > **Services** >

Type	Default value	Supported platforms	Description
			Enterprise Directory > **Enterprise Directory**
DIRSSO			
Numeric	1	• Mac • Windows	This parameter indicates the authentication mechanism that LDAP uses. The options are: • 0: Indicates that you need to manually enter the credentials. • 1: Indicates that LDAP uses unified login. Client Navigation: **Settings** > **Services** > **Sign In Service** > **Enterprise Directory**
DIRSRVR			
String	Null	• Mac • Windows	The IP address or fully qualified domain name of the LDAP server. Client Navigation: **Settings** > **Services** > **Enterprise Directory** > **Server Address**
DIRSRVRPRT			
Numeric	636	• Mac • Windows	The port number of the LDAP server. Client Navigation: **Settings** > **Services** >

Type	Default value	Supported platforms	Description
			Enterprise Directory > **Server Port**
DIRUSERNAME			
String	Null	• Mac • Windows	The LDAP authentication user name. Client Navigation: **Settings** > **Accounts** > **Enterprise Directory** > **Username**
DIRPASSWORD			
String	Null	• Mac • Windows	The LDAP authentication password. Client Navigation: **Settings** > **Accounts** > **Enterprise Directory** > **Password**
DIRTOPDN			
String	Null	• Mac • Windows	The LDAP search base. For example, `OU=Global Users,DC=global,DC=avaya,DC=com`. Client Navigation: **Settings** > **Services** > **Enterprise Directory** > **LDAP Search Base**
DIRSECURE			
Numeric	1	• Mac • Windows	This parameter indicates whether to use TLS or TCP for LDAP. The options are: • 0: Indicates TCP.

Type	Default value	Supported platforms	Description
			- 1: Indicates TLS. Client Navigation: **Settings** > **Services** > **Enterprise Directory** > **Use TLS**
DIRIMATTRIBUTE			
String	mail	- Mac - Windows	This parameter value is processed as an instant messaging address. The client provides access to the enterprise directory search using a direct LDAP connection. While processing the results, the client can process the attribute, such as telephoneNumber, specified in this parameter 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. **Note:** If LDAP search is used, then the user's LDAP profile must have the same attribute configured which is specified in this parameter. Client Navigation: Not Applicable

Type	Default value	Supported platforms	Description
DIRUSEIMDOMAIN			
Numeric	1	• Mac • Windows	This parameter indicates whether the client must perform a mapping to the IM domain. The options are: • 0: Indicates disabled. • 1: Indicates enabled. In this parameter, the telephone number of the user is mapped into the IM domain. Example: 16135551212 becomes **16135551212@presence.example.com** if the IM domain is presence.example.com. This parameter is also used if an email address field is used. For example, alice@example.com becomes **alice@presence.example.com**. This parameter is only enabled in single domain deployments. You must not use domain mapping if any form of messaging federation is in place. Instead, ensure that the correct IM address is stored in an LDAP attribute. Client Navigation: Not Applicable

Type	Default value	Supported platforms	Description
DIRTYPE			
String	ACTIVEDIRECTORY	• Mac • Windows	The type of LDAP directory to which the endpoint connects. Valid values are: • ACTIVEDIRECTORY • DOMINO • NOVELL Client Navigation: Not Applicable
DIRSCOPE			
String	LDAP_SCOPE_SUBTREE	• Mac • Windows	This parameter defines the scope of the LDAP search. Valid values are: • LDAP_SCOPE_BASE • LDAP_SCOPE_ONELEVEL • LDAP_SCOPE_SUBTREE Client Navigation: Not Applicable
DIRTIMEOUT			
Numeric	100	• Mac • Windows	The search time-out interval in seconds. The range is 10 to 200.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable
DIRMAXENTRIES			
Numeric	50	• Mac • Windows	The maximum number of matching entries to display. The range is 10 to 100. **Note:** If you are using Avaya Aura® Device Services, you must not configure a value greater than 50. Client Navigation: Not Applicable
DIR_CONTACT_RESOLUTION_ENABLED			
Numeric	1	• Mac • Windows	This parameter enables quick search contact resolution by using the LDAP provider. The options are: • 0: Indicates disabled. • 1: Indicates enabled. Client Navigation: Not Applicable

Media parameters

Type	Default value	Supported platforms	Description
DTMF_PAYLOAD_TYPE			
Numeric	120	• Android • iOS • Mac • Windows	This parameter specifies the RTP payload type for RFC 2833 signaling. Valid values are 96 through 127. Client Navigation: Not Applicable
RTP_PORT_LOW			
Numeric	5004	• Android • iOS • Mac • Windows	This parameter specifies the lower limit of the UDP port range used by RTP/RTCP or SRTP/SRTCP connections. Valid values are 1024 through 65503. Client Navigation: Not Applicable
RTP_PORT_RANGE			
Numeric	200	• Android • iOS • Mac • Windows	This parameter specifies the range or number of UDP ports available for RTP/RTCP or SRTP/SRTCP connections. This value is added to RTP_PORT_LOW to determine the upper limit of the UDP port range. Valid values are 32 through 64511. If you configure a value less than 32, the value changes automatically to 32.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable
ECHO_CANCELLATION			
String	aec	Android	The echo cancellation algorithm. Echo cancellation is a process that removes echo from voice communication to improve voice quality on a telephone call. The supported values are: • aec • aecm • off Client Navigation: Not Applicable
ENABLE_OPUS			
Numeric	1	• Android • iOS • Mac • Windows	This parameter controls the Opus codec capability. The supported values are: • 0: The parameter is disabled. • 1: ENABLE_OPUS_WIDEBAND_20K. • 2: ENABLE_OPUS_NARROWBAND_16K. • 3: ENABLE_OPU

Type	Default value	Supported platforms	Description
			S_NARROWBAND_12K. Client Navigation: Not Applicable
OPUS_PAYLOAD_TYPE			
Numeric	116	• Android • iOS • Mac • Windows	This parameter specifies the RTP dynamic payload type used for the Opus codec. This parameter is used when the media offer is sent to the far end in an INVITE or 200 OK when INVITE with no SDP is received. Valid values are 96 through 127. Client Navigation: Not Applicable
DSCPAUD			
Numeric	46	• Android • iOS • Mac • Windows	This parameter indicates the DSCP marking for audio frames that the endpoint generates. This parameter is used only in OTT deployments. In TE deployments, DSCP values are obtained from PPM as Avaya Aura® is available. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPSIG			

Type	Default value	Supported platforms	Description
Numeric	24	• Android • iOS • Mac • Windows	This parameter indicates the DSCP marking for signaling frames that the endpoint generates. This parameter is used only in OTT deployments. In TE deployments, DSCP values are obtained from PPM as Avaya Aura® is available. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPAUD_PRIORITY			
Numeric	46	Windows	This parameter indicates the DSCP marking of audio packets for the PRIORITY level calls. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPAUD_IMMEDIATE			
Numeric	46	Windows	This parameter indicates the DSCP marking of audio packets for the IMMEDIATE level calls. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPAUD_FLASH			
Numeric	46	Windows	This parameter indicates the DSCP marking of

Type	Default value	Supported platforms	Description
			audio packets for the FLASH level calls. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPAUD_FLASHOVERRIDE			
Numeric	46	Windows	This parameter indicates the DSCP marking of audio packets for the FLASH OVERRIDE level calls. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPVID			
Numeric	34	• Android • iOS • Mac • Windows	This parameter indicates the DSCP marking for video frames that the endpoint generates. This parameter is used only in OTT deployments. In TE deployments, DSCP values are obtained from PPM as Avaya Aura® is available. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPVID_PRIORITY			
Numeric	34	Windows	This parameter indicates the DSCP marking of

Type	Default value	Supported platforms	Description
			video packets for the PRIORITY level calls. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPVID_IMMEDIATE			
Numeric	34	Windows	This parameter indicates the DSCP marking of video packets for the IMMEDIATE level calls. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPVID_FLASH			
Numeric	34	Windows	This parameter indicates the DSCP marking of video packets for the FLASH level calls. Valid values are 0 through 63. Client Navigation: Not Applicable
DSCPVID_FLASHOVERRIDE			
Numeric	34	Windows	This parameter indicates the DSCP marking of video packets for the FLASH OVERRIDE level calls. Valid values are 0 through 63. Client Navigation: Not Applicable

Type	Default value	Supported platforms	Description
MEDIAENCRYPTION			
Numeric	10,1,2,9	• Android • iOS • Mac • Windows	This parameter specifies the media encryption ciphers. The supported values are: • 1: Indicates aescm128-hmac80 • 2: Indicates aescm128-hmac32 • 9: Indicates none • 10: Indicates aescm256-hmac80 • 11: Indicates aescm256-hmac32 Avaya Workplace Client supports any combinations of 1, 2, 10, 11, and 9, such as 1,9 or 2,9 or 1,2,9 or 10,9 or 11,9 or 10,11,9 or 1,2,10,11,9. The digit order does not affect the functionality of Avaya Workplace Client. To support the Best Effort SRTP negotiation, the parameter must contain 9 and at least one other value of 1, 2, 10, and 11. For interoperability with Avaya Aura®: • For the Avaya Aura® 6.x

Type	Default value	Supported platforms	Description
			environment, the recommended value is 1,9. - For the Avaya Aura® 7.x environment, the recommended value is 10,1,9. Client Navigation: Not Applicable
ENCRYPT_SRTCP			
Numeric	0	- Android - iOS - Mac - Windows	This parameter is used to enable the SRTCP encryption. The options are: - 0: Indicates that the SRTCP encryption is disabled. - 1: Indicates that the SRTCP encryption is enabled. Client Navigation: Not Applicable
ENABLE_MEDIA_HTTP_TUNNEL			
Numeric	1	- Android - iOS - Mac - Windows	This parameter is used to enable the Media HTTP Tunneling feature. The options are: - 0: Indicates that the Media

Type	Default value	Supported platforms	Description
			HTTP Tunneling feature is disabled. - 1: Indicates that the Media HTTP Tunneling feature is enabled. This parameter applies only to Avaya Equinox® Conferencing. Client Navigation: Not Applicable
MEDIA_ADDR_MODE			
Numeric	4	- Android - iOS - Mac - Windows	This parameter specifies the preference of the SDP media group lines and the SDP answer/offer format. The options are: - 4: IPv4. - 6: IPv6. - 46: Prefer IPv4 over IPv6 media. This value is used only when the client is in a dual-stack network. - 64: Prefer IPv6 over IPv4 media. This value is used only when the

Type	Default value	Supported platforms	Description
			client is in a dual-stack network. Client Navigation: Not Applicable
MEDIA_ADDR_MODE_HTTP			
Numeric	4	• Android • iOS	This parameter specifies the preference of the IP address offered in the SDP media line for HTTP calls. This parameter is used only by dual-stack clients, which are configured with IPv4 and IPv6 addresses. The options are: • 4: Prefer IPv4 in outgoing call SDP. • 6: Prefer IPv6 in outgoing call SDP. Client Navigation: Not Applicable

Video parameters

Type	Default value	Supported platforms	Description
ENABLE_VIDEO			
Numeric	1	• Android • iOS • Mac	This parameter indicates whether the video is enabled.

Type	Default value	Supported platforms	Description
		- Windows	The options are: - 0: Indicates that the video is disabled. - 1: Indicates that the video is enabled. Client Navigation: **Settings** > **User Preferences** > **Audio / Video** > **Video Calling**.
VIDEO_MAX_BANDWIDTH_ANY_NETWORK			
Numeric	- 512 for mobile clients - 1024 for MacOS client - 1280 for Windows client	- Android - iOS - Mac - Windows	This parameter indicates the video bandwidth on any network. The supported values in kilobits per second (kbps) are: - 0: The value to indicate that the video is blocked - 128 - 256 - 384 - 512 - 768 - 1024 - 1280 - 1792 You can also specify a custom value between 0 to 10000. Client Navigation: Not Applicable.
VIDEO_MAX_BANDWIDTH_CELLULAR_DATA			

Type	Default value	Supported platforms	Description
Numeric	512	• Android • iOS	This parameter indicates the video bandwidth on the cellular data network. The supported values are the same as that for VIDEO_MAX_BANDWIDTH_ANY_NETWORK. Client Navigation: Not Applicable.
VIDEO_MAX_RESOLUTION			
Numeric	0	• Android • iOS	This parameter indicates the maximum video resolution that Avaya Workplace Client can receive. The supported values are the following: • 0 = MAX_AUTO • 1 = MAX_1080P • 2 = MAX_720P • 3 = MAX_480P • 4 = MAX_360P • 5 = MAX_240P • 6 = MAX_180P Use the default value to receive the highest-resolution video. Mobile devices capture all the above video resolutions at Level 3.1. This level means that the maximum video resolution that Avaya Workplace Client receives is 720p at 30 frames per second.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
VIDEO_CAPTURE_RESOLUTION			
Numeric	0	• Android • iOS	This parameter indicates the maximum video resolution that Avaya Workplace Client uses to send a video to the network. The supported values are the following: • 0 = Max • 3 = 540p • 4 = 360p • 5 = 270p • 6 = Min Use the default value to send a video with the highest resolution to the network. The maximum video resolution that a mobile device can support is 540p. If a mobile device does not support 540p resolution, Avaya Workplace Client selects the lower supported resolution automatically. Client Navigation: Not Applicable.
BFCP_TRANSPORT			
Numeric	• 0 for UC mode • 1 for OTT mode	• Android • iOS • Mac • Windows	If enabled, this parameter indicates non-power suite users can use BFCP to share screen on the point-to-point video call between two clients on desktop platforms. Users

Type	Default value	Supported platforms	Description
			can also share screens on point-to-point video calls between the Avaya Workplace Client on desktop platforms and a video room system, such as an XT Series endpoint. The options are: • 0: Indicates that BFCP is disabled. 0 is the default value for Avaya Workplace Client in the UC mode. Also, 0 is the default value if you are using Avaya Aura® Device Services. **Note:** BFCP is not supported in ANAT deployments. Hence, you must disable BFCP in any ANAT environment. • 1: Indicates UDP only. 1 is the default value for Avaya Workplace Client in the OTT mode.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
BFCP_UDP_MINIMUM_PORT			
Numeric	5204	• Android • iOS • Mac • Windows	This parameter specifies the lower limit of the UDP port range used by the BFCP signaling channel. The value range is 1024 through 65503. Usually, the BFCP minimum port value equals the RTP UDP port maximum value + 1. Client Navigation: Not Applicable.
BFCP_UDP_MAXIMUM_PORT			
Numeric	5224	• Android • iOS • Mac • Windows	This parameter specifies the upper limit of the UDP port range used by the BFCP signaling channel. The value range is 1024 through 65503. Client Navigation: Not Applicable.
ENABLE_MSS_VIDEO			
Numeric	1	• Mac • Windows	This parameter controls the Multi-Stream Switching (MSS) video feature. The options are: • 0: Indicates that the MSS video feature is disabled. • 1: Indicates that the video

Type	Default value	Supported platforms	Description
			feature is enabled for MSS v1. Client Navigation: Not Applicable.
FORWARD_ERROR_CORRECTION			
Numeric	3	• Android • iOS • Mac • Windows	This parameter is used to configure the Forward Error Correction (FEC) for video streams. • 0: Indicates that FEC is disabled. • 1: Indicates that Standard RFC5109 FEC is used as a redundant encoding. This value is reserved for a future release. • 2: Indicates that Standard RFC5109 FEC is used as a separate stream. This value is reserved for a future release. • 3: Indicates that Scopia Proprietary FEC is used in Session Description

Type	Default value	Supported platforms	Description
			Protocol (SDP) negotiation. Scopia FEC is used to maintain video quality during Avaya Workplace Client meetings in network-packet lost conditions. Client Navigation: Not Applicable.
ENABLE_H263			
Numeric	0	Windows	This parameter controls the H263 and H263+ video codecs. The options are: • 0: Indicates that the H263 and H263+ video codecs are disabled. • 1: Indicates that the H263 and H263+ video codecs are enabled. Client Navigation: Not Applicable.
VIDEO_BACKGROUND_ENABLED			
Numeric	0	Windows	This parameter indicates whether you have enabled blurred or virtual

Type	Default value	Supported platforms	Description
			video background so that users have the privacy of location during video calls. The options are: • 0: Indicates that the video background is disabled. Avaya Workplace Client displays the actual background during video calls. • 1: Indicates that Avaya Workplace Client displays a blurred background during video calls. • 2: Indicates that Avaya Workplace Client displays a virtual background during video calls. You must include the location of the virtual background image in VIDEO_BACKGROUND_URL.

Type	Default value	Supported platforms	Description
			- 3: Indicates that Avaya Workplace Client displays a blurred or virtual background during video calls. To display a virtual background, you must include the location of the virtual background image in VIDEO_BACKGROUND_URL. Client Navigation: **Settings** > **User Preferences** > **Audio / Video** > **Virtual Background**.
VIDEO_BACKGROUND_URL			
String	Null	Windows	This parameter indicates the location of the virtual background image. You must use a .jpg or .png image format. At a minimum, the image size must be 360p with a 16:9 aspect ratio. If you enable virtual background and the background image is unavailable, Avaya Workplace Client blurs the background during video calls.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.

Voice mail parameters

Type	Default value	Supported platforms	Description
MESSAGING_VVM_ENABLED			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether the Avaya Messaging Visual Voice Mail service is enabled. The options are: • 0: Indicates that the Avaya Messaging Visual Voice Mail service is disabled. 1: Indicates that the Avaya Messaging Visual Voice Mail service is enabled. Client Navigation: Not Applicable
MESSAGING_VVM_SRVR			
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the IP address or FQDN of the Avaya Messaging Visual Voice Mail server.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable
MESSAGING_VVM_PORT			
Numeric	Null	• Android • iOS • Mac • Windows	This parameter indicates the port number of the Avaya Messaging Visual Voice Mail server. Client Navigation: Not Applicable
MESSAGING_SSO			
Numeric	2	• Android • iOS • Mac • Windows	This parameter indicates that the messaging server uses the Avaya Cloud Authorization service. To use the visual voice mail feature, you must not change the default value. **Note:** On the Avaya Messaging server, you must enable and configure Hybrid SSO. This is the Avaya Messaging SAML SSO through accounts.avayacloud.com. For more information, see the chapter on Single Sign-On in the *Avaya Messaging Server Installation Guide*. Client Navigation: Not Applicable

Avaya Cloud parameters

Type	Default value	Supported platforms	Description
ENABLE_AVAYA_CLOUD_ACCOUNTS			
Numeric	1	• Android • iOS • Mac • Windows	This parameter controls the Avaya Cloud accounts integration. The options are: • 0: Indicates that the Avaya Cloud accounts integration is disabled. Avaya Workplace Client does not display the Spaces area in the Workplace Meetings panel on the Top of Mind screen. • 1: Indicates that the Avaya Cloud accounts integration is enabled. Avaya Workplace Client displays the Spaces area in the Workplace Meetings panel on the Top of Mind screen. Client Navigation: **Settings** > **Services** > **Avaya Cloud Services** > **Avaya Cloud Services**
AVAYA_CLOUD_ACCOUNTS_URI			

Type	Default value	Supported platforms	Description
String	accounts.avayacloud.com	- Android - iOS - Mac - Windows	This parameter indicates the Avaya Cloud accounts service address. The options are: - 1: Default string - 2: You can change the address to any URI string for testing. For example, onexampletesting.example.com or onexamplestaging.example.com. Client Navigation: Not Applicable
AVAYA_CLOUD_SPACES_URI			
String	spaces.avayacloud.com	- Android - iOS - Mac - Windows	This parameter indicates the Avaya Spaces service address. The options are: - 1: Default string - 2: You can change the address to any URI string for testing. For example, logontesting.example.com or logonstaging.example.com.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable
AVAYA_CLOUD_SPACES_API_URI			
String	spacesapis.avayacloud.com	• Android • iOS • Mac • Windows	This parameter indicates the Avaya Spaces API address. The options are: • 1: Default string • 2: You can change the address to any URI string for testing. For example, logontestingapis.example.com or logonstagingapis.example.com. Client Navigation: Not Applicable
ENABLE_EQUINOX_MEETING_ACCOUNT_DISCOVERY			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Workplace Client auto discovers the Avaya Equinox® Meetings Online account. The options are: • 0: Indicates that Avaya Workplace Client does not auto discover the Avaya

Type	Default value	Supported platforms	Description
			Equinox® Meetings Online account. - 1: Indicates that Avaya Workplace Client auto discovers the Avaya Equinox® Meetings Online account. Client Navigation: Not Applicable
EQUINOX_MEETING_ACCOUNT_DISCOVERY_URL			
String	https://meetings.avaya.com/acs/resources/	- Android - iOS - Mac - Windows	This parameter indicates the Avaya Equinox® Meetings Online account auto discovery address. The options are: - 1: Default string - 2: You can change the address to any URI string for testing. For example, https://meetingsstg.avaya.com/acs/resources/. Client Navigation: Not Applicable
ENABLE_EWS_ACCOUNT_DISCOVERY			

Type	Default value	Supported platforms	Description
Numeric	1	• Mac • Windows	This parameter indicates whether Avaya Workplace Client auto discovers the Exchange Web Services (EWS) account. The options are: • 0: Indicates that Avaya Workplace Client does not auto discover the EWS account. • 1: Indicates that Avaya Workplace Client auto discovers the EWS account. Client Navigation: Not Applicable
ENABLE_GOTO_MEETING_PORTAL			
Numeric	1	Android	This parameter indicates whether the Top of Mind screen displays the Go to My Meeting Portal option in Avaya Workplace Client. The options are: • 0: Indicates that the Top of Mind screen does not display the Go to My Meeting Portal option in Avaya

Type	Default value	Supported platforms	Description
			Workplace Client. • 1: Indicates that the Top of Mind screen displays the Go to My Meeting Portal option in Avaya Workplace Client. Default value is for Android, Avaya Vantage™ K165 device, and Avaya Vantage™ K175 device. **Note:** On the Avaya Vantage™ K155 device, the Top of Mind screen does not display the Go to My Meeting Portal option in Avaya Workplace Client regardless of the value that you set for this parameter. Client Navigation: Not Applicable
ENABLE_SPACES_MESSAGING			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Spaces Messaging is available on the Avaya Workplace Client UI. The options are: • 0: Indicates Avaya Spaces

Type	Default value	Supported platforms	Description
			Messaging is disabled and removed from the Avaya Workplace Client UI. 1: Indicates Avaya Spaces Messaging is enabled and available on the Avaya Workplace Client UI. Client Navigation: Not Applicable

Avaya Cloud account management in UC or OTT deployments

Avaya Cloud account rules:

- Only the same email address with the domain matching the company's domain can be invited to be an employee.
- A company can have multiple domains. Each domain must be unique across the whole system.
- If a user signs up to Avaya Cloud with Google+, this user can add the company email address into the Avaya Spaces profile. Avaya Spaces auto-links this user with the company ID that has the company domain matching the user’s company email domain.
- If a user signs up to Avaya Cloud with the company email address, this user can add the Gmail email address into the Avaya Spaces profile. The user can then use Google+ to log in to Avaya Cloud.

Administration parameters

Type	Default value	Supported platforms	Description
SUPPORTEMAIL			
String	Null	- Android - iOS - Mac - Windows	This parameter indicates the default email address to send diagnostic logs. Client Navigation: On Avaya Workplace Client for Android: **Settings** > **Support** > **Report a Problem** > **Support Email Address**
SUPPORTURL			
String	Null	- Android - iOS - Mac - Windows	This parameter indicates the default URL to get support. Client Navigation: Not Applicable.
SUPPORTEMAIL_REPORT_ATTACHMENT_SIZE			
Numeric	10	Windows	This parameter is used to override the default log file size. Client Navigation: Not Applicable.
LOG_VERBOSITY			
Numeric	- For Avaya Workplace Client on Avaya Vantage™: 0 - For Avaya Workplace Client: 1	- Android - iOS - Mac - Windows	This parameter indicates whether verbose logging is enabled in the local client. The options are: - 0: Indicates disabled. - 1: Indicates enabled.

Type	Default value	Supported platforms	Description
			Client Navigation: **Settings** > **Support** > **Enable Diagnostics**
UC_DATA_PRIVACY_URL			
String	https://downloads.avaya.com/css/P8/documents/101075962	• Android • iOS • Mac • Windows	This parameter indicates the URL to view the data privacy statement. Customers might use the Data Privacy setting to link to their Consent Management mechanism indirectly. Client Navigation: **Settings** > **Legal** > **Data Privacy**
ANALYTICSENABLED			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates whether you can collect data on behalf of your users. The options are: • 0: Indicates disabled. • 1: Indicates enabled. Client Navigation: **Settings** > **Support** > **Quality Improvement**
CELLULAR_DIRECT_ENABLED			
Numeric	0	• Android • iOS	This parameter indicates whether the Cellular Direct feature is enabled. The options are:

Type	Default value	Supported platforms	Description
			- 0: Indicates disabled. - 1: Indicates enabled. Avaya Workplace Client starts a call by using the cellular network if the following conditions are met: - The value of this parameter is set to 1. - The dialed number matches any number specified in the CELLULAR_DIRECT_NUMBER_LIST parameter. For example, if you set the value of this parameter to 1 and if the user dials 911, which is specified in CELLULAR_DIRECT_NUMBER_LIST, Avaya Workplace Client starts the call by using the cellular network. You cannot use these configuration parameters for mobile devices without cellular radio capabilities. For example, iPad, iPod Touch. Client Navigation: Not Applicable.
CELLULAR_DIRECT_NUMBER_LIST			

Type	Default value	Supported platforms	Description
String	Null	• Android • iOS	A multivalue parameter that contains the list of phone numbers sent directly to the native phone client on iOS or Android. The numbers can contain any digits or characters that can be dialed from the client UI or the native dialer, including: • Special characters, such as plus (+), asterisk (*), and hash (#). • Any alphanumeric character, such as A-Z, a-z, or 0-9. **Note:** iOS does not support numbers containing an asterisk (*) or a hash (#). Client Navigation: Not Applicable.
SIP_CRLF_PING_INTERVAL			
Numeric	30	• Android • iOS • Windows	This parameter indicates the number of seconds Avaya Workplace Client waits before re-transmitting a Carriage Return and Line Feed (CRLF) ping. Valid values are 0 through 840 seconds. 0 means that the CRLF ping mechanism is off. Avaya recommends not changing the default

Type	Default value	Supported platforms	Description
			value unless you receive specific guidance from Avaya. Updates to this value can negatively impact failover detection on the PBX and may result in missed calls. **Note:** Smaller values of CRLF ping interval may lead to server overload and overconsumption of mobile device battery. Greater values of CRLF ping interval affect how fast the connection loss is detected. Avaya Workplace Client sends the first CRLF ping immediately after a successful connection. If there is a connection refresh, the CRLP ping logic starts again. Hence, reconnection initiates Avaya Workplace Client to send the CRLF ping again. To reduce security exposure, firewalls and NAT occasionally automatically close the firewall pinholes and NAT bindings after a time duration. If a firewall pinhole or NAT binding must remain open for an application, the application must generate artificial traffic through the firewall pinhole or NAT binding. Artificial traffic ensures that the firewall or NAT restarts its timer. In such environments, applications do not expect a response to the CRLF ping request.

Type	Default value	Supported platforms	Description
			However, the application sends frequent CRLF pings to ensure that the firewall pinholes or NAT bindings stay open. Client Navigation: Not Applicable.
HTTP_PROXY_CSDK_ENABLE			
Numeric	2	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Workplace Client uses the HTTP proxy that is configured in the OS. The options are: • 0: Indicates that Avaya Workplace Client does not use the HTTP proxy. • 1: Indicates that Avaya Workplace Client uses the HTTP proxy configured in the OS. It does not perform a STUN check for HTTPUA calls before enforcing HTTP tunneling in the media engine. • 2: Indicates that Avaya Workplace Client uses the

Type	Default value	Supported platforms	Description
			HTTP proxy configured in the OS. It performs a STUN check for HTTPUA calls before enforcing HTTP tunneling in the media engine. Client Navigation: Not Applicable.
TELEPHONY_PUSH_NOTIFICATION_SERVICE_URL			
String	Null	iOS	This parameter indicates the FQDN or resource URL of the Avaya Aura® Web Gateway server that provides the telephony events for the Push Notification solution. The accepted value formats are: • https://server-fqdn: Client SDK appends /csa/resources/tenants/default to the FQDN to create a resource URL that the SDK can use to request push service activation or deactivation.

Type	Default value	Supported platforms	Description
			• server-fqdn: Client SDK prepends https:// and appends /csa/resources/tenants/default to the FQDN to create a resource URL that the SDK can use to request push service activation or deactivation. • https://<fqdn>/csa/resources/tenants/default: Client SDK uses the URL as is, with no modification. • Empty: Push Notification for telephony events is not supported. Client Navigation: Not Applicable.
TELEPHONY_PUSH_NOTIFICATION_ENABLED			
Numeric	0	• Android • iOS	This parameter indicates the policy for enabling the activation mode type of Telephony Push Notification service on Client SDK.

Type	Default value	Supported platforms	Description
			The options are: • 0: Indicates that the Push Notification activation mode is disabled. Client SDK sets the VoIP flag for the used sockets in the background. The Android or iOS system accepts this marking when Client SDK is used with Avaya Workplace Client. • 1: Indicates that the Push Notification activation mode is HTTP. Push Notification service is activated using Avaya Aura® Web Gateway. The client relies on the Apple Push Notification service to provide telephony and other events to

Type	Default value	Supported platforms	Description
			the client application. - 2: Indicates that the Push Notification activation mode is SIP. Push Notification service is activated using Session Manager. The client relies on the Android or Apple Push Notification service to provide telephony and other events to the client application. ❗ **Important:** Avaya recommends the use of Session Manager for push notifications on Android and iOS devices. Client Navigation: Not Applicable.
ESM_PUSH_NOTIFICATION_ENABLED			
Numeric	0	- Android - iOS	This parameter indicates the policy for enabling the Avaya Multimedia Messaging Push Notification service on Client SDK. The options are:

Type	Default value	Supported platforms	Description
			• 0: Indicates that the policy for enabling the Avaya Multimedia Messaging Push Notification service on Client SDK is disabled. Client SDK sets the VoIP flag for the Avaya Multimedia Messaging sockets in the background. The Android or iOS system accepts this marking when Client SDK is used with Avaya Workplace Client. • 1: Indicates that the policy for enabling the Avaya Multimedia Messaging Push Notification service on Client SDK is enabled. The client relies on the Android or

Type	Default value	Supported platforms	Description
			Apple Push Notification service to provide Avaya Multimedia Messaging events towards the client application. Client Navigation: Not Applicable.
PRESENT_USER_NAME_ONLY			
Numeric	0	• Mac • Windows	This parameter indicates whether Avaya Workplace Client displays the user name portion of a numeric display name. This parameter does not apply to alphanumeric user names. The options are: • 0: Indicates that Avaya Workplace Client does not display the user name portion of a numeric display name • 1: Indicates that Avaya Workplace Client displays the user name portion of a numeric display name.

Type	Default value	Supported platforms	Description
			If you enable this parameter, Avaya Workplace Client displays 17805551234@pstn.yourcompany.com as 17805551234. This property is applicable to improve the user experience when services are configured using the Avaya SIP End-to-End V2 spec. Client Navigation: Not Applicable.
OTHER_PHONE_MODE_ENABLED			
Numeric	1	• Mac • Windows	This parameter indicates whether the Other Phone mode is available for the user. The options are: • 0: Indicates that the Other Phone mode is unavailable for the user. • 1: Indicates that the Other Phone mode is available for the user. Client Navigation: Not Applicable.
INITIATE_OTHER_PHONE_INCOMING_WHEN_FORWARDING_ENABLED			
Numeric	0	• Mac • Windows	When incoming call features such as Send All Calls and Call Forwarding are enabled, incoming call notification continues

Type	Default value	Supported platforms	Description
			to arrive at Avaya Workplace Client. This parameter indicates whether the incoming call is forwarded to the Other Phone Mode device and canceled when the Avaya Aura® coverage timer is up. The options are: • 0: Indicates that the incoming call is not forwarded to the Other Phone Mode device to avoid unnecessary signaling. • 1: Indicates that the incoming call is forwarded to the Other Phone Mode device and canceled when the Avaya Aura® coverage timer is up. Client Navigation: Not Applicable.
OTHER_PHONE_MODE_REMOTE_MEDIA_RESPONSE_TIMEOUT			
Numeric	30	• Mac • Windows	This parameter indicates the time in seconds for which Avaya Workplace Client waits for a response from the callee.

Type	Default value	Supported platforms	Description
			Callee is the person who receives the call. You can enter a value between 0 to 30 seconds. If Avaya Workplace Client does not receive a response within this time, it sends a dummy response to the Other Phone device so that the call is not dropped. Client Navigation: Not Applicable.
ENABLE_DESKPHONE_SHARE_CONTROL			
Numeric	1	Windows	This parameter indicates whether the deskphone share control feature is available for the user. The options are: • 0: Indicates that the deskphone share control feature is unavailable for the user. Avaya Workplace Client disables and hides the My Desk Phone button. • 1: Indicates that the deskphone share control feature is available for the user. In a VM environment, Avaya Workplace Client

Type	Default value	Supported platforms	Description
			ignores this parameter because only the desk phone share control mode is supported in the VM environment. Client Navigation: Not Applicable.
ENABLE_DESKPHONE_SHARE_CONTROL_MULTI			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client displays multiple controlled clients for the user to select in the **My Softphone** or **My Deskphone** list. The options are: • 0: Indicates that Avaya Workplace Client displays the **My Softphone** or **My Deskphone** option if available. 1: Indicates that Avaya Workplace Client displays multiple controlled clients for the user to select in the **My Softphone** or **My Deskphone** list.

Type	Default value	Supported platforms	Description
			Client Navigation: ☎ > **Place and Receive Calls Using** > **My Softphone** OR ☎ > **Place and Receive Calls Using** > **My Deskphone**.
ENABLE_CONTROLLED_SOFTPHONE			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client acts as a controlled client. The options are: • 0: Indicates that Avaya Workplace Client does not act as a controlled client. Avaya Workplace Client operates in the normal mode. 1: Indicates that Avaya Workplace Client acts as a controlled client. Client Navigation: Not Applicable.
CONTROLLEDEP_CONFIGURL			
String	Null	Windows	This parameter indicates the configuration URL pushed from the controlling client to the controlled Avaya

Type	Default value	Supported platforms	Description
			Workplace Client in a VDI environment while using the My Paired Softphone mode on the controlling client. Client Navigation: Not Applicable.
ENABLE_ALTERNATE_CLI			
Numeric	0	• Mac • Windows	This parameter indicates whether the Other Phone device displays the actual name or number of the caller or called number. The Other Phone device receives this information from Communication Manager or Session Manager (Alternate Calling Line Identification). This parameter is specific to the Other Phone mode. The options are: • 0: Indicates that the Other Phone device does not display the actual name or number of the caller or called number. The Other Phone device displays the corresponding work extension. • 1: Indicates that the Other

Type	Default value	Supported platforms	Description
			Phone device displays the actual name or number of the caller or called number. Client Navigation: Not Applicable.
AUDIO_DEVICE_CALL_CONTROL_ENABLED			
Numeric	1	- Android - Mac - Windows	This parameter indicates whether call control is enabled for Avaya headsets. The options are: - 0: Indicates that call control is disabled for Avaya headsets. 1: Indicates that call control is enabled for Avaya headsets. Client Navigation: Not Applicable.
SUPPORTEMAIL_ENCRYPTED			
Numeric	0	- Android - iOS - Mac - Windows	This parameter indicates whether the logs are encrypted before the user sends the logs by email to Avaya support. The options are:

Type	Default value	Supported platforms	Description
			• 0: Indicates that the logs are not encrypted. • 1: Indicates that the logs are encrypted. Client Navigation: Not Applicable.
SUPPORTEMAIL_ENCRYPTIONPASSPHRASE			
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the encryption passphrase when the logs are encrypted. • If you provide the encryption passphrase, Avaya Workplace Client similarly encrypts all support logs. • If you do not provide the encryption passphrase, Avaya Workplace Client prompts the user to provide a custom passphrase to encrypt the logs. Client Navigation: Not Applicable.

Type	Default value	Supported platforms	Description
ENABLE_IN_APP_RATING			
Numeric	1	• Android • iOS	This parameter indicates whether the user can view the option to rate the application. The options are: • 0: Indicates that the user cannot view the option to rate the application. • 1: Indicates that the user can view the option to rate the application. Client Navigation: **Settings** > **Support** > **Rate this app**
ATTACHMENT_FILETYPE_BLACKLIST			
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the list of file extensions that the user cannot download in messaging attachments so that the client does not download common malware. If you keep the default value or do not specify this parameter in the settings file, Avaya Workplace Client does not allow the user to download messaging attachments with the following file extensions: ".exe", ".ade", ".adp", ".app", ".asp", ".bas", ".bat", ".cer", ".chm",

Type	Default value	Supported platforms	Description
			".cmd", ".com", ".cpl", ".crt", ".csh", ".fxp", ".grp", ".hlp", ".hta", ".inf", ".ins", ".isp", ".its", ".js", ".jse", ".ksh", ".lnk", ".mad", ".maf", ".mag", ".mam", ".maq", ".mar", ".mas", ".mat", ".mau", ".mav", ".maw", ".mda", ".mdb", ".mde", ".mdt", ".mdw", ".mdz", ".msc", ".msi", ".msp", ".mst", ".ocx", ".ops", ".pcd", ".pif", ".pl", ".pnp", ".prf", ".prg", ".pst", ".reg", ".scf", ".scr", ".sct", ".shb", ".shs", ".tmp", ".url", ".vb", ".vbe", ".vbs", ".vsd", ".vsmacros", ".vss", ".vst", ".vsw", ".ws", ".wsc", ".wsf", ".wsh" If you specify a value for this parameter, Avaya Workplace Client does not allow the user to download messaging attachments with the extensions that you specify along with the default list of file extensions. For example, `SET ATTACHMENT_FILETYPE_BLACKLIST "docx,zip,txt"`. Client Navigation: Not Applicable.
EXACT_SIP_DOMAIN_COMPARISON			
Numeric	1	• Android • iOS • Mac • Windows	This parameter indicates whether the algorithms are checked for exact or weak matching. The options are:

Type	Default value	Supported platforms	Description
			- 0: Indicates that the algorithms are not checked for exact or weak matching. - 1: Indicates that the algorithms are checked for exact or weak matching. The contact matching algorithm on the call appearance and in call logs requires an exact match of the domain of the registered Avaya Workplace Client and caller or called user. If you set EXACT_SIP_DOMAIN_COMPARISON to 1 for an Avaya Workplace Client user and the domains do not match completely, Avaya Workplace Client displays the domain name of the caller along with the number. If you do not want Avaya Workplace Client to display the domain names on the call appearance, disable this parameter by setting EXACT_SIP_DOMAIN_COMPARISON to 0. Client Navigation: Not Applicable.
ACTIVATE_DESKPHONE_MODE_ON_STARTUP			
Numeric	0	Windows	This parameter indicates whether the user can log in to the Desk Phone mode after a new installation if the user is

Type	Default value	Supported platforms	Description
			already logged in to the deskphone with the same extension. Also, on System Manager, you must set Max. Simultaneous Devices to 1, that is, MDA=1. The options are: • 0: Indicates that the user can log in to the This Computer mode after a new installation. • 1: Indicates that the user can log in to the Desk Phone mode after a new installation without using the This Computer mode. Client Navigation: Not Applicable.
ENABLE_CALL_NOTIFICATIONS			
Numeric	1	• Android • Windows	This parameter indicates whether the user receives visual notifications for incoming calls. The options are: • 0: Indicates that the user does not receive visual

Type	Default value	Supported platforms	Description
			notifications for incoming calls. • 1: Indicates that the user receives visual notifications for incoming calls. If you set the value to 0 and the user minimizes Avaya Workplace Client for Windows to the taskbar or notification area and answers an incoming call using a CTI controlling application, Avaya Workplace Client for Windows remains minimized. If Avaya Workplace Client for Android runs in the foreground, the user receives alerts through custom in-app notifications. If Avaya Workplace Client for Android runs in the background, the user receives alerts through system notifications with the Answer and Ignore labels. An application is considered to be running in the background if each of the following conditions is met: • None of the application activities are currently visible to the user. • The application does not run

Type	Default value	Supported platforms	Description
			any foreground services, started when the application activity was visible to the user. Client Navigation: Not Applicable.
ENABLE_AUDIBLE_CALL_NOTIFICATIONS			
Numeric	1	Windows	This parameter indicates whether the user receives audible notifications for incoming calls. The options are: • 0: Indicates that the user does not receive audible notifications for incoming calls. • 1: Indicates that the user receives audible notification for incoming calls. Client Navigation: Not Applicable.
ENABLE_TUTORIAL			
Numeric	1	• Android • Windows	This parameter indicates whether the tutorial is available. The options are:

Type	Default value	Supported platforms	Description
			- 0: Indicates that the tutorial is unavailable. - 1: Indicates that the tutorial is available. Client Navigation: Not Applicable.
SCREEN_ALWAYS_AWAKE_ON_FOREGROUND			
Numeric	0	- Android - iOS	This parameter indicates whether the device screen gets locked due to inactivity when Avaya Workplace Client runs in the foreground. You can specify the time interval of inactivity from the OS settings on your device. The options are: - 0: Indicates that the device screen gets locked due to inactivity when Avaya Workplace Client runs in the foreground. - 1: Indicates that the device screen does not get locked due to inactivity when Avaya Workplace Client runs in the foreground.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
LOCALLY_ENFORCE_PRIVACY_HEADER			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether to display the calling party information as Restricted in the localized language when a user receives Calling Party Name (CPN) blocked calls. The options are: • 0: Indicates that the responsibility for privacy is with Communication Manager or Session Manager. Hence, the endpoint displays any Caller ID received in the Contact headers for CPN blocked calls. 1: Indicates that the responsibility for privacy is with the endpoint. Hence, the endpoint displays the

Type	Default value	Supported platforms	Description
			localized string Restricted when Incoming Invite has Privacy Header for CPN blocked calls. Client Navigation: Not Applicable.
DISABLE_COPY_PASTE			
Numeric	0	iOS	This parameter indicates whether copying and pasting are allowed from and to Avaya Workplace Client. The options are: • 0: Indicates that copying and pasting are allowed from and to Avaya Workplace Client. 1: Indicates that copying and pasting are not allowed from and to Avaya Workplace Client. Users cannot copy editable text strings to any screens or applications. Similarly, users cannot paste anything in the

Type	Default value	Supported platforms	Description
			editable text boxes. Client Navigation: Not Applicable.
XCALLBACK_LOGOUT_ENABLED			
Numeric	0	• Android • iOS	When deploying Avaya Workplace Client using Imprivata IDP, enterprises might install Imprivata Mobile Device Access (MDA) on the local device to send a logout request to specified applications when the user logs off the device. The options are: • 0: Indicates that Avaya Workplace Client does not monitor logout requests. 1: Indicates that Avaya Workplace Client monitors logout requests and resets after receiving the logout request. Avaya Workplace Client sends a response with the operation result.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
DISABLE_END_CALL			
Numeric	0	Windows	This parameter indicates whether to hide the End Call option for specific deployments such as Computer Telephony Integration (CTI) and Application Enablement Services (AES), where Avaya Workplace Client is used only as a media endpoint. The options are: • 0: Indicates that Avaya Workplace Client displays the End Call option. 1: Indicates that Avaya Workplace Client hides the End Call option for deployments where Avaya Workplace Client is used only as a media endpoint. The End Call option is hidden for all types of answered, active calls and incoming calls except

Type	Default value	Supported platforms	Description
			conference calls using Avaya Equinox® Conferencing. Client Navigation: Not Applicable.
SHOW_IDENTITY_CERTIFICATE_UI			

String	Null	Windows	This parameter must be used only with the OBSCURE_PREFERENCES parameter to hide the Identity Certificate UI in Avaya Workplace Client.
			To hide the Identity Certificate UI:
			`SET`
			`OBSCURE_PREFERENCES`
			`"SHOW_IDENTITY_CERTIFICATE_UI"`
			By default, Avaya Workplace Client displays the Identity Certificate UI.
			Client Navigation: **Settings** > **Advanced** > **Identity Certificate**

RESET_ON_SIGNOUT			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether Avaya Workplace Client resets all settings and removes configuration data when the user logs out or shuts down the application.

Type	Default value	Supported platforms	Description
			This parameter is useful in work environments where multiple users share the same devices. The options are: • 0: Indicates that Avaya Workplace Client does not reset settings and remove configuration data when the user logs out or shuts down the application. • 1: Indicates that Avaya Workplace Client resets all settings and removes configuration data when the user logs out or shuts down the application. Client Navigation: Not Applicable.
ENABLE_BLIND_TRANSFER			
Numeric	1	Windows	This parameter indicates whether the blind transfer is enabled. The options are: • 0: Indicates that the blind

Type	Default value	Supported platforms	Description
			transfer is disabled. 1: Indicates that the blind transfer is enabled. Client Navigation: Not Applicable.
ONLINE_HELP_ENABLED			
Numeric	1	• Android • iOS • Windows	This parameter indicates whether Avaya Workplace Client displays the video tutorials link. The options are: • 0: Indicates that Avaya Workplace Client does not display the video tutorials link. 1: Indicates that Avaya Workplace Client displays the video tutorials link. Client Navigation: **Settings** > **Support** > **Video Tutorials**.
ENABLE_BLA_NO_RING_CALL_NOTIFICATIONS			
Numeric	1	• Android • iOS • Windows	This parameter indicates whether Avaya Workplace Client hides the visual alert notifications when the

Type	Default value	Supported platforms	Description
			BLA button configuration includes `no-ring` . The options are: • 0: Indicates that Avaya Workplace Client hides the visual alert notifications for incoming BLA calls. 1: Indicates that Avaya Workplace Client displays the visual alert notifications for incoming BLA calls. Client Navigation: Not Applicable.
ADMIN_PASSWORD			
String	Null	• Android • iOS	This parameter indicates whether the user must enter the administrator password to reset or sign out of Avaya Workplace Client. If you set a password, the user must enter the password before resetting or signing out of Avaya Workplace Client. **Note:** If the user changes any service settings requiring a client restart, the user

Type	Default value	Supported platforms	Description
			does not require to enter the password before signing out or restarting Avaya Workplace Client. The password must contain 6 to 31 characters. Password can include an uppercase letter, a lowercase letter, a number, or a special character except ". Client Navigation: Not Applicable.
ALTERNATE_EMERGENCY_CALL_DISCLAIMER			
Numeric	0	• Android • iOS	This parameter indicates whether Avaya Workplace Client displays the alternate emergency message text when the cellular service or SIM card is unavailable, but Wi-Fi is available on the device. The options are: • 0: Indicates that Avaya Workplace Client displays the standard emergency message text in Emergency Disclaimer when the cellular service or SIM card is available on the device. Also, when the user installs and

Type	Default value	Supported platforms	Description
			opens Avaya Workplace Client for the first time, the user can view the message not to use Avaya Workplace Client to make 911 calls. 1: Indicates that Avaya Workplace Client displays the alternate emergency message text in Emergency Disclaimer when the cellular service or SIM card is unavailable, but Wi-Fi is available on the device. Also, when the user installs and opens Avaya Workplace Client for the first time, the user cannot view any message regarding 911 calls. **Note:**

Type	Default value	Supported platforms	Description
			If the device includes a SIM card and the user enables airplane mode to disable the cellular service, Avaya Workplace Client displays the standard emergency text even if you set the parameter value to 1. This is because Avaya Workplace Client detects the SIM card. Client Navigation: **Settings** > **Support** > **Emergency Disclaimer**.
SHOW_CALLERID_ON_CALL_APPEARANCE			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client displays the caller or callee number besides the name on the active call appearance for all calls. The options are: • 0: Indicates that Avaya Workplace Client displays only the caller or callee number on the call appearance. 1: Indicates that Avaya Workplace Client displays the name and number of the caller or callee

Type	Default value	Supported platforms	Description
			on the call appearance. Client Navigation: Not Applicable.
BLIND_TRANSFER_AUTO_HOLD			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client puts the active call on hold after the user performs a blind transfer. The options are: • 0: Indicates that Avaya Workplace Client does not put the active call on hold after the user performs a blind transfer. 1: Indicates that Avaya Workplace Client puts the active call on hold and then transfers the call after the user performs a blind transfer. Client Navigation: Not Applicable.
CONF_TRANS_ON_PRIMARY_APPR			

Type	Default value	Supported platforms	Description
Numeric	0	Windows	This parameter indicates whether the conference and transfer setup uses the idle bridged call or primary call appearance. The options are the following: • 0: Indicates that the conference and transfer setup initiated from a bridged call appearance uses an idle bridged call appearance of the same extension during the first attempt. If an idle bridged call appearance of the same extension is unavailable and AUTO_SELECT_ANY_IDLE_APPR is set to the following: • 1: the conference and transfer setup uses any primary or bridged idle call appeara

Type	Default value	Supported platforms	Description
			nce if the primary call appearance is unavailable. - 0: Avaya Workplace Client denies the conference and transfer setup initiated on a bridged call appearance. The conference and transfer setup initiated from a primary call appearance uses an idle primary call appearance during the first attempt. However, if an idle primary call appearance is unavailable, the conference and transfer setup uses an idle

Type	Default value	Supported platforms	Description
			bridged call appearance regardless of the parameter value of AUTO_SELECT_ANY_IDLE_APPR. 1: Indicates that the conference and transfer setup initiated from a bridged call appearance uses an idle primary call appearance during the first attempt. If an idle primary call appearance is unavailable, the conference and transfer setup uses an idle bridged call appearance of the same extension. However, if the same extension is unavailable, Avaya Workplace Client uses an idle bridged call appearance of a different extension. Avaya

Type	Default value	Supported platforms	Description
			Workplace Client ignores the parameter value for AUTO_SELECT_ANY_IDLE_APPR. Client Navigation: Not Applicable.
AUTO_SELECT_ANY_IDLE_APPR			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client denies the conference and transfer setup or uses the primary or bridged idle call appearance. This parameter works along with the CONF_TRANS_ON_PRIMARY_APPR parameter when set to 1. The options are the following: • 0: Indicates that if an idle bridged call appearance of the same extension is unavailable, Avaya Workplace Client denies the conference and transfer setup initiated on a bridged

Type	Default value	Supported platforms	Description
			call appearance. 1: Indicates that the conference and transfer setup initiated from a bridged call appearance uses the primary or bridged idle call appearance. The conference and transfer setup uses an idle primary call appearance during the first attempt. However, if an idle primary call appearance is unavailable, the conference and transfer setup uses an idle bridged call appearance of a different extension. Client Navigation: Not Applicable.
ENABLE_OAUTH_LOGIN_AUTO_POPUP			
Numeric	1	Windows	This parameter indicates whether to control the display of the automatic OAuth credential popup

Type	Default value	Supported platforms	Description
			window when the refresh token expires. The options are the following: • 0: Avaya Workplace Client does not automatically display credentials/login window when the refresh token expires. To display the OAuth credentials/login window, the user must click on the red error triangle. 1: Avaya Workplace Client automatically displays OAuth credentials/login window popup when the refresh token expires. **Note:** Avaya Workplace Client displays the credentials/login window automatically in

Type	Default value	Supported platforms	Description
			the following scenarios: • Auto configuration update is available • If the machine restarts after the refresh token expires • The application restarts after the refresh token expires Client Navigation: Not Applicable.
ENABLE_MINIMIZE_AFTER_CALL_END			
Numeric	0	Android	This parameter indicates whether the Avaya Workplace Client application minimizes after ending a call on a mobile device. The options are: • 0: Indicates that the Avaya Workplace Client

Type	Default value	Supported platforms	Description
			application does not minimize after ending a call on a mobile device. The Avaya Workplace Client application remains active in the foreground. 1: Indicates that the Avaya Workplace Client application minimizes after ending a call on a mobile device. The Avaya Workplace Client application runs in the background. Client Navigation: Not Applicable.
ENABLE_MESSAGE_COALESCING			
Numeric	1	• Android • iOS • Windows	This parameter indicates whether Avaya Workplace Client coalesces or merges separate messages into one.

Type	Default value	Supported platforms	Description
			The options are: - 0: Indicates that Avaya Workplace Client does not coalesce or merge separate messages into one. Avaya Workplace Client displays each message as a separate message to the user. 1: Indicates that Avaya Workplace Client coalesces or merges separate messages into one. Client Navigation: Not Applicable.
ENABLE_TRANSFER_ACTIVE_CALL			
Numeric	1	- Android - iOS - Windows	This parameter indicates whether to hide the transfer call option on an active call when you receive multiple incoming or outgoing calls on Avaya Workplace Client. The options are: - 0: Indicates that Avaya

Type	Default value	Supported platforms	Description
			Workplace Client hides the transfer call option on an active call when you receive multiple incoming or outgoing calls. 1: Indicates that Avaya Workplace Client does not hide the transfer call option on an active call when you receive multiple incoming or outgoing calls. Client Navigation: Not Applicable.

Security settings parameters

Type	Default value	Supported platforms	Description
REVOCATIONCHECKENABLED			
Numeric	• Android: 0 • Desktop clients: 1	• Android • Mac • Windows	This parameter indicates whether certificate revocation is checked. Supported values are: • 0: Disabled.

Type	Default value	Supported platforms	Description
			• 1: Best effort. Certificate revocation is checked. The revocation checking failures in this type of checking, such as no response and no revocation authority, are not fatal. • 2: Mandatory. Certificate revocation is checked. The revocation checking failures in this type of checking are fatal. Client Navigation: Not Applicable
TLSSRVRID			
Numeric	0	• Android • iOS • Mac • Windows	This parameter defines the actions to be taken when the server identity validation fails. Supported values are: • 0: Allow the connection to continue.

Type	Default value	Supported platforms	Description
			- 1: Abort the connection. This parameter applies to all protocols for all configured services on the endpoint. **Note:** If you correct the Subject Alternative Name value in the System Manager certificate after a server identity validation failure, you must inform the user to log in again to Avaya Workplace Client. Client Navigation: Not Applicable
SUPPORTWINDOWSAUTHENTICATION			
Numeric	0	Windows	This parameter indicates whether Windows Authentication is used when challenged for authentication using Microsoft Negotiate or NTLM on a device that is logged in to the domain. Supported values are: - 0: Disabled. - 1: Enabled. The following services support the use of this parameter: - Avaya Aura® Device Services. - Avaya Multimedia Messaging or

Type	Default value	Supported platforms	Description
			Presence Multimedia Messaging. • Unified Portal. • Exchange Web Services (EWS) using on-premise Exchange. This service does not work with Office 365 EWS. • LDAP, when Avaya Aura® Device Services are not used. To set up IWA in both FIPS and non-FIPS environments, see Avaya Aura® Device Services documentation. Client Navigation: Not Applicable
PKCS12URL			
String	Null	• Android • iOS	This parameter indicates the URL to be used to download a PKCS #12 file containing a client identity certificate and its private key. Avaya Aura® Device Services validates the entry for standard URL format. Client Navigation: Not Applicable

Type	Default value	Supported platforms	Description
PKCS12PASSWORD			
String	Null	• Android • iOS	This parameter indicates the password for the PKCS#12 certificate that you specified in PKCS12URL. This parameter is optional. You must use this parameter only in cases where you want to ensure that access to the settings file is protected appropriately. If the password is absent, but is required to install the certificate, the user is prompted in the application to enter the PKCS12PASSWORD as required. Client Navigation: **Certificate Password**
MYCERTURL			
String	Null	• Android • iOS	This parameter indicates the URL of the SCEP server from which the client must obtain an identity certificate. This is needed if the client does not already have an identity certificate from that SCEP server. The default value is an empty string, which means that the client does not attempt to retrieve an identity certificate using SCEP. Client Navigation: Not Applicable

Type	Default value	Supported platforms	Description
MYCERTCN			
String	Null	• Android • iOS	This parameter indicates the Common Name (CN) that is used in the subject of an SCEP certificate request. If you keep this parameter value blank, Avaya Workplace Client prompts the user to enter a value before starting SCEP enrollment. Client Navigation: Not Applicable
SCEPPASSWORD			
String	Null	• Android • iOS	This parameter indicates the password to be included in the challengePassword attribute of an SCEP certificate request. If you keep this parameter value blank, Avaya Workplace Client prompts the user to enter a value before starting SCEP enrollment. Client Navigation: **Password**
SCEP_USESSO			
Numeric	0	• Android • iOS	This parameter indicates whether SCEP uses unified login. The options are: • 0: Indicates that SCEP does not

Type	Default value	Supported platforms	Description
			use unified login. - 1: Indicates that SCEP uses unified login. Client Navigation: Not Applicable
MYCERTDN			
String	Null	- Android - iOS	This parameter indicates the part of the certificate subject that is common to all clients. The value must begin with a forward slash "/" and might include the OU, O, L, ST, and C values. Use a forward-slash character "/" as a separator between components because commas do not work with some servers. If the value includes spaces, ensure that you enter the entire value. For example, `SET MYCERTDN /C=US/ST=NJ/L=MyTown/O=MyCompany`. Client Navigation: Not Applicable
MYCERTCAID			
String	CAIdentifier	- Android - iOS	If the server hosts multiple certificate authorities, this parameter indicates an identifier for the CA

Type	Default value	Supported platforms	Description
			certificate with which the certificate request must be signed. Client Navigation: Not Applicable
MYCERTKEYLEN			
Numeric	2048	• Android • iOS	This parameter indicates the bit length of the public and private keys generated for the SCEP certificate request. The value range is 1024 through 2048. Client Navigation: Not Applicable
MYCERTRENEW			
Numeric	90	• Android • iOS	This parameter indicates the validity interval percentage, of the identity certificate, after which you must begin the renewal procedure. The value range is 1 through 99. When the client certificate passes this interval, a visual warning is presented to the user stating that the certificate will expire shortly and must be renewed. Client Navigation: Not Applicable
TLS_VERSION			
Numeric	0	• Android • iOS	This parameter indicates the minimum version of

Type	Default value	Supported platforms	Description
		• Mac • Windows	the TLS protocol, which clients support. The options are: • 0: Indicates that TLS 1.0 is used as the minimum version of the TLS protocol. Default value in SDK, supports TLS 1.0, 1.1, 1.2, and 1.3. • 1: Indicates that TLS 1.2 is used as the minimum version of the TLS protocol. • 2: Indicates that TLS 1.3 is used as the minimum version of the TLS protocol. **Note:** • To enforce TLS 1.2 or TLS 1.3, set the following configurations as locked or obscured: • APPCAST_ENABLED = 0 • DIRENA

Type	Default value	Supported platforms	Description
			BLED = 0 • Sparkle library does not support setting the minimum version of the TLS protocol. Hence, this parameter value is ignored for Sparkle. For example, if you set the value for this parameter as 1 or 2 and the Sparkle back-end software does not support TLS 1.2 and TLS 1.3, the upgrade process continues regardless of the parameter value. • Avaya Workplace Client for Windows (FIPS) does not support TLS 1.3. • Avaya Workplace Client for

Type	Default value	Supported platforms	Description
			Android supports TLS 1.3 only when you use Android 10 and later versions. Client Navigation: Not Applicable.
CIPHER_SUITE_BLACKLIST			
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the list of blacklisted ciphers that will not be included during the TLS connection negotiation. For example, `SET CIPHER_SUITE_BLACKLIST "TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256"`. Client Navigation: Not Applicable
CERTIFICATE_MIN_RSA_KEY_LENGTH			
Numeric	1024	• Android • iOS • Mac • Windows	This parameter indicates the minimum RSA key length to be used for validating the certificate received from the server during the TLS handshake. If the value that you configure for this parameter is greater than the server certificate's key length, then Client SDK rejects the server certificate. **Note:**

Type	Default value	Supported platforms	Description
			If the previous parameter value is greater than the server certificate's key length and now you configure the parameter value to be less than the certificate key length, Avaya Workplace Client continues to remain in the failed state. The impact is significant when the misconfiguration applies to Avaya Aura® Device Services or the configuration server. You must correct the configuration on Avaya Aura® Device Services or the configuration server. Users can then reset the client and configure the client with the new settings file. Client Navigation: Not Applicable

User policy settings parameters

Type	Default value	Supported platforms	Description
LOCKED_PREFERENCES			
String	Not locked	• Android • iOS • Mac • Windows	The list of locked preferences. For example, `SET LOCKED_PREFERENCES "CESSRVR","CESPORT","CESENABLED"`

Type	Default value	Supported platforms	Description
			. The user cannot modify the values of the locked preferences in the client as locked preferences appear as read-only. To reset locked preferences, use `SET LOCKED_PREFERENCES ""` . The name of a setting must be the same across all clients. Client Navigation: Not Applicable.
OBSCURE_PREFERENCES			
String	Not obscured	• Android • iOS • Mac • Windows	The list of obscured preferences. If you specify any parameters in this attribute, Avaya Workplace Client makes the value read-only. Also, the data itself is hidden from end-users. **Note:** If you use the OBSCURE_PREFERENCES parameter to hide a setting but now want to display that setting, the user must reset and reconfigure Avaya Workplace Client. You cannot display a previously hidden setting by simply removing the setting from OBSCURE_PREFERENCES.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
VOIPCALLINGENABLED			
Numeric	1	• Android • iOS	This parameter indicates whether Wi-Fi or cellular data is used to make calls. The supported values are: • 0: Never. • 1: Prefer Wi-Fi. • 2: Wi-Fi only. • 3: Prefer cellular data. Client Navigation: **Settings** > **User Preferences** > **Audio / Video** > **Use VoIP for calls**.
TRUSTCERTS			
String	Null	• Android • iOS • Mac • Windows	The list of URLs, absolute or relative, to CA certificates that will be stored in the private trust store and used to validate certificates of various servers. Set a blank value to clear the private trust store and go back to the platform trust store. Certificates stored in binary DER form, commonly known as .cer, .crt, or .der files, and Base64-encoded DER form, commonly known as .pem files, are supported.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
TRUST_STORE			
Numeric	1	• Android • iOS • Mac • Windows	This parameter is used to enable the trust stores in the server certificate chain validation. The options are: • 0: Indicates that only private trust store is used for all CSDK HTTPS and TLS connections. • 1: Indicates that both platform and private trust stores are used for all CSDK HTTPS and TLS connections. **Note:** If you disable the private trust store in the TRUSTCERTS setting, then all HTTPS and TLS connections use the platform trust store and this setting does not apply. Client Navigation: Not Applicable.
DISABLE_PASSWORD_STORAGE			

Type	Default value	Supported platforms	Description
Numeric	0	• Android • iOS • Mac • Windows	This parameter stops the client from storing passwords locally. The options are: • 0: Indicates False. • 1: Indicates True. When this parameter is enabled, the client can continue to cache the credentials in RAM only. The client does not store passwords in persistent storage. This implies that each time the client starts, users are prompted to enter their password. The Push Notification solution from Avaya requires the DISABLE_PASSWORD_STORAGE parameter to be set to 0. If the Avaya Workplace Client user needs to provide a password prior to answering the call, the probability of the user successfully logging in is relatively low before the: • Call is routed. • Call originator cancels the call. Client Navigation: Not Applicable.
FORCE_LOGOUT_AFTER			
Numeric	0	• Android	This parameter represents the number of days before the client

Type	Default value	Supported platforms	Description
		- iOS	automatically logs out. It forces users to enter their credentials to log in again. The range is from 0 to 365 days. The options are: - 0: Indicates that the parameter is disabled. - 1 to 365: Indicates the number of days before the client automatically logs out. Client Navigation: Not Applicable.
DISABLE_COOKIE_STORAGE			
Numeric	1	- Mac - Windows	This parameter indicates whether browser cookies are persisted into the platform cookie store. The options are: - 0: Indicates False. Browser cookies are persisted in the cookie management of the platform, accessible to other application browsers.

Type	Default value	Supported platforms	Description
			- 1: Indicates True. Browser cookies are not persisted beyond the life cycle of the application process. For OAuth and SSO deployments, you can disable this parameter to improve the user login experience, enabling users to only log in once to each IDP. For shared workstations, that is, different client account and same shared OS account, you can enable this parameter to force sign-in of different client users for each client login. Client Navigation: Not Applicable.
CUSTOMIZED_FEATURE_LABEL_URL			
String	Null	Windows	This parameter indicates the URL of an XML file. Avaya Workplace Client uses this XML file to display the customized feature button labels on Button Module and Incoming Call Features. For example, `CUSTOMIZED_FEATURE_LABEL_URL` `"https://test.domain.com/featureButtonLabels.xml"`

Type	Default value	Supported platforms	Description
			. **Note:** Avaya Workplace Client does not support customized feature button labels on Feature Manager. Client Navigation: Not Applicable.
INVERT_HUNT_GROUP_LED_STATE			
Numeric	0	Windows	This parameter is used to invert the LED state of the Hunt Group Busy feature button on Button Module. The options are: • 0: Indicates that Avaya Workplace Client does not invert the LED state of the Hunt Group Busy feature button. 1: Indicates that Avaya Workplace Client inverts the LED state of the Hunt Group Busy feature button. For example, if you enable the Hunt Group Busy feature, Avaya Workplace Client displays the green LED state on

Type	Default value	Supported platforms	Description
			Button Module by default. However, if you set this parameter to 1, Avaya Workplace Client inverts the LED state to red. Client Navigation: Not Applicable.
ENABLE_DISCONNECT_TONE			
Numeric	1	• Android • Windows	This parameter indicates whether Avaya Workplace Client plays the disconnected tone when the other participant disconnects from an active call. The options are the following: • 0: Indicates that Avaya Workplace Client does not play the disconnected tone. 1: Indicates that Avaya Workplace Client plays the disconnected tone when the other participant disconnects from an active call.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.

VoIP calls

The administrator can configure the following values for the VOIPCALLINGENABLED attribute in the settings file:

- 0: Never
- 1: Prefer Wi-Fi
- 2: Wi-Fi only
- 3: Prefer cellular data

Avaya Workplace Client maintains an internal variable to represent user preferences for the **Use VoIP for calls** setting:

- 0: Never
- 1: Prefer Wi-Fi
- 2: Wi-Fi only
- 3: Prefer cellular data

The Avaya Workplace Client logic depends on both the administrative setting in the settings file and the user preference in Avaya Workplace Client.

Note:

If you enable telephony push notification, Avaya Workplace Client for iOS does not support VoIP calling preferences. Hence, Avaya Workplace Client for iOS does not display the **Use VoIP for calls** option. When you enable push notifications, you must set VOIPCALLINGENABLED as 1 (Always) or 3 (Cellular). If you set VOIPCALLINGENABLED as 0 (Never) or 2 (Wi-Fi only), the user receives incoming calls but cannot answer the calls.

Variable	Use VoIP for calls = Never	Use VoIP for calls = Prefer Wi-Fi	Use VoIP for calls = Wi-Fi only	Use VoIP for calls = Prefer cellular data
VOIPCALLINGENABLED = 0	Avaya Workplace Client displays this option as selected by the administrator.	The user cannot select this option.	The user cannot select this option.	The user cannot select this option.

Variable	Use VoIP for calls = Never	Use VoIP for calls = Prefer Wi-Fi	Use VoIP for calls = Wi-Fi only	Use VoIP for calls = Prefer cellular data
	The user cannot edit the setting.			
VOIPCALLINGENABLED = 1	The user can select this option. The Avaya Workplace Client logic depends on the user setting.	Avaya Workplace Client displays this option as selected by the administrator. The user can select this option. The Avaya Workplace Client logic depends on the user setting.	The user can select this option. The Avaya Workplace Client logic depends on the user setting.	The user cannot select this option.
VOIPCALLINGENABLED = 2	The user can select this option. The Avaya Workplace Client logic depends on the user setting.	The user cannot select this option.	Avaya Workplace Client displays this option as selected by the administrator. The user can select this option. The Avaya Workplace Client logic depends on the user setting.	The user cannot select this option.
VOIPCALLINGENABLED = 3	The user can select this option. The Avaya Workplace Client logic depends on the user setting.	The user cannot select this option.	The user cannot select this option.	Avaya Workplace Client displays this option as selected by the administrator. The user can select this option. The Avaya Workplace Client logic depends on the user setting.

The Wi-Fi network’s DNS resolves the domain name when both Wi-Fi and mobile data are enabled on the OS. To resolve the connection to the Avaya SBC IP addresses, you must correctly map the domain names on the DNS server. If the DNS mapping is incorrect, Avaya Workplace Client cannot register to Avaya SBC with the Prefer cellular data option.

On Avaya Workplace Client for iOS, consider a situation where you configure the VOIPCALLINGENABLED parameter with the value 3 (Cellular) and the user selects the Prefer cellular data option. In this case, if the user selects Wi-Fi when the mobile data, 3G, or 4G is enabled, only the SIP traffic uses mobile data, 3G, or 4G. The other Avaya Workplace Client for iOS traffic, which is HTTPS, uses Wi-Fi only, including PPM. Enterprises must configure their Wi-Fi networks to allow the ports and traffic to register to Avaya SBC.

On Avaya Workplace Client for Android, if the user selects the Prefer cellular data option, both SIP and HTTPS traffic use mobile data, 3G, or 4G.

User preferences parameters

After a fresh installation of Avaya Workplace Client, you can configure the parameters in the following table using automatic configuration only once. After the user configures the settings corresponding to these parameters in Avaya Workplace Client, you cannot change the values using automatic configuration except for the PREF_MUTE_MIC_WHEN_JOINING_MEETING and PREF_BLOCK_CAMERA_WHEN_JOINING_MEETING parameters.

To change the value of the PREF_MUTE_MIC_WHEN_JOINING_MEETING and PREF_BLOCK_CAMERA_WHEN_JOINING_MEETING parameters, do the following:

1. Lock or obscure the setting by using the LOCKED_PREFERENCES or OBSCURE_PREFERENCES parameter, and set the default value to an empty string.
2. Wait for the user to log in to the client, and implement the settings change.
3. Set the desired property value in the settings service or 46xx settings file.

Type	Default value	Supported platforms	Description
ADDRESS_VALIDATION			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether messaging address validation is enabled. The options are: • 0: Indicates disabled. • 1: Indicates enabled.

Type	Default value	Supported platforms	Description
			Client Navigation: **Settings** > **User Preferences** > **Contacts** > **Messaging Address Validation**.
PHONE_NUMBER_PRIORITY			
String	Work, Mobile, Home	• Android • iOS • Mac • Windows	This parameter indicates the default phone number priority. The value is a list of comma-separated strings, listed from left to right to indicate the order in which the phone numbers are used. If the PHONE_NUMBER_PRIORITY parameter is not defined, the default order is used. Client Navigation: Not Applicable.
NAME_SORT_ORDER			
String	Last name	• Android • Windows	This parameter indicates how names are sorted in the UI. The value is a comma-separated list of the following strings: • last • first By default, names are sorted according to the last name. Client Navigation: **Settings** > **User Preferences** >

Type	Default value	Supported platforms	Description
			Contacts > **Name Sort Preferences**.
NAME_DISPLAY_ORDER			
String	First name	• Android • Windows	This parameter indicates how names are displayed in the UI. The value is a comma-separated list of the following strings: • last • first By default, the first name is displayed first. Client Navigation: **Settings** > **User Preferences** > **Contacts** > **Name Display Preferences**.
HOMESCREENLAYOUT			
Numeric	0	• Android • iOS • Windows	This parameter indicates which Home screen layout Avaya Workplace Client must display. The options are: • 0: Displays Top of Mind. The user can change the preference on the mobile device. • 1: Displays the Top of Mind layout on mobile devices.

Type	Default value	Supported platforms	Description
			• 2: Displays the large dialpad layout on mobile and Windows devices. **Note:** Avaya recommends using the large dialpad layout on Windows devices in media-only deployments. On mobile devices, you can lock options 1 and 2 to prevent the user from changing them. Client Navigation: • On the home screen of mobile clients, tap the **Top of Mind** filter and then tap the **Top of Mind** switch. • On Windows client: Not Applicable.
APPLICATION_AUTO_START			
Numeric	• Desktop clients: 1 • Android: 0	• Android • Mac • Windows	This parameter indicates whether to start the client automatically. For desktop clients, the options are: • 0: No. • 1: Yes.

Type	Default value	Supported platforms	Description
			For Android, the options are: • 0: Does not start on reboot. • 1: Starts on reboot except for Samsung devices. This value prevents Samsung ML from starting regularly. This is a limitation for Samsung devices with Android 9 and later. If the user uses the Exit menu option, the application starts after the user manually presses the application icon. The application does not start automatically after the device reboots. • 2: Starts on reboot, including Samsung devices. This value allows Samsung ML to start at any time. This is a workaround for

Type	Default value	Supported platforms	Description
			Samsung devices with Android 9 and later. Even if the user uses the Exit menu option, the application starts without any user confirmation. The application starts automatically after the device reboots. **Note:** Depending on the Android version, the user might need to unlock the device after a reboot to receive calls and messages. Client Navigation: **Settings** > **User Preferences** > **General** > **Auto Start/Login**.
APPLICATION_CLOSE_WINDOW			
Numeric	0	• Mac • Windows	This parameter indicates how the client functions when the user clicks **X** in the main application window. The supported options are: • 0: Minimize the client to the taskbar or dock bar.

Type	Default value	Supported platforms	Description
			- 1: Minimize the client to the notification area. - 2: Exit the client. Client Navigation: **Settings** > **User Preferences** > **Display** > **Main Window X Preferences**.
ENABLE_SPELL_CHECK			
Numeric	1	Windows	This parameter indicates whether the spell check is enabled. The options are: - 0: Indicates that the spell check is disabled. - 1: Indicates that the spell check is enabled. Client Navigation: **Settings** > **User Preferences** > **Messaging** > **Spell check enabled**.
HIDDEN_MODE_ENABLED			
Numeric	0	Windows	This parameter indicates whether the hidden mode is enabled. The options are: - 0: Indicates that the hidden

Type	Default value	Supported platforms	Description
			mode is disabled. - 1: Indicates that the hidden mode is enabled. Client Navigation: **Settings** > **User Preferences** > **Display** > **Hidden Mode**.
ALTERNATIVE_DEFAULT_SHORTCUTS			
Numeric	0	Windows	This parameter indicates whether alternative shortcuts based on the Shift button are enabled. The options are: - 0: Indicates that alternative shortcuts based on the Shift button are disabled. - 1: Indicates that alternative shortcuts based on the Shift button are enabled. Client Navigation: Not Applicable.
CONTACT_COLOR_SCHEME			
Numeric	1	- Android - iOS - Mac	This parameter indicates the color scheme used with the contact's initials instead of the default avatar.

Type	Default value	Supported platforms	Description
		• Windows	The options are: • 0: Indicates that the color scheme for contacts is disabled. 1: Indicates that Avaya Workplace Client uses a muted color scheme for contacts. 2: Indicates that Avaya Workplace Client uses a vibrant color scheme for contacts. 3: Indicates that Avaya Workplace Client uses a monochrome color scheme for contacts. Client Navigation: • On mobile clients: **Settings** > **User Preferences** > **Contacts** > **Contact Color Scheme**. • On desktop clients: **Settings** >

Type	Default value	Supported platforms	Description
			User Preferences > **Display** > **Contact Color Scheme**.
ALWAYS_ON_TOP			
Numeric	0	Windows	This parameter indicates whether the Avaya Workplace Client application is always displayed on top of other applications on your desktop screen. This functionality is useful if Avaya Workplace Client is the primary application for users. The options are: • 0: Indicates that the Avaya Workplace Client application is not always displayed on top of other applications. 1: Indicates that the Avaya Workplace Client application is always displayed on top of other applications. Client Navigation: **Settings** > **User Preferences** > **Display** >

Type	Default value	Supported platforms	Description
			Always Display the Main Window on Top.
DISPLAY_MIDDLE_NAME			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client displays the middle name of a Microsoft Outlook contact. If you enable this parameter, you must also enable the ENABLE_LOCAL_CONTACT parameter, as Microsoft Outlook contacts are local. The options are: • 0: Indicates Avaya Workplace Client does not display the middle name of a Microsoft Outlook contact. • 1: Indicates Avaya Workplace Client displays the middle name of a Microsoft Outlook contact. Client Navigation: **Settings** > **User Preferences** >

Type	Default value	Supported platforms	Description
			Contacts > **Local Contacts Middle Name**.

SMS and Fax parameters

Type	Default value	Supported platforms	Description
SMS_GATEWAY_ENABLED			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether the user can initiate the SMS message creation using the default email client. The options are: • 0: Indicates that the user cannot initiate the SMS message creation using the default email client. 1: Indicates that the user can initiate the SMS message creation using the default email client if the gateway and contact mobile number are set. Client Navigation: Not Applicable

Type	Default value	Supported platforms	Description
SMS_GATEWAY			
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the SMS gateway, which is used to compose the email address. The gateway is added as a suffix to the contact mobile number in the following format: contact_mobile_number @sms_gateway Client Navigation: Not Applicable
SMS_PREFIX			
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the prefix for the SMS. This value is optional. If present, it is added before the contact mobile number when composing the email address in the following format: sms_prefixContact_mobile_number@sms_gateway Client Navigation: Not Applicable
FAX_GATEWAY_ENABLED			
Numeric	0	• Android • iOS • Mac • Windows	This parameter indicates whether the user can initiate the Fax message creation using the default email client. The options are: • 0: Indicates that the user cannot initiate the Fax

Type	Default value	Supported platforms	Description
			message creation using the default email client. 1: Indicates that the user can initiate the Fax message creation using the default email client if the gateway and contact Fax number are set. Client Navigation: Not Applicable
FAX_GATEWAY			
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the Fax gateway, which is used to compose the email address. The gateway is added as a suffix to the contact Fax number in the following format: contact_fax_number@fax_gateway Client Navigation: Not Applicable
FAX_PREFIX			
String	Null	• Android • iOS • Mac • Windows	This parameter indicates the prefix for the Fax. This value is optional. If present, it is added before the contact Fax number when composing the email address in the

Type	Default value	Supported platforms	Description
			following format: fax_prefixContact_fax_number@fax_gateway Client Navigation: Not Applicable

Contact parameters

Type	Default value	Supported platforms	Description
SELF_AVATAR_ENABLED			
Numeric	1	Windows	This parameter indicates whether to use the Exchange self-image as a self-avatar in Avaya Workplace Client. The Exchange self-image supersedes the image referenced by Avaya Aura® Device Services. The options are: • 0: Indicates that Avaya Workplace Client uses the enterprise LDAP directory self-image as a self-avatar. 1: Indicates that Avaya Workplace Client uses the Exchange self-

Type	Default value	Supported platforms	Description
			image as a self-avatar. **Note:** - The Exchange Server version must be 2013 or later. - You must enable the Exchange Calendar service in Avaya Workplace Client. - This functionality and the Exchange Calendar feature do not work if you deploy an earlier version of Exchange Server. Client Navigation: Not Applicable
CONTACT_MATCHING_CONDITION			
Numeric	0	Windows	This parameter controls the method of contact resolution. The options are: - 0: Indicates that Avaya Workplace

Type	Default value	Supported platforms	Description
			Client selects the first contact with picture from the list of matches. 1: Indicates that Avaya Workplace Client selects the first contact from the list of matches. Client Navigation: Not Applicable

Export Conversation parameter

Type	Default value	Supported platforms	Description
ARCHIVING_ENABLED			
Numeric	0	Windows	This parameter indicates whether the user can export an instant messaging conversation or public conference chat to an HTML file. To export a public conference chat, the user must be the conference call moderator. ✱ **Note:** The user cannot export a Spaces conversation. The options are:

Type	Default value	Supported platforms	Description
			• 0: Indicates that the user cannot export an instant messaging conversation or conference chat to an HTML file. • 1: Indicates that the user can export an instant messaging conversation or conference chat to an HTML file. Client Navigation: Not Applicable

MLPP parameters

Type	Default value	Supported platforms	Description
ENABLE_MLPP			
Numeric	0	Windows	This parameter controls the MLPP feature. The options are: • 0: Indicates that the MLPP feature is disabled.

Type	Default value	Supported platforms	Description
			• 1: Indicates that the MLPP feature is enabled. Client Navigation: Not Applicable
MLPP_NETWORK_DOMAIN			
String	Null	Windows	This parameter indicates the MLPP network domain, which is used in the SIP Resource-Priority header. Client Navigation: Not Applicable
MLPP_PRECEDENCE_DOMAIN			
Numeric	000000	Windows	This parameter indicates the MLPP precedence domain, which is used in the SIP Resource-Priority header. Client Navigation: Not Applicable
MLPP_MAX_PREC_LEVEL			
Numeric	1	Windows	This parameter controls the maximum allowed precedence level for the user. The range is 1 to 5, where 1 is the lowest.

Type	Default value	Supported platforms	Description
			The options are: • 1: Indicates Routine. • 2: Indicates Priority. • 3: Indicates Immediate. • 4: Indicates Flash. • 5: Indicates Flash Override. Client Navigation: Not Applicable
ENABLE_PRECEDENCE_SOFT_KEY			
Numeric	1	Windows	This parameter controls the user capability to select a precedence level from a list when dialing an outbound call. The options are: • 0: Indicates that the user cannot select a precedence level from a list when dialing an outbound call. • 1: Indicates that the user can select a precedence level from a list when dialing an outbound call.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable

Parameter configuration to improve experience on Google Chromebook

You can configure the following parameters to improve your Workplace experience on Chromebook:

- SCREEN_ALWAYS_AWAKE_ON_FOREGROUND as 1: Keep device screen awake when Avaya Workplace Client is running in the foreground.
- ENABLE_AUTO_ANSWER_MOBILE as 1: Configure Avaya Workplace Client to answer a call automatically.
- ENABLE_LOCAL_AUTO_ANSWER as 1: Avaya Workplace Client plays a zip tone to alert the user about the incoming call. Avaya Workplace Client then automatically answers the call as an audio-only call.
- ENABLE_CALL_NOTIFICATIONS as 0: Suppress incoming call notifications.
- ENABLE_TUTORIAL as 0: Disable the Avaya Workplace Client tutorial.
- HOMESCREENLAYOUT as 2: Display a simplified dialpad view on the Home screen.
- ENABLE_AVAYA_CLOUD_ACCOUNTS as 0: Disables the Avaya Cloud accounts integration. Avaya Workplace Client does not display the Spaces area in the Workplace Meetings panel on the Top of Mind screen.
- ENABLE_TOP_OF_MIND as 0: Disables the Top Of Mind feature. Avaya Workplace Client does not retrieve any calendar information. Also, the Top Of Mind and Calendar buttons are unavailable.

Settings file template for Avaya Workplace Client

In the settings file, you can:

- Clear the existing value for a setting in the client by using a blank string.
  For example,
  ```
  SET SIPUSERNAME
  ""
  ```

  . You can use a blank string only for non-User preference parameters and PREF_MUTE_MIC_WHEN_JOINING_MEETING and PREF_BLOCK_CAMERA_WHEN_JOINING_MEETING parameters.

- Exclude a parameter if you want to use the default value for the parameter in the client. For example, to use the default value for the AUTO_AWAY_TIME parameter, use `##SET AUTO_AWAY_TIME` .

Note:

Ensure that the setting for each parameter does not include line breaks. Avaya Workplace Client cannot parse settings file parameters with line breaks.

The following example shows the settings in the Avaya settings text file format, that is, 46xxsettings.txt. You can download the latest 46xxsettings.txt file for Avaya Workplace Client from http://support.avaya.com.

```
SET SIPUSERNAME ""
SET SIPPASSWORD ""
SET UNIFIED_PORTAL_USERNAME ""
SET UNIFIED_PORTAL_PASSWORD ""
SET CESUSERNAME ""
SET CESPASSWORD ""
SET EWSUSERNAME ""
SET EWSPASSWORD ""
SET ESMUSERNAME ""
SET ESMPASSWORD ""
SET ACSUSERNAME ""
SET ACSPASSWORD ""
SET SUPPORTEMAIL support@slav.com
SET SUPPORTURL ""
SET SUPPORTEMAIL_REPORT_ATTACHMENT_SIZE 10
SET LOG_VERBOSITY 1
SET SUPPORTEMAIL_ENCRYPTED 0
SET SUPPORTEMAIL_ENCRYPTIONPASSPHRASE ""
SET UC_DATA_PRIVACY_URL ""
SET ENABLE_IN_APP_RATING 1
SET ATTACHMENT_FILETYPE_BLACKLIST ""
SET EXACT_SIP_DOMAIN_COMPARISON 1
SET ACTIVATE_DESKPHONE_MODE_ON_STARTUP 0
SET ENABLE_CALL_NOTIFICATIONS 1
SET ENABLE_AUDIBLE_CALL_NOTIFICATIONS 1
SET ENABLE_TUTORIAL 1
SET SCREEN_ALWAYS_AWAKE_ON_FOREGROUND 0
SET LOCALLY_ENFORCE_PRIVACY_HEADER 0
SET DISABLE_COPY_PASTE 0
SET XCALLBACK_LOGOUT_ENABLED 0
SET DISABLE_END_CALL 0
SET RESET_ON_SIGNOUT 0
SET ENABLE_BLIND_TRANSFER 1
SET ONLINE_HELP_ENABLED 1
SET ENABLE_BLA_NO_RING_CALL_NOTIFICATIONS 1
SET ADMIN_PASSWORD ""
SET ALTERNATE_EMERGENCY_CALL_DISCLAIMER 0
SET SHOW_CALLERID_ON_CALL_APPEARANCE 0
SET BLIND_TRANSFER_AUTO_HOLD 0
SET CONF_TRANS_ON_PRIMARY_APPR 0
SET AUTO_SELECT_ANY_IDLE_APPR 0
SET ENABLE_OAUTH_LOGIN_AUTO_POPUP
SET ENABLE_MINIMIZE_AFTER_CALL_END
SET ENABLE_MESSAGE_COALESCING
SET TELEPHONY_PUSH_EXPIRY
SET ACTIVATE_OTHERPHONE_MODE_ON_STARTUP
SET TC_NUMBER
SET ENABLE_TRANSFER_ACTIVE_CALL

##Enable Unified Login
SET SSOENABLED 1
SET UNIFIED_PORTAL_SSO 1
SET ESMSSO 1
SET CESSSO 1
SET EWSSSO 1
SET SSOUSERID ""
SET SSOPASSWORD ""

SET AUTOCONFIG_USESSO 1
SET SETTINGS_CHECK_INTERVAL 1
SET SETTINGS_FILE_URL ""
SET SETTINGS_CHECK_POLICY 0

SET LOCKED_PREFERENCES ""
SET OBSCURE_PREFERENCES ""
SET VOIPCALLINGENABLED 1
SET TRUSTCERTS ""
SET TRUST_STORE 1
SET DISABLE_PASSWORD_STORAGE 0
SET FORCE_LOGOUT_AFTER 0
SET DISABLE_COOKIE_STORAGE 1
SET CUSTOMIZED_FEATURE_LABEL_URL ""
SET INVERT_HUNT_GROUP_LED_STATE 0
SET ENABLE_DISCONNECT_TONE
SET REVOCATIONCHECKENABLED 1
SET TLSSRVRID 0
SET SUPPORTWINDOWSAUTHENTICATION 0
SET PKCS12URL ""
SET PKCS12PASSWORD ""
SET MYCERTURL ""
SET MYCERTCN ""
SET SCEPPASSWORD ""
SET SCEP_USESSO 0
SET MYCERTDN ""
SET MYCERTCAID CAIdentifier
SET MYCERTKEYLEN 2048
SET MYCERTRENEW 90
SET TLS_VERSION 0
SET CIPHER_SUITE_BLACKLIST ""
SET CERTIFICATE_MIN_RSA_KEY_LENGTH 1024
SET ADDRESS_VALIDATION 0
SET PHONE_NUMBER_PRIORITY ""
SET NAME_SORT_ORDER ""
SET NAME_DISPLAY_ORDER ""
SET HOMESCREENLAYOUT 0
SET APPLICATION_AUTO_START 0
SET APPLICATION_CLOSE_WINDOW 2
SET ENABLE_SPELL_CHECK 1
SET HIDDEN_MODE_ENABLED 0
SET ALTERNATIVE_DEFAULT_SHORTCUTS 0
SET CONTACT_COLOR_SCHEME 1
SET ALWAYS_ON_TOP 0
SET DISPLAY_MIDDLE_NAME 0

##LDAP search
SET DIRENABLED 0
SET DIRSSO 1
SET DIRSRVR ldap.customer.com
SET DIRSRVRPRT 636
SET DIRUSERNAME ""
SET DIRPASSWORD ""
SET DIRTOPDN "cn=users,dc=svucacl,dc=com"
SET DIRSECURE 1
SET DIRIMATTRIBUTE mail
SET DIRUSEIMDOMAIN 1
SET DIRTYPE ACTIVEDIRECTORY
SET DIRSCOPE LDAP_SCOPE_SUBTREE
SET DIRTIMEOUT 100
SET DIRMAXENTRIES 50
SET DIR_CONTACT_RESOLUTION_ENABLED 1

SET EC500ENABLED 0
SET EC500VOICEMAILNUMBER
SET FNUSACCANCEL 02066070504
SET FNUSACENABLE 02066070505
SET FNUIDLEAPPEARANCESELECT 02066070506
SET FNUSIMRINGENABLE 02066070507
SET FNUSIMRINGDISABLE 02066070508
SET FNUCFWDENABLE 02066070509
SET FNUCFWDDISABLE 02002066070511
SET FNUACTIVEAPPEARANCESELECT 02066070512
SET STATION_SECURITY_ENABLED 0

SET DIALPLANLOCALCALLPREFIX 0
SET PHNLDLENGTH 10
SET ENHDIALSTAT 0
SET PHNOL 9
SET PHNCC 91
SET DIALPLANAREACODE 20
SET PHNPBXMAINPREFIX 6607
SET PHNLD 0
SET PHNIC 00
SET PHNDPLENGTH 8
SET DIALPLANEXTENSIONLENGTHLIST ""
SET DIALPLANNATIONALPHONENUMLENGTHLIST ""
SET AUTOAPPLY_ARS_TO_SHORTNUMBERS 1
SET APPLY_DIALINGRULES_TO_PLUS_NUMBERS 0
SET ELD_SYSNUM 1

SET ECHO_CANCELLATION aec

SET DND_SAC_LINK 0
SET WINDOWS_IMPROVIDER 0
SET WINDOWS_IMPROVIDER_RESOLVE_CONTACT_EXTERNAL 0
SET OBSCURE_PRESENCE_STATES ""
SET AUTO_AWAY_TIME 10
SET ENABLE_PRESENCE 1
SET ANALYTICSENABLED 1

SET DTMF_PAYLOAD_TYPE 120
SET RTP_PORT_LOW 5004
SET RTP_PORT_RANGE 40
SET ENABLE_OPUS 1
SET OPUS_PAYLOAD_TYPE 116
SET DSCPAUD 46
SET DSCPSIG 24
SET DSCPAUD_PRIORITY 46
SET DSCPAUD_IMMEDIATE 46
SET DSCPAUD_FLASH 46
SET DSCPAUD_FLASHOVERRIDE 46
SET DSCPVID 34
SET DSCPVID_PRIORITY 34
SET DSCPVID_IMMEDIATE 34
SET DSCPVID_FLASH 34
SET DSCPVID_FLASHOVERRIDE 34
SET MEDIAENCRYPTION 10,1,2,9
SET ENCRYPT_SRTCP 0
SET ENABLE_MEDIA_HTTP_TUNNEL 1
SET MEDIA_ADDR_MODE 4
SET MEDIA_ADDR_MODE_HTTP 4

SET ENABLE_VIDEO 1
SET VIDEO_MAX_BANDWIDTH_ANY_NETWORK 512
SET VIDEO_MAX_BANDWIDTH_CELLULAR_DATA 512
SET VIDEO_MAX_RESOLUTION 0
SET VIDEO_CAPTURE_RESOLUTION 0
SET BFCP_TRANSPORT 0
SET BFCP_UDP_MINIMUM_PORT 5204
SET BFCP_UDP_MAXIMUM_PORT 5224
SET ENABLE_MSS_VIDEO 1
SET FORWARD_ERROR_CORRECTION 3
SET ENABLE_H263 0
SET VIDEO_BACKGROUND_ENABLED 0
SET VIDEO_BACKGROUND_URL ""

SET MESSAGING_VVM_ENABLED 0
SET MESSAGING_VVM_SRVR ""
SET MESSAGING_VVM_PORT
SET MESSAGING_SSO 2

SET ENABLE_AVAYA_CLOUD_ACCOUNTS 1
SET AVAYA_CLOUD_ACCOUNTS_URI accounts.avayacloud.com
SET AVAYA_CLOUD_SPACES_URI spaces.avayacloud.com
SET AVAYA_CLOUD_SPACES_API_URI spacesapis.avayacloud.com
SET ENABLE_EQUINOX_MEETING_ACCOUNT_DISCOVERY 1
SET EQUINOX_MEETING_ACCOUNT_DISCOVERY_URL https://meetings.avaya.com/acs/resources/
SET ENABLE_EWS_ACCOUNT_DISCOVERY 1
SET ENABLE_GOTO_MEETING_PORTAL 1
SET ENABLE_SPACES_MESSAGING 1

SET SIPENABLED 1
SET SIP_CONTROLLER_LIST svsm01.slav.com:5061;transport=tls,svsm02.slav.com:5061;transport=tls
SET SIPDOMAIN svucacl.com
SET SIPSSO 0
SET SIMULTANEOUS_REGISTRATIONS 0
SET ENABLE_MDA_JOIN 0
SET ENFORCE_SIPS_URI 1
SET ENABLE_PUBLISH_MAC_ADDRESS 0
SET ENABLE_PPM 1
SET ENABLE_PPM_CALL_JOURNALING 1
SET SHOW_TEAM_BUTTON_VISUAL_ALERT 1
SET SHOW_TEAM_BUTTON_CALLER_ID 1
SET SIGNALING_ADDR_MODE 4
SET FAILED_SESSION_REMOVAL_TIMER 15
SET CALL_DECLINE_POLICY 0
SET ENABLE_PPM_PERSISTENT_DATA 0
SET NO_SUBSCRIBE_ON_SIP_CONNECTION_RECOVERY 0
SET ENABLE_PPM_CONTACTS 1
SET PPM_CONFIG_REQUEST_TIMEOUT 10
SET ENABLE_CALLBACK_SERVICE 0

SET EWSENABLED 0
SET EWSSERVERADDRESS usmail.slav.com
SET EWSDOMAIN slav.com
SET EWSREADTIMEOUT 300
SET CALENDAR_INTEGRATION_ENABLED 1
SET GOOGLE_CALENDAR_INTEGRATION_ENABLED 0

SET CESENABLED 0
SET CESSRVR abd.xyz.com
SET CESPORT 7777
SET CESSECURE 1
SET CESVMPIN

SET DESKTOP_HTTP_APPLICATION_INTEGRATION 1
SET ENABLE_OUTLOOK_ADDON 1
SET OUTLOOK_CALL_CONTACT 1
SET ENABLE_LOCAL_CONTACT 1
SET OUTLOOK_ADDON_HOST_URI ""
SET ENABLE_PLT_OOB_HEADSET_CALL_CONTROL 1
SET ENABLE_JABRA_OOB_HEADSET_CALL_CONTROL 1
SET ENABLE_TOP_OF_MIND 1

##AMM setting details
SET ESMENABLED 1
SET ESMSRVR abe.xyz.com
SET ESMPORT 8443
SET ESMSECURE 1
SET ESMREFRESH 0
SET ESMHIDEONDISCONNECT 0
SET ESMSENDREADRECEIPTS 1

##AADS setting details
SET ACSENABLED 0
SET ACSSRVR 10.133.67.10
SET ACSPORT 443
SET ACSSECURE 1
SET ACSSSO 1
SET CONTACT_MATCHING_SEARCH_LOCATION 1
SET AVAYA_AUTHORIZATION_REALM ""

SET CONFERENCE_FACTORY_URI "66078889@slav.com"
SET CONFERENCE_ACCESS_NUMBER ""
SET ADDITIONAL_CONFERENCE_ACCESS_NUMBER_LIST ""
SET UNIFIEDPORTALENABLED 0
SET CONFERENCE_PORTAL_URI "https://conf.portal.com:8043/aacpa/"
SET CONFERENCE_MODERATOR_CODE 20111
SET CONFERENCE_PARTICIPANT_CODE 2011
SET CONFERENCE_PARTICIPANT_URL ""
SET CONFERENCE_VIRTUAL_ROOM ""
SET CONFERENCE_FQDN_SIP_DIAL_LIST "alphascopia.slav.com,scopia.slav.com,alphaconfportal.slav.com"
SET UCCPENABLED 0
SET SHOW_EQUINOX_MEETING_PANEL_IN_TOM 1
SET RECEIVE_ONLY_SHARING_ENABLED 0
SET PREF_MUTE_MIC_WHEN_JOINING_MEETING 1
SET PREF_BLOCK_CAMERA_WHEN_JOINING_MEETING 1
SET HTTPUAENABLED 1
SET COLLAB_WHITEBOARDING_ENABLED 1
SET COLLAB_SCREENSHARE_ENABLED 1
SET COLLAB_SHAREAPPLICATION_ENABLED 1
SET COLLAB_SHAREAPPLICATION_FILTER ""

SET APPCAST_ENABLED 0
SET APPCAST_URL ""
SET APPCAST_CHECK_INTERVAL 1

SET FNE_SETUP_DELAY 3
SET CELLULAR_DIRECT_ENABLED 0
SET CELLULAR_DIRECT_NUMBER_LIST "03","94","193","93","92","91","444444","2681
1","+91{}12'3'45","\12345/","[12345]","?12345?%","03","01","+91 98-60-406784"
,"6886432@slav.com","sip:6886432@slav.com","23456","*9860406784","116","999",
"112","666","987654","45042","000#"
SET SIP_CRLF_PING_INTERVAL 30
SET HTTP_PROXY_CSDK_ENABLE 2
SET TELEPHONY_PUSH_NOTIFICATION_SERVICE_URL "https://<AAWG FQDN>:Port"
SET TELEPHONY_PUSH_NOTIFICATION_ENABLED 0
SET ESM_PUSH_NOTIFICATION_ENABLED 0
SET PRESENT_USER_NAME_ONLY 0
SET OTHER_PHONE_MODE_ENABLED 1
SET INITIATE_OTHER_PHONE_INCOMING_WHEN_FORWARDING_ENABLED 0
SET OTHER_PHONE_MODE_REMOTE_MEDIA_RESPONSE_TIMEOUT 30
SET ENABLE_DESKPHONE_SHARE_CONTROL 1
SET ENABLE_DESKPHONE_SHARE_CONTROL_MULTI 0
SET ENABLE_CONTROLLED_SOFTPHONE 0
SET CONTROLLEDEP_CONFIGURL ""
SET ENABLE_ALTERNATE_CLI 0
SET AUDIO_DEVICE_CALL_CONTROL_ENABLED 1

SET ARCHIVING_ENABLED 0

SET SCREEN_POP_LIST ""
SET APPLICATION_SCREEN_POP_LIST ""
SET SMS_GATEWAY_ENABLED 0
SET SMS_GATEWAY ""
SET SMS_PREFIX ""
SET FAX_GATEWAY_ENABLED 0
SET FAX_GATEWAY ""
SET FAX_PREFIX ""

SET SELF_AVATAR_ENABLED 1
SET CONTACT_MATCHING_CONDITION 0

SET ENABLE_MLPP 0
SET MLPP_NETWORK_DOMAIN ""
SET MLPP_PRECEDENCE_DOMAIN 000000
SET MLPP_MAX_PREC_LEVEL 1
SET ENABLE_PRECEDENCE_SOFT_KEY 1
```

Setting up the DNS server

About this task

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

Create records on the DNS server of the enterprise to link your DNS server to the settings file. Use split-horizon DNS and the same FQDN for Session Border Controller and Session Manager if you want to prevent users from re-configuring their clients when working outside 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 Workplace Client 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.

Before you begin

- Create the settings file.

- Configure a web server and save the settings file to that web server. You must know the URL of 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. You can enter 0 to keep the default port number for the protocol.
    - SRV record priority. For example, 0.
    - SRV record weight. For example, 0.

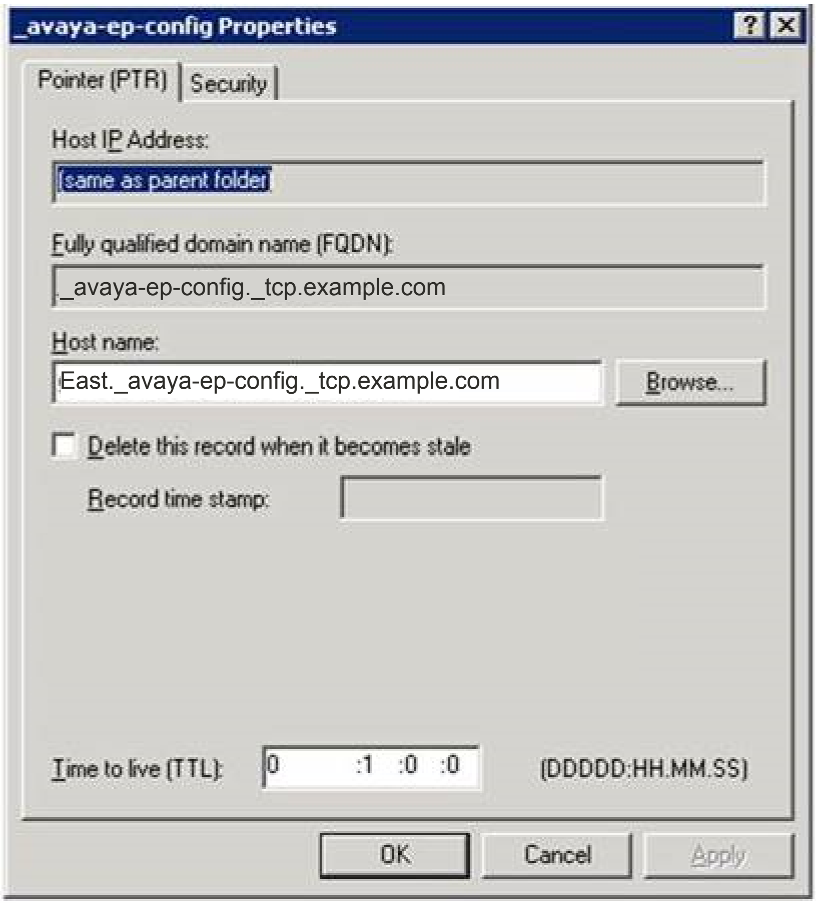
Procedure

1. Create a PTR record that links the descriptive name of your settings 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 settings 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.co
    m
    ```
    .

    In case of Microsoft DNS Manager, the following is an example of a PTR record:



Host IP Address: (same as parent folder)

Fully qualified domain name (FQDN): _avaya-ep-config._tcp.example.com

Host name: East._avaya-ep-config._tcp.example.com

□ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

Tip:

In the left pane of Microsoft DNS Manager, you must create the PTR, SRV, and TXT records at the _avaya-ep-config level. If the _avaya-ep-config level does not exist, you must manually create it. Right-click _avaya-ep-config and then click **Other New Records**, select the resource record type, and then click **Create Record**.

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

   If the URL to the settings 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:

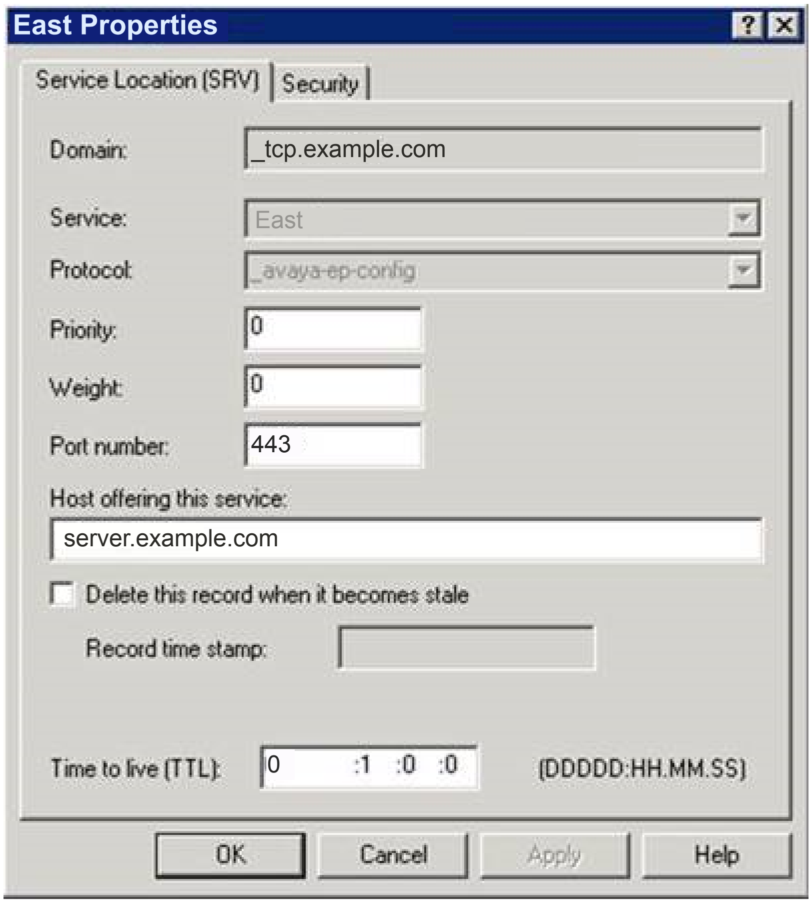
   ```
   East._avaya-ep-config._tcp.example.com. 300 IN SRV 0 0 443 server.example.com
   ```

.

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.

In case of Microsoft DNS Manager, the following is an example of an SRV record:



Domain: _tcp.example.com

Service: East

Protocol: _avaya-ep-config

Priority: 0

Weight: 0

Port number: 443

Host offering this service:

server.example.com

☐ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

3. Create a TXT record linking the descriptive name of your settings 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 settings file. An example value is

     ```
     path=/East_settings.txt
     ```

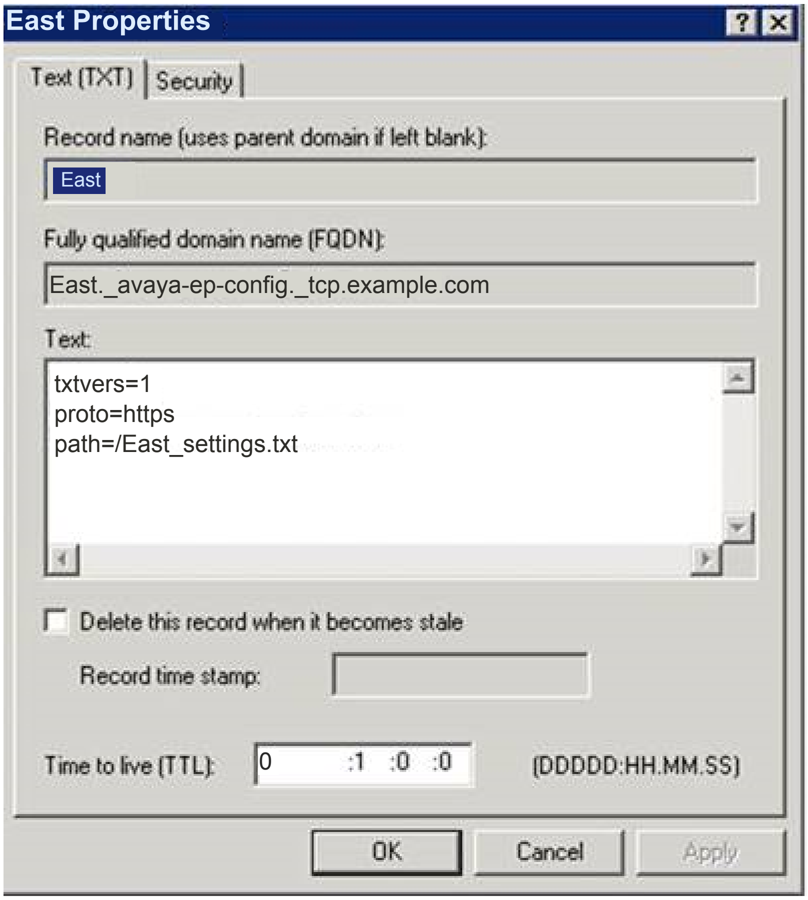
     .
   - proto: The web server access scheme. This value is usually `http` or `https`.

   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.

In case of Microsoft DNS Manager, the following is an example of a TXT record:



Record name (uses parent domain if left blank): East

Fully qualified domain name (FQDN): East._avaya-ep-config._tcp.example.com

Text:

```
txtvers=1
proto=https
path=/East_settings.txt
```

□ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

Sample DNS SRV records configuration

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 Workplace Client 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.

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

PTR records

PTR records provide a list of configurations with multiple PTR records. Avaya Workplace Client supports multiple PTR records. Avaya Workplace Client displays each one of the PTR records in a drop-down list that allows the user to choose from different environments.

Format:

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

The following are 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

SRV records provide a link from the descriptive name to the web server where you stored the file. If you have multiple SRV records for the same PTR record, then the priority of the SRV records must be different.

Note:

Avaya Workplace Client for mobile platforms does not support multiple SRV records. Hence, one PTR record supports only one SRV record.

Format:

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

The following are 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

TXT records provide 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>"
```

The following are examples with Avaya Aura® Device Services:

- `East._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/acs/resources/configurations"`

- West._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/acs/resources/configurations"

The following are examples without Avaya Aura® Device Services:

- 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"

The following are examples with Avaya Aura® Device Services and OAuth2:

- East._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/acs/resources/configurations?preferredAuth=bearer"
- West._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/acs/resources/configurations?preferredAuth=bearer"

DNS-based automatic configuration for DNS servers not compliant with RFC 6763

The sample DNS SRV records configuration in the earlier section is based on RFC 6763 and is the preferred method for deploying Avaya Workplace Client. However, some third-party DNS services, such as GoDaddy and Verisign, do not fully support RFC 6763. Deployments that rely on these third-party DNS services do not offer the ability to provision multiple parameters in the TXT record response. This prevents those deployments from using DNS-based automatic configuration.

To work around the limitations of third-party DNS services, you can use a TXT record format that condenses the parameters into a single parameter from a DNS configuration perspective.

Note:

Define the TXT record in the DNS file in one line. The parameters must be delimited by a comma.

TXT records

The TXT record 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>"
```

The following are examples:

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

You can either use the original solution parameter set or the new condensed parameter set. Do not combine both sets of parameters. The following combinations are invalid:

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

Avaya Cloud account method for configuring URL discovery

The recommended way to allow users to configure Avaya Workplace Client is by entering an email address. If you are unable to configure the required PTR records in DNS, use Avaya Cloud accounts to create a mapping for your company domain to one or more settings files.

- Create an Avaya Cloud account.
- Set up a company domain on https://accounts.avayacloud.com/.
- Map your domain to the settings file URL.

Registering an account

About this task

Use this procedure to register an account using your email address.

Procedure

1. In your web browser, enter https://accounts.avayacloud.com/.
2. In the **Email or Phone** field, type your email address.
3. Click **Yes, sign me up!**.
   sends a confirmation email to the email address you specified.
4. In your mailbox, open the confirmation email and then click the **Confirm** button.
   You are redirected to the My Account page.
5. Provide your first name, last name, password, and, optionally, a photo.
6. Click **Create an account**.

Setting up a company domain in Avaya Cloud accounts

Before you begin

- Ensure that your customer domain matches the email address domain for logging in to Avaya Workplace Client.
- Ensure that you have access to the DNS server settings for the domain.

Procedure

1. Log in to Avaya Cloud accounts at https://accounts.avayacloud.com/.
2. **Optional** If you have not set up your company or want to configure a new company, do the following:
   a. Click on your user name in the top-right of the screen, and click **Add Company**.
   b. Type a name and description for your company.
   c. Click **Save**.

3. Click **Manage Companies**, and click the existing company name.
4. Click **Domains**.
5. Click **Add Domain**.
6. Type the domain address, and click **OK**.
7. To verify ownership of the domain, next to the domain name, click **Verify**.
   You can view a verification code.
8. Copy the verification code and add it as a text record to the DNS entries on the domain's DNS server.

9. Click **Verify**.

Mapping your domain to the settings file URL

About this task

Add Equinox Cloud Client to the company domain on https://accounts.avayacloud.com/ and put the settings file URL in the public settings in the correct JSON format.

You can specify multiple systems in the network by adding multiple Profile_Name sections, one for each system that can be used for Avaya Workplace Client registration. You can use this procedure while waiting for the company domain to be verified.

Procedure

1. Log in to your Avaya Cloud account and click **Manage Companies**.
2. Click the company name.
3. Click **Apps**.
4. Click **Configure New App**.
5. In the **Product** field, select **Equinox Cloud Client**.
6. In the **Public Settings** field, enter the following settings, which are altered to match the customer system URL:
    - Single login system

    ```
    {
      "Client_Settings_File_Address": [
        {
          "Profile_Name": "Production",
          "Client_Settings_File_Url": "https://productionserver.example.c
    om/acs/resources/configurations?preferredAuth=Bearer"
        }
      ]
    }
    ```

    - Multiple login systems: If there are multiple servers, the user receives a prompt from a list of profile names when they log in.

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Url": "https://servereast.example.com/acs
/resources/configurations?preferredAuth=Bearer"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Url": "https://serverwest.example.com/acs
/resources/configurations?preferredAuth=Bearer"
    }
  ]
}
```

7. Click **Save**.

Modifying registry entries to discover the settings file URL on Windows

About this task

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

The user does not need to install Avaya Workplace Client for Windows and provide the email address for service discovery.

Important:

This procedure only applies to Avaya Workplace Client for Windows.

Before you begin

Install Avaya Workplace Client for Windows.

Procedure

Modify the registry entry at HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Avaya\Avaya IX Workplace\AutoconfigPath.

If the registry entry does not exist, you must create a new entry of string value. The registry entry value must be the URL where the settings file for service discovery is stored.

For more information about configuring a registry item, see Microsoft help documentation.

Moving the settings file

About this task

Use this procedure if you need to move the settings file to a different server location. This procedure works for both new and existing users.

Before you begin

Configure endpoints to automatically check for updates by setting the SETTINGS_CHECK_INTERVAL parameter in the settings file.

Procedure

1. Configure the web server hosting the settings file to redirect incoming client HTTP requests from the old URL to the new URL.
2. **Optional** For new users, if step 1 does not work, do the following:
   a. Inform users about the new URL required for automatic configuration.
   b. Update DNS entries to point to the new file.
   c. Update your Windows registry entries with the new URL.
3. **Optional** For existing users, if step 1 does not work, add the SETTINGS_FILE_URL parameter to the existing settings file.

   This step ensures that as the existing clients pick up the settings file, the clients are migrated to the new server location.

Agent functionality configuration on mobile platforms

You must perform the following tasks to integrate the Agent functionality with Avaya Workplace Client on mobile platforms:

- For all SIP extensions, on page 1 of the Station screen, set **Type** to `J169CC` or `J179CC`.
- For all SIP extensions, configure the Agent Login, Auto In, Manual In, After Call Work, Not Ready that is AUX, Change Skill, and Call Work Code buttons.
- Add the **add-rem-sk** button for the user extension so that the user can add or remove any available skills when needed.
- Enable the **Add/Remove Agent Skills** field on the Class of Restriction page that is assigned to the station with agent ID.
- Configure the hunt groups and agent skills, and assign users to each hunt group or skill. Avaya Workplace Client then routes calls to users depending on the skill set.
- Configure the **Allow Agent to Activate Call Forward** field on the Class of Restriction page so that the user can activate call forwarding when needed.
- Configure the agent specific parameters in the settings file.

Agent settings parameters on mobile platforms

Type	Default value	Supported platforms	Description
AGENT_ENABLED			
Numeric	0	• Android • iOS	This parameter indicates whether Agent Service is enabled for the user. **Note:** You must enable Agent Service for each user on only a single device or workstation at any time. To enable Agent Service, you must enable this parameter on the client or platform on which the user handles customer calls. On the other clients

Type	Default value	Supported platforms	Description
			or platforms, you must disable this parameter. The options are: • 0: Indicates that Agent Service is disabled and unavailable for the user. • 1: Indicates that Agent Service is enabled for the user. Client Navigation: **Settings** > **Services** > **Agent Service** > **Agent Service**.
AGENT_AVAILABILITY_AUTO			
Numeric	0	• Android • iOS	This parameter indicates whether the user goes into the Auto In or Manual In work mode after the user taps Available. The options are: • 0: Indicates that the user goes into the Manual In work mode after the user taps Available. • 1: Indicates that the user goes into the Auto In work mode after the user taps Available.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
AGENT_LOGIN_ID			
String	Null	• Android • iOS	This parameter indicates the ID for the agent login. You must include a maximum of 16 characters as Avaya Workplace Client does not parse any additional characters. This parameter might be populated automatically. For more information, see *Administering Avaya Aura® Device Services*. Client Navigation: **Settings** > **Accounts** > **Agent Login** > **Agent Login ID**.
AGENT_PASSWORD			
String	Null	• Android • iOS	This parameter indicates the password for the agent login. If you enable agent login and set the agent login ID and password, the user can directly log in to UC and CC. Client Navigation: **Settings** > **Accounts** > **Agent Login** > **Password**.
LOGOUT_REASON_CODES			
String	Null	• Android • iOS	This parameter indicates the list of reason codes to log the user out.

Type	Default value	Supported platforms	Description
			The syntax for this parameter is: `SET LOGOUT_REASON_CODES "0:Label0,1:Label1,2:Label2,3:Label3.."` For example, `SET LOGOUT_REASON_CODES "0:Manual Logout,1:End Of Day,2:Out Of Office,3:Vacation"`. You need to configure the logout reason code labels on Avaya Aura® Device Services. The list of reason code labels is synchronous with the reason codes configured on Communication Manager. On Communication Manager, digits are used to indicate the reason code. You need to map the digits on Communication Manager with the specific logout reason code label. You can view the reason codes on Communication Manager using the display reason-code-names command. Client Navigation: Presence status indicator > **Agent Login** > Reason codes.
AGENT_WORK_CODE			
String	Null	• Android • iOS	This parameter indicates the list of work codes available for a user. The syntax for this parameter is: `SET`

Type	Default value	Supported platforms	Description
			`AGENT_WORK_CODE "0:Label0,1:Label1,2:Label2,3:Label3.."` For example, `SET AGENT_WORK_CODE "0:Offer Sent,1:Follow up with Call back,2:Offer Document preparation,3:Discuss Discount"`. You need to configure the work code labels on Avaya Aura® Device Services. The list of work code labels is synchronous with the work codes configured on Communication Manager. On Communication Manager, digits are used to indicate the work code. You need to map the digits on Communication Manager with the specific work code label. Client Navigation: Agent bar (●) > ⌄ > Work codes.
AUX_REASON_CODES			
String	Null	• Android • iOS	This parameter indicates the list of reason codes to change the work mode to AUX. The syntax for this parameter is: `SET AUX_REASON_CODES "0:Label0,1:Label1,2:Label2,3:Label3.."`

Type	Default value	Supported platforms	Description
			For example, `SET AUX_REASON_CODES "0:General Break,1:Coffee Break,2:Tea Break,3:Snack Break,4:Lunch code,5:Meeting"`. You need to configure the reason code labels on Avaya Aura® Device Services. The list of reason code labels is synchronous with the auxiliary reason codes configured on Communication Manager. On Communication Manager, digits are used to indicate the reason code. You need to map the digits on Communication Manager with the specific reason code label. You can view the reason codes on Communication Manager using the display reason-code-names command. Client Navigation: Agent bar (⊖) > ⌄ > Reason codes.
AGENT_SKILLS			
String	Null	• Android • iOS	This parameter indicates the list of agent skills available for a user. The syntax for this parameter is: `SET AGENT_SKILLS "1:Label1,2:Label2,3:Label3.."` For example, `SET AGENT_SKILLS "1:Painting,2:Main`

Type	Default value	Supported platforms	Description
			`tenance,3:Electronics".` You need to configure the skill labels on Avaya Aura® Device Services. The list of skill labels is synchronous with the skills configured on Communication Manager. On Communication Manager, digits are used to indicate the skills. You need to map the digits on Communication Manager with the specific skill label. Client Navigation: 🎧 > **My Skills**.
ENABLE_AUTO_ANSWER_MOBILE			
Numeric	0	Android	This parameter indicates whether Avaya Workplace Client for Android answers the incoming call automatically for the CC user. The options are: • 0: Indicates that Avaya Workplace Client for Android does not answer the incoming call automatically for the CC user. • 1: Indicates that Avaya Workplace Client for

Type	Default value	Supported platforms	Description
			Android answers the incoming call automatically for the CC user. Client Navigation: **Settings** > **Services** > **Phone Service** > **Auto-Answer Calls**.
ENABLE_LOCAL_AUTO_ANSWER			
Numeric	0	Android	This parameter indicates whether the local auto-answer is enabled on Google Chromebook. If you enable this parameter and a user receives an audio or video call, Avaya Workplace Client plays a zip tone to alert the user about the incoming call. Avaya Workplace Client then automatically answers the call as an audio-only call. **Note:** If you use Avaya Workplace Client on Google Chromebook and this parameter is enabled, Avaya Workplace Client automatically answers the incoming call even if your device is locked. The options are: • 0: Indicates that local auto-answer is disabled.

Type	Default value	Supported platforms	Description
			1: Indicates that local auto-answer is enabled. Client Navigation: Not Applicable.
ENABLE_CCELITE_OFF_HOOK_INVITE_SUPPORT			
Numeric	0	• iOS • Android	This parameter indicates whether Avaya Workplace Client sends an off-hook invitation when an agent logs in to Call Center Elite and performs one of the following actions: • Initiates an outgoing call • Initiates a call transfer • Merges two calls • Enables Call Forward All/ Busy/No Answer • Parks or unparks a call • Activates automatic callback • Activates Malicious Call Trace The options are: • 0: Indicates that Avaya Workplace

Type	Default value	Supported platforms	Description
			Client does not send an off-hook invitation. 1: Indicates that Avaya Workplace Client sends an off-hook invitation. Client Navigation: Not Applicable.

AUX and logout reason codes

Avaya Workplace Client retrieves the AUX and logout reason codes from Avaya Aura® Device Services. If Avaya Aura® Device Services is available and reason codes are available, Avaya Workplace Client displays these reason codes.

Communication Manager feature buttons include the backup list of AUX reason codes. If reason codes are unavailable on Avaya Aura® Device Services, Avaya Workplace Client checks if you have configured the feature buttons with AUX reason codes on Communication Manager. If Avaya Workplace Client finds the feature buttons in the user's station, Avaya Workplace Client displays these AUX reason codes.

Configuring an agent hunt group for Avaya Workplace Client

About this task

Configure agent hunt groups so that Avaya Workplace Client can route calls to users. You can add multiple hunt groups.

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Element Cut-Through**.
2. On the Element Cut-Through page, click a Communication Manager instance.
3. In the **Command** field, type `add hunt-group next` or `add hunt-group n`.
   n is the hunt group number.
4. Click **Send**.
5. Click **Next Page**.
6. On page 1 of the Hunt Group screen, do the following:
   a. In the **Group Number** field, enter the number of the hunt group.
   b. In the **Group Name** field, enter the name of the hunt group.
   c. In the **Group Extension** field, enter the extension number for this hunt group.
   d. In the **ACD** field, type `y`.
   e. In the **Queue** field, type `y`.
   f. In the **Vector** field, type `y`.
7. Click **Next Page**.
8. On page 2 of the Hunt Group screen, do the following:
   a. In the **Skill** field, type `y`.
   b. In the **Timed ACW Interval** field, type the number of seconds for which the Avaya Workplace Client users remain in the ACW state after completing a call.
9. Click **Next Page**.
10. On page 3 of the Hunt Group screen, do the following:
    a. In the **Redirect on No Answer (rings)** field, type the number of rings for which Avaya Workplace Client must wait before redirecting the call.
    b. In the **Redirect on No Answer to VDN** field, type the required value.
    c. In the **Redirect on IP/OPTIM Failure to VDN** field, type the duration for which Communication Manager must wait for a SIP 18x provisional response before canceling the call for Avaya Workplace Client.

11. To apply the configuration changes, click **Enter**.

Configuring the agent login state on mobile platforms

About this task

Use this procedure to configure the agent login state for Avaya Workplace Client.

If you set the value in the **Work Mode On Login** field to:

- Auto In or Manual In, after the user logs out and logs in to Avaya Workplace Client, the agent state changes to Available irrespective of the agent state before exit.
- AUX, after the user logs out and logs in to Avaya Workplace Client, the agent state changes to AUX irrespective of the agent state before exit.

If the user logs in and sets any agent state, on forceful shutdown and restart of Avaya Workplace Client, the user logs in successfully with the same agent state before forceful shutdown.

If the user logs in and sets any agent state when Push Notification:

- Is active, on forceful shutdown and restart of Avaya Workplace Client, the user logs in successfully with the agent state that you configure in the **Work Mode On Login** field.
- Is inactive, on forceful shutdown and restart of Avaya Workplace Client, the user logs in successfully with the same agent state before forceful shutdown.

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Element Cut-Through**.
2. On the Element Cut-Through page, click a Communication Manager instance.
3. In the **Command** field, type `change system-parameters features`.
4. Click **Send**.
5. Click **Next Page** until you reach page 11.
6. In the **Work Mode On Login** field, set the agent login state.
   You can set Auto In, Manual In, or AUX.

7. To apply the configuration changes, click **Enter**.

Call redirection

If the user does not answer an agent call and if you have configured Redirect on no Answer (RONA), then Avaya Workplace Client redirects the call depending on the configuration.

If Avaya Workplace Client loses network connectivity and if you have configured Redirect On OPTIM Failure (ROOF), then Avaya Workplace Client redirects the call depending on the configuration.

Avaya Workplace Client redirects the call after specified rings or connectivity loss to one of the following based on your RONA and ROOF configuration:

- Configured Vector Directory Number (VDN)
- Other available agents in the hunt group
- Coverage path

  Avaya Workplace Client redirects the Direct Agent Calls (DAC) calls to voice mail but does not redirect the Automatic Call Distribution (ACD) calls to voice mail.

If Avaya Workplace Client invokes RONA or regains connectivity, your current agent state changes to Not Ready and you do not receive any further agent calls.

Button Module and agent functionality configuration on Windows platform

This chapter describes information to configure Button Module on Windows platform.

You must configure the ENABLE_BUTTON_MODULE parameter with value 1 to enable Button Module. You can then view the Unified Communications feature buttons depending on your configuration.

To view the Contact Center feature buttons on Button Module with Avaya Workplace Client on Windows, you must perform the following tasks:

- For all SIP extensions, on page 1 of the Station screen, set **Type** to `J169CC` or `J179CC`.
- For all SIP extensions, configure the Agent Login, Auto In, Manual In, After Call Work, Not Ready that is AUX, Change Skill, and Call Work Code buttons.
- Add the **add-rem-sk** button for the user extension so that the user can add or remove any available skills when needed.
- Enable the **Add/Remove Agent Skills** field on the Class of Restriction page that is assigned to the station with agent ID.
- Configure the hunt groups and agent skills, and assign users to each hunt group or skill. Avaya Workplace Client then routes calls to users depending on the skill set.
- Configure the **Allow Agent to Activate Call Forward** field on the Class of Restriction page so that the user can activate call forwarding when needed.
- Configure the agent specific parameters in the settings file.

Button Module

Currently, Avaya Workplace Client for Windows supports different Communication Manager features as feature buttons in Feature Manager.

Hard endpoints, such as 96x1 SIP and J100 Series SIP phones, support the expansion module as separate hardware. This expansion module has all the supported features configured on System Manager for SIP extensions.

To support the configuration of multiple feature buttons and its functionality, Avaya Workplace Client for Windows now supports Button Module, which is similar to the expansion module.

By default, Avaya Workplace Client for Windows does not display Button Module but displays Feature Manager. To enable Button Module, you must set the ENABLE_BUTTON_MODULE parameter to 1.

Currently, Avaya Workplace Client for Windows does not support all feature buttons.

Avaya Workplace Client for Windows supports the following Unified Communications (UC) feature buttons:

- Autodial: To dial a preconfigured number.
- Automatic Callback: To activate the feature when you call a busy or an unanswered internal telephone. Communication Manager monitors the called party. When the called party is available to receive the call, Communication Manager automatically initiates Automatic Callback. You receive priority ringing. After you answer the call, the called party receives the call.
- Automatic Message Waiting: To monitor the voice mailbox of another user.
  If a new message arrives in the voice mailbox, you receive a visual notification.
- AUDIX One-Step Recording: To record telephone conversations for point-to-point calls and Communication Manager adhoc conference calls.
- Block Calling Party Name (CPN): To block the calling party information and replace it with a hard-coded text.
- Bridge Line Appearance: To give single-line and multiappearance telephones the appearance of another telephone number.
- Busy Indicator: To make a speed dial call to the configured extension number. It also provides multiappearance telephone users and attendants a visual indicator of the busy or idle status of an extension number.
- Call Park: To park an active call on Communication Manager.
- Call Pickup: To answer calls for another pickup group member.
- Call Redirection features for other extensions: To activate the following feature buttons for other extensions:
  - Send All Calls
  - Call Forward
  - Call Forward Busy/No Answer
  - Enhanced Call Forward

  Note:

  You can continue to activate Call Redirection features for your extension from the Incoming Call Features screen.
- Call Unpark: To retrieve a parked call from the same or another extension.
- Directed Call Pickup: To specify which telephone a user wants to answer.
- Exclusion: To maintain the privacy of telephonic conversations and ensure that unwanted parties cannot join the call.
- Extended Call Pickup: To answer an incoming call which is ringing in another pickup group.
  User must enter the extended pickup group number as per your configuration on Communication Manager.
- Hunt Group Busy: To allow or avoid incoming calls on your extension from a specific hunt group.
- Limit Number of Concurrent Calls (LNCC): To restrict the number of incoming calls to one call at a time.
- Malicious Call Trace: To identify malicious communication on calls.
- No-Hold Conference: To add a new participant into an active call without holding the active call. You can start this Adhoc audio conference call only by using Communication Manager.
- Service Observe: To listen in and possibly talk on calls to extensions, attendants, agents, or VDNs.
- Team Button: To monitor other extensions that are part of a team of extensions.

You must be on an active call to use some of these feature buttons. You can use the feature buttons in the My Computer mode and the Other Phone mode.

Agent functionality from Button Module

Contact Center agent features on Windows platform are available through Button Module and require a feature license. You can also use some of the agent features from the Agent bar even if Button Module is disabled but you have a valid WebLM license. The Contact Center agent features in Avaya Workplace Client for Windows are available with a feature license that is not included with the Core or Power Suite license or subscription.

You must load the feature license in WebLM for the total concurrent quantity of agents that are going to use the feature.

To enable the agent functionality, you must set the AGENT_ENABLED parameter to 1. If the user attempts to use the agent functionality, Avaya Workplace Client for Windows checks if licenses are available on the WebLM server. You must configure the LICENSE_SERVER_URL parameter with the URL of the WebLM server.

Avaya Workplace Client for Windows supports the following Contact Center (CC) agent feature buttons:

- Agent Login and Agent Logout: Agent Login and Agent Logout are the same buttons. After you log in as an agent, the Agent Login button changes to Agent Logout. To use the CC agent capabilities with Avaya Workplace Client, you must log in as an agent.
- Auto In and Manual In: To change the availability state from After Call Work (ACW) or Not Ready to Available.
- After Call Work: To change the availability state to ACW.
- Aux Work: To change the availability state to Not Ready.
- Queue Status: To view the queue statistics for the associated skill.
- Service Observe: To listen in and possibly talk on calls to extensions, attendants, agents, or VDNs.
- Skill Set: To update your skill set based on your acquired skills.
- Supervisor Assist: To speed dial your supervisor, and to easily add or transfer a held call to your supervisor.
- User To User Information: To view the Adjunct/Switch Application Interface User-to-User Information (ASAI UUI) data that Communication Manager provides about a specific Vector Directory Number (VDN) call or direct agent call.
- Logout Override: To override the logout configuration when you want to extend your working hours.
- VuStats: To view the statistics for agents, skills, VDNs, and trunk groups.

You can enable greetings for the user using the AGTGREETINGSTAT parameter. Users can then select or add a new greeting for incoming calls using Avaya Workplace Client for Windows. Avaya Workplace Client supports greetings for Contact Center and Unified Communications users.

You can configure screen pops for incoming and outgoing calls for Contact Center and Unified Communications users using the SCREEN_POP_LIST parameter. A screen pop is a window or dialog box that separately appears on the desktop. The screen pop displays information for a call simultaneously sent to that agent's telephone. Screen pop is an essential feature for agents as they need to perform work on certain web pages, sites, or specific accessible URLs. Screen pops are also increasingly used by hospital nurses and hospitality employees.

Note:

You must enable Agent Service for each user on only a single device or workstation at any time. To enable Agent Service, you must enable the AGENT_ENABLED parameter on the client or platform on which the user handles customer calls. For example, if the user is using Avaya Workplace Client for Windows, you must configure

```
SET AGENT_ENABLED 1
```

on Windows. Also, on mobile platforms, you must configure

```
SET AGENT_ENABLED 0
```

.

Avaya Workplace Client settings in Avaya Aura Communication Manager for UC feature buttons

Use the Avaya Aura® System Manager administration interface to change the Avaya Aura® Communication Manager settings.

For more information about the individual settings, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Task or feature	Configuration
Autodial	Configure the Autodial button for the user with the appropriate extension number.
Automatic Callback	Do the following: • Assign an FAC for Automatic Callback. • Enable **Automatic Callback With Called Party Queuing**. • Set the no-answer timeout interval for Automatic Callback. • Assign a feature button for Automatic Callback. • Set the Queue length for Ringback Queuing.

Task or feature	Configuration
	• Enable CCBS.
Automatic Message Waiting	Configure the **aut-msg-wt** button for the user with an appropriate extension number. The user can then monitor the voice mailbox of another user.
AUDIX One-Step Recording	Do the following: • Assign AUDIX One-Step Recording parameters. • Translate AUDIX One-Step Recording telephone feature buttons and labels. • Assign the AUDIX One-Step Recording feature button. • Change the zip tone for AUDIX One-Step recording.
Block Calling Party Name	Do the following: • Configure the **cpn-blk** and **cpn-unblk** buttons for the user. • To hide the display of calling or called party numbers and administered names on internal calls, on the Class of Restriction screen, set the **Mask CPN/ NAME for Internal Calls** field to y. • To override the Mask CLI/Station Name for internal calls capability, on the Class of Restriction screen, set the **Masking CPN/Name Override** field to y.
Busy Indicator	Configure the Busy Indicator button for the user with the appropriate extension number.
Call Park	If a user parks a call and does not disconnect after hearing the confirmation tone, the user stays connected to other parties on the call. To automatically disconnect the call, set the **Drop Parking User From The Call After Timeout** field on the Feature-Related System Parameters screen to y. The system then drops the parked call after the

Task or feature	Configuration
	default time limit of 5 seconds if the user does not disconnect the call. You cannot change the default time limit. On the Station screen, to add the Call Park button for a SIP station, set the value in the **Button Assignments** area.
Call Pickup	Do the following: • Ensure that the no-ring parameter is disabled. • To enable call pickup alerting, on the Feature-Related System Parameters screen, set the **Call Pickup Alerting** field to `y`. • To enable the enhanced call pickup alerting capability, on the Feature-Related System Parameters screen, set the **Enhanced Call Pickup Alerting** field to `y`. The system displays the **Enhanced Call Pickup Delay Timer (sec.) Display** and **Audible Notification** fields only if you set the Enhanced Call Pickup Alerting field to y. To administer the alerting options for a button, set the button assignment by using the `change station n` command. • To enable audible indication of incoming calls to a member of the call pickup group, on page 2 of the Class of Restriction screen, set the **Block Enhanced Call Pickup Alerting** field to `n`. • On the Station screen, to add the Call Pickup button for a SIP station, set the value in the **Button Assignments** area.
Call Redirection features for other extensions	Configure the following Call Redirection features for other extensions:

Task or feature	Configuration
	• Call Forward • Call Forward Busy /No Answer • Send All Calls • Enhanced Call Forward
Call Unpark	On the Station screen, to add the Call Unpark button for a SIP station, set the value in the **Button Assignments** area.
Directed Call Pickup	Do the following: • Configure the **dir-pkup** button for the user. • To enable directed call pickup, on the Feature-Related System Parameters screen, set the **Directed Call Pickup?** field to *y*.
Exclusion	Do the following: • On the Feature-Related System Parameters screen, set the value of the **Automatic Exclusion by COS** field to `y`. • For automatic exclusion, on the Class of Service screen, set the value of the **Automatic Exclusion** field of the COS group to `y`. For non-automatic exclusion, set the value to `n`. • On the Station screen, to add the Exclusion button for a SIP station, set the value in the **Button Assignments** area.
Extended Call Pickup	Do the following: • To enable simple extended pickup groups, on the Feature-Related System Parameters screen, in the **Extended Group Call Pickup** field, type `simple`.

Task or feature	Configuration
	• To enable flexible extended pickup groups, on the Feature-Related System Parameters screen, in the **Extended Group Call Pickup** field, type `flexible`. ✱ **Note:** You cannot have simple and flexible extended pickup groups on your system simultaneously. • On the Station screen, to add the Call Pickup Extended button for a SIP station, configure the **ext-pkup** button for the user.
Hunt Group Busy	• On the station screen, add a Hunt Group for a user in the Group Membership area. Users receive calls for a Hunt Group when they are members of that Hunt Group. • Configure the **hntpos-bsy** button for the user with a group number of the Hunt Group that you add.
Limit Number of Concurrent Calls (LNCC)	Do the following: • Configure the **limit-call** button for the user. • Assign an FAC for LNCC. • Activate the LNCC feature. • Configure the coverage path for LNCC. • View the status of the LNCC feature.
No-Hold Conference	Do the following: • Configure the **no-hld-cnf** button for the user. • On the Feature-Related System Parameters screen, type the number of seconds in the **No Hold Conference Timeout** field. If the called user does not

Task or feature	Configuration
	answer the call within the specified time, the system deactivates the No-Hold Conference capability for the call.
Malicious Call Trace (MCT)	Configure the **mct-act** button. When a user activates the MCT button, the system notifies the potential MCT controllers. A potential MCT controller is a station or an attendant that has an **mct-contr** button. On the Station screen, to add the MCT buttons for a SIP station, set the values in the **Button Assignments** area.
Service Observe	Do the following: • Configure the **sip-sobsrv** button for the user. • Configure the ListenOnly parameter. If you set the value to: • Y, the service observer user can only listen. • N, the service observer user can have a 2-way speech path with the user and the caller.
Team Button	Do the following: • Adding the team button to the monitoring station. • Administering the team button functionality. • Administering the team button override functionality. • Viewing the system capacity for team button.
Send-nn	Do the following: • On the Station screen, to add the send-nn button for a SIP station, set the value in the **Button Assignments** area. In the **Ext** field, type the extension of a station,

Task or feature	Configuration
	or a hunt group, or a Vector Directory Number (VDN). In the **Md** field, type P Variant or T Variant as required. • Configure the **send-nn** button for the user to alter the displayed phone number of the calling party.

Avaya Workplace Client settings in Avaya Aura Communication Manager for CC feature buttons

Use the Avaya Aura® System Manager administration interface to change the Avaya Aura® Communication Manager settings.

For more information about the individual settings, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Task or feature	Configuration
Adjunct/Switch Application Interface User-to-User Information (ASAI UUI)	Do the following: • Configure the **uui-info** button for the user. • In the Class of Restriction (COR) number that you want to use, set the **Station-Button Display of UUI IE Data?** COR parameter to Yes.
Agent Login	Do the following: • Configure the **agnt-login** button for the user. • On page 14 of the Feature-Related System Parameters screen on Communication Manager, configure one of the following values in the **Logout Reason Code Type** field:

Task or feature	Configuration
	• **None**: Avaya Workplace Client does not display an option to enter the logout reason code. • **Requested**: Avaya Workplace Client displays an option to enter the reason code when logging out. If the user enters an invalid code or does not enter a code, Communication Manager logs out the user with the default code 0 that you configure on Communication Manager. • **Forced**: Avaya Workplace Client displays an option to enter the reason code when logging out. The user must enter the logout reason code. If the user enters an invalid code or does not enter a code, Communication Manager does not log out the user.
After Call Work (ACW)	Configure the **after-call** button for the user. Also, configure the call work codes.
Auto In	Configure the **auto-in** button for the user.
AUX, that is, Not Ready	Do the following: • Configure the **aux-work** button for the user. • Configure the auxiliary work reason codes. This is optional. If you configure the auxiliary work reason codes, Avaya Workplace Client does not display an option to enter the auxiliary work reason code when the user changes the work mode to AUX. • On page 14 of the Feature-Related System Parameters screen on Communication Manager, configure one

Task or feature	Configuration
	of the following values in the **Aux Work Reason Code Type** field: • **None**: Avaya Workplace Client does not display an option to enter the auxiliary work reason code. • **Requested**: Avaya Workplace Client displays an option to enter the auxiliary work reason code when the user changes the work mode to AUX. If the user enters an invalid code or does not enter a code, Communication Manager changes the work mode to AUX with the default code 0 that you configure on Communication Manager. • **Forced**: Avaya Workplace Client displays an option to enter the auxiliary work reason code when the user changes the work mode to AUX. The user must enter the auxiliary work reason code. If the user enters an invalid code or does not enter a code, Communication Manager does not change the work mode to AUX, and the user remains in the current work mode. • Configure one of the following values in the **Two-Digit Aux Work Reason Codes** field: • **Yes**: The user must enter a single-digit or double-digit auxiliary work reason code. • **No**: The user must enter a single-digit auxiliary work reason code.
Call Work Code	Configure the **work-code** button for the user.

Task or feature	Configuration
Logout Override	Do the following: • Configure the Logout Override feature for the user. • Configure the **logout-ovr** button for the user. • To automatically log out the user, configure the time in the **Forced Agent Logout Time** field.
Manual In	Configure the **manual-in** button for the user.
Queue Status	Do the following: • Configure the **q-calls** button for the user with the appropriate skill ID. You can configure multiple **q-calls** buttons for the user. • On the Skill Hunt Group page, configure the **Calls Warning Threshold** and **Time Warning Threshold** fields. This is optional.
Service Observe	Do the following: • Configure the **sip-sobsrv** button for the user. • Configure the ListenOnly parameter. If you set the value to: • Y, the service observer user can only listen. • N, the service observer user can have a 2-way speech path with the agent and the caller. • Configure the Coach parameter. If you set the value to Y, the service observer user can have a 2-way speech path only with the agent.
Skills	• Configure multiple skills for users.

Task or feature	Configuration
	• Configure the **add-rem-sk** button for the user extension to add or remove any available skills. • Enable the **Add/Remove Agent Skills** field on the Class of Restriction page assigned to the station with agent ID.
Supervisor Assist	Do the following: • Configure the **assist** button for the SIP extension with or without skill (hunt group). • Configure the supervisor extension for the skill (hunt group).
VuStats	Configure the **vu-display** button for the user. ✱ **Note:** Avaya Workplace Client for Windows displays a maximum of 18 **vu-display** buttons.

Button Module parameter on Windows platform

Type	Default value	Supported platforms	Description
ENABLE_BUTTON_MODULE			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client displays Button Module. The options are: • 0: Indicates that Avaya Workplace Client does not display Button

Type	Default value	Supported platforms	Description
			Module but displays Feature Manager. • 1: Indicates that Avaya Workplace Client displays Button Module but does not display Feature Manager. Users can then view the features configured for their extension on System Manager and any customizations done on Button Module of their J1xx phone. Also, users can perform all supported customizations such as edit label, add contacts to Button Module. Client Navigation: Not Applicable

Agent settings parameters on Windows platform

Type	Default value	Supported platforms	Description
AGENT_ENABLED			
Numeric	0	Windows	This parameter indicates whether Agent Service is enabled for the user. **Note:** You must enable Agent Service for each user on only a single device or workstation at any time. To enable Agent Service, you must enable this parameter on the client or platform on which the user handles customer calls. On the other clients or platforms, you must disable this parameter. The options are: • 0: Indicates that Agent Service is disabled and unavailable for the user. • 1: Indicates that Agent Service is enabled for the user. Client Navigation: Not Applicable.
LICENSE_SERVER_URL			
String	Null	Windows	This parameter indicates the URL of the WebLM server. If you set AGENT_ENABLED = 1 and the user attempts to use the agent functionality, Avaya Workplace Client checks

Type	Default value	Supported platforms	Description
			if licenses are available on the WebLM server. If Avaya Workplace Client finds that a license is: • Available or expired within a grace period of 30 days, the user can use the agent functionality. • Unavailable or expired and the grace period is over, the user cannot use the agent functionality. Client Navigation: Not Applicable.
AGENT_LOGIN_ID			
String	Null	Windows	This parameter indicates the ID for the agent login. You must include a maximum of 16 characters as Avaya Workplace Client does not parse any additional characters. This parameter might be populated automatically. For more information, see *Administering Avaya Aura® Device Services*. Client Navigation: Not Applicable.

Type	Default value	Supported platforms	Description
AGENT_PASSWORD			
String	Null	Windows	This parameter indicates the password for the agent login. If you enable agent login and set the agent login ID and password, the user can directly log in to Unified Communications (UC) and Contact Center (CC). Client Navigation: Not Applicable.
LOGOUT_REASON_CODES			
String	Null	Windows	This parameter indicates the list of reason codes to log the user out. The syntax for this parameter is: `SET LOGOUT_REASON_CODES "0:Label0,1:Label1,2:Label2,3:Label3.."` For example, `SET LOGOUT_REASON_CODES "0:Manual Logout,1:End Of Day,2:Out Of Office,3:Vacation"`. You need to configure the logout reason code labels on Avaya Aura® Device Services. The list of reason code labels is synchronous with the reason codes configured on Communication Manager. On Communication Manager, digits are used to indicate the reason code. You

Type	Default value	Supported platforms	Description
			need to map the digits on Communication Manager with the specific logout reason code label. You can view the reason codes on Communication Manager using the display reason-code-names command. Client Navigation: Presence status indicator > **Agent Login** > Reason codes.
AGENT_WORK_CODE			
String	Null	Windows	This parameter indicates the list of work codes available for a user. The syntax for this parameter is: `SET AGENT_WORK_CODE "0:Label0,1:Label1,2:Label2,3:Label3.."` For example, `SET AGENT_WORK_CODE "0:Offer Sent,1:Follow up with Call back,2:Offer Document preparation,3:Discuss Discount"`. You need to configure the work code labels on Avaya Aura® Device Services. The list of work code labels is synchronous with the work codes configured on Communication Manager. On Communication Manager, digits are used to indicate the work code. You need to map the

Type	Default value	Supported platforms	Description
			digits on Communication Manager with the specific work code label. Client Navigation: Agent bar (ⓘ) > ⌄ > Work codes.
AUX_REASON_CODES			
String	Null	Windows	This parameter indicates the list of reason codes to change the work mode to AUX. The syntax for this parameter is: `SET AUX_REASON_CODES "0:Label0,1:Label1,2:Label2,3:Label3.."` For example, `SET AUX_REASON_CODES "0:General Break,1:Coffee Break,2:Tea Break,3:Snack Break,4:Lunch code,5:Meeting"`. You need to configure the reason code labels on Avaya Aura® Device Services. The list of reason code labels is synchronous with the auxiliary reason codes configured on Communication Manager. On Communication Manager, digits are used to indicate the reason code. You need to map the digits on Communication Manager with the specific reason code label. You can view the reason codes on Communication Manager

Type	Default value	Supported platforms	Description
			using the display reason-code-names command. Client Navigation: Agent bar (⊖) > ⌄ > Reason codes.
AGTGREETINGSTAT			
Numeric	0	Windows	This parameter indicates if greetings are enabled for the user. The options are: • 0: Indicates that greetings are disabled for the user. • 1: Indicates that agent greetings are enabled for the user. • 2: Indicates that UC greetings are enabled for the user. Client Navigation: Not Applicable.
AGTGREETLOGOUTDEL			
Numeric	0	Windows	This parameter indicates whether the local greetings are deleted after the agent logs out from Avaya Workplace Client. The options are: • 0: Indicates that the local greetings are

Type	Default value	Supported platforms	Description
			not deleted after the agent logs out. • 1: Indicates that the local greetings are deleted every time after the agent logs out. Client Navigation: Not Applicable.
BRURI			
String	Null	Windows	This parameter indicates the HTTP or HTTPS server from which Avaya Workplace Client downloads the stored recordings. The HTTP or HTTPS server also stores the modified recordings. For example, `SET BRURI "https://148.147.200.211/sites/"`. Client Navigation: Not Applicable.
FORCE_HTTP_AUTH_USERNAME			
String	Null	Windows	This parameter indicates the user name to authenticate to the HTTP or HTTPS server. This parameter is dependent on the BRURI parameter.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.
FORCE_HTTP_AUTH_PASSWORD			
String	Null	Windows	This parameter indicates the password to authenticate to the HTTP or HTTPS server. This parameter is dependent on the BRURI parameter. Client Navigation: Not Applicable.
AGENT_SKILLS			
String	Null	Windows	This parameter indicates the list of agent skills available for a user. The syntax for this parameter is: `SET AGENT_SKILLS "1:Label1,2:Label2,3:Label3.."` For example, `SET AGENT_SKILLS "1:Painting,2:Maintenance,3:Electronics"`. You need to configure the skill labels on Avaya Aura® Device Services. The list of skill labels is synchronous with the skills configured on Communication Manager. On Communication Manager, digits are used to indicate the skills. Map the digits on Communication Manager

Type	Default value	Supported platforms	Description
			with the specific skill label. Client Navigation: **Settings** > **User Preferences** > **Agent Service** > **My Skills**.
Q_STATS_DEFAULTREFRESHTIMER			
Numeric	0	Windows	This parameter indicates the refresh interval for queue statistics. The default value indicates that refresh is disabled. The range is from 0 to 3600 seconds. Client Navigation: Not Applicable.
UUIDISPLAYTIME			
Numeric	10	Windows	This parameter indicates the time in seconds for which Avaya Workplace Client displays the User to User Information (UUI) data. The range is from 5 to 60 seconds. Client Navigation: Not Applicable.
ENABLE_LOCAL_AUTO_ANSWER			
Numeric	0	Windows	This parameter indicates whether local auto answer is enabled. If you enable this parameter and a user receives an audio or video call, Avaya

Type	Default value	Supported platforms	Description
			Workplace Client plays a zip tone to alert the user about the incoming call. Avaya Workplace Client then automatically answers the call as an audio-only call. The options are: • 0: Indicates that local auto answer is disabled. 1: Indicates that local auto answer is enabled. Client Navigation: Not Applicable.
ENABLE_CCELITE_OFF_HOOK_INVITE_SUPPORT			
Numeric	0	Windows	This parameter indicates whether Avaya Workplace Client sends an off-hook invitation when an agent logs in to Call Center Elite and performs one of the following actions: • Initiates an outgoing call • Initiates a call transfer • Merges two calls • Enables Call Forward All/Busy/No Answer • Parks or unparks a call

Type	Default value	Supported platforms	Description
			• Activates automatic callback • Activates Malicious Call Trace The options are: • 0: Indicates that Avaya Workplace Client does not send an off-hook invitation. 1: Indicates that Avaya Workplace Client sends an off-hook invitation. Client Navigation: Not Applicable.

Greetings

Greeting types include:

- Automatic Number Identification (ANI): ANI routes a call based on the caller's identity and the originating line number.
- Vector Directory Number (VDN): Call vectors are commands that route incoming calls and determine how the contact center processes these calls. VDNs distribute calls depending on factors such as the number the caller dials, the number the caller calls from, the number of calls in the queue, and the time of the call.
- Prompted Digits: Avaya Workplace Client plays this greeting when the caller enters the prompted digits during a VDN call. If the VDN greeting matches the VDN name, Avaya Workplace Client does not play the Prompted Digit greeting, as the VDN greeting has a higher priority.

- Auto Answer: Avaya Workplace Client plays this greeting automatically when an incoming call does not match the VDN or ANI greeting type criteria.
- Manual: Avaya Workplace Client plays this greeting when you click Play Greeting (▶) during the active incoming or outgoing call. If there are multiple manual greetings, click the greeting you want Avaya Workplace Client to play.

Avaya Workplace Client compares greeting types using the following priorities:

1. VDN
2. ANI
3. Prompted Digits
4. Auto Answer

Greeting server

The Greetings server is the HTTP or HTTPS server where Avaya Workplace Client saves recordings. To save the recording on the server, you must set the BRURI parameter.

For example, `SET BRURI "https://148.147.200.211/sites/john"`

Where,

- `148.147.200.211` is the server IP address.
- `sites` is the folder on the server.
- `john` is the name of the SIP account.

The name of the configuration file is stored in the AgentId_CCdata.txt format. For example, 1100036_CCdata.txt, where 1100036 is the agent ID.

The TXT file includes information such as the greeting name, WAVE file name, greeting type, and recording duration. For example:

```
GREETINGLBL001=alpha
GREETINGFILE001=1100036_1.wav
GREETINGTYPE001=0.000000
GREETINGDUR001=0:15
```

Where,

- `GREETINGLBL001` displays the greeting name.
- `GREETINGFILE001` displays the name of the WAVE file on the server.
- `GREETINGTYPE001` displays the greeting type.
- `GREETINGDUR001` displays the duration of the recording.

The information displayed in the greeting type is in the `N.000000` format, where `N` is the type of greeting from the following options:

- 0: Manual
- 1: Auto Answer
- 2: Vector Directory Number (VDN)
- 3: Automatic Number Identification (ANI)
- 4: Prompted Digits

The recorded file name of the greeting is stored on the server in the UCuserextension_numberofgreeting.wav format. Recordings are saved in the Waveform Audio File format.

For example, 1100036_3.wav

Where,

- 1100036 is the user extension.
- 3 is the number of the recording saved by that user.

Configuring an agent hunt group for Avaya Workplace Client

About this task

Configure agent hunt groups so that Avaya Workplace Client can route calls to users. You can add multiple hunt groups.

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Element Cut-Through**.
2. On the Element Cut-Through page, click a Communication Manager instance.
3. In the **Command** field, type `add hunt-group next` or `add hunt-group n`.
   n is the hunt group number.
4. Click **Send**.
5. Click **Next Page**.
6. On page 1 of the Hunt Group screen, do the following:
   a. In the **Group Number** field, enter the number of the hunt group.
   b. In the **Group Name** field, enter the name of the hunt group.
   c. In the **Group Extension** field, enter the extension number for this hunt group.
   d. In the **ACD** field, type `y`.
   e. In the **Queue** field, type `y`.
   f. In the **Vector** field, type `y`.
7. Click **Next Page**.
8. On page 2 of the Hunt Group screen, do the following:
   a. In the **Skill** field, type `y`.
   b. In the **Timed ACW Interval** field, type the number of seconds for which the Avaya Workplace Client users remain in the ACW state after completing a call.
9. Click **Next Page**.
10. On page 3 of the Hunt Group screen, do the following:
    a. In the **Redirect on No Answer (rings)** field, type the number of rings for which Avaya Workplace Client must wait before redirecting the call.
    b. In the **Redirect on No Answer to VDN** field, type the required value.
    c. In the **Redirect on IP/OPTIM Failure to VDN** field, type the duration for which Communication Manager must wait for a SIP 18x provisional response before canceling the call for Avaya Workplace Client.

11. To apply the configuration changes, click **Enter**.

Configuring the agent login state

About this task

Use this procedure to configure the agent login state for Avaya Workplace Client.

If you set the value in the **Work Mode On Login** field to:

- Auto In or Manual In, after the user logs out and logs in to Avaya Workplace Client, the agent login state changes to Available irrespective of the agent login state before exit.
- AUX, after the user logs out and logs in to Avaya Workplace Client, the agent login state changes to AUX irrespective of the agent login state before exit.

If the user logs in and sets any agent login state, on forceful shutdown and restart of Avaya Workplace Client, the user logs in successfully with the same agent login state before forceful shutdown.

Procedure

1. On the System Manager web console, in **Elements**, click **Communication Manager** > **Element Cut-Through**.
2. On the Element Cut-Through page, click a Communication Manager instance.
3. In the **Command** field, type `change system-parameters features`.
4. Click **Send**.
5. Click **Next Page** until you reach page 11.
6. In the **Work Mode On Login** field, set the agent login state.
   You can set Auto In, Manual In, or AUX.

7. To apply the configuration changes, click **Enter**.

Screen pop

Screen pop

In Call Centers that integrate a telephone system and an agent's desktop, a screen pop is a window or dialog box that separately opens on the desktop. The screen pop displays information for a call simultaneously sent to that agent's telephone. Screen pop is an essential feature for agents as they must perform work on certain web pages, sites, or accessible URLs. Hospital nurses and hospitality employees increasingly use screen pops

With Avaya Workplace Client for Windows, you can configure screen pops for incoming and outgoing calls for Contact Center and Unified Communications users.

You can configure a maximum of 99 screen pop rules. When Avaya Workplace Client for Windows triggers a rule, a screen pop appears and a URL opens in an internal or external browser. The internal browser requires the WebView2 Runtime component on the user's machine. If the user does not install this component, any requests to display a web page in the internal browser result in the page URL being displayed in the external browser instead.

To create configuration values, use the Avaya Screen Pop Configurator tool at https://downloads.avaya.com/css/P8/documents/101075011. For automatic configuration, specify the configuration value with the SCREEN_POP_LIST parameter in the settings file or in Avaya Aura® Device Services.

You can also manually configure the screen pop rules in the following format, which you must specify with the SCREEN_POP_LIST parameter in the settings file:

```
"param1=val1,param2=val2;param12=val12,param22=val22" Parameters
                of the one ScreenPop are divided by "," ScreenPop objects divide
d by ";" List of the
                parameters (* - required not-empty parameters): "name" - default
: "New Rule"
                [string] "url" - (*) [string] "params" - default: "" [string] "t
riggerOnlyForVDN" -
                default: false [bool] "vdn" - default: "" (* if triggerOnlyForVD
N == true) [string]
                "delay" - default: 1000 (* if trigger == "INCOMINGBLAANSWERED" o
r trigger ==
                "INCOMINGBLARELEASED") [bool] "type" - default: "EXTERNALBROWSER
" [string from list:
                "APPLICATION","INTERNALBROWSER","EXTERNALBROWSER"] "trigger" - d
```

```
efault:
                 "INCOMINGRINGING" [string from list:
                 "INCOMINGRINGING","INCOMINGANSWERED","INCOMINGMISSED","INCOMINGR
ELEASED","OUTGOINGESTABLISHED","OUTGOINGRELEASED","INCOMINGBLAANSWERED","INCOMIN
GBLARELEASED"]
```

Where, you can use the following:

- `name`
  element to specify the name for the screen pop.
- `url`
  element to specify the URL.
- `params`
  element to specify the following additional attributes to get more information about the call:
  - <n> to pass the name of the other party on the call.
  - <m> to pass the telephone number of the other party on the call.
  - <p> to pass the digits (prompted digits) the caller selects when dialing VDN.
  - <v> to pass the VDN name through which the call connects.
  - <u> to pass User-to-User-Information that Communication Manager collects from a centralized application.
  - <s> to pass the time when the user or agent accepts the call.
  - <e> to pass the time when the user or agent ends the call.
  - <d> to pass the current date when the agent receives the call.
  - <a> to pass the current agent ID.
  - <i> to pass the current station ID.
  - <ucid> to pass the unique call ID.
  - <vdntime> to pass the duration the call was on VDN.
  - <asai> to pass the associated ASAI.
- `triggerOnlyForVDN`
  element to specify if you want to trigger the screen pop only when an ACD call arrives. The options are 0 and 1.
- `vdn`
  element to specify the VDN number only when you enable the
  `triggerOnlyForVDN`
  parameter.
- `type`
  element to specify whether to open an application or a web URL in an external or internal browser. The options are the following:
  - APPLICATION
  - INTERNALBROWSER
  - EXTERNALBROWSER
- `trigger`

  element to specify when Avaya Workplace Client must trigger the screen pop. The options are the following:
    - INCOMINGRINGING: To open the screen pop when the phone rings.
    - INCOMINGANSWERED: To open the screen pop when a user answers the call.
    - INCOMINGMISSED: To open the screen pop when the call appearance from an incoming call disappears after no response and the caller hangs up.
    - INCOMINGRELEASED: To open the screen pop when a user or customer drops or disconnects an incoming call.
    - INCOMINGBLAANSWERED: To open the screen pop when a user answers the BLA call.
    - INCOMINGBLARELEASED: To open the screen pop when a user or customer drops or disconnects an incoming BLA call.
    - OUTGOINGESTABLISHED: To open the screen pop when the called party answers the phone.
    - OUTGOINGRELEASED: To open the screen pop when a user or customer drops or disconnects an outgoing call.
- `delay`
  element to open the screen pop with a delay for BLA calls. The default delay is 1000ms.

For example,

```
"name=ScreenPop1,trigger=INCOMINGRINGING,triggerOnlyForVDN=1,vdn=<VDNnumber>,type=EXTERNALBROWSER,url=https://www.google.com/search?q=<ucid><asai><vdntime>;name=ScreenPop2,trigger=OUTGOINGESTABLISHED,triggerOnlyForVDN=0,type=APPLICATION,url=notepad.exe;name=ScreenPop3,trigger=INCOMINGBLAANSWERED,triggerOnlyForVDN=0,type=APPLICATION,url=notepad.exe,delay=1000;"
```

Note:

Enclose the arguments with double quotation marks to use any arguments that include dots or spaces with the SCREEN_POP_LIST parameter to open applications such as the PowerShell script. For an incoming external call, if the value of the parameter m contains dots, use the

`m:"<m>"`

format instead of the

`m:<m>`

format. For example,

`m:"123456789@sbc.xyx.com"`

Adding a screen pop rule

Procedure

1. To open Avaya Screen Pop Configurator, go to https://downloads.avaya.com/css/P8/documents/101075011.
2. Click **New Pop**.
   Avaya Screen Pop Configurator displays the New Screen Pop Rule screen.
3. In the **Name** field, type a name for the screen pop.

4. In the **Type** field, click one of the following:
    - **Application**: To open an application in an external browser.
    - **Internal browser**: To open a web URL in an internal browser.
    - **External browser**: To open a web URL in an external browser.
5. Do one of the following:
    - If you choose Application in the previous step, type a valid directory path in the **Application Name** field. For example, type C:/Program Files/Adobe/Acrobat 7.0/Acrobat/Acrobat.exe.
      The application can be a file name with an extension specified in Windows Registry. For example, .html, .doc, or .txt extensions. If you specify an extension not specified in Windows Registry, Avaya Workplace Client displays an error message.
    - If you choose Internal browser in the previous step, type a valid web address in the **URL** field.
      The URL opens in the browser window of the Avaya Workplace Client application, which uses an integrated version of the Microsoft Edge browser.
    - If you choose External browser in the previous step, type a valid web address in the **URL** field.
      The URL can be CGI scripts, Java scripts, or any other web-based tool. To view a URL on a telephone number parameter, the example must contain one of the Avaya Workplace Client (%) parameters as http://mycompany.com/data?tel. The URL format depends on the data and format of the web program.

   You can pass additional parameters with the URL to get more information about the call. Agents or supervisors find this information useful to analyze customer calls.
   If you use any arguments that include dots or spaces to open applications such as PowerShell script, you must enclose the arguments with double quotation marks. For an incoming external call from a number, for example,
   `123456789@sbc.xyx.com`
   , you must use the
   `m:"<m>"`
   format. For example,
   `m:"123456789@sbc.xyx.com"`
6. In the **Trigger** field, click one of the following:
    - **Incoming**
    - **Outgoing**
7. In the **Incoming trigger** or **Outgoing trigger** field, select the appropriate trigger to indicate when Avaya Workplace Client must trigger the screen pop.
8. **Optional** For the incoming trigger, you can select the **VDN-Only trigger** check box and type the VDN name in the **VDN** field.
9. **Optional** For the incoming trigger for BLA calls, in the **Delay** field, you can specify the delay time for opening screen pops.
   The default delay is 1000ms.
10. Click **Save**.

Updating a screen pop rule

Procedure

1. To open Avaya Screen Pop Configurator, go to https://downloads.avaya.com/css/P8/documents/101075011.
2. To update a screen pop rule, click ✎ next to an existing screen pop.
   The system displays the Edit Screen Pop Rule screen.
3. Update the screen pop rules as needed.
4. Click **Save**.

Deleting a screen pop rule

Procedure

1. To open Avaya Screen Pop Configurator, go to https://downloads.avaya.com/css/P8/documents/101075011.
2. To delete a screen pop rule, click 🗑 next to an existing screen pop.
   The system displays a confirmation dialog box.
3. Click **OK**.

Ordering screen pops

About this task

If you create multiple screen pop rules, you can order the screen pops according to your preference.

Procedure

1. To open Avaya Screen Pop Configurator, go to https://downloads.avaya.com/css/P8/documents/101075011.
2. To change the order of a screen pop rule, click one of the following:
   - ↑: To move the screen pop rule up.
   - ↓: To move the screen pop rule down.

Using the screen pop configuration options

Procedure

1. To open Avaya Screen Pop Configurator, go to https://downloads.avaya.com/css/P8/documents/101075011.
2. In the Current Configuration area, you can click the following:
   - ⤒: To select an existing configuration file and use it as a starting point.
   - ⊗: To clear the existing configuration.
3. In the New Configuration area, you can click the following:
   - ⤓: To download the new configuration.
   - 📋: To copy the new configuration content to your clipboard.

Enhanced screen pop

Enhanced screen pop

With Avaya Workplace Client for Mac and Windows, you can configure enhanced screen pops so that Avaya Workplace Client displays the screen pop-up for the following conditions:

- When a user starts the application
- When a user logs in to the application for the first time
- When a user resets the application
- When a user signs out or signs in to the SIP server
- When an agent user logs in or logs out of the application: Only on the Windows client

You can configure a maximum of 99 screen pop rules. When Avaya Workplace Client for Windows triggers a rule, a screen pop appears and a URL opens in an internal or external browser. The internal browser requires the WebView2 Runtime component on the user's machine. If the user does not install this component, any requests to display a web page in the internal browser result in the page URL being displayed in the external browser instead.

To create configuration values, use the Avaya Workplace Screen Pop Configurator tool at https://downloads.avaya.com/css/P8/documents/101076665. For automatic configuration, specify the configuration value with the APPLICATION_SCREEN_POP_LIST parameter in the settings file or in Avaya Aura® Device Services.

You can also manually configure the screen pop rules in the following format, which you must specify with the APPLICATION_SCREEN_POP_LIST parameter in the settings file:

```
"name" - default: "New Rule" [string] "trigger" - default:
                "CLIENTLAUNCH" [string from list: "CLIENTLAUNCH", "INITIALCLIENT
LAUNCH",
                "RESETAPPLICATION", "SIPLOGIN", "SIPLOGOUT", "AGENTLOGIN", "AGEN
TLOGOUT"] "type" -
                default: "EXTERNALBROWSER" [string from list: "APPLICATION","INT
ERNALBROWSER",
                "EXTERNALBROWSER", "DIALOG"] "url" - (*) [string] "dialog" - (*)
            [string]]
```

Where, you can use the following:

- `name`
  element to specify the name for the enhanced screen pop.
- `trigger`
  element to specify when Avaya Workplace Client must trigger the enhanced screen pop. The options are the following:
  - CLIENTLAUNCH: To open the screen pop when the user starts the application.
  - INITIALCLIENTLAUNCH: To open the screen pop when a user logs in to the application for the first time.
  - RESETAPPLICATION: To open the screen pop when a user resets the application. This trigger type always opens the URL in the external browser because this trigger occurs when the internal browser is unavailable as the application is resetting.
  - SIPLOGIN: To open the screen pop when a user logs in to the SIP server.
  - SIPLOGOUT: To open the screen pop when a user logs out of the SIP server.
  - AGENTLOGIN: To open the screen pop when an agent user logs in to the application.
  - AGENTLOGOUT: To open the screen pop when an agent user logs out of the application.
- `type`
  element to specify whether to open an application or web URL in an internal or external browser or dialog box. The options are the following:
  - APPLICATION
  - INTERNALBROWSER
  - EXTERNALBROWSER
  - DIALOG
- `url`
  element to specify the URL.
- `dialog`
  element to specify the text in a dialog box.

For example:

- `"name=ClientLaunch,trigger=CLIENTLAUNCH,type=APPLICATION,url=C:/Program Files (x86)/Notepad/notepad.exe;"`
- `"name=ClientLaunch,trigger=CLIENTLAUNCH,type=EXTERNALBROWSER,url=https://www.google.com;"`
- `"name=AgentLogin,trigger=AGENTLOGIN,type=DIALOG,dialog=Hello;"`

Adding an enhanced screen pop rule

Procedure

1. To open the enhanced screen pop configurator, go to https://downloads.avaya.com/css/P8/documents/101076665.
2. Click **New Pop**.
   Avaya Workplace Screen Pop Configurator displays the New Screen Pop Rule screen.
3. In the **Name** field, type a name for the screen pop.
4. In the **Type** field, click one of the following:
   - **Application**: To open an application in an external browser.
   - **Internal browser**: To open a web URL in an internal browser.
   - **External browser**: To open a web URL in an external browser.
   - **Dialog**: To specify the text in a dialog box.
5. Do one of the following:
   - If you choose Application in the previous step, type a valid directory path in the **Application Name** field. For example, on Windows, type C:/Program Files/Adobe/Acrobat 7.0/Acrobat/Acrobat.exe.
     The application can be a file name with an extension specified in Windows Registry. For example, .html, .doc, or .txt extensions. If you specify an extension not specified in Windows Registry, Avaya Workplace Client displays an error message.
   - If you choose Internal browser in the previous step, type a valid web address in the **URL** field.
     The URL opens in the browser window of the Avaya Workplace Client application, which uses an integrated version of the Microsoft Edge browser.
   - If you choose External browser in the previous step, type a valid web address in the **URL** field.
     The URL can be CGI scripts, Java scripts, or any other web-based tool. To view a URL on a telephone number parameter, the example must contain one of the Avaya Workplace Client (%) parameters as http://mycompany.com/data?tel. The URL format depends on the data and format of the web program.
   - If you choose Dialog in the previous step, type a custom text in the **Dialog Content** field.
     You can include URLs in the **Dialog Content** field to navigate users to a website or invite them to a meeting. Avaya Workplace Client supports standard URLs, such as https and Avaya URLs.
     Avaya Workplace Client for Mac does not support the use of the keyboard for URL navigation in the dialog box.
6. In the **Trigger** field, click one of the following:
   - **Workplace client launch**

   - **Initial Workplace client launch**
   - **SIP Login**
   - **SIP Logout**
   - **Reset Application**
   - **Agent Login**: Only on Windows client
   - **Agent Logout**: Only on Windows client

7. Click **Save**.

Updating an enhanced screen pop rule

Procedure

1. To open the enhanced screen pop configurator, go to https://downloads.avaya.com/css/P8/documents/101076665.
2. To update a screen pop rule, click ✎ next to an existing screen pop.
   The system displays the Edit Screen Pop Rule screen.
3. Update the screen pop rules as needed.
4. Click **Save**.

Deleting an enhanced screen pop rule

Procedure

1. To open the enhanced screen pop configurator, go to https://downloads.avaya.com/css/P8/documents/101076665.
2. To delete a screen pop rule, click 🗑 next to an existing screen pop.
   The system displays a confirmation dialog box.
3. Click **OK**.

Ordering enhanced screen pops

About this task

If you create multiple enhanced screen pop rules, you can order the screen pops according to your preference.

Procedure

1. To open the enhanced screen pop configurator, go to https://downloads.avaya.com/css/P8/documents/101076665.
2. To change the order of a screen pop rule, click one of the following:
   - ↑: To move the screen pop rule up.
   - ↓: To move the screen pop rule down.

Using the enhanced screen pop configuration options

Procedure

1. To open the enhanced screen pop configurator, go to https://downloads.avaya.com/css/P8/documents/101076665.
2. In the Current Configuration area, you can click the following:
   - ⭱: To select an existing configuration file and use it as a starting point.
   - ⊗: To clear the existing configuration.
3. In the New Configuration area, you can click the following:
   - ⭳: To download the new configuration.
   - 📋: To copy the new configuration content to your clipboard.

Screen pop parameters

Type	Default value	Supported platforms	Description
SCREEN_POP_LIST			
String	Null	Windows	In Call Centers that integrate a telephone system and an agent's desktop, a screen pop is a window or dialog box that separately opens on the desktop. The screen pop displays information for a call simultaneously sent to that agent's

Type	Default value	Supported platforms	Description
			telephone. Screen pop is an essential feature for agents as they must perform work on certain web pages, sites, or accessible URLs. Hospital nurses and hospitality employees increasingly use screen pops With Avaya Workplace Client for Windows, you can configure screen pops for incoming and outgoing calls for Contact Center and Unified Communications users. You can configure a maximum of 99 screen pop rules. When Avaya Workplace Client for Windows triggers a rule, a screen pop appears and a URL opens in an internal or external browser. The internal browser requires the WebView2 Runtime component on the user's machine. If the user does not install this component, any requests to display a web page in the internal browser result in the page URL being displayed in the external browser instead. You must configure the screen pop rules in the following format: `"param1=val1,param2=val2;param12=val12,param22=val22" Parameters of the one ScreenPop are divided by ",`

Type	Default value	Supported platforms	Description
			" ScreenPop objects divided by ";" List of the parameters (* - required not-empty parameters): "name" - default: "New Rule" [string] "url" - (*) [string] "params" - default: "" [string] "triggerOnlyForVDN" - default: false [bool] "vdn" - default: "" (* if triggerOnlyForVDN == true) [string] "delay" - default: 1000 (* if trigger == "INCOMINGBLAANSWERED" or trigger == "INCOMINGBLARELEASED") [bool] "type" - default: "EXTERNALBROWSER" [string from list: "APPLICATION","INTERNALBROWSER","EXTERNALBROWSER"] "trigger" - default: "INCOMINGRINGING" [string from list: "INCOMINGRINGING","INCOMINGANSWERED","INCOMINGMISSED","INCOMINGRELEASED","OUTGOINGESTABLISHED","OUTGOINGRELEASED","INCOMINGBLAANSWERED","INCOMINGBLARELEASED"]

Type	Default value	Supported platforms	Description
			For more information on the screen pop format, see Screen pop. Client Navigation: Not Applicable.
APPLICATION_SCREEN_POP_LIST			
String	Null	• Mac • Windows	This parameter indicates whether Avaya Workplace Client displays the screen pop up for the following conditions: • When a user starts the application • When a user logs in to the application for the first time • When a user resets the application • When a user signs out or signs in to the SIP server • When an agent user logs in or logs out of the application: Only on the Windows client You must configure the enhanced screen pop rules in the following format:

Type	Default value	Supported platforms	Description
			"name" - default: "New Rule" [string] "trigger" - default: "CLIENTLAUNCH" [string from list: "CLIENTLAUNCH", "INITIALCLIENTLAUNCH", "RESETAPPLICATION", "SIPLOGIN", "SIPLOGOUT", "AGENTLOGIN", "AGENTLOGOUT"] "type" - default: "EXTERNALBROWSER" [string from list: "APPLICATION","INTERNALBROWSER", "EXTERNALBROWSER", "DIALOG"] "url" - (*) [string] "dialog" - (*) [string]] For more information on the enhanced screen pop format, see Enhanced screen pop.

Type	Default value	Supported platforms	Description
			Client Navigation: Not Applicable.

Avaya Feature Label Configurator

Avaya Feature Label Configurator

With Avaya Workplace Client for Windows, you can customize the feature button labels on Button Module for Contact Center features. Avaya Workplace Client uses an XML file to display the customized feature button labels on Button Module. Use Avaya Feature Label Configurator to import an existing XML file or create a new XML file.

To create customized feature button labels, use the Avaya Feature Label Configurator tool at https://downloads.avaya.com/css/P8/documents/101084836.

For automatic configuration, specify the configuration value with the CUSTOMIZED_FEATURE_LABEL_URL parameter in the settings file or Avaya Aura® Device Services.

You can manually customize the feature button labels in an XML file. For example,

```
<?xml version="1.0" encoding="utf-8"?>
<FeatureButtonLabels xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xmlns="http://xml.avaya.com/endpoi
ntAPI">
        <FeatureLabels>
                <FeatureLabel>
                        <Language>en-US</Language>
                        <FeatureLabelsForLanguage>
                                <Button>
                                        <Fnu>uui-info</Fnu>
                                        <Label>User Interface</Label>
                                </Button>
                        ↙FeatureLabelsForLanguage>
                ↙FeatureLabel>
        ↙FeatureLabels>
↙FeatureButtonLabels>
```

Adding a customized feature button label on Button Module

Procedure

1. To open Avaya Feature Label Configurator, go to https://downloads.avaya.com/css/P8/documents/101084836.
2. Click a feature from the **FNU to use** list.
   The list includes all features for which you can customize feature button labels on Button Module.
3. In the **Label translation** field, type a name for the feature label.
4. In the **Language** field, click one of the available languages.
   You can include only one unique label with a selected language and FNU.
5. Click **Save Label**.

Updating a customized feature button label on Button Module

Procedure

1. To open Avaya Feature Label Configurator, go to https://downloads.avaya.com/css/P8/documents/101084836.
2. **Optional** To filter the labels by languages, in **Filter language**, click a language.
3. To update a feature button label, click ✎ next to an existing feature button label.
   The system displays the selected fields.
4. Update the feature button label as needed.
5. Click **Save Label**.

Deleting a customized feature button label on Button Module

Procedure

1. To open Avaya Feature Label Configurator, go to https://downloads.avaya.com/css/P8/documents/101084836.
2. To delete a feature button label, click 🗑 next to an existing feature button label.
   Avaya Feature Label Configurator displays a confirmation dialog box.
3. Click **OK**.

Using the feature button label configuration options

Procedure

1. To open Avaya Feature Label Configurator, go to https://downloads.avaya.com/css/P8/documents/101084836.
2. In the Current Configuration area, you can click the following:
   - ⭱: To select an existing XML configuration file and use it as a starting point.
   - ⊗: To clear the existing XML configuration.
3. In the New Configuration area, you can click the following:
   - ⭳: To download the new XML configuration.
   - 📋: To copy the new XML configuration content to your clipboard.

Additional setup options for Avaya Workplace Client for Windows and Mac platforms

End users can install Avaya Workplace Client on mobile and desktop platforms. You can install Avaya Workplace Client on desktop platforms using a command line option. Command line installation only works with administrative privileges.

You can also deploy Avaya Workplace Client for Windows to work in a Citrix, XenApp, or VMWare environment.

Command line and silent installation options

Avaya Workplace Client for Mac command line and silent installation options

The following table lists silent installation commands and other command-line options available with Avaya Workplace Client for Mac. Silent install only works with administrator privileges. With the silent option, end-users do not need to install and uninstall their client manually.

⚠ **Tip:**

To mount the Avaya Workplace Client for Mac dmg file automatically, double-click the file.

Action	Command
Perform a silent installation.	`/Volumes/Avaya\ Workplace/Install.app/Contents/MacOS/install -silent`
Perform a silent installation with automatic configuration enabled.	`/Volumes/Avaya\ Workplace/Install.app/Contents/MacOS/install -silent -autoconfigURL <URL>`

Action	Command
	Replace `<URL>` with the appropriate automatic configuration URL.
Perform a silent uninstallation.	`sudo /Volumes/Avaya\ Workplace/Uninstall.app/Contents/MacOS/uninstall -silent`

Print help information about installation and uninstallation command usage.	For help with installing, use the following command:
	`/Volumes/Avaya\ Workplace/Install.app/Contents/MacOS/install -help`
	For help with uninstalling, use the following command:
	`/Volumes/Avaya\ Workplace/Uninstall.app/Contents/MacOS/uninstall -help`

Avaya Workplace Client for Windows command line and silent installation options

The following table lists silent installation commands and other command-line options available with Avaya Workplace Client for Windows. Silent install only works with administrator privileges. With the silent option, end-users do not need to install and uninstall their client manually.

Action	Option
Perform a silent installation.	`msiexec /i "Avaya Workplace Setup.msi" /qn`
Perform an installation with automatic configuration enabled.	`msiexec /i "Avaya Workplace Setup.msi" AUTOCONFIG="<URL/path to auto-config-file>"` Replace `URL` with the appropriate automatic configuration URL.
Perform a silent uninstallation.	`msiexec /qn /x "Avaya Workplace Setup.msi"`
Print help information for Windows installer command line.	`msiexec /?`
Open Avaya Workplace Client following passive installation	`msiexec /i "Avaya Workplace Setup.msi" /passive AUTOSTARTONINSTALLCOMPLETE=1`

Action	Option
Open Avaya Workplace Client following silent installation	`msiexec /i "Avaya Workplace Setup.msi" /qn AUTOSTARTONINSTALLCOMPLETE=1`
Create install log.	`msiexec /i <path_to_ACW_installer> /L*v <path_for_logs>`
Create uninstall log.	`msiexec /x <path_to_ACW_installer> /L*v <path_for_logs>`
Enable ImProvider.	`msiexec /i "Avaya Workplace Setup.msi" IMPROVIDER=1 /qn` **Note:** Do not include the WINDOWS_IMPROVIDER parameter in the settings file if you are using the command line option.
Enable the DSCP driver installation, which is disabled by default.	`msiexec /i "Avaya Workplace Setup.msi" NOQOS=0 /qn`
Disable the outlook plug-in installation.	`msiexec /i "Avaya Workplace Setup.msi" OP=0 /qn`

Action	Option
Disable the browser plug-in installation.	`msiexec /i "Avaya Workplace Setup.msi" BP=0 /qn`
Authenticate Avaya Workplace Client Single Sign-On (SSO) with Security Assertion Mark-up Language (SAML) using Azure Active Directory (AAD).	`msiexec /i "Avaya Workplace Setup.msi" ALLOWSSOUSINGOSPRIMARYACCOUNT=1`
Install Avaya Workplace Client as a controlled client.	`msiexec /i "Avaya Workplace Setup.msi" VDICONTROLLEDEP=1`
Install Avaya Workplace Client as a controlling client.	`msiexec /i "Avaya Workplace Setup.msi" VDIENV=1`

By default, the Avaya QoS service, that is, the DSCP driver is not installed. If you do not install the Avaya QoS service while installing the client, Avaya Workplace Client for Windows uses the Microsoft QWAVE API. To set the DSCP value, follow the instructions on the MS QoS policy.

If the customer wants to set audio and video separately, use the silent install parameter to install the Avaya DSCP driver. This method precedes the Microsoft APIs, which have the limitation that they can only set audio and video with the same value.

Supported languages for silent installation

Use the following command to perform a silent installation of Avaya Workplace Client for Windows for the supported languages:

```
msiexec /i "Avaya Workplace Setup.msi"
                        Language=xxxx ProductLanguage=xxxx
                    /L*v install_log.txt /qn
```

, where Language is the Avaya Workplace Client language and ProductLanguage is the OS language.

Note:

The Language value in the command is applied only if the local language is not stored in the following registry path: HKLU\Avaya\Avaya IX Workplace\Language. If you configure the local-user entries in the registry before a new Avaya Workplace Client installation or before the user changes the language from the User Preferences setting, then the Language value is not applied.

Replace *xxxx* in the command with the Language Code Identifier (LCID) values from the following table:

Language	Culture code	LCID
Arabic	ar-SA	1025
Malay	ms-MY	1086
Czech	cs-CZ	1029
Danish	da-DK	1030
English (U.K.)	en-GB	2057
English (U.S.)	en-US	1033
German	de-DE	1031
Spanish	es-ES	1034
French	fr-FR	1036
Indonesian	id-ID	1057
Italian	it-IT	1040
Hungarian	hu-HU	1038
Dutch	nl-NL	1043
Norwegian	nb-NO	1044
Polish	pl-PL	1045
Brazilian Portuguese	pt-BR	1046
Swedish	sv-SE	1053
Turkish	tr-TR	1055

Language	Culture code	LCID
Russian	ru-RU	1049
Hebrew	he-IL	1037
Thai	th-TH	1054
Korean	ko-KR	1042
Japanese	ja-JP	1041
Simplified Chinese	zh-CN	2052
Traditional Chinese	zh-TW	1028

Profile configuration

You can use the following methods to create multiple profiles in Avaya Workplace Client:

- A JSON file hosted on a web server
- A registry key

Users can select a profile from the list of configured profiles when configuring Avaya Workplace Client.

Configuring a list of profiles in a JSON file hosted on a web server

About this task

Use this procedure to create a new registry value AutoconfigProfilesPath within the main Avaya IX Workplace registry key. The new registry value must be of a type string.

Within this new registry value, you must specify the path of a JSON file that includes the list of profile names and 46xx settings file paths associated with each profile name.

Procedure

1. Open the Registry Editor window.
2. Go to one of the following:
    - Computer\HKEY_CURRENT_USER\SOFTWARE\Avaya\Avaya IX Workplace
    - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Avaya\Avaya IX Workplace

   If Avaya Workplace Client is installed only for the current user, use HKEY_CURRRENT_USER. If Avaya Workplace Client is installed for all users on the local computer, use HKEY_LOCAL_MACHINE.
3. Right-click the Avaya IX Workplace folder and click **New** > **String Value**.
4. Rename the new string value to `AutoconfigProfilesPath`.
5. Right-click **AutoconfigProfilesPath** and click **Modify**.
6. In the **Value data** field, enter the path of a JSON file.

   This JSON file must include the list of profiles and 46xx settings file paths associated with each profile.

   For example, the format of the JSON file with profile names and 46xx settings file paths is as follows:

```
{
        "ClientSettingsProfiles":
        [
                {
                        "ProfileName": "Profile 1",
                        "SettingsFileUrl": "http://server/profile1.txt"
                },
                {
                        "ProfileName": "Profile 2",
                        "SettingsFileUrl": "http://server/profile2.txt"
                }
        ]
}
```

7. Click **OK**.

Configuring a list of profiles using a registry key

About this task

Use this procedure to create a new registry subkey AutoconfigProfiles within the main Avaya IX Workplace registry key. Within this new subkey, include the list of profiles that Avaya Workplace Client displays to the user.

Any string values discovered within this subkey are considered to be profile choices. The value name is the profile name that Avaya Workplace Client displays and the value is the 46xx settings file path associated with the profile name.

You can use the 46xx settings file path associated with the profile to create multiple profiles.

Procedure

1. Open the Registry Editor window.
2. Go to one of the following:
    - Computer\HKEY_CURRENT_USER\SOFTWARE\Avaya\Avaya IX Workplace
    - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Avaya\Avaya IX Workplace

   If Avaya Workplace Client is installed only for the current user, use HKEY_CURRRENT_USER. If Avaya Workplace Client is installed for all users on the local computer, use HKEY_LOCAL_MACHINE.
3. Right-click the Avaya IX Workplace folder and click **New** > **Key**.
4. Rename the new key to `AutoconfigProfiles`.
5. Right-click the AutoconfigProfiles folder and click **New** > **String Value**.
6. Specify a profile name.
7. Right-click the profile name and click **Modify**.
8. In the **Value data** field, enter the 46xx settings file path associated with the profile.

   For example, http://server/profile1.txt.
9. Click **OK**.
10. Repeat steps 5 to 9 to add a new profile.

Deploying Avaya Workplace Client on a Windows server by using Group Policy

About this task

Use this procedure to deploy Avaya Workplace Client on a Windows server by using Group Policy. For information about using Group Policy to remotely install any software on a Windows server, see Microsoft Support site.

Before you begin

Ensure that the Windows server is part of a corporate network.

Procedure

1. To open **Group Policy Management**, click **Start** > **run** > **GPMC.MSC**.
2. Navigate to Default Domain Policy.
3. Right-click **Default Domain Policy** and click **Edit**.
4. Navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Scripts**.
5. In the Scripts/Startup folder, place the Avaya Workplace Client for Windows MSI installer.
   You can open the location by clicking **Show Files**.
6. To add a new script, click **Add**.
   a. Browse to go to the Avaya Workplace Client for Windows MSI installer.
   b. In the **Script Parameters** field, add the `/qn` parameter and click **Ok**.

If a user who is already a part of the corporate domain logs in to a Windows system, the system automatically installs the Avaya Workplace Client application.

Installing Avaya Workplace Client for Windows to work in a Citrix or VMWare environment

Installing Avaya Workplace Client for Windows to work in a Citrix or VMWare environment

About this task

Use this procedure when users need to log in to and use Avaya Workplace Client for Windows in a Citrix or VMWare environment.

Note:

- In a virtual environment, non-supported features such as video and computer-based audio are disabled. Also, the DSCP driver is not installed.

- Do not use Avaya Aura® Device Services to auto-update the client.

Before you begin

- Install Quality Windows Audio Video Experience (QWAVE) on the Citrix server. For example, for Windows Server 2016, see https://docs.microsoft.com/en-us/windows-server/administration/server-manager/install-or-uninstall-roles-role-services-or-features.

  Note:

  Copy and paste the URL in your supported browser if the hyperlink does not work.
- Obtain a supported deskphone as the Desk Phone mode is used in the virtual environment. Alternatively, you can also use a software client such as Avaya Workplace VDI or Avaya Agent for Desktop.

Procedure

1. Open Command Prompt.
2. Go to the location of the .msi file for Avaya Workplace Client for Windows.
3. Use the -VDIENV command to perform the installation.
   For example,

   ```
   msiexec /i "Avaya Workplace Setup.msi" VDIENV=1
   ```

   .

Citrix and VMWare environment specifications

Avaya Workplace Client for Windows supports the following specifications in a Citrix or VMWare environment:

Supported environments

- Citrix XenApp 6.5
- Citrix XenApp and XenDesktop 7.8
- Citrix XenApp and XenDesktop 7.9
- Citrix XenApp and XenDesktop 7.11
- VMware Horizon View 7.0 and later versions
- VMware Horizon Client 4.1 and later versions

Server capacity

Can scale up to 60 users on a single server with 80 GB of RAM and Intel Xeon Processor E5-2640 at 2.5 GHz.

Controlling and controlled client for Windows platform

Installing Avaya Workplace Client for Windows as a controlled client

About this task

Users can log in to and use Avaya Workplace Client for Windows on a local personal computer. A Controlled client means that Avaya Workplace Client is running in the My Computer mode on a local personal computer connecting to a remote virtual desktop.

Procedure

1. Open Command Prompt as an administrator.
2. Go to the location of the .msi file for Avaya Workplace Client for Windows.
3. Use the following command:

   ```
   msiexec /i "Avaya Workplace Setup.msi" VDICONTROLLEDEP=1
   ```

4. Start Avaya Workplace Client.

   When you install Avaya Workplace Client as a controlled client, and the client configuration is done, you can view the following message: `Waiting for paired sign-in request from controlling application....`

When you install Avaya Workplace Client as a controlled client, and if the client configuration is not done, a configuration request from the controlling client precedes the paired sign-on request.

Installing Avaya Workplace Client for Windows as a controlling client

About this task

Users can log in to and use Avaya Workplace Client for Windows in a virtual environment. Controlling client means that Avaya Workplace Client is running on a remote virtual desktop.

Procedure

1. Open Command Prompt as an administrator.
2. Go to the location of the .msi file for Avaya Workplace Client for Windows.
3. Use the following command:

   ```
   msiexec /i "Avaya Workplace Setup.msi" VDIENV=1
   ```

4. Start Avaya Workplace Client.
   When you install Avaya Workplace Client as a controlling client, you can view the Welcome screen with **Join a Meeting** and **Configure my account** options if the client configuration is not done.

Deployment considerations while upgrading to Avaya Workplace Client

Wireless data limitations

Avaya recommends that customers thoroughly test Avaya Workplace Client in their environment prior to operational deployment. This is to determine if the functionality and performance meet the customer's specific requirements. Due to the variability of Wi-Fi and Cellular 3G or 4G data connections, the application's VoIP stability and voice quality can vary widely.

Avaya Workplace Client is designed to support the VoIP requirements of mobile business professionals, not for deployment of mission critical workflows.

Analytics

By default, as described in the end-user license agreement, Avaya Workplace Client sends anonymous information about the application events to a third-party analytics service. This is to assist in analysis of the application feature usage and support quality improvements.

You can opt-out of the analytics feature for all users by configuring the ANALYTICSENABLED parameter in the settings file. In addition, end-users can opt-out by disabling the **Quality Improvement** setting in the **Support** tab of the Avaya Workplace Client settings.

Note:

If you are using a proxy that requires authentication, then Google Analytics does not work for Avaya Workplace Client.

Instant messaging

You can use the following for instant messaging:

- Avaya Multimedia Messaging service on Avaya Aura® Presence Services
- Avaya Multimedia Messaging
- Spaces Direct Messaging

You can exchange instant messages with other users using both Avaya Multimedia Messaging and Spaces Direct Messaging. Avaya Multimedia Messaging is used as the default over Spaces Direct Messaging.

Upgrade from Avaya one-X Communicator for Windows to Avaya Workplace Client for Windows

Avaya Workplace Client for Windows is recommended for all new Avaya Aura® deployments as the Windows-based soft client of choice. In addition, most users of Avaya one-X® Communicator for Windows can benefit from the new features and capabilities in Avaya Workplace Client. However, not all Avaya one-X® Communicator for Windows features are provided in Avaya Workplace Client.

Note:

If you have installed and configured Avaya one-X® Communicator and Avaya Collaboration Services and if you install Avaya Workplace Client for Windows, you can view the prompt to close Google Chrome and Microsoft Excel and then try the installation of Avaya Workplace Client for Windows. To avoid viewing this prompt, uninstall Avaya one-X® Communicator and Avaya Collaboration Services before you install Avaya Workplace Client for Windows.

Before deploying Avaya Workplace Client, ensure that all critical features that you require are available. The following features are unavailable in Avaya Workplace Client:

- H.323 support
- Client Enablement Services integration for Visual Voice Mail and other features
- Lotus Notes support for local contacts
- Personal or private Call
- Other telephony features not listed in this document including but not limited to Whisper Page.

Desk Phone mode limitations

Using Avaya Workplace Client in the Desk Phone mode on desktop platforms has the following limitations:

- Video calling is disabled.
- Screen sharing cannot be initiated from a point-to-point call.
- BFCP screen sharing is not supported as BFCP needs video call.

You cannot use the Desk Phone mode on mobile clients.

Avaya Workplace Client on Avaya Vantage

If you are using Avaya Vantage™ 2.x, the Avaya Workplace Client APK is bundled in the Avaya Vantage™ firmware zip file and is then pushed automatically to the Avaya Vantage™ device. If a new version of Avaya Workplace Client is available in Google Play, the Avaya Vantage™ device displays an upgrade notification.

- For Avaya Workplace Client to work as a phone application on the Avaya Vantage™ device, the ACTIVE_CSDK_BASED_PHONE_APP parameter in the settings file includes the package name. For example,

  ```
  SET
                               ACTIVE_CSDK_BASED_PHONE_APP com.avaya.android.flare
  ```

  .
- For Avaya Workplace Client to display the tutorial screen, you must add the com.google.android.webview package name to the white list of allowed applications on Avaya Vantage™.

If you are using Avaya Vantage™ 3.0 or any later version, you must download Avaya Workplace Client from Google Play. This is because the Avaya Workplace Client APK is no longer bundled in the Avaya Vantage™ firmware zip file. Also, the Avaya Vantage™ device configuration is similar to any other Android device.

Emergency calls

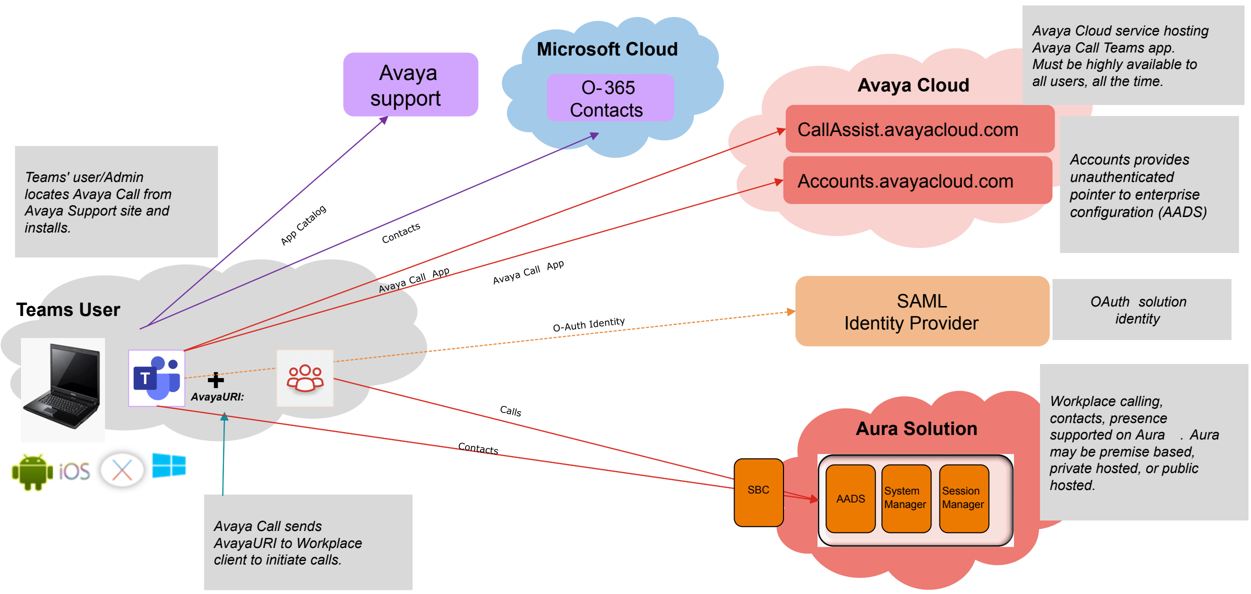
Users can use Avaya Workplace Client on Avaya Vantage™ to make calls to a preconfigured emergency services number. You must configure the emergency services numbers.

In the Avaya Aura® environment, users can make an emergency call even when they are logged out of Avaya Vantage™ or when Avaya Vantage™ is in the locked state.

Avaya Calling for Microsoft Teams configuration

Avaya Calling for Microsoft Teams overview

Avaya Calling for Microsoft Teams is an application that seamlessly integrates Avaya calling into Microsoft Teams. Avaya Calling for Microsoft Teams uses Avaya Workplace Client for call control and call handling.


Avaya support
Microsoft Cloud
O-365 Contacts
Avaya Cloud
CallAssist.avayacloud.com
Accounts.avayacloud.com
Avaya Cloud service hosting Avaya Call Teams app. Must be highly available to all users, all the time.
Accounts provides unauthenticated pointer to enterprise configuration (AADS)
Teams' user/Admin locates Avaya Call from Avaya Support site and installs.
App Catalog
Contacts
Avaya Call App
Avaya Call App
Teams User
O-Auth Identity
SAML Identity Provider
OAuth solution identity
AvayaURI:
iOS
Calls
Contacts
Aura Solution
SBC
AADS
System Manager
Session Manager
Workplace calling, contacts, presence supported on Aura . Aura may be premise based, private hosted, or public hosted.
Avaya Call sends AvayaURI to Workplace client to initiate calls.

You can view the following categories of contacts in the Avaya Contacts tab of the Avaya Calling for Microsoft Teams application:

- **Favorites**: Avaya Calling for Microsoft Teams retrieves your favorite contacts from Avaya Aura® Device Services. Favorites get synchronized with favorite contacts in Avaya Workplace Client.
- **Avaya Contacts**: Avaya Calling for Microsoft Teams retrieves Avaya Contacts from Avaya Aura® Device Services. Avaya Contacts get synchronized with Workplace Contacts in Avaya Workplace Client.
- **Office 365 Contacts**: Avaya Calling for Microsoft Teams retrieves your Office 365 contacts for quick calling.

Note:

Favorites and Avaya Contacts are unavailable on iOS.

You can perform the following actions from the Avaya Contacts tab:

- Make an audio or video call using Avaya Workplace Client. You must install, configure, and log in to Avaya Workplace Client to make calls.
- Send an email using the native application.
- Compose a message using Microsoft Teams.
- Search for an enterprise contact in Avaya Contacts and Office 365 Contacts.
- Add an enterprise contact to Avaya Contacts and Favorites.
- Remove an enterprise contact from Avaya Contacts and Favorites.
- Change the order of your favorites.

Checklist for configuring Avaya Calling for Microsoft Teams

The following checklist outlines the high-level setup and configuration tasks for Avaya Calling for Microsoft Teams:

Task	Reference	✔
Implement the certificate requirements. This is mandatory.	Certificate requirements	
Use Avaya Cloud accounts to set up a company domain on https://accounts.avayacloud.com/. This is mandatory.	• Configuration discovery • Registering an account • Setting up a company domain in Avaya Cloud accounts • Mapping your domain to the settings file URL	
Provision the OAuth configuration. This is optional. Use OAuth or basic authentication.	• OAuth • Provisioning the OAuth configuration for Avaya Calling for Microsoft Teams	
Provision the basic authentication configuration.	Provisioning the basic authentication configuration for Avaya Calling for Microsoft Teams	

Task	Reference	✔
This is optional. Use OAuth or basic authentication.		
Provision the configuration parameters. This is mandatory.	Configuration parameters for Avaya Calling for Microsoft Teams application	
Configure resource sharing on Avaya Aura® Device Services. This is mandatory.	Configuring resource sharing on Avaya Aura Device Services	
Configure a new client on Avaya Aura® Device Services. This is mandatory if you are using OAuth.	Configuring a new client on Avaya Aura Device Services	
Enable third-party cookies. This is mandatory if you are using Microsoft Teams in a web browser.	Third-party cookies	
Grant permissions in the Microsoft Teams admin center. This is mandatory.	Avaya Calling for Microsoft Teams permissions in the Microsoft Teams admin center	
Implement the requirements for Office 365 enterprise search. This is mandatory if you want to view Office 365 enterprise search results and call the contacts.	Office 365 enterprise search	

Certificate requirements

To understand the certificate requirements, see the chapter on Security and certificate configuration.

Configuration discovery

Avaya Calling for Microsoft Teams application discovers the Avaya Workplace Client settings file from your enterprise settings on https://accounts.avayacloud.com.

Use Avaya Cloud accounts to:

- Create an Avaya Cloud account.
- Set up a company domain on https://accounts.avayacloud.com/.

Registering an account

About this task

Use this procedure to register an account using your email address.

Procedure

1. In your web browser, enter https://accounts.avayacloud.com/.
2. In the **Email or Phone** field, type your email address.
3. Click **Yes, sign me up!**.
   sends a confirmation email to the email address you specified.
4. In your mailbox, open the confirmation email and then click the **Confirm** button.
   You are redirected to the My Account page.
5. Provide your first name, last name, password, and, optionally, a photo.
6. Click **Create an account**.

Setting up a company domain in Avaya Cloud accounts

Before you begin

- Ensure that your customer domain matches the email address domain for logging in to Avaya Workplace Client.
- Ensure that you have access to the DNS server settings for the domain.

Procedure

1. Log in to Avaya Cloud accounts at https://accounts.avayacloud.com/.
2. **Optional** If you have not set up your company or want to configure a new company, do the following:
    a. Click on your user name in the top-right of the screen, and click **Add Company**.
    b. Type a name and description for your company.
    c. Click **Save**.
3. Click **Manage Companies**, and click the existing company name.
4. Click **Domains**.
5. Click **Add Domain**.
6. Type the domain address, and click **OK**.
7. To verify ownership of the domain, next to the domain name, click **Verify**.
   You can view a verification code.
8. Copy the verification code and add it as a text record to the DNS entries on the domain's DNS server.
9. Click **Verify**.

Mapping your domain to the settings file URL

About this task

Add Avaya Calling For Teams to the company domain on https://accounts.avayacloud.com/ and put the settings file URL in the public settings in the correct JSON format.

Important:

If you were previously using Equinox Cloud Client, you must now use Avaya Calling For Teams.

You can specify multiple systems in the network by adding multiple Profile_Name sections, one for each system that can be used for Avaya Workplace Client registration. You can use this procedure while waiting for the company domain to be verified.

Procedure

1. Log in to your Avaya Cloud account and click **Manage Companies**.
2. Click the company name.
3. Click **Apps**.
4. Click **Configure New App**.
5. In the **Product** field, select **Avaya Calling For Teams**.
6. In the **Public Settings** field, enter the following settings, which are altered to match the customer system URL:
    - Single login system

      ```
      {
        "Client_Settings_File_Address": [
          {
            "Profile_Name": "Production",
            "Client_Settings_File_Url": "https://productionserver.example.com/acs/resources/configurations"
          }
        ]
      }
      ```

      In the example, productionserver.example.com is the URL of the Avaya Aura® Device Services server. If your configuration includes OAuth support, you must include `?preferredAuth=Bearer` at the end of the URL.
    - Multiple login systems: If there are multiple servers, the user receives a prompt from a list of profile names when they log in.

      ```
      {
        "Client_Settings_File_Address": [
          {
            "Profile_Name": "East",
            "Client_Settings_File_Url": "https://servereast.example.com/acs/resources/configurations"
          },
          {
            "Profile_Name": "West",
      ```

```
      "Client_Settings_File_Url": "https://serverwest.example.com/acs
/resources/configurations"
    }
  ]
}
```

In the example, servereast.example.com and serverwest.example.com are URLs of the Avaya Aura® Device Services servers. If your configuration includes OAuth support, you must include `?preferredAuth=Bearer` at the end of the URLs.

7. Click **Save**.

OAuth

Avaya Calling for Microsoft Teams application supports SSO with Open Authorization (OAuth).

To configure the Avaya Calling for Microsoft Teams application to use OAuth for the Avaya Aura® Device Services configuration service, you must append the configuration URL with the preferredAuth property. This property directs the Avaya Aura® Device Services configuration service not to provide the user name and password authentication.

The preferredAuth property directs Avaya Aura® Device Services to return a single authorization mechanism. Also, `bearer` indicates that OAuth is supported.

Provisioning the OAuth configuration for Avaya Calling for Microsoft Teams

About this task

Use this procedure if you want provision the OAuth configuration for Avaya Calling for Microsoft Teams. The Avaya_Authorization_Enabled property in this procedure directs the type of login flow. No indicates Basic authentication is used, and Yes indicates OAuth is used.

You can use this procedure for single and multiple login systems.

Procedure

1. Log in to your Avaya Cloud account and click **Manage Companies**.
2. Click the company name.
3. Click **Apps**.
4. Click **Configure New App**.
5. In the **Product** field, select **Avaya Calling For Teams**.

   Important:

   If you were previously using Equinox Cloud Client, you must now use Avaya Calling For Teams.
6. In the **Public Settings** field, enter the following settings, which are altered to match the customer system URL:
   - Profile_Name in Client_Authorization_Address must match with Profile_Name in Client_Settings_File_Address.
   - In the example, productionserver.example.com is the URL of the Avaya Aura® Device Services server.
   - The property names are case-sensitive. For example, Client_Settings_File_Url is valid, but Client_Settings_File_URL is invalid.
   - The property values are case insensitive, except for URLs and the Profile_Name property. For example, Yes and yes are both valid.
   - Single login system

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "Production",
      "Client_Settings_File_Url": "https://productionserver.example.c
om/acs/resources/configurations?preferredAuth=Bearer"
    }
  ],
  "Client_Authorization_Address": [
    {
      "Profile_Name": "Production",
      "Avaya_Authorization_Enabled": "yes",
      "Avaya_Authorization_Location_Url": "https://productionserver.e
xample.com/acs/resources/authorize"
    }
  ]
}
```

- Multiple login systems: If there are multiple servers, the user receives a prompt from a list of profile names when they log in.

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Url": "https://servereast.example.com/acs
/resources/configurations?preferredAuth=Bearer"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Url": "https://serverwest.example.com/acs
/resources/configurations?preferredAuth=Bearer"
    }
  ],
  " Client_Authorization_Address": [
    {
      "Profile_Name": "East",
      "Avaya_Authorization_Enabled": "yes",
      "Avaya_Authorization_Location_Url": "https://servereast.example
.com/acs/resources/authorize"
    },
    {
      "Profile_Name": "West",
      "Avaya_Authorization_Enabled": "yes",
      "Avaya_Authorization_Location_Url": "https://serverwest.example
.com/acs/resources/authorize"
    }
  ]
}
```

7. Click **Save**.

Provisioning the basic authentication configuration for Avaya Calling for Microsoft Teams

About this task

Use this procedure if you want to provision the basic authentication configuration for Avaya Calling for Microsoft Teams. The Client_Settings_File_Auth_Mode property in this procedure directs the type of login flow.

You can use this procedure for single and multiple login systems.

Before you begin

The 46xx settings file must include the ACSSRVR, ACSPORT, and ACSSECURE (TLS) parameters.

Procedure

1. Log in to your Avaya Cloud account and click **Manage Companies**.
2. Click the company name.
3. Click **Apps**.
4. Click **Configure New App**.
5. In the **Product** field, select **Avaya Calling For Teams**.

   Important:

   If you were previously using Equinox Cloud Client, you must now use Avaya Calling For Teams.
6. In the **Public Settings** field, enter the following settings, which are altered to match the customer system URL:
   - Profile_Name in Client_Authorization_Address must match with Profile_Name in Client_Settings_File_Address.
   - In the example, productionserver.example.com is the URL of the Avaya Aura® Device Services server.
   - The property names are case-sensitive. For example, Client_Settings_File_Url is valid, but Client_Settings_File_URL is invalid.
   - The property values are case insensitive, except for URLs and the Profile_Name property. For example, Basic and basic are both valid.
   - Single login system.

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "Production",
      "Client_Settings_File_Url": "https://productionserver.example.c
om/acs/resources/configurations"
    }
  ],
  "Client_Authorization_Address": [
    {
      "Profile_Name": "Production",
      "Client_Settings_File_Auth_Mode": "Basic"
    }
  ]
}
```

- Multiple login systems: If there are multiple servers, the user receives a prompt from a list of profile names when they log in.

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Url": "https://servereast.example.com/acs
/resources/configurations"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Url": "https://serverwest.example.com/acs
/resources/configurations"
    }
  ],
  " Client_Authorization_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Auth_Mode": "Basic"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Auth_Mode": "Basic"
    }
  ]
}
```

7. Click **Save**.

Configuration parameters for Avaya Calling for Microsoft Teams application

Avaya Aura® Device Services

You must provision a few parameters in the 46xx settings file so that users can use the Avaya Calling for Microsoft Teams application features.

Avaya Calling for Microsoft Teams application retrieves the UC configuration from Avaya Aura® Device Services to discover network capabilities and integrate with Avaya Workplace Client.

Parameter name	Description
ACSENABLED	This parameter indicates whether Avaya Aura® Device Services is enabled. This parameter is mandatory. The options are: • 0: Indicates that Avaya Aura® Device Services is disabled. 0 is the default value. • 1: Indicates that Avaya Aura® Device Services is enabled.

Parameter name	Description
ACSSRVR	The Avaya Aura® Device Services IP address or FQDN. This parameter is mandatory.
ACSPORT	The Avaya Aura® Device Services port. This parameter is mandatory. The default value is 443.
ACSSECURE	This parameter indicates whether TLS is used. This parameter is mandatory. The options are: • 0: Indicates that TLS is not used. • 1: Indicates that TLS is used. 1 is the default value.
ACSUSERNAME	The Avaya Aura® Device Services user name. This parameter is optional.
ACSPASSWORD	The Avaya Aura® Device Services password. This parameter is optional.
ACSSSO	This parameter indicates the authentication mechanism that Avaya Aura® Device Services uses. This parameter is mandatory. The options are: • 1: Indicates that Avaya Aura® Device Services uses unified login. 1 is the default value. • 3: Indicates that Avaya Aura® Device Services uses Avaya Authorization Service.

Unified Login

Parameter name	Description
SSOENABLED	This parameter indicates whether Unified Login is enabled. The options are: • 0: Indicates disabled. Avaya Workplace Client does not display Unified Login as an authentication mechanism for any service. • 1: Indicates enabled. 1 is the default value. Avaya Workplace Client displays Unified Login as an authentication mechanism for each service.
SSOUSERID	The unified login user ID. This parameter is optional.
SSOPASSWORD	The unified login password. This parameter is optional.

Video

Parameter name	Description
ENABLE_VIDEO	This parameter indicates whether video calling is enabled. The options are: • 0: Indicates that video calling is disabled.

Parameter name	Description
	- 1: Indicates that video calling is enabled. 1 is the default value.

Configuring resource sharing on Avaya Aura Device Services

About this task

To allow the Avaya Calling for Microsoft Teams application to access your enterprise UC services securely, update the Avaya Aura® Device Services configuration to allow requests from the avayacloud.com domain.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Server Connections** > **CORS Configuration** > **Service Interface**.
2. Select the **Enable Cross-Origin Resource Sharing** check box.
3. In the **Specific Domain(s)** field, type `avayacloud.com`.
4. In the **SameSite cookie attribute value** field, click **None**.
5. Click **Save**.

Configuring a new client on Avaya Aura Device Services

About this task

In the authorization flow, if OAuth is used, Avaya Aura® Device Services interacts with Keycloak on behalf of Avaya Calling for Microsoft Teams. To enable Avaya Aura® Device Services to communicate with Keycloak, provide Avaya Aura® Device Services with the Keycloak client secret and the URL to discover Keycloak resources. Create a client mapping for each client that your deployment supports.

Before you begin

Obtain the client secret.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings** > **Client ID Mapping**.
3. Click **Add**.
4. In the Create new client mapping window, complete the fields as follows:
    a. In **Client ID**, for Avaya Calling for Microsoft Teams, type `CallAssist`.
    This value is case-sensitive.
    b. In **OIDC Discovery URL**, enter `https://<AADS front-end FQDN>:<AADS PORT>/auth/realms/<Realm>/.well-known/openid-configuration`
    In this string:
        - `<AADS front-end FQDN>` is the Avaya Aura® Device Services front-end FQDN.
        - `<AADS PORT>` is the Avaya Aura® Device Services front-end FQDN service port.
        - `<Realm>` is the Keycloak realm, which is SolutionRealm by default.

    c. In **Client Secret**, enter the string copied from the Keycloak web administration interface.
5. Click **OK**.
    Avaya Aura® Device Services displays the new client mapping on the page.
6. **Optional** Create a client mapping for any additional clients that your deployment supports.

Third-party cookies

To access contacts in the Avaya Calling for Microsoft Teams application using a web browser, you must enable third-party cookies in the browser settings. However, if the third-party cookies policy is enforced at the enterprise level, your enterprise IT team must enable third-party cookies.

If third-party cookies are disabled due to network policies and the user enters valid credentials on the login screen, they cannot log in. Hence, the user cannot view any contacts. Avaya Calling for Microsoft Teams application displays a continuous spinner to the user.

Avaya Calling for Microsoft Teams permissions in the Microsoft Teams admin center

Use the Manage apps page in the Microsoft Teams admin center to view and manage Avaya Calling for Microsoft Teams. For example, you can view the org-level status and properties of the application, view permissions requested by the application, grant administrator consent to the application, and manage org-wide application settings.

To display Office 365 contacts, you need to grant the following permissions to Avaya Calling for Microsoft Teams:

- Sign in and read user profile
- Read all users' basic profiles
- Read user contacts

To display Office 365 enterprise search results with phone numbers, you need to grant the Read directory data permission to Avaya Calling for Microsoft Teams.

You can use the following URL to grant permissions to Avaya Calling for Microsoft Teams: https://admin.teams.microsoft.com/policies/manage-apps

For more information about how to view application permissions and grant administrator consent in the Microsoft Teams admin center, see Microsoft Teams documentation.

Office 365 enterprise search

Avaya Calling for Microsoft Teams application displays the Office 365 enterprise directory contacts that match the search criteria in the Enterprise Directory area.

Avaya Calling for Microsoft Teams populates the search results after running a query for the following fields:

- displayName
- mail

Avaya Calling for Microsoft Teams defines the default call target and additional call targets by using the following fields:

- bussinessPhones
- mobilePhone

The call targets are available from the contact card of Office 365 enterprise directory results.

Azure Virtual Desktop configuration

Azure Virtual Desktop overview

Azure Virtual Desktop is a flexible cloud Virtual Desktop Infrastructure (VDI) platform that securely delivers virtual desktops and remote apps with maximum control. Avaya Workplace Client is tested with virtual desktops and remote applications. Avaya Aura® applications are installed on Avaya on-premises, and Avaya Workplace Client is installed on Microsoft Azure Virtual Desktop. The ports must be open to communicate between Avaya Aura® applications and Avaya Workplace Client. You can refer to the Avaya Workplace Client port matrix document to check which ports must be opened. You can view the Avaya Workplace Client port settings document at https://downloads.avaya.com/css/P8/documents/101065872. This document describes the configuration steps required for using Avaya Workplace Client on Windows 10 Enterprise OS with Azure Virtual Desktop VDI.

Azure Virtual Desktop supports Windows 10 Enterprise Multi-session, version 20H2. Windows 10 Enterprise Multi-session is a new Remote Desktop Session Host that allows multiple concurrent interactive sessions.

This chapter describes the following two sections:

- General settings required for MS Azure. For example, resource groups and virtual networks.
- Configuration required for Azure Virtual Desktop. For example, host pool, session hosts, application groups, and user and role assignments.

Azure Virtual Desktop is supported with the following configurations:

- Deskphone mode with supported hard endpoint
- Deskphone mode with Avaya Workplace VDI

Note:

Avaya Workplace VDI support requires the audio stream to be located outside the VDI path. Avaya accepts support if the issue can be replicated outside of the VDI in a supported environment.

Creating a resource group

About this task

A resource group is a container with related resources for an Azure solution. The resource group can include all the resources for the solution or only those you can manage as a group. You must decide how to allocate resources to resource groups per your requirements. You can add resources sharing the same lifecycle to the same resource group so you can easily deploy, update, and delete them as a group.

Procedure

1. Login to https://portal.azure.com/.
2. In the **Search** field, type `Resource Group` and click **Resource Group**.
3. Click **Create**.
4. In the **Subscription** field, click your Azure subscription.
5. In the **Resource Group** field, type the name of the resource group.

   For example, type `Avaya-Client`.
6. In the **Region** field, click an Azure location.
7. Click **Review + Create**.
8. Click **Create** to create the resource group.

   After successfully creating a group, you can view the group in the Resource Group section.

Creating an Azure Virtual Network

About this task

Azure Virtual Network is the fundamental building block for your private network in Azure. A virtual network enables Azure resources like VMs to communicate securely with each other and the internet. For example, Azure Virtual Machines. A virtual network is similar to a traditional network in that you can operate in your data center. An Azure Virtual Network has extra benefits of Azure infrastructure, such as scale, availability, and isolation.

Procedure

1. Login to https://portal.azure.com/.
2. In the **Search** field, type `Virtual network` and click **Virtual network**.
3. Click **Create**.
4. In the **Subscription** field, click your Azure subscription.
5. In the **Resource** field, click the resource group.
6. In the **Name** field, type the name of the virtual network.

   For example, `Avaya-Client-VNET`.
7. In the **Region** field, click an Azure location.
8. Click **Review + Create** to create the resource group.

After successfully creating a virtual network, you can view the virtual network in the Go to resource section.

Creating an Azure Virtual Desktop host pool

About this task

Host pools are a collection of one or more identical virtual machines (VMs). In the Azure Virtual Desktop environments, host pools are also known as Session hosts. Each host pool has an app group that users can interact as they have on a physical desktop. This host pool contains all the Windows virtual machines pooled for remote desktop users to log in.

Procedure

1. Login to https://portal.azure.com/.
2. In the **Search** field, type `Azure Virtual Desktop` and click **Azure Virtual Desktop**.
3. Click **Create a host pool**.
   The Create a host pool section includes Basics, Virtual Machines, Workspace, Advanced, tags, and Review + create tabs.
4. Navigate to the Basic tab.
5. In the **Subscription** field, click your Azure subscription.
6. In the **Resource** field, click the resource group.
7. In the **Host pool name** field, type the name of the host pool.
   For example, `Avaya-Client-HP`.
8. In the **Location** field, click the Azure region where your host pool is deployed.
9. In the **Validation environment** field, click **Yes**.
10. Click one of the following:
    - **Personal**: Each virtual machine is dedicated to one user.
    - **Pooled**: All remote users can share multiple virtual machine session hosts in the pool.
11. In the **Load balancing algorithm** field, click **breadth-first**.
12. In the **Max session limit** field, enter the maximum number of users you want load balanced to a single session host.

13. Click **Next: Virtual Machines**.

Creating virtual machines or session host and assigning virtual machines to the host pool

Procedure

1. On the Create a host pool screen, navigate to the Virtual Machines tab.
2. In the **Add Azure virtual machines** field, click **Yes**.
3. In the **Resource** field, type the name of the resource group.
   For example, type `Avaya-Client`.
4. In the **Name prefix** field, type the virtual machine name prefix.
   The created virtual machines have a name starting with a prefix. For example, type `AVD-0, AVD-1, AVD-2`.
5. In the **Virtual machine location** field, click the geographic location that hosts the virtual machines.
6. In the **Availability options** field, click the required option.
7. In the **Security type** field, click the required security type.
8. In the **Image** field, click an image you want to upload.
   You can select your customized images from the gallery.
9. In the **Virtual machine size** field, click the Stock-Keeping unit.
10. In the **Number of VMs** field, type the number of virtual machines to deploy.
11. In the **OS disk type** field, click the disk type for your session hosts.
12. In the **Boot Diagnostics** field, click whether to enable boot diagnostics.
13. In the Network and security section, click your virtual network and subnet from your virtual network.
14. In the **Network security group** field, click **Basic**.
15. In the **Public inbound ports** field, click **No**.
16. In the **Select which directory you would like to join** field, click **Azure Active Directory**.
17. In the **Enroll VM with Intune** field, click **No**.
18. In the Virtual Machine Administrator account section, type the credentials of the local administrator account.
19. Click **Next: Workspace**.

Creating a workspace

Procedure

1. On the Create a host pool screen, navigate to the **Workspace** tab.
2. In the **Register desktop app group** field, click **Yes**.
3. In the **To this workspace** field, do one of the following:
    - Click an existing workspace from the list.
    - Click **Create new**, and in the **Workspace name** field, type the name, and click **OK**.
4. To enable diagnostic and tag to the newly created resource, click **Next: Advanced** and then click **Next:Tags**.
5. Click **Review + create**.

Creating an application group

About this task

If you have already created a host pool and session host virtual machines, you can add application groups from the Azure portal. The default application group created for a new Azure Virtual Desktop host pool also publishes the full desktop. You can create one or more RemoteApp application groups for the host pool.

Procedure

1. Login to https://portal.azure.com/.
2. In the **Search** field, type `Azure Virtual Desktop` and click **Azure Virtual Desktop**.
3. Click **Application group** > **Add**.
4. In the **Subscription** field, click your Azure subscription.
5. In the **Resource** field, click the resource group.
6. In the **Host pool** field, click the host pool associated with the application group.
7. In the **Location** field, select the location.
8. In the **Application group type** field, click **RemoteApp**.
9. In the **Application group name** field, type the name of the application group.
10. Click **Next: Applications** > **Add applications**.
11. In the **Application source** field, click one of the following:
    - File path
    - Start menu
12. Click **Next: Assignments** > **tab**.
13. To assign individual users or user groups to the application group, click **+Add Azure AD users or user groups**.

14. To register the application group to a workspace, click **Yes** for **Register application group**.
15. Enter Advanced and tags tab details.
16. Click **Review + create**.
17. After successful validation, click **Create** to deploy your application group.

Assigning users to a virtual machine or session host

Procedure

1. Login to https://portal.azure.com/.
2. In the **Search** field, type `Azure Machines` and then click the virtual machine or session host you want to grant access to the user.
3. Click **Access Control (IAM)**.
4. Click **Add**.
5. Click **Add Role Assignment**.
6. In the **Search** field, search and click **Virtual Machine Administrator Login / Virtual machine User Login**.
7. In the **Assign access to** field, click **User, group, or service principal**.
8. Click **Select members**.
9. In the **Search** field, search and click the users to add.
10. Click **Next**.
11. Click **Review and assign**.

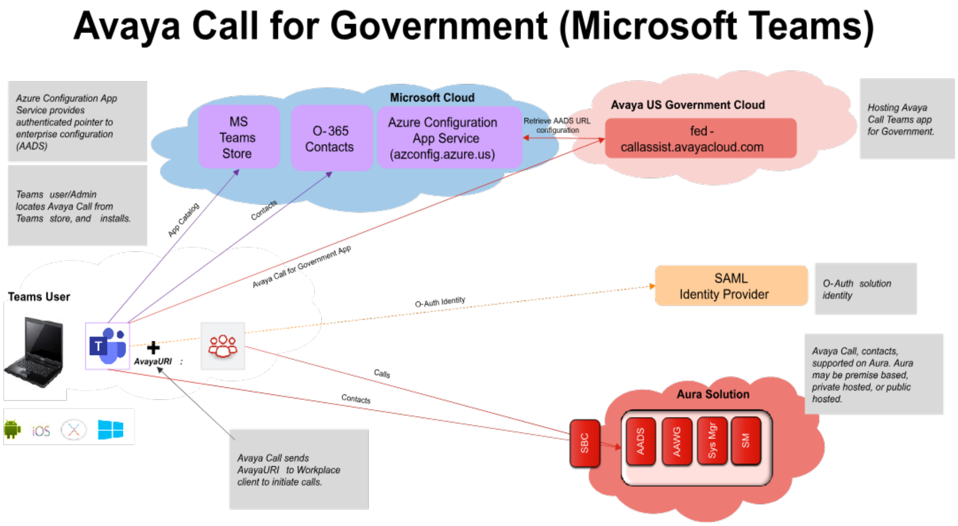
Avaya Call for Government configuration

Avaya Call for Government overview

Avaya Call for Government is an application that seamlessly integrates Avaya calling into Microsoft Teams. Avaya Call for Government is only for United States Government users. Avaya Call for Government uses Avaya Workplace Client for call control and call handling.

Note:

Avaya Call for Government requires United States Government Microsoft Azure Application Configuration Service. Microsoft offers this service as Free or Standard, which is a non-free service. To know about the pricing information for the Standard service, see https://azure.microsoft.com/en-us/pricing/details/app-configuration/#pricing%20for%20pricing. Avaya recommends that you use the Standard service. This is to ensure that Avaya Call for Government retrieves the configuration successfully from the Application Configuration Service.



Avaya Call for Government (Microsoft Teams)

Azure Configuration App Service provides authenticated pointer to enterprise configuration (AADS)

Teams user/Admin locates Avaya Call from Teams store, and installs.

Hosting Avaya Call Teams app for Government.

O-Auth solution identity

Avaya Call, contacts, supported on Aura. Aura may be premise based, private hosted, or public hosted.

Avaya Call sends AvayaURI to Workplace client to initiate calls.

You can view the following categories of contacts in the Avaya Contacts tab of the Avaya Call for Government application:

- **Favorites**: Avaya Call for Government retrieves your favorite contacts from Avaya Aura® Device Services. Favorites get synchronized with favorite contacts in Avaya Workplace Client.
- **Avaya Contacts**: Avaya Call for Government retrieves Avaya Contacts from Avaya Aura® Device Services. Avaya Contacts get synchronized with Workplace Contacts in Avaya Workplace Client.

- **Office 365 Contacts**: Avaya Call for Government retrieves your Office 365 contacts for quick calling.

Note:

Favorites and Avaya Contacts are unavailable on iOS.

You can perform the following actions from the Avaya Contacts tab:

- Make an audio or video call using Avaya Workplace Client. You must install, configure, and log in to Avaya Workplace Client to make calls.
- Send an email using the native application.
- Compose a message using Microsoft Teams.
- Search for an enterprise contact in Avaya Contacts and Office 365 Contacts.
- Add an enterprise contact to Avaya Contacts and Favorites.
- Remove an enterprise contact from Avaya Contacts and Favorites.
- Change the order of your favorites.

Checklist for configuring Avaya Call for Government

The following checklist outlines the high-level setup and configuration tasks for Avaya Call for Government:

Task	Reference	✔
Implement the certificate requirements. This is mandatory.	Certificate requirements	
Use U.S. Government Microsoft Azure tenant to perform configuration discovery. To create a new subscription, you must provide details of payment information such as credit card. This is mandatory.	• Configuration discovery • Creating a new subscription • Creating a new Application Configuration Service resource • Granting tenant-wide admin consent to Avaya Call for Government • Assigning Reader and App Configuration Data	

Task	Reference	✔
	Reader roles to the service principal - Configuring Avaya Aura Device Services mapping for Microsoft Azure Directory tenant	
Configure Microsoft Azure Directory tenant to only display Office 365 contacts. This is optional. Use only if you want Avaya Call for Government to display Office 365 Contacts and not Avaya Contacts and Favorites.	Configuring Microsoft Azure Directory tenant to display Office 365 contacts by Avaya Call for Government	
Provision the OAuth configuration. This is optional. Use OAuth or basic authentication.	- OAuth - Provisioning the OAuth configuration for Avaya Call for Government	
Provision the basic authentication configuration. This is optional. Use OAuth or basic authentication.	Provisioning the basic authentication configuration for Avaya Call for Government	
Provision the configuration parameters. This is mandatory.	Configuration parameters for Avaya Call for Government application	
Configure resource sharing on Avaya Aura® Device Services. This is mandatory.	Configuring resource sharing on Avaya Aura Device Services	
Configure a new client on Avaya Aura® Device Services. This is mandatory if you use OAuth.	Configuring a new client on Avaya Aura Device Services	
Enable third-party cookies.	Third-party cookies	

Task	Reference	✔
This is mandatory if you use Microsoft Teams in a web browser.		
Implement the requirements for Office 365 enterprise search. This is mandatory to view Office 365 enterprise search results and call the contacts.	Office 365 enterprise search	
Add Avaya Call for Government to Microsoft Teams Apps Store. This is mandatory.	Adding Avaya Call for Government to Microsoft Teams Apps Store	

Certificate requirements

To understand the certificate requirements, see the chapter on Security and certificate configuration.

Configuration discovery

Avaya Call for Government application discovers the Avaya Workplace Client settings file from your U.S. Government Microsoft Azure tenant.

Use your U.S. Government Microsoft Azure tenant to:

- Create a new subscription or use an existing subscription.
- Create a new resource of Application Configuration Service.
- Grant tenant-wide admin consent to Avaya Call for Government.
- Assign Reader and App Configuration Data Reader roles to the service principal.
- Configure Avaya Aura® Device Services mapping.

Creating a new subscription

About this task

Use this procedure to create a new subscription for Avaya Call for Government in U.S. Government Microsoft Azure tenant. To create a new subscription, you must provide details of payment information such as credit card. You must join one of the relevant Azure offers to create a subscription. After creating a subscription, you can define an application configuration service.

Note:

If you have an existing subscription, you can use the same.

Before you begin

Choose the appropriate Azure offer.

Procedure

1. Log in to the Microsoft Azure portal as an administrator.
2. In the Azure services area, click **Subscriptions**.
3. To add a new subscription, click **Add** and enter the relevant details.
   For example, create a subscription with the name `Azure Government Free Trial` and role as `Account admin`.
4. Click the subscription that you created.
5. Click **Access control (IAM)**.
6. To grant access to users and groups, click **Add role assignment** in the Grant access to this resource area.
7. Assign roles to users and groups to access the subscription.
8. To view the roles that you assign to a subscription, click **View** in the View access to this resource area.
   The roles you assign to a subscription level are automatically inherited to a resource level, for example, application configuration service. Hence, provide contributor access to only a few administrator users. All other users must have read-only access to the application configuration service.

Creating a new Application Configuration Service resource

About this task

Create a new Application Configuration Service resource under the subscription for Avaya Call for Government.

The Avaya back-end service supports caching mechanism, which enables storing the last successful access to the application configuration service for each tenant. Hence, the caching mechanism reduces the access to the application configuration service to 1 per 5 minutes or 288 per day for each tenant. An update to the configuration propagates within 5 minutes to clients that perform discovery. Also, the caching mechanism helps to support downtime periods where the application configuration service is down, but a cache response for the specific tenant was received earlier. However, if there is no cache, Avaya Call for Government is unable to get the configuration until the application configuration service is up again. You can use this information to choose between the Free or Paid Microsoft Azure application configuration service.

Procedure

1. Log in to the Microsoft Azure portal as an administrator.
2. In the Azure services area, click **App Configuration**.
3. Click **Create** and enter the relevant details in the following fields:
    - **Subscription**: Select a subscription to create the application configuration under it.
    - **Resource group**: Select the resource group. If there is no resource group, create the same.
    - **Resource name**: Configure a resource name for the application configuration.
      The resource name is part of the endpoint URL. The Avaya Call for Government back-end service tries to retrieve the configuration from https://<resource-name>.azconfig.azure.us.
    - **Location**
    - **Pricing tier**
4. Click **Review + create**.
5. After you verify the details you added in the earlier steps, click **Create**.
6. After the deployment is complete, click **Go to resource**.

Granting tenant-wide admin consent to Avaya Call for Government

About this task

Use this procedure to add Avaya Call for Government to U.S. Government Microsoft Azure Active Directory tenant as a service principal. Also, you must grant administrator access to the Avaya Call for Government application to access the customer application configuration service.

1. Use the following link: https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id={client-id}

Where tenant-id is the tenant ID of the customer organization or any verified domain name. You can get the tenant ID or primary domain from the Azure Active Directory screen. Also, client_id is the App ID for Avaya Call for Government, 613c121f-9730-4a33-bb64-8ccf7862d778.

2. Use the administrator credentials of the tenant that supports Avaya Call for Government.

3. Accept the permission consent request.

Assigning Reader and App Configuration Data Reader roles to the service principal

About this task

Use this procedure to assign Reader and App Configuration Data Reader roles to the service principal to access the application configuration service. Configure the service principal to provide access to only one application configuration service and in one specific subscription. Avaya Call for Government works with one application configuration service configured to the service principal.

Procedure

1. Log in to the Microsoft Azure portal as an administrator.
2. In the Azure services area, click **App Configuration**.
3. Click the application configuration service name you created earlier.
   For example, avaya-configuration-service.
4. Click **Access control (IAM)**.
5. Click **Add** > **Add role assignment**.
6. Click **Reader**, and click **Next**.
7. Click **Select Members**.
8. In the **Select** field, type Avaya Call for Government.
9. Click Avaya Call for Government, and click **Select**.
10. After you review the added members, click **Review + assign**.
11. Repeat steps 2 to 5.
12. Click **App Configuration Data Reader**, and click **Next**.
13. Click **Select Members**.
14. In the **Select** field, type Avaya Call for Government.
15. Click Avaya Call for Government, and click **Select**.

16. After you review the added members, click **Review + assign**.

Configuring Avaya Aura Device Services mapping for Microsoft Azure Directory tenant

About this task

To specify multiple systems in the network, you can add multiple Profile_Name sections, one for each system that can be used for Avaya Workplace Client registration.

Procedure

1. Log in to the Microsoft Azure portal as an administrator.
2. In the Azure services area, click **App Configuration**.
3. Click the application configuration service name you created earlier.
   For example, avaya-configuration-service.
4. In the Operations area, click **Configuration explorer**.
5. Click **Create** > **Key-value**.
6. In the **Key** field, type `avaya-call-configuration`.
7. In the **Value** field, enter one of the following settings, which are altered to match the URL of the customer's system:
   - Single login system:

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "Production",
      "Client_Settings_File_Url": "https://productionserver.example.c
om/acs/resources/configurations"
    }
  ]
}
```

In the example, productionserver.example.com is the URL of the Avaya Aura® Device Services server. If your configuration includes OAuth support, include
`?preferredAuth=Bearer`
at the end of the URL.

- Multiple login systems: If there are multiple servers, the user receives a prompt from a list of profile names when they log in.

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Url": "https://servereast.example.com/acs
/resources/configurations"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Url": "https://serverwest.example.com/acs
/resources/configurations"
    }
  ]
}
```

In the example, servereast.example.com and serverwest.example.com are URLs of the Avaya Aura® Device Services servers. If your configuration includes OAuth support, include
`?preferredAuth=Bearer`
at the end of the URLs.

8. In the **Content type** field, type `application/json`.
9. Click **Apply**.

Configuring Microsoft Azure Directory tenant to display Office 365 contacts by Avaya Call for Government

About this task

Use this procedure if you want Avaya Call for Government to only display Office 365 Contacts and not Avaya Contacts and Favorites.

Procedure

1. Log in to the Microsoft Azure portal as an administrator.
2. In the Azure services area, click **App Configuration**.
3. Click the application configuration service name you created earlier.
   For example, avaya-configuration-service.
4. In the Operations area, click **Configuration explorer**.
5. Click **Create** > **Key-value**.
6. In the **Key** field, type `avaya-call-configuration`.
7. In the **Value** field, configure [] for Client_Settings_File_Address as follows:

   ```
   {
   "Client_Settings_File_Address": []
   }
   ```

8. In the **Content type** field, type `application/json`.
9. Click **Apply**.

OAuth

Avaya Call for Government application supports SSO with Open Authorization (OAuth).

To configure the Avaya Call for Government application to use OAuth for the Avaya Aura® Device Services configuration service, append the configuration URL with the preferredAuth property. This property directs the Avaya Aura® Device Services configuration service not to provide the username and password authentication.

The preferredAuth property directs Avaya Aura® Device Services to return a single authorization mechanism. Also, `bearer` indicates that OAuth is supported.

Provisioning the OAuth configuration for Avaya Call for Government

About this task

Use this procedure to provision the OAuth configuration for Avaya Call for Government. The Avaya_Authorization_Enabled property in this procedure directs the type of login flow. No indicates Basic authentication is used, and Yes indicates OAuth is used.

You can use this procedure for single and multiple login systems.

Procedure

1. Log in to the Microsoft Azure portal as an administrator.
2. In the Azure services area, click **App Configuration**.
3. Click the application configuration service name you created earlier.
   For example, avaya-configuration-service.
4. In the Operations area, click **Configuration explorer**.
5. Click **Create** > **Key-value**.
6. In the **Key** field, type `avaya-call-configuration`.
7. In the **Value** field, enter one of the following settings, which are altered to match the URL of the customer's system:
   - Profile_Name in Client_Authorization_Address must match with Profile_Name in Client_Settings_File_Address.
   - In the example, productionserver.example.com is the URL of the Avaya Aura® Device Services server.
   - The property names are case-sensitive. For example, Client_Settings_File_Url is valid, but Client_Settings_File_URL is invalid.
   - The property values are case insensitive, except for URLs and the Profile_Name property. For example, Yes and yes are both valid.
   - Single login system:

     ```
     {
       "Client_Settings_File_Address": [
     ```

```
    {
      "Profile_Name": "Production",
      "Client_Settings_File_Url": "https://productionserver.example.c
om/acs/resources/configurations?preferredAuth=Bearer"
    }
  ],
  "Client_Authorization_Address": [
    {
      "Profile_Name": "Production",
      "Avaya_Authorization_Enabled": "yes",
      "Avaya_Authorization_Location_Url": "https://productionserver.e
xample.com/acs/resources/authorize"
    }
  ]
}
```

- Multiple login systems: If there are multiple servers, the user receives a prompt from a list of profile names when they log in.

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Url": "https://servereast.example.com/acs
/resources/configurations?preferredAuth=Bearer"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Url": "https://serverwest.example.com/acs
/resources/configurations?preferredAuth=Bearer"
    }
  ],
  " Client_Authorization_Address": [
    {
      "Profile_Name": "East",
      "Avaya_Authorization_Enabled": "yes",
      "Avaya_Authorization_Location_Url": "https://servereast.example
.com/acs/resources/authorize"
    },
    {
      "Profile_Name": "West",
      "Avaya_Authorization_Enabled": "yes",
      "Avaya_Authorization_Location_Url": "https://serverwest.example
.com/acs/resources/authorize"
    }
  ]
}
```

8. In the **Content type** field, type `application/json`.
9. Click **Apply**.

Provisioning the basic authentication configuration for Avaya Call for Government

About this task

Use this procedure to provision the basic authentication configuration for Avaya Call for Government. The Client_Settings_File_Auth_Mode property in this procedure directs the type of login flow.

You can use this procedure for single and multiple login systems.

Procedure

1. Log in to the Microsoft Azure portal as an administrator.
2. In the Azure services area, click **App Configuration**.
3. Click the application configuration service name you created earlier.
   For example, avaya-configuration-service.
4. In the Operations area, click **Configuration explorer**.
5. Click **Create** > **Key-value**.

6. In the **Key** field, type `avaya-call-configuration`.
7. In the **Value** field, enter one of the following settings, which are altered to match the URL of the customer's system:
    - Profile_Name in Client_Authorization_Address must match with Profile_Name in Client_Settings_File_Address.
    - In the example, productionserver.example.com is the URL of the Avaya Aura® Device Services server.
    - The property names are case-sensitive. For example, Client_Settings_File_Url is valid, but Client_Settings_File_URL is invalid.
    - The property values are case insensitive, except for URLs and the Profile_Name property. For example, Basic and basic are both valid.
    - Single login system:

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "Production",
      "Client_Settings_File_Url": "https://productionserver.example.c
om/acs/resources/configurations"
    }
  ],
  "Client_Authorization_Address": [
    {
      "Profile_Name": "Production",
      "Client_Settings_File_Auth_Mode": "Basic"
    }
  ]
}
```

    - Multiple login systems: If there are multiple servers, the user receives a prompt from a list of profile names when they log in.

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Url": "https://servereast.example.com/acs
/resources/configurations"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Url": "https://serverwest.example.com/acs
/resources/configurations"
    }
  ],
  " Client_Authorization_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Auth_Mode": "Basic"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Auth_Mode": "Basic"
    }
  ]
}
```

8. In the **Content type** field, type `application/json`.
9. Click **Apply**.

Configuration parameters for Avaya Call for Government application

Avaya Aura® Device Services

You must provision a few parameters in the 46xx settings file so that users can use the Avaya Call for Government application features.

Avaya Call for Government application retrieves the UC configuration from Avaya Aura® Device Services to discover network capabilities and integrate with Avaya Workplace Client.

Parameter name	Description
ACSENABLED	This parameter indicates whether Avaya Aura® Device Services is enabled. This parameter is mandatory. The options are: • 0: Indicates that Avaya Aura® Device Services is disabled. 0 is the default value. • 1: Indicates that Avaya Aura® Device Services is enabled.
ACSSRVR	The Avaya Aura® Device Services IP address or FQDN. This parameter is mandatory.
ACSPORT	The Avaya Aura® Device Services port. This parameter is mandatory. The default value is 443.
ACSSECURE	This parameter indicates whether TLS is used. This parameter is mandatory. The options are: • 0: Indicates that TLS is not used. • 1: Indicates that TLS is used. 1 is the default value.
ACSSSO	This parameter indicates the authentication mechanism that Avaya Aura® Device Services uses. This parameter is mandatory. The options are: • 1: Indicates that Avaya Aura® Device Services uses unified login. 1 is the default value.

Parameter name	Description
	• 3: Indicates that Avaya Aura® Device Services uses Avaya Authorization Service.

Video

Parameter name	Description
ENABLE_VIDEO	This parameter indicates whether video calling is enabled. The options are: • 0: Indicates that video calling is disabled. • 1: Indicates that video calling is enabled. 1 is the default value.

Configuring resource sharing on Avaya Aura Device Services

About this task

To allow the Avaya Call for Government application to access your enterprise UC services securely, update the Avaya Aura® Device Services configuration to allow requests from the avayacloud.com domain.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Server Connections** > **CORS Configuration** > **Service Interface**.
2. Select the **Enable Cross-Origin Resource Sharing** check box.
3. In the **Specific Domain(s)** field, type `avayacloud.com`.
4. In the **SameSite cookie attribute value** field, click **None**.

5. Click **Save**.

Configuring a new client on Avaya Aura Device Services

About this task

In the authorization flow, if OAuth is used, Avaya Aura® Device Services interacts with Keycloak on behalf of Avaya Call for Government. To enable Avaya Aura® Device Services to communicate with Keycloak, provide Avaya Aura® Device Services with the Keycloak client secret and the URL to discover Keycloak resources. Create a client mapping for each client that your deployment supports.

Before you begin

Obtain the client secret.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings** > **Client ID Mapping**.
3. Click **Add**.
4. In the Create new client mapping window, complete the fields as follows:
    a. In **Client ID**, for Avaya Call for Government, type `CallAssist`.
    This value is case-sensitive.
    b. In **OIDC Discovery URL**, enter `https://<AADS front-end FQDN>:<AADS PORT>/auth/realms/<Realm>/.well-known/openid-configuration`
    In this string:
    - `<AADS front-end FQDN>` is the Avaya Aura® Device Services front-end FQDN.
    - `<AADS PORT>` is the Avaya Aura® Device Services front-end FQDN service port.
    - `<Realm>` is the Keycloak realm, which is SolutionRealm by default.

    c. In **Client Secret**, enter the string copied from the Keycloak web administration interface.

5. Click **OK**.
   Avaya Aura® Device Services displays the new client mapping on the page.

6. **Optional** Create a client mapping for any additional clients that your deployment supports.

Third-party cookies

To access contacts in the Avaya Call for Government application using a web browser, you must enable third-party cookies in the browser settings. However, if the third-party cookies policy is enforced at the enterprise level, your enterprise IT team must enable third-party cookies.

If third-party cookies are disabled due to network policies and the user enters valid credentials on the login screen, they cannot log in. Hence, the user cannot view any contacts. Avaya Call for Government application displays a continuous spinner to the user.

Office 365 enterprise search

Avaya Call for Government application displays the Office 365 enterprise directory contacts that match the search criteria in the Enterprise Directory area.

Avaya Call for Government populates the search results after running a query for the following fields:

- displayName
- mail

Avaya Call for Government uses the following fields to define the default call target and additional call targets:

- bussinessPhones
- mobilePhone

The call targets are available from the contact card of Office 365 enterprise directory results.

Adding Avaya Call for Government to Microsoft Teams Apps Store

Procedure

1. Open Microsoft Teams web client: https://gov.teams.microsoft.us/.

2. Click **Apps**.
3. Click **Upload a custom app** > **Upload for my org**.
4. In the File Upload dialog box, locate the manifest zip file and click **Open**.
5. In the Caution dialog box, select the check box after reading the terms and click **Agree**.

   Avaya Call for Government displays in the Apps menu for all users.

Avaya Workplace Client add-in for Microsoft Outlook

Avaya Workplace Client provides a new and improved Outlook add-in for desktop platforms that includes the following features:

- Add meeting details to an appointment.
- Start and join conferences from your calendar.
- Start a call from within Outlook to a contact using Avaya Workplace Client for Windows.

Additionally:

- You can add meeting invites on behalf of someone who has given you delegate access to their Exchange Calendar.
- You can automatically configure the meeting information for Avaya Workplace Client.
- The conferencing system provides the meeting invite templates for Avaya Equinox® Conferencing.
- Microsoft Windows IM Provider integration, which is optional, activates click-to-IM and presence in Outlook for Avaya Workplace Client contacts.

Note:

Microsoft Outlook add-in for web mail does not support calendar delegation and IM provider.

The Outlook add-in includes support for Avaya Spaces. Besides the existing capabilities, the Outlook add-in integrates the workflow from the existing Avaya Spaces Outlook add-in. You need to sign in to Avaya Spaces on Avaya Workplace Client to enable Avaya Spaces in the Outlook add-in.

By integrating with Avaya Spaces, you can use the Search feature to search for a meeting if multiple meetings are configured.

Microsoft Outlook requirements

- Microsoft Outlook add-in for Windows is supported on Exchange Server 2010 SP1 and later versions, including Office 365.
- Microsoft Outlook add-in for Mac and web mail is supported on Exchange Server 2013 and later versions, including Office 365.
- Internet access must be available because portions of the add-in are hosted on the Internet as a part of the new Avaya Workplace Client add-in for Microsoft Outlook architecture.
  If the add-in is hosted internally on the private network with the OUTLOOK_ADDON_HOST_URI configuration parameter, then Internet access is not required.

- To use the Delegate feature, you must be provided with delegate access to the calendars that you wish to access. Contact your IT department for assistance.

Avaya Workplace Client for Windows add-in for Microsoft Outlook installation

The Avaya Workplace Client for Windows add-in for Microsoft Outlook is installed by default.

To prevent the default installation on Avaya Workplace Client for Windows, select the **Custom** setup type in the interactive installer or use the silent install parameter. The add-in is also enabled by default for non-guest users.

To disable the Outlook add-in on Avaya Workplace Client for Windows, you can set the ENABLE_OUTLOOK_ADDON parameter to `0`. Alternatively, if you do not specify ENABLE_OUTLOOK_ADDON in LOCKED_PREFERENCES or OBSCURE_PREFERENCES, the user can manually disable the Outlook add-in from Avaya Workplace Client for Windows.

If the user reports that the Avaya Workplace Client for Windows add-in for Microsoft Outlook is automatically disabled after restarting Microsoft Outlook, you can check the values for the following attributes using the registry. If it is disabled, you must set the value to 1:

- Equinox.MSO.Addin value in Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\x.0\Outlook\Resiliency\DoNotDisableAddinList
- LoadBehavior value in Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\AddIns\Equinox.MSO.Addin

Avaya Workplace Client for Mac add-in for Microsoft Outlook installation

The Outlook add-in is not installed by default during the Avaya Workplace Client for Mac installation.

To add the Outlook add-in to Microsoft Outlook, you must authenticate Exchange Web Services and the Unified Portal in Avaya Workplace Client for Mac. You must restart Microsoft Outlook to view the Outlook add-in in your Microsoft Outlook.

Disabling the Avaya Workplace Client add-in for Microsoft Outlook by using the registry

Procedure

1. Open the Registry Editor window.
2. Go to **Computer** > **HKEY_CURRENT_USER** > **SOFTWARE** > **Microsoft** > **Office** > **Outlook** > **Addins** > **Avaya.Outlook.Addin**.
3. Set the value of **LoadBehavior** to `0`.

Avaya Workplace Client add-in for Microsoft Outlook hosted on customer web server

Supported clients

- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Equinox® Conferencing

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Automatic configuration settings

- SET ENABLE_OUTLOOK_ADDON 1
  ENABLE_OUTLOOK_ADDON must be set to 1 to enable the Avaya Workplace Client add-in for Microsoft Outlook.
- SET OUTLOOK_CALL_CONTACT 1

OUTLOOK_CALL_CONTACT must be set to 1 to enable click to call from the Avaya Workplace Client add-in for Microsoft Outlook. This parameter is only applicable for UC deployments. Disable this parameter for OTT deployments.

- SET OUTLOOK_ADDON_HOST_URI HTTPS://enterprise-FQDN/path/to/Addon
  OUTLOOK_ADDON_HOST_URI can be defined for enterprises that host the Avaya Workplace Client add-in for Microsoft Outlook files locally.

Hosting the Avaya Workplace Client add-in for Microsoft Outlook

About this task

By default, the Avaya Workplace Client add-in for Microsoft Outlook is an Avaya cloud-hosted Microsoft Outlook add-in. The Microsoft Outlook client downloads the add-in from the Internet during startup. Enterprises might choose to use this procedure to host the Avaya Workplace Client add-in for Microsoft Outlook in the enterprise environment.

Procedure

1. Download the latest package.
   For example, for release 3.33, from https://manage1.esna.com/workplace.mso/3.33.0/current.zip.
2. Create a workplace.mso folder on a web server that hosts the Avaya Workplace Client add-in for Microsoft Outlook files.
   The Web server does not have any special requirements. Only static files hosting and https are preferred.
3. Unzip the package content in the workplace.mso folder.
   The unzipped package includes a folder with the package version. For example, 3.33.0.4.
   After you deploy a new version of the Outlook add-in, the same workplace.mso folder includes the Outlook add-in.
4. Create a virtual directory that points to the location of the unzipped package.
   For example, https://somesite.intranet.dev/workplace.mso –> /data/workplace.mso/.
5. Check that you can load the manifest.xml file.
   For example, for release 3.33, open `https://somesite.intranet.dev/workplace.mso/3.33.0.4/manifest.xml`.
6. In the location where you downloaded and unzipped the package, edit the content of the manifest.xml file to replace https://manage1.esna.com/workplace.mso/ with the new location of the Avaya Workplace Client add-in for Microsoft Outlook.
   For example, `https://somesite.intranet.dev/workplace.mso`.

7. Update the Avaya Workplace Client configuration property OUTLOOK_ADDON_HOST_URI with the location of the Avaya Workplace Client add-in for Microsoft Outlook.

   For example, `https://somesite.intranet.dev/workplace.mso`.
8. **Optional** To support the OAuth authentication using the Microsoft Outlook add-in, perform the following. OAuth authentication is supported only in HTTPS.
   a. Move the token.redirect file from the unzipped package to the workplace.mso folder if the workplace.mso folder does not include the file.
   b. Edit the Identity Provider and Avaya Aura® Device Services keycloak settings and add the redirect.token URI to the valid redirect URIs list.

The default Avaya Equinox® Management server template includes two external references to images that are rendered in the meeting invitation. Perform the following steps to resolve issues that cause placeholders to be inserted instead of the actual images. If the customer does not use these images in the meeting invitation, you do not need to perform the following steps:

9. Download the following images:
   - branding.png: From https://manage1.esna.com/workplace.mso/img/branding.png
   - meeting.png: From https://manage1.esna.com/workplace.mso/img/meeting.png
10. Host the downloaded images within the customer network. For example:
    - `https://somehost.customer.com/workplace/img/branding.png`
    - `https://somehost.customer.com/workplace/img/meeting.png`

    You can host these images on the server used to host the Outlook extension files.
11. To replace the default branding and meeting pictures on the Avaya Equinox® Management server, go to **Settings** > **Invitations** and use the images hosted in Step 10.

Avaya Workplace Client add-in for Microsoft Outlook enhanced template

Avaya Equinox® Conferencing supports separate HTML and TEXT invitation templates. The HTML template is used by the Outlook plug-in and meeting scheduling to send email invitations. The TEXT template is used by Avaya Workplace Client to display the dialing information during a meeting.

Supported clients

- Avaya Workplace Client on desktop platforms

Supported servers

- Avaya Equinox® Conferencing

- Unified Portal
- Avaya Aura® Web Gateway

For information about the minimum supported versions, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Avaya Equinox® Management server configuration

Avaya Equinox® Management 9.1 CD6 supports the following new variables:

- [VIRTUAL_ROOM_NAME]
- [DESKTOP_MOBILE_ACCESS_LINK]

Existing variables supported on Avaya Equinox® Management 9.0.2 or before 9.1 CD6 include:

- [MEETING_ID]
- [PIN]
- [E164]

Customizing the email template

About this task

Use this procedure to customize the email template provided by the Avaya Workplace Client add-in for Microsoft Outlook.

Procedure

1. Replace the example bridge numbers and location labels with the appropriate information.

If the simple custom logo is configured, you can replace the default logo location in the HTML template with the custom logo stored on the User Portal.

2. **Optional** Discover the custom logo URL by browsing to one of the following links and the **customLogo** field:
   - https://alphaconfportal.avaya.com:8443/ups/resources/tenants/default/
   - https://alphaconfportal.avaya.com:8443/ups/resources/tenants/{tenantAlias}/
3. **Optional** For a single tenant deployment, the URL can be one of the following:

   - https://alphaconfportal.avaya.com:8443/portal/custom-styles/999/customLogo.svg
   - https://alphaconfportal.avaya.com:8443/portal/custom-styles/999/customLogo.png

4. **Optional** For a multi-tenant deployment, the URL can be one of the following:
   - https://alphaconfportal.avaya.com:8443/portal/custom-styles/{tenantID}/customLogo.svg
   - https://alphaconfportal.avaya.com:8443/portal/custom-styles/{tenantID)/customLogo.png
5. **Optional** To use an invitation template other than the default English language, you can download the localized invitation template files.

Configuration for Avaya Equinox Conferencing

You must configure the following parameters for Avaya Equinox® Conferencing :

- CONFERENCE_ACCESS_NUMBER
- CONFERENCE_PORTAL_URI

Avaya recommends the use of Avaya Aura® Device Services to provide per-user configuration parameters. Else, end users need to manually update the Avaya Workplace Client settings in **Services** > **Meetings**.

External dependencies

The Avaya Workplace Client add-in for Microsoft Outlook runs in a sandbox, that is, no access to the file system. The add-in template is hosted centrally in the cloud as a hosted service. As such, the Avaya Workplace Client add-in for Microsoft Outlook requires access to the domain manage1.esna.com using the HTTPS protocol.

Set up appropriate firewall rules in the enterprise to allow access to this domain. You can confirm whether the domain is accessible by using a web browser and the following URL: `https://manage1.esna.com/workplace/manifest.xml`. If the XML file loads into the browser, then there is connectivity to the external domain.

Avaya URI

Avaya provides many URI formats that third-party applications can use. Avaya supports the following verbs as part of the URI:

- Audio calls
- Video calls
- Instant messaging
- Configuration

By using Avaya URIs, third-party applications can direct Avaya Workplace Client to:

- Create an audio call.
- Create a video call.
- Create a conference call.
- Create a new or open an existing conversation.
- Update the automatic configuration URL.

Note:

Avaya Workplace Client for Windows also supports the tel and CallTo URIs. For example, tel:`+16135959132` and CallTo:`+16135959132`. If the user clicks on these URIs in a browser or elsewhere, the call is dialed immediately after choosing the default application.

Avaya URIs have the following format with optional parameters: avaya://verb?address&parm1=value1&parm2.

Verb	Android - Mobile	Android - Vantage	iOS	Mac	Windows
Call	Yes	Yes	Yes	Yes	Yes
Video	Yes	Yes	Yes	Yes	Yes
Message	No	No	No	Yes	Yes
Config	Yes	No	Yes	Yes	Yes

All platforms do not support all Avaya URI parameters. If you provide an unsupported parameter within the Avaya URI, Avaya Workplace Client ignores the parameter but continues to invoke the verb. The verb invocation is only one-way because Avaya Workplace Client does not provide status updates to the third-party application.

Note:

Android does not detect any custom URIs, such as non-global URIs, in emails and text messages. On Android, you must create custom URIs as HTML or web pages so that the URIs are clickable, and Avaya Workplace Client for Android initiates the desired action.

Application integration

Avaya Workplace Client uses Avaya URIs for many of its own solution components. This ensures that Avaya URIs utilization is a stable construct for you to build your own integration into Avaya Workplace Client.

Avaya URI purpose

URIs are a universally understood construct for developers and can be implemented consistently across many operating systems. URIs are simple, open, and interoperable. You can easily append data and parameters to Avaya URIs to provide additional context from the calling application to Avaya Workplace Client. URIs can be read by humans, which makes adoption simple and debugging straightforward.

A key aspect of Avaya URIs is that the verb passed to Avaya Workplace Client renders in the Avaya Workplace Client application. This makes the integration simple without the need to review log files for detailed integration.

URI encoding

In some cases, parameter values might require a special encoding, often referred to as Percent-Encoding. Percent-Encoding might not be necessary for most Avaya URI invocations. The following table contains a list of some of the reserved characters that must be percent-encoded:

Character	Escape code
Space	%20
<	%3C

Character	Escape code
>	%3E
?	%3F
@	%40
=	%3D
$	%24

URI for audio and video calls

URI for audio and video calls

In the Avaya URI for audio or video calls, the primary parameter is the phone number that you want to dial. The phone number is subjected to the Avaya Workplace Client dialing rules configuration, if enabled.

As phone numbers vary across sites and regions, local numbers might not work for all Avaya Workplace Client platforms. Use international format numbers. Do not use phone number formatting characters such as hyphens, dashes, and brackets.

While many web browsers automatically detect phone numbers and convert the numbers to links, it is safer if you do the conversion directly in the code. By linking each phone number, you can ensure that phone numbers are always enabled for click-to-call and the Avaya URI style matches your site.

The generalized Avaya URI format for calls is avaya://[video|call]?<phonenumber>.

Avaya URI embedded in a web page for calls

```
Telephone Service
```

<a href="avaya://call?+123456789123451">+1 (234) 567-8912</a>

<a href="avaya://video?+123456789123451">+1 (234) 567-8912</a>

Your browser displays the following links:

avaya://call?+123456789123451

avaya://video?+123456789123451

Invoking an Avaya URI for calls

Procedure

- To test your URI on a Microsoft Windows workstation, invoke the following commands in a command window or from the start menu:
  - `start avaya://call?+12345678912`
  - `start avaya://video?+12345678912`
- To test your URI on an Apple Macintosh workstation, invoke the following command in a command shell:
  - `open avaya://call?+12345678912`
  - `open avaya://video?+12345678912`

Optional parameter for audio and video

Parameter	Value	Description
CallbackURL	UTF-8 string	Avaya Workplace Client can invoke a callback when the call is dialed. Callback is invoked if the call succeeds or fails. The callback handler must be registered on the operating system. The Callback URL might be a standard URL, such as http, https, mailto, or an application custom URL. The Callback URL allows flow control to be passed back to the invoking application. This parameter is not supported on all platforms.

Avaya URI for audio calls and conference

Third-party applications can use the following Avaya URI formats to direct Avaya Workplace Client to create an audio call and conference:

Note:

If you want to make an audio conference call by using the custom URI and Avaya Equinox® Conferencing, you must include the meeting ID in the URI.

Scenario	Example and result
Avaya URI with valid number	avaya://call?+912012345678 Avaya Workplace Client dials the call by applying the existing dialing rules.
Avaya URI with valid number appended with CallBack URL	avaya://call?+912012345678&callbackURL=http://www.google.com Avaya Workplace Client dials the call by applying the existing dialing rules, and the callback URL opens in the default browser.
Avaya URI with valid conference access number appended with meeting ID	avaya://call?+98765432198&MeetingId=123451234512345 Avaya Workplace Client dials the call to the conference with the meeting ID.
Avaya URI with valid conference access number appended with meeting passcode	avaya://call?+7654321&MeetingPasscode=7651234 Avaya Workplace Client dials the call to the conference with the meeting passcode.
Avaya URI with valid conference access number appended with meeting ID and meeting passcode	avaya://call?+98765432198&MeetingId=123451234512345&MeetingPasscode=1234 Avaya Workplace Client dials the call to the conference with the meeting ID and passcode.

Scenario	Example and result
Avaya Workplace Client is not running Avaya URI with valid conference access number appended with meeting ID and meeting passcode	avaya://call?+98765432198&MeetingId=123451234512345&MeetingPasscode=1234 Avaya Workplace Client starts, and the configured user is logged in automatically. Avaya Workplace Client dials the call to the conference with the meeting ID and passcode.

Avaya URI for video calls and conference

Third-party applications can use the following Avaya URI formats to direct Avaya Workplace Client to create a video call and conference:

Note:

If you want to make a video conference call by using the custom URI and Avaya Equinox® Conferencing, you must include the meeting ID in the URI.

Scenario	Example and result
Avaya URI with video to a valid number	avaya://video?+912012345678 Avaya Workplace Client dials the video call by applying the existing dialing rules.
Avaya URI with video to a valid number appended with CallBack URL	avaya://video?+912012345678&callbackURL=http://www.google.com Avaya Workplace Client dials the video call by applying the existing dialing rules, and the callback URL opens in the default browser.
Avaya URI with video to a valid conference access number appended with meeting ID	avaya://video?+98765432198&MeetingId=123451234512345 Avaya Workplace Client dials the video call to the conference with the meeting ID.

Scenario	Example and result
Avaya URI with video to a valid conference access number appended with meeting passcode	avaya://video?+7654321&MeetingPasscode=7651234 Avaya Workplace Client dials the video call to the conference with the meeting passcode.
Avaya URI with video to a valid conference access number appended with meeting ID and meeting passcode	avaya://video?+98765432198&MeetingId=123451234512345&MeetingPasscode=1234 Avaya Workplace Client dials the video call to the conference with the meeting ID and passcode.
Avaya Workplace Client is not running Avaya URI with video to a valid conference access number appended with meeting ID and meeting passcode	avaya://video?+98765432198&MeetingId=123451234512345&MeetingPasscode=1234 Avaya Workplace Client starts, and the configured user is logged in automatically. Avaya Workplace Client dials the video call to the conference with the meeting ID and passcode.

URI for instant messaging

URI for instant messaging

In the Avaya URI format for messaging, the primary parameter is the comma-delimited list of participant addresses to a message. If a participant address is not reachable by Avaya Workplace Client, the address is not added to the conversation. If the Avaya Workplace Client messaging provider does not support multi-party instant messaging, only the address of the first participant is added to the conversation.

The generalized Avaya URI format for messaging is avaya://message?participantAddress1,participantAddress2,...&subject=Sample%20%Subject.

Avaya URI embedded in a web page for messaging

```
Support Service
Telephone Service
```

<a href="avaya://message?support@example.com">support@avaya.com</a>

Invoking an Avaya URI for messaging

Procedure

- To test your URI on a Microsoft Windows workstation, invoke the following command in a command window or from the start menu:
  `start avaya://message?support@avaya.com`
  .
- To test your URI on an Apple Macintosh workstation, invoke the following command in a command shell:
  ```
  open
                        avaya://message?support@avaya.com
  ```
  .

Optional parameters for messaging

Parameter	Value	Description
Subject	UTF-8 string, with html escapes.	The conversation subject is created or opened if the subject conversation with matching participants is found.
MessageBody	UTF-8 string, with html escapes.	The message body is inserted into the message dialog window. The actual message is not sent until the Avaya Workplace Client user invokes send. This parameter is not supported on all platforms.

Avaya URI for messaging

Third-party applications can use the following Avaya URI formats to direct Avaya Workplace Client on desktop platforms to create a new conversation or open an existing conversation:

Scenario	Example and result
Avaya URI with a single valid messaging address	avaya://message?abc@avaya.com Avaya Workplace Client checks whether there is an existing conversation with the contact. • If an existing conversation is available, Avaya Workplace Client opens the existing conversation with the specified contact. • If an existing conversation is unavailable, Avaya Workplace Client creates a new conversation with the specified contact.
Avaya URI with two or more valid messaging addresses	avaya://message?abc@avaya.com,xyz@avaya.com Avaya Workplace Client checks whether there is an existing conversation with the two contacts. • If an existing conversation is available, Avaya Workplace Client opens the existing conversation with the two specified contacts. • If an existing conversation is unavailable, Avaya Workplace Client creates a new multiparty conversation with the two specified contacts.
Avaya URI with two or more valid messaging addresses appended with subject	avaya://message?abc@avaya.com,xyz@avaya.com&subject=Test%20%Subject

Scenario	Example and result
	Avaya Workplace Client checks whether there is an existing conversation with the two contacts for the specified subject. • If an existing conversation is available, Avaya Workplace Client opens the existing conversation with the two specified contacts with the matching subject. • If an existing conversation is unavailable, Avaya Workplace Client creates a new multiparty conversation with the two specified contacts for the specified subject.
Avaya URI with two or more valid messaging addresses appended with subject and message body	avaya://message?abc@avaya.com,xyz@avaya.com&subject=Test%20%Subject&MessageBody="Message Body Sample" Avaya Workplace Client checks whether there is an existing conversation with the two contacts for the specified subject. • If an existing conversation is available, Avaya Workplace Client opens the existing conversation with the two specified contacts with the matching subject. The opened conversation must have the provided message body text. • If an existing conversation is unavailable, Avaya Workplace Client creates a new multiparty conversation with the two specified contacts for the specified subject and message body text.
Avaya URI with two or more valid messaging addresses appended with subject and message body and CallBack URL	avaya://message?abc@avaya.com,xyz@avaya.com&subject=Test%20%Subject&MessageBody="Message Body Sample"&callbackURL=http://www.google.com

Scenario	Example and result
	Avaya Workplace Client checks whether there is an existing conversation with the two contacts for the specified subject. • If an existing conversation is available, Avaya Workplace Client opens the existing conversation with the two specified contacts with the matching subject. The opened conversation must have the provided message body text. The callback URL opens in the default browser after the message is sent. • If an existing conversation is unavailable, Avaya Workplace Client creates a new multiparty conversation with the two specified contacts for the specified subject and message body text. The callback URL opens in the default browser after the message is sent.

URI for configuration

URI for configuration

You can use the Avaya URI to provide a configuration URI to the Avaya Workplace Client user, which the user can use to update the Avaya Workplace Client configuration. Optionally, the Avaya Workplace Client application might be reset. During the application reset, the existing configuration is cleared and the configuration is updated. This is useful for administrative and support personnel to assist their customers with initial configuration or correcting existing configurations. The Avaya Workplace Client user must always confirm the configuration activity.

The generalized Avaya URI format for configuration is avaya://config?ConfigURL.

Avaya URI for automatic configuration

Third-party applications can use the following Avaya URI formats to direct Avaya Workplace Client to update the automatic configuration URL:

Scenario	Example and result
Avaya URI with configuration URL	`avaya://config?https://alphablue-aadscluster.avaya.com:8443/acs/resources/configurations` Avaya Workplace Client displays a dialog to the user indicating that a configuration update is available. The user can choose to configure the application or cancel the configuration update.
Avaya URI with configuration URL for OAuth2 clients	`avaya://config?https://alphablue-aadscluster.avaya.com:8443/acs/resources/configurations&PreferredAuth=bearer` Avaya Workplace Client displays a dialog to the user indicating that a configuration update is available. The user can choose to configure the application or cancel the configuration update.
Avaya URI with configuration URL appended with the reset parameter	`avaya://config?https://alphablue-aadscluster.avaya.com:8443/acs/resources/configurations&reset` Avaya Workplace Client displays a dialog to the user indicating that a configuration update is available. The user can choose to reset the application to a new install state and then configure the application, or cancel the configuration update.
Avaya URI with configuration URL for OAuth2 clients appended with the reset parameter	`avaya://config?https://alphablue-aadscluster.avaya.com:8443/acs/resources/configurations%26PreferredAuth%3DBearer&reset` Avaya Workplace Client displays a dialog to the user indicating that a configuration update is available. The user can choose to reset the application to a

Scenario	Example and result
	new install state and then configure the application, or cancel the configuration update.

Troubleshooting, interoperability limitations, system artifacts, and call statistics

Login issues

Users cannot log in to Avaya Workplace Client

Condition

In an Avaya Workplace Client deployment that includes Session Border Controller, the user might see the following error message while trying to log in: `Invalid extension and password`.

Solution

Procedure

Set up the user-agent string correctly in Session Border Controller.
For more information, see *Administering Avaya Session Border Controller*.

Users cannot log in to the Desk Phone mode

User Alert

Avaya Workplace Client users cannot log in to the Desk Phone mode.

Logs/Alarms

The system displays the following error:

```
403 Endpoint Routing
Forbidden.
```

Recovery Action

Procedure

1. Log in to Avaya Aura® Session Manager.
2. In the **Session Manager Administration** tab, enable **Direct Routing to Endpoints**.
3. In the **Max. Simultaneous Devices** field of the Session Manager communication profile section of the User Profile page, set the value to 2 or higher.
4. To complete user configuration, check the following:
    a. Avaya Aura® Session Manager profile and endpoint profile on Avaya Aura® System Manager.
    b. *Station profile*, *aar analysis*, *trunk group*, *signaling group*, and *numbering plan* on Avaya Aura® Communication Manager.

    The extension range for the numbering plan must follow the same numbering format that is configured for the trunk group. For more information about user configuration, see *Administering Avaya Aura® Session Manager* and *Administering Avaya Aura® Communication Manager.*

Users cannot use Avaya Workplace Client for Android to log in to Client Enablement Services when using Avaya SBC

Cause

Avaya SBC uses a strong cipher suite. Except for Client Enablement Services, users can log in to all services when using Avaya SBC.

Solution

Procedure

As Client Enablement Services does not support strong cipher suites, you must align the cipher suite configuration across all elements of the solution.

Delay while logging into Avaya Workplace Client in the Desk Phone mode in a Citrix environment

Cause

The URL for Certificate Revocation List validation is unreachable or timed out when the Windows API validates the certificate revocation lists.

Solution

Procedure

Ensure that the URL for Certificate Revocation List validation is accessible and not timed out.

Credential information

Windows system saves your login credentials for Avaya Workplace Client for Windows in Credential Manager. You can access Credential Manager from **Control Panel** > **User Accounts**. When you uninstall Avaya Workplace Client for Windows, the uninstallation process removes your credential information.

Mac system saves your login credentials for Avaya Workplace Client for Mac in **Keychain Access** > **Keychains** > **login**. You can access Keychain Access from **Applications** > **Utilities**. When you uninstall Avaya Workplace Client for Mac, the uninstallation process removes your credential information.

Audio and video issues

Audio is lost for a few seconds during a call

Cause

Opening and closing other applications on your device during a call results in audio loss for a few seconds.

Solution

Procedure

Workaround is unavailable.

Video functionality is inconsistent across mobile clients

Condition

During a video call on mobile platforms, when you put Avaya Workplace Client in the background:

- Video freezes on the far-end iOS device.
- Video works fine on the far-end Android device.

Cause

When Avaya Workplace Client is in the background, due to platform limitations with iOS, Avaya Workplace Client does not have access to the camera.

Solution

Procedure

Workaround is unavailable.

Call history issues

User can view incorrect call name in native call history

Condition

There are two users, A and B. B has A as a local contact on the iOS device.

1. A calls B.

   On the iOS device of B, the call history displays a name different than the contact name provided by Avaya Workplace Client for iOS.

Cause

The native CallKit prefers a local contact name instead of the application contact name. Hence, if the user has local contacts on the iOS device, the local contact names are used for incoming calls and native call history entries.

Solution

Procedure

1. B must remove A from local contacts.

2. B must add A as a Workplace contact in Avaya Workplace Client for iOS.

User can view incorrect log entry in native call history

Condition

There are two users, A and B. A uses MDA and logs in to more than one Avaya Workplace Client simultaneously.

1. B calls A.

   A answers the incoming call on Avaya Workplace Client for Mac.

2. B ends the outgoing call.

3. A checks the call logs on the iOS device.

   Avaya Workplace Client for iOS displays the call log as an incoming call. However, the iOS native call log displays a missed call.

Solution

Procedure

Avaya confirms that this functionality is as intended.

Avaya uses the Apple CallKit framework for call handling. Hence, the call log is created automatically in the native iOS history as a missed call as user A did not answer the incoming call on the iOS device.

Contact issues

Avaya Workplace Client does not display photos for some Microsoft Outlook local contacts

Cause

This is a known Outlook issue. This issue occurs due to a problem with the Outlook connection protocol.

Solution

Procedure

Workaround is unavailable.

Avaya Workplace Client does not display the user’s self-picture

Condition

The user's self-picture is available in Avaya Aura® Device Services. However, Avaya Workplace Client does not display the user’s self-picture.

Cause

Without WebSocket support, the contact resolution does not work. With WebSocket support, Avaya Workplace Client sends a request to Avaya Aura® Device Services to retrieve the self-picture.

Solution

Add WebSocket support on Avaya Session Border Controller.

Avaya Workplace Client for iOS displays local contact details for an incoming call instead of aggregate contact details

Condition

If iOS CallKit is enabled, Avaya Workplace Client for iOS displays local contact details for an incoming call instead of aggregate contact details.

Cause

Apple confirms that this functionality is as intended. Apple intentionally prioritizes by showing a user local contact card information for a caller over the caller information given by CallKit if there is a contact card.

Solution

Procedure

Workaround is unavailable.

Avaya Workplace Client for iOS displays the contact name as nickname on the New Contact screen

Condition

If you create a new Avaya Workplace Client contact from your call history, the **Nickname** field on the New Contact screen is automatically populated with the contact name.

Cause

The call history details include the display name and phone number. In iOS, the display name and nickname are considered the same. Hence, the nickname is automatically populated with the display name.

Solution

Procedure

Workaround is unavailable.

Miscellaneous issues

Users receive two notifications for group and team button calls

Cause

If users use Avaya Workplace Client on a device with iOS 13 or an earlier version, for group and team button calls, the device displays extra notifications.

Solution

Procedure

To avoid viewing these extra notifications, users must use iOS 13.2 or a later version.
Avaya Workplace Client uses the notifications filtering entitlement that Apple provides with iOS 13.2 and later versions to fix the issue of the extra notifications.

Presence status on the team button is not working for some users

Condition

Avaya Workplace Client displays offline presence status on the team button for some users.

Cause

If a contact name is unresolved through Avaya Aura® Device Services, the team button does not display the presence for that contact.

Solution

Procedure

Ensure that the network connection and name resolution from Avaya Aura® Device Services is working correctly.

Avaya Workplace Client does not register to Session Manager

Cause

If the following conditions exist, Avaya Workplace Client will not get PPM data as the user does not exist on Session Manager 1:

- On System Manager, user profile has single Session Manager 2 entry.
- On Avaya Workplace Client, in the Phone Service area, Session Manager 1 IP address or FQDN is mentioned manually or using the settings file.

Solution

Procedure

Do one of the following:

- Add the correct Session Manager details in the settings file for automatic configuration.

- Ask the user to type the correct IP address or FQDN in the Phone Service area of Avaya Workplace Client.

Remote users can view the Phone Service is currently limited error

Condition

In an Avaya Workplace Client deployment that includes Session Border Controller, remote users might receive the following error message: `Phone service is currently limited, you can still make and receive calls`.

Solution

Procedure

- On Session Border Controller, do the following:
  1. Configure the PPM mapping profile and Presence server address correctly for the SIP telephony features, presence, and PPM contacts to work.
  2. Ensure that the SIP, port number 5061, and PPM, port number 443, interfaces are configured to use the same certificate.
     Often, the SIP interface is configured to use a third-party certificate, but the PPM interface uses the demo certificate.

- On Communication Manager, in the Private-Numbering table, ensure that the SIP extension range is mapped to the SIP trunk of Session Manager. If it is not mapped, Avaya Workplace Client cannot subscribe to the full telephony services.

Android device setting changes automatically from the silent and vibrate mode to the general mode

Condition

On some Android devices, for incoming and outgoing VoIP calls, the device setting changes automatically from the silent and vibrate mode to the general mode.

Solution

Procedure

Workaround is unavailable.

Unable to dial Avaya Aura Messaging extension to read messages in a dual stack IPv6 network

Condition

Avaya Workplace Client is configured as a dual stack network. The Avaya Aura® Messaging extension supports IPv6.

Cause

Avaya Aura® Messaging does not support ANAT. Hence, Communication Manager drops the call.

Solution

Procedure

Workaround is unavailable.

Avaya Workplace Client call stops responding when you uninstall QoS from network settings

Condition

1. In Network Connections, go to the properties of your network connection.
2. In the Networking tab, select **QoS Packet Scheduler**.
3. Click **Uninstall**.

4. Make a call using Avaya Workplace Client for Windows.

   When the call is answered at the other end, the call stops responding.

Cause

The QoS Packet Scheduler is required for Avaya Workplace Client for Windows to function properly.

Solution

Do not uninstall any run-time dependencies such as QoS Packet Scheduler while using Avaya Workplace Client for Windows.

Media preserved call is not dropped when you answer a cellular call

Condition

When you are on a VoIP call and Session Manager becomes unreachable, the VoIP call becomes unreachable. At the same time, you receive an incoming cellular call.

When you end the cellular call, the media preserved call is still active and not dropped. The media preserved call should have ended.

Solution

Procedure

Workaround is unavailable.

Users cannot join a scheduled conference

Cause

This issue can occur due to any of the following reasons:

- The conference bridge was not cleared or dropped from the previous call.

- One of the participants did not end the meeting. Hence, the bridge remains active for that virtual room.

Solution

On the Avaya Equinox® Management server, in Advanced Parameters, set a value in seconds for the vnex.vcms.core.conference.timeToCloseConfWithOneEP property.

For example, `600`, that is, 10 minutes. Avaya Workplace Client ends the conference call after 10 minutes if only one participant remains in the conference call.

The Web Collaboration window displays a shared document on another conference

Condition

This condition might occur in the following situations:

- You are the moderator on a MeetMe conference and you start web collaboration.
- While the MeetMe conference and web collaboration are active, you start an Adhoc conference and then start a second web collaboration session for the same call.

Solution

Procedure

Workaround is unavailable.

Connecting to a protocol sniffer

About this task

You cannot run a protocol sniffing tool such as Wireshark directly on mobile devices. Use this procedure so that Avaya Workplace Client for Android and iOS can connect to and support Wireshark. Use such tools to capture network traces associated with the VoIP service.

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.

Interoperability limitations

Known interoperability limitations

Interoperability limitations exist between Avaya Workplace Client and other products.

The following are examples of limitations that occur when you use Avaya one-X® Mobile and Avaya Workplace Client:

- Call logs are inconsistent between Avaya one-X® Mobile and Avaya Workplace Client.
- When you add contacts in Avaya one-X® Mobile, the contacts do not appear in Avaya Workplace Client.

Similar limitations might also exist between Avaya Workplace Client and other products.

Interoperability and limitations with voice mail privacy enforcement

The Client Enablement Services server and Avaya Workplace Client have a limitation with respect to private voice mail. If you configure the Messaging service for voice mail-style privacy, voice mail messages do not contain the voice mail attachment. Hence, the user cannot play the audio for the voice mail message using Avaya Workplace Client.

The Client Enablement Services server and Avaya Workplace Client 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 Workplace Client.

File system artifacts

Avaya Workplace Client for Windows file system artifacts

Avaya Workplace Client for Windows uses the following directories to save application data:

- %APPDATA%/Avaya/Avaya IX Workplace/configdata.xml: Removing configuration data causes Avaya Workplace Client to reacquire configuration the next time you start the application. Configuration data files are managed by the Avaya Workplace Client application and do not require additional administration.
- %APPDATA%/Avaya/Avaya IX Workplace/CallLogs: Removing call logs removes call history from the Avaya Workplace Client application. Call log data is not restored the next time you start the application.
- %LOCALAPPDATA%/Avaya/Avaya IX Workplace/logs: Removing runtime logs affects supportability of Avaya Workplace Client. Runtime logs are managed by the Avaya Workplace Client application and do not require additional administration.
- %LOCALAPPDATA%/Avaya/Avaya IX Workplace/Dumps: Crash dump files are not managed by the Avaya Workplace Client application and must be managed by you. For support, you might need to send these files to Avaya.
- %LOCALAPPDATA%/Avaya/Avaya IX Workplace/preferences_local.xml: Local preferences include devices and their gains, last window position, a call mode, and default URI handler.

  ⚠ **Caution:**

  Many Citrix deployments use administrative policies that clear the local AppData folder periodically. In such cases, all local preferences are restored to their default values.
- %APPDATA%/Avaya/Avaya IX Workplace/preferences_roaming.xml: Roaming preferences include the user preferences not included in local preferences.

When the user uninstalls Avaya Workplace Client for Windows, the uninstallation process does not remove the application data from the associated directories. After uninstalling Avaya Workplace Client for Windows, you or the user must delete the %APPDATA% folders.

Avaya Workplace Client for Mac file system artifacts

Avaya Workplace Client for Mac uses the following directories to save application data:

- ~/Library/Application Support/com.avaya.Avaya-IX-Workplace/configdata.xml: Removing configuration data causes Avaya Workplace Client to reacquire configuration the next time you start the application. Configuration data files are managed by the Avaya Workplace Client application and do not require additional administration.
- ~/Library/Application Support/com.avaya.Avaya-IX-Workplace/callLogs: Removing call logs removes call history from the Avaya Workplace Client application. Call log data is not restored the next time you start the application.
- ~/Library/Logs/com.avaya.Avaya-IX-Workplace/logs: Removing runtime logs affects supportability of Avaya Workplace Client. Runtime logs are managed by the Avaya Workplace Client application and do not require additional administration.
- ~/Library/Logs/com.avaya.Avaya-IX-Workplace/logs/crashes: Crash dump files are not managed by the Avaya Workplace Client application and must be managed by you. For support, you might need to send these files to Avaya.
- ~/Library/Preferences/com.avaya.Avaya-Equinox.plist: Preferences include devices and their gains, last window position, a call mode, and default URI handler.

When you uninstall Avaya Workplace Client for Mac, the uninstallation process removes the application data from the associated directories.

Call statistics

While on an active call, you can view the call statistics on Avaya Workplace Client. Use the call statistics to analyze and troubleshoot network issues that might affect the call.

The following sections include call statistics information on audio, video, and collaboration depending on the call type.

Call statistics — Audio details

Represents details of transmitted and received audio stream properties.

Attribute name	Description
Codec	The name of the codec that is being used for the audio session.
Packetization Millis	The packetization interval in milliseconds. This represents the duration of the audio data contained in each packet. It is retrieved from the ptime attribute from the SDP audio codec config.
RFC2833 Payload Type	The payload type negotiated for telephony events (DTMF tones).
Local IP Address	The local IP address used to receive audio packets from the far-end.
Remote IP Address	The remote IP address used to send audio packets to the far-end.
Local Port	The local RTP receive port for the audio session according to SDP offer and answer exchange.
Remote Port	The remote RTP receive port for the audio session according to SDP offer and answer exchange.
Encryption Type	The encryption type used for the audio session.

Attribute name	Description
Media Tunneled	The status indication for whether there is audio tunneling.
RTCP Encrypted	The RTCP encryption status of the audio session. The value is true if feedback RTCP packets are encrypted. Else the value is false. If it is true, RTCP packets must be decrypted before reading audio stream details.
Round Trip Time Millis	The round-trip audio delay in milliseconds calculated according to RFC 3550. This is the time required for an RTP packet to go from sender to receiver and back.
Packets Transmitted	The total number of RTP packets transmitted.
Packets Received	The total number of RTP packets received.
Bytes Transmitted	The total number of RTP payload bytes transmitted.
Bytes Received	The total number of RTP payload bytes received.
Fraction Lost Local	The fractional loss seen locally. This is an 8-bits size value. This is the fraction of RTP data packets from source that got lost since the previous SR or RR packet was sent. The loss is expressed as a fixed point number with the binary point at the left edge of the field. This is equivalent to taking the integer part after multiplying the loss fraction by 256. This fraction is defined as the number of packets lost divided by the number of packets expected. If the loss is negative due to duplicates, the fraction lost is set to zero.

Attribute name	Description
Fraction Lost Remote	The fractional loss seen remotely, which the far end sends to the local end through RTCP. This is an 8-bits size value. This is the fraction of RTP data packets from source that got lost since the previous SR or RR packet was sent. The loss is expressed as a fixed point number with the binary point at the left edge of the field. This is equivalent to taking the integer part after multiplying the loss fraction by 256. This fraction is defined as the number of packets lost divided by the number of packets expected. If the loss is negative due to duplicates, the fraction lost is set to zero.
Average Jitter Local Millis	The average jitter buffer size in milliseconds that the local end is experiencing on a received RTP stream. In VoIP, a jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called jitter, can occur because of network congestion, timing drift, or route changes. The jitter buffer, which is located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion.
Average Jitter Remote Millis	The average jitter buffer size in milliseconds that the far-end is experiencing. In VoIP, a jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called jitter, can occur because of network congestion, timing drift, or route changes. The jitter buffer, which is located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion.
Current Buffer Size	The current jitter buffer size in milliseconds.

Attribute name	Description
	In VoIP, a jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called jitter, can occur because of network congestion, timing drift, or route changes. The jitter buffer, which is located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion.
Preferred Buffer Size	The preferred or optimal jitter buffer size in milliseconds. In VoIP, a jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called jitter, can occur because of network congestion, timing drift, or route changes. The jitter buffer, which is located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion.
Current Packet Loss Rate	The rate of percentage packet loss because of network and late packets.
Current Discard Rate	The rate of percentage packet loss because of late packets.
Current Expand Rate	The fraction of synthesized speech frames inserted through expansion in the total frame count in buffer. In case of a starved jitter buffer, synthesized speech frames are added. This process is called expand.
Current Preemptive Rate	The fraction of synthesized speech frames inserted through pre-emptive expansion in the total frame count in buffer.

Attribute name	Description
	In case of a shallow jitter buffer, synthesized speech frames are added. This process is called pre-emptive expand and is based on previous frames.
Current Accelerate Rate	The fraction of data removed through acceleration. In case of a full jitter buffer speech, frames are deleted. This process is called acceleration.

Call statistics — Video statistics

Represents detailed statistics of a video call.

Attribute Name	Description
Target Frame Rate	The target sent and received frame rate in frames per second.
Actual Frame Rate	The actual sent and received frame rate in frames per second.
Resolution Width	The width of the sent and received video stream.
Resolution Height	The height of the sent and received video stream.
Jitter Buffer Size Millis	The actual sent and received side jitter buffer size in milliseconds. In VoIP, a jitter buffer is a shared data area where video packets can be collected, stored, and sent to the video processor in evenly spaced intervals. Variations in packet arrival time, called jitter, can occur because of network congestion, timing drift, or route changes. The jitter buffer, which is located at

Attribute Name	Description
	the receiving end of the video connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very few video delays.
Target Bit Rate	The target sent and received bit rate per second.
Actual Bit Rate	The actual sent and received bit rate per second.
Packet Count	The total number of packets sent and received.
Byte Count	The total number of bytes sent and received.
Key Frame Count	The number of key frames locally requested (receive direction) or remotely requested (send direction).
Packet Loss Total	The total number of packets lost in transmit and receive direction.
Packet Loss Fraction	The fraction of packets lost in transmit and receive direction.

Call statistics — Video transmission statistics

Represents detailed transmission statistics of a video call.

Attribute name	Description
802.1p Tag	The 802.1p Layer 2 priority tag if set

Attribute name	Description
DSCP Tag	The DSCP tag if set

Call statistics — Collaboration statistics

Transmission statistics.

Attribute name	Description
Resolution Width	The frame resolution width. If the value is undefined, -1 is returned.
Resolution Height	The frame resolution height. If the value is undefined, -1 is returned.
Actual Frame Rate	The actual frame rate. If the value is undefined, -1 is returned.
Codec	The codec type used in collaboration data sharing. If the value is undefined, -1 is returned.
Round Trip Time Milliseconds	The packets round trip time in milliseconds. If the value is undefined, -1 is returned.
Actual Bit Rate	The actual bit rate used during data sharing. If the value is undefined, -1 is returned.

Attribute name	Description
Target Bit Rate	The target bit rate setting. If the value is undefined, -1 is returned.
Jitter Milliseconds	The average jitter in milliseconds. If the value is undefined, -1 is returned.
Packet Loss Count	The lost packets count. If the value is undefined, -1 is returned.
Packet Loss Percentage	The percentage of lost packets. If the value is undefined, -1 is returned.

Call statistics — Collaboration receive statistics

Received statistics with additional three values received from Web Collaboration Server.

Attribute name	Description
Frame Count	The received frame count. If the value is undefined, -1 is returned.
Frame Loss Percentage	The frame loss percentage. If the value is undefined, -1 is returned.
Queue Size	The receiving frame queue size. If the value is undefined, -1 is returned.

Resources

Documentation

See the following documents at http://support.avaya.com.

Table 1: Avaya Workplace Client, Avaya Multimedia Messaging, Avaya Aura® Device Services, and Avaya Workplace VDI documentation

Title	Use this document to	Audience
Overview		
Avaya Workplace Client Overview and Specification for Android, iOS, Mac, and Windows	Understand high-level product functionality, performance specifications, security, and licensing.	Customers and sales, services, and support personnel
Avaya Workplace VDI Overview and Planning	Understand high-level product functionality, security, and licensing. Also, perform deployment planning.	• System administrators • Customers and sales, services, and support personnel
Planning		
Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows	Perform system planning and configuration for: • Avaya Workplace Client for Android • Avaya Workplace Client for iOS • Avaya Workplace Client for Mac • Avaya Workplace Client for Windows	• System administrators • Customers and sales, services, and support personnel

Title	Use this document to	Audience
Avaya Multimedia Messaging Reference Configuration	Understand technical overview information, system architecture, functional limitations, and capacity and scalability for Avaya Multimedia Messaging.	Customers and sales, services, and support personnel
Implementing		
Deploying Avaya Multimedia Messaging	Install, configure, and administer Avaya Multimedia Messaging.	Implementation personnel
Deploying Avaya Aura® Device Services	Install, configure, and administer Avaya Aura® Device Services.	Implementation personnel
Deploying the Avaya Aura® Web Gateway	Install, configure, and administer the Avaya Aura® Web Gateway.	Implementation personnel
Implementing, administering, and troubleshooting Avaya Workplace VDI	Install, configure, administer, and troubleshoot Avaya Workplace VDI.	Implementation personnel
Administering		
Administering Avaya Multimedia Messaging	Administer and manage Avaya Multimedia Messaging.	Implementation personnel
Administering Avaya Aura® Device Services	Administer and manage Avaya Aura® Device Services.	Implementation personnel
Administering the Avaya Aura® Web Gateway	Administer, manage, and troubleshoot the Avaya Aura® Web Gateway.	Implementation personnel
Maintaining		

Title	Use this document to	Audience
Updating server certificates to improve end-user security and client user experience	Understand and administer certificates on Avaya Workplace Client.	• System administrators • Customers and sales, services, and support personnel
Using		
Using Avaya Workplace Client for Android, iOS, Mac, and Windows	Install and use Avaya Workplace Client.	Enterprise users
Avaya Workplace Client Quick Reference Guide	View the functionality in Avaya Workplace Client.	Enterprise users
Using Avaya Workplace Client on Avaya Vantage™	Set up and use Avaya Workplace Client on Avaya Vantage™.	Enterprise users
Using Unified Portal	Set up and use Avaya Workplace Client Unified Portal.	Enterprise users
Using Avaya Workplace VDI	Set up and use Avaya Workplace VDI.	Enterprise users

Table 2: Back-end server documentation for Avaya Workplace Client planning

Title	Use this document to	Audience
Overview		
Avaya Aura® Communication Manager Overview and Specification	Understand high-level product functionality, performance specifications, security, and licensing.	Customers and sales, services, and support personnel

Title	Use this document to	Audience
Avaya Aura® System Manager Overview and Specification		
Avaya Aura® Session Manager Overview and Specification		
Avaya one-X® Client Enablement Services Overview and Specification		
Planning		
Avaya IP Voice Quality Network Requirements	Understand quality of service requirements and codec selection.	• System administrators • Customers and sales, services, and support personnel
Implementing		
Avaya Aura® Communication Manager Special Application Features	Perform installation, configuration, and initial administration tasks.	Implementation personnel
Deploying Avaya Aura® Communication Manager		
Deploying Avaya Aura® System Manager on System Platform		
Deploying Avaya Aura® System Manager		
Deploying Avaya Aura® applications from System Manager		

Title	Use this document to	Audience
Deploying Avaya Aura® Session Manager		
Deploying Avaya Aura® Presence Services		
Avaya Aura® Presence Services Overview and Specification		
Implementing Avaya one-X® Client Enablement Services		
Administering		
Administering Avaya Aura® Communication Manager	Perform ongoing administration tasks, including maintenance and upgrades.	• System administrators • Architects • Implementation personnel
Administering Avaya Aura® System Manager		
Upgrading and Migrating Avaya Aura® applications from System Manager		
Administering Avaya Aura® Session Manager		
Administering Avaya Aura® Presence Services		

Title	Use this document to	Audience
Administering Avaya one-X® Client Enablement Services		

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.
   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.
   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.
  To filter by product, click **Filters** and select a product.
- Search for documents.

From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** (🌐) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** (☆).
  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon (👁).
  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press `Enter` to search for the course.

Course code	Course title
20391W	Using the Avaya Workplace Client
20381W	Using Avaya Workplace Client for iOS/Android

Course code	Course title
21511W	Using Avaya Spaces
21551W	Administering Avaya Spaces

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 https://support.avaya.com/ and do one of the following:
    - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
    - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

      The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
    - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
    - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://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.

Using the Avaya InSite Knowledge Base

Using the Avaya InSite Knowledge Base

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

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

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.

2. Log in to the Avaya support website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.

3. Click **Support by Product** > **Product-specific Support**.

4. In **Enter Product Name**, enter the product, and press `Enter`.

5. Select the product from the list, and select a release.

6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) when there is no update, service pack, or release fix, but the business unit or Avaya Services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new service packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to https://support.avaya.com and search for “Guide to Managing Your Avaya Access Profile for Customers and Partners”.
   Under the Search Results section, click Guide to Managing Your Avaya Access Profile for Customers and Partners.
2. Set up e-notifications.
   For detailed information, see the **Subscribe to E-Notifications** procedure.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at https://support.avaya.com and log in.
2. On the top of the page, in **Search Product**, type the product name.
   The Avaya Support website displays the product name.
3. Select the required product name.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. On the product page, click **Product Documents**.
6. In the Latest Support, Service and Product Correction Notices section, click **View All Notices**.
7. Select the appropriate filters as per your search requirement.
   For example, if you select Product Support Notices, the system displays only PSNs in the documents list.
   You can apply multiple filters to search for the required documents.

Data privacy controls

Personal data is stored on the file system that is accessible by the current user or a privileged user. The file system content is not encrypted, but might be encrypted using platform technologies. When personal data is transmitted over a network, the data is encrypted with the most latest protocols.

You can view the data privacy factsheet for Avaya Workplace Client at https://downloads.avaya.com/css/P8/documents/101075962.

Data categories containing personal data

User data in memory

- Remote-party phone number from calls
- Participant display name, roster list, and active talker from conference calls
- Participants on conversations and messages from Avaya Multimedia Messaging messages
- End user preferences information
- Configuration information
- Contacts retrieved from the network
- Contacts retrieved from the local contacts application on mobile platforms
- Calendar event information

User data on disk

The following information is saved on the disk:

- Local call logs
- Configuration information
- End-user preferences information

On Windows, user's credentials are saved in the Windows Credential Manager. You can access this area through Windows APIs. On Mac and iOS, the system saves the credentials to keychain. On Android, the system saves the credentials in user preferences.

User data logs

The following information is saved:

- User handle or email
- SIP user name
- Display name information from SIP messages
- Virtual room information

The following information is not saved:

- Active talker changes
- Avaya Multimedia Messaging message content
- Passwords

Personal data human access controls

User data in memory

None

User data on disk

Users can access the data on:

- Desktops: By browsing through the file system
- Mobiles: Through debug port or iTunes

User data logs

Users can access the data logs:

- Through file system
- By using the **Report a problem** option in Avaya Workplace Client

Personal data programmatic or API access controls

User data in memory

Users can access the data in memory through internal programmatic access. External application API for desktops can be turned off. For example, for headset integration, named pipe or JSON.

Series of Avaya URIs are configured on the system such that when clicked from a browser or Outlook plug-in, the link opens in Avaya Workplace Client.

User data on disk

Users can access the file system through the OS file system APIs.

User data logs

None

Personal data “at rest” encryption controls

User data in memory

Avaya Workplace Client does not encrypt the user data in memory.

User data on disk

The host platform configuration might encrypt the file system content.

User data logs

The host platform configuration might encrypt the file system content.

Personal data “in transit” encryption controls

User data in memory

HTTPs or TLS 1.3 sends or receives data with servers. External application interface done through named pipe uses local OS facilities and is not encrypted. This is implemented on Windows and Mac OSX.

User data on disk

TLS 1.3

User data logs

Email sent as a result of **Report a problem** is sent using standard email protocols. Log files sent in email as attachment are compressed into a single file and the compressed file might be encrypted by the user.

Personal data retention period controls

User data in memory

The data saved in the memory is removed based on use cases. For example, during a call, a call object remains in memory. When the call ends, the object is removed from the memory, but a new CallLog object is created.

User data on disk

The user data on disk is permanent until rolled over, application reset or uninstalled, or until the user deletes the data from the file system.

User data logs

The user data logs are not configurable but can be manually deleted.

Personal data export controls and procedures

User data in memory

Not applicable

User data on disk

User or administrators can access the user data on disk.

- Desktops: Local configuration, call log, and log files can be copied to an external system.
- Mobile platforms: Local files are accessible through the Android debug port or iTunes and can be copied from the mobile endpoint to a desktop.

Report a problem serviceability option can be selected to compress and email all local files including configuration and call log files.

User data logs

- Desktops: Local configuration, call log, and log files can be copied to an external system.

- Mobile platforms: Local files are accessible through the Android debug port or iTunes and can be copied from the mobile endpoint to a desktop.

Personal data view, modify, delete controls and procedures

User data in memory

Not applicable

User data on disk

The user or administrator has access to the file system on desktops, or through Android Debug Bridge (adb) on Android, or iTunes on iOS. On desktop systems, the user or administrator can edit the files.

User data logs

- Desktops: The administrator has full read or write access to the file system.
- Mobile platforms: The user or administrator can access the logs through the adb port on Android or iTunes on iOS.

Personal data pseudonymization operations statement

User data in memory

None

User data on disk

None

User data logs

Not applicable

Settings file template for specific deployments

Settings file template for Avaya Workplace Client as a media client in Unified Communications deployments

Use this settings file template as a starting point for your deployment. Replace the email addresses and URLs in the template with the values that are specific to your organization.

```
## SIP Parameters

SET SIPENABLED 1
SET SIP_CONTROLLER_LIST "sm.abc.com:5061;transport=tls"
SET SIPDOMAIN abc.com
SET SIMULTANEOUS_REGISTRATIONS 2
SET ENFORCE_SIPS_URI 1

## PPM Parameters

SET ENABLE_PPM 1
SET ENABLE_PPM_CALL_JOURNALING 0
SET ENABLE_PPM_CONTACTS 0

## AECC Properties

SET NO_SUBSCRIBE_ON_SIP_CONNECTION_RECOVERY 15
SET ENABLE_PPM_PERSISTENT_DATA 1
SET AGTGREETINGSTAT 2
SET ENABLE_PLT_OOB_HEADSET_CALL_CONTROL 0
SET ENABLE_JABRA_OOB_HEADSET_CALL_CONTROL 0
SET AUDIO_DEVICE_CALL_CONTROL_ENABLED 0
```

```
## AUTO UPDATE SETTINGS

SET SETTINGS_CHECK_POLICY 1
SET SETTINGS_FILE_URL "https://store.abc.com/settings/Workplace_Config_MegaRAP
_UC.txt"
SET SETTINGS_CHECK_INTERVAL 1

## CLIENT UPDATE SETTINGS  (APPCAST)

SET APPCAST_ENABLED 1
SET APPCAST_CHECK_INTERVAL 1
SET APPCAST_URL "https://aads.abc.com:8442/acs/resources/webdeployment"

## UI Notifications:

SET SHOW_TEAM_BUTTON_VISUAL_ALERT 0
SET SHOW_EQUINOX_MEETING_PANEL_IN_TOM 0
SET DESKTOP_HTTP_APPLICATION_INTEGRATION 0
SET ENABLE_CALL_NOTIFICATIONS 0
SET ENABLE_AUDIBLE_CALL_NOTIFICATIONS 0

## SSO Settings

SET SSOENABLED 0
SET AUTOCONFIG_USESSO 0

## Disabling unnecessary Workplace services

SET UNIFIEDPORTALENABLED 0
SET HTTPUAENABLED 0
SET ESMENABLED 0
SET ACSENABLED 0
SET ENHDIALSTAT 0
SET ENABLE_VIDEO 0
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 0
SET ENABLE_EQUINOX_MEETING_ACCOUNT_DISCOVERY 0
SET ENABLE_EWS_ACCOUNT_DISCOVERY 0
SET ENABLE_GOTO_MEETING_PORTAL 0
SET ENABLE_SPACES_MESSAGING 0

## Present Large Dial pad view for UC Media client

SET HOMESCREENLAYOUT 2

## Outlook Properties

SET ENABLE_OUTLOOK_ADDON 0
SET OUTLOOK_CALL_CONTACT 0
SET ENABLE_LOCAL_CONTACT 0
SET ENABLE_TOP_OF_MIND 1
SET CALENDAR_INTEGRATION_ENABLED 0
SET EWSENABLED 0

## LDAP Dir settings

SET DIRENABLED 0
SET DIRSRVR ""
SET DIRSRVRPRT 636
SET DIRUSERNAME abc
SET DIRPASSWORD ##
SET DIRTOPDN " "
SET DIRSECURE 1
SET DIRIMATTRIBUTE
SET DIRTYPE (0,1,2)
SET DIRSCOPE ' '
SET DIRMAXENTRIES

## Media parameters
```

```
SET ENCRYPT_SRTCP 0
SET ENABLE_MEDIA_HTTP_TUNNEL 0

SET SUPPORTEMAIL 'support@abc.com'
SET OTHER_PHONE_MODE_ENABLED 0
SET ENABLE_DESKPHONE_SHARE_CONTROL 0
SET ENABLE_BLIND_TRANSFER 0
SET ONLINE_HELP_ENABLED 0
SET ENABLE_TUTORIAL 0
SET TRUSTCERTS "SMabc.crt","IntermediateCA.crt","OpenSSLRootCA.crt"

## Agent parameters (CC Elite Features)

SET AGENT_ENABLED 0
SET AGENT_WORK_CODE ""
SET AUX_REASON_CODES ""
SET LOGOUT_REASON_CODES ""



SET OBSCURE_PREFERENCES "SHOW_EQUINOX_MEETING_PANEL_IN_TOM, DESKTOP_HTTP_APPL
ICATION_INTEGRATION, UNIFIEDPORTALENABLED, ESMENABLED, ACSENABLED, ENABLE_OUT
LOOK_ADDON, ENABLE_LOCAL_CONTACT, ENABLE_TOP_OF_MIND, CALENDAR_INTEGRATION_EN
ABLED, DIRENABLED, ENHDIALSTAT, EWSENABLED, ENABLE_VIDEO,  ENABLE_AVAYA_CLOUD
_ACCOUNTS, ENABLE_GOTO_MEETING_PORTAL, ENABLE_SPACES_MESSAGING, OTHER_PHONE_M
ODE_ENABLED, ENABLE_DESKPHONE_SHARE_CONTROL,  ENABLE_TUTORIAL, AGENT_ENABLED,
 SET OBSCURE_PREFERENCES "SIP_CONTROLLER_LIST,SIPPROXYSRVR,SIPPORT,SIPSECURE,
SIPENABLED,SIPDOMAIN,SIPUSERNAME,SIPHA1,SIPPASSWORD,ESMSRVR,CONFERENCE_VIRTUA
L_ROOM,DIR_CONTACT_RESOLUTION_ENABLED,CONFERENCE_ACCESS_NUMBER,SSOENABLED,ISO
_SYSTEM_LANGUAGE,UNIFIEDPORTALENABLED,WINDOWS_IMPROVIDER,CONTACT_MATCHING_SEA
RCH_LOCATION,ENABLE_OPUS,SUPPORTURL,DIRENABLED,DIRSRVR,DIRSRVRPRT,DIRTOPDN,DI
RSECURE,CONFERENCE_MODERATOR_CODE,CONFERENCE_PARTICIPANT_CODE,CONFERENCE_PART
ICIPANT_URL,RTP_PORT_RANGE,CONFERENCE_FACTORY_URI,ACSSSO,SETTINGS_CHECK_INTER
```

```
VAL,RTP_PORT_LOW,ACSSECURE,DSCPVID,DSCPAUD_FLASHOVERRIDE,SIPREGPROXYPOLICY,PH
NLDLENGTH,DSCPAUD_PRIORITY,ENABLE_MEDIA_HTTP_TUNNEL,SIPSSO,SP_AC,PHNOL,IOS10C
ALLKIT_ENABLED,PHNLD,PHNIC,PHNPBXMAINPREFIX,PHNREMOVEAREACODE,AUTOAPPLY_ARS_T
O_SHORTNUMBERS,APPLY_DIALINGRULES_TO_PLUS_NUMBERS,PHNCC,DSCPAUD_FLASH,EWSSSO,
EWSDOMAIN,ENABLE_DESKPHONE_SHARE_CONTROL,ESMSSO,VIDEO_MAX_BANDWIDTH_CELLULAR_
DATA,OPUS_PAYLOAD_TYPE,SUPPORTWINDOWSAUTHENTICATION,ALLOW_CREATE_LOCAL_CONTAC
TS,ESMREFRESH,MEDIAENCRYPTION,EWSENABLED,DSCPAUD,SUPPORTEMAIL,ACSSRVR,DIALPLA
NEXTENSIONLENGTHLIST,ENCRYPT_SRTCP,ESMSECURE,VIDEO_MAX_BANDWIDTH_ANY_NETWORK,
AUTO_AWAY_TIME,LOG_VERBOSITY,UNIFIED_PORTAL_SSO,DSCPAUD_IMMEDIATE,ANALYTICSEN
ABLED,DSCPVID_FLASHOVERRIDE,BFCP_TRANSPORT,DSCPVID_IMMEDIATE,ENABLE_LOCAL_CON
TACT,DSCPSIG,DSCPVID_FLASH,ESMPORT,ACSPORT,CONFERENCE_PORTAL_URI,ESMENABLED,A
UTOCONFIG_USESSO,ENABLE_AVAYA_CLOUD_ACCOUNTS,ESMHIDEONDISCONNECT,ENHDIALSTAT,
EWSSERVERADDRESS,ACSENABLED,CONFERENCE_FQDN_SIP_DIAL_LIST,APPLICATION_CLOSE_W
INDOW,ADDRESS_VALIDATION,WINDOWS_IMPROVIDER_RESOLVE_CONTACT_EXTERNAL,ENABLE_B
ROWSER_EXTENSION,PSTN_VM_NUM,OUTLOOK_CALL_CONTACT,ENABLE_OUTLOOK_ADDON,WINDOW
S_IMPROVIDER,ENABLE_BROWSER_EXTENSION,ADDRESS_VALIDATION,TRUST_STORE,VIDEO_MA
X_BANDWIDTH_ANY_NETWORK,DND_SAC_LINK,PSTN_VM_NUM,ENABLE_OUTLOOK_ADDON,OUTLOOK
_CALL_CONTACT,ENABLE_LOCAL_CONTACT,HIDDEN_MODE_ENABLED"

SET LOCKED_PREFERENCES "SIP_CONTROLLER_LIST, SIPDOMAIN, SIPUSERNAME,  AGTGREE
TINGSTAT"
```

Settings file template for Avaya Workplace Client as a media client in Contact Center deployments

Use this settings file template as a starting point for your deployment. Replace the email addresses and URLs in the template with the values that are specific to your organization.

```
## SIP Parameters

SET SIPENABLED 1
SET SIP_CONTROLLER_LIST "sm.abc.com:5061;transport=tls"
SET SIPDOMAIN abc.com
SET SIMULTANEOUS_REGISTRATIONS 2
SET ENFORCE_SIPS_URI 1

## PPM Parameters

SET ENABLE_PPM 1
SET ENABLE_PPM_CALL_JOURNALING 0
SET ENABLE_PPM_CONTACTS 0

## AECC Properties

SET NO_SUBSCRIBE_ON_SIP_CONNECTION_RECOVERY 15
SET ENABLE_PPM_PERSISTENT_DATA 1
SET AGTGREETINGSTAT 2
SET ENABLE_PLT_OOB_HEADSET_CALL_CONTROL 0
SET ENABLE_JABRA_OOB_HEADSET_CALL_CONTROL 0
SET AUDIO_DEVICE_CALL_CONTROL_ENABLED 0

## AUTO UPDATE SETTINGS

SET SETTINGS_CHECK_POLICY 1
SET SETTINGS_FILE_URL "https://store.abc.com/settings/Workplace_Config_Mega_CC.txt"
SET SETTINGS_CHECK_INTERVAL 1

## CLIENT UPDATE SETTINGS  (APPCAST)

SET APPCAST_ENABLED 1
SET APPCAST_CHECK_INTERVAL 1
SET APPCAST_URL "https://aads.abc.com:8442/acs/resources/webdeployment"
## UI Notifications:

SET SHOW_TEAM_BUTTON_VISUAL_ALERT 0
SET SHOW_EQUINOX_MEETING_PANEL_IN_TOM 0
SET DESKTOP_HTTP_APPLICATION_INTEGRATION 0
SET ENABLE_CALL_NOTIFICATIONS 0
SET ENABLE_AUDIBLE_CALL_NOTIFICATIONS 0

## SSO Settings

SET SSOENABLED 0
SET AUTOCONFIG_USESSO 0

## Disabling unnecessary Workplace services

SET UNIFIEDPORTALENABLED 0
SET HTTPUAENABLED 0
SET ESMENABLED 0
SET ACSENABLED 0
SET ENHDIALSTAT 0
SET ENABLE_VIDEO 0
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 0
SET ENABLE_EQUINOX_MEETING_ACCOUNT_DISCOVERY 0
SET ENABLE_EWS_ACCOUNT_DISCOVERY 0
SET ENABLE_GOTO_MEETING_PORTAL 0
SET ENABLE_SPACES_MESSAGING 0

## Present Large Dial pad view for Media client

SET HOMESCREENLAYOUT 2

## Outlook Properties

SET ENABLE_OUTLOOK_ADDON 0
SET OUTLOOK_CALL_CONTACT 0
SET ENABLE_LOCAL_CONTACT 0
SET ENABLE_TOP_OF_MIND 1
SET CALENDAR_INTEGRATION_ENABLED 0
SET EWSENABLED 0

## LDAP Dir settings

SET DIRENABLED 0
SET DIRSRVR ""
SET DIRSRVRPRT 636
SET DIRUSERNAME abc
SET DIRPASSWORD ##
SET DIRTOPDN " "
SET DIRSECURE 1
SET DIRIMATTRIBUTE
SET DIRTYPE (0,1,2)
SET DIRSCOPE ' '
SET DIRMAXENTRIES

## Media parameters

SET ENCRYPT_SRTCP 0
SET ENABLE_MEDIA_HTTP_TUNNEL 0

SET SUPPORTEMAIL 'support@abc.com'
SET OTHER_PHONE_MODE_ENABLED 0
SET ENABLE_DESKPHONE_SHARE_CONTROL 0
SET ENABLE_BLIND_TRANSFER 0
SET ONLINE_HELP_ENABLED 0
SET ENABLE_TUTORIAL 0
SET CONTROLLEDEP_CONFIGURL ""
SET TRUSTCERTS "SMabc.crt","IntermediateCA.crt","OpenSSLRootCA.crt"



## Agent parameters (CC Elite Features)
```

```
SET AGENT_ENABLED 0
SET ENABLE_BUTTON_MODULE 1
SET AGENT_WORK_CODE ""
SET AUX_REASON_CODES ""
SET LOGOUT_REASON_CODES ""
SET Q_STATS_DEFAULTREFRESHTIMER 20
SET UUIDISPLAYTIME 10
SET LICENSE_SERVER_URL
SET ENABLE_CCELITE_OFF_HOOK_INVITE_SUPPORT 1

SET OBSCURE_PREFERENCES "SHOW_EQUINOX_MEETING_PANEL_IN_TOM, DESKTOP_HTTP_APPL
ICATION_INTEGRATION, UNIFIEDPORTALENABLED, ESMENABLED, ACSENABLED, ENABLE_OUT
LOOK_ADDON, ENABLE_LOCAL_CONTACT, ENABLE_TOP_OF_MIND, CALENDAR_INTEGRATION_EN
ABLED, DIRENABLED, ENHDIALSTAT, EWSENABLED, ENABLE_VIDEO,  ENABLE_AVAYA_CLOUD
_ACCOUNTS, ENABLE_GOTO_MEETING_PORTAL, ENABLE_SPACES_MESSAGING, OTHER_PHONE_M
ODE_ENABLED, ENABLE_DESKPHONE_SHARE_CONTROL,  ENABLE_TUTORIAL, AGENT_ENABLED,
 SET OBSCURE_PREFERENCES "SIP_CONTROLLER_LIST,SIPPROXYSRVR,SIPPORT,SIPSECURE,
SIPENABLED,SIPDOMAIN,SIPUSERNAME,SIPHA1,SIPPASSWORD,ESMSRVR,CONFERENCE_VIRTUA
L_ROOM,DIR_CONTACT_RESOLUTION_ENABLED,CONFERENCE_ACCESS_NUMBER,SSOENABLED,ISO
_SYSTEM_LANGUAGE,UNIFIEDPORTALENABLED,WINDOWS_IMPROVIDER,CONTACT_MATCHING_SEA
RCH_LOCATION,ENABLE_OPUS,SUPPORTURL,DIRENABLED,DIRSRVR,DIRSRVRPRT,DIRTOPDN,DI
RSECURE,CONFERENCE_MODERATOR_CODE,CONFERENCE_PARTICIPANT_CODE,CONFERENCE_PART
ICIPANT_URL,RTP_PORT_RANGE,CONFERENCE_FACTORY_URI,ACSSSO,SETTINGS_CHECK_INTER
VAL,RTP_PORT_LOW,ACSSECURE,DSCPVID,DSCPAUD_FLASHOVERRIDE,SIPREGPROXYPOLICY,PH
NLDLENGTH,DSCPAUD_PRIORITY,ENABLE_MEDIA_HTTP_TUNNEL,SIPSSO,SP_AC,PHNOL,IOS10C
ALLKIT_ENABLED,PHNLD,PHNIC,PHNPBXMAINPREFIX,PHNREMOVEAREACODE,AUTOAPPLY_ARS_T
O_SHORTNUMBERS,APPLY_DIALINGRULES_TO_PLUS_NUMBERS,PHNCC,DSCPAUD_FLASH,EWSSSO,
EWSDOMAIN,ENABLE_DESKPHONE_SHARE_CONTROL,ESMSSO,VIDEO_MAX_BANDWIDTH_CELLULAR_
DATA,OPUS_PAYLOAD_TYPE,SUPPORTWINDOWSAUTHENTICATION,ALLOW_CREATE_LOCAL_CONTAC
TS,ESMREFRESH,MEDIAENCRYPTION,EWSENABLED,DSCPAUD,SUPPORTEMAIL,ACSSRVR,DIALPLA
NEXTENSIONLENGTHLIST,ENCRYPT_SRTCP,ESMSECURE,VIDEO_MAX_BANDWIDTH_ANY_NETWORK,
AUTO_AWAY_TIME,LOG_VERBOSITY,UNIFIED_PORTAL_SSO,DSCPAUD_IMMEDIATE,ANALYTICSEN
ABLED,DSCPVID_FLASHOVERRIDE,BFCP_TRANSPORT,DSCPVID_IMMEDIATE,ENABLE_LOCAL_CON
```

```
TACT,DSCPSIG,DSCPVID_FLASH,ESMPORT,ACSPORT,CONFERENCE_PORTAL_URI,ESMENABLED,A
UTOCONFIG_USESSO,ENABLE_AVAYA_CLOUD_ACCOUNTS,ESMHIDEONDISCONNECT,ENHDIALSTAT,
EWSSERVERADDRESS,ACSENABLED,CONFERENCE_FQDN_SIP_DIAL_LIST,APPLICATION_CLOSE_W
INDOW,ADDRESS_VALIDATION,WINDOWS_IMPROVIDER_RESOLVE_CONTACT_EXTERNAL,ENABLE_B
ROWSER_EXTENSION,PSTN_VM_NUM,OUTLOOK_CALL_CONTACT,ENABLE_OUTLOOK_ADDON,WINDOW
S_IMPROVIDER,ENABLE_BROWSER_EXTENSION,ADDRESS_VALIDATION,TRUST_STORE,VIDEO_MA
X_BANDWIDTH_ANY_NETWORK,DND_SAC_LINK,PSTN_VM_NUM,ENABLE_OUTLOOK_ADDON,OUTLOOK
_CALL_CONTACT,ENABLE_LOCAL_CONTACT,HIDDEN_MODE_ENABLED"

SET LOCKED_PREFERENCES "SIP_CONTROLLER_LIST, SIPDOMAIN, SIPUSERNAME,  AGTGREE
TINGSTAT"
```

Glossary

Communication Manager

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.

EC500

A feature that bridges calls received by the Avaya Aura® Communication Manager server to any mobile phone, regardless of location or wireless service provider.

Extension to Cellular access number

The phone number dialed to connect to the Avaya server that is running Communication Manager. The Extension to Cellular access number initiates the process of enabling or disabling Extension to Cellular or changing the station security code.

FNE

FNE

An extension assigned to a feature within Communication Manager. The system administrator configures a Feature Name Extension (FNE) to correspond to a FAC that activates the feature.

FECC

Far End Camera Control (FECC) is a feature of endpoint cameras, where an endpoint in the call can remotely control the camera of another endpoint in the call.

Off-PBX telephone

A method used to extend Communication Manager extensions and features outside of Communication Manager.

OTT

Over the Top (OTT) deployment means that you can use Avaya Workplace Client in a non-Avaya Aura® environment as a conferencing client for users that have a virtual room assigned to them.

Product Licensing and Delivery System (PLDS)

The Avaya licensing and download website and management system. Avaya Business Partners and customers use this site to obtain ISO image files and other software downloads.

Real-time Transport Protocol

A network protocol that delivers audio and video over IP networks.

RFC 2833

A standards-based mechanism used to send DTMF digits inband with Real time Transport Protocol (RTP).

Secure Real-Time Transport Protocol

An extension to Real-Time Transport Protocol (RTP) that incorporates enhanced security features. Like RTP, Secure RTP or SRTP is intended mostly for VoIP communications.

Session Border Controller

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

Session Manager

Session Manager

An enterprise SIP proxy registrar and router that is the core component within the Avaya Aura® solution.

System Manager

System Manager

A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity. System Manager can also function as a self-signed Root Certificate Authority (CA) or as an intermediate CA. System Manager enables the Simple Certificate Enrollment Protocol (SCEP) application to sign certificates for Avaya deskphones.

UCCP

Unified Conference Control Protocol (UCCP) is a web-based protocol. It is used by Conferencing clients to have conference control including roster, moderator commands, and user commands.